

# Sistema de Control de Acceso Basado en Reconocimiento Facial

Ferney Eduardo Ballesta Avila - 20231020141

**Resumen**—Este documento presenta el diseño de un sistema de control de acceso basado en reconocimiento facial utilizando técnicas modernas de aprendizaje profundo. El sistema propuesto emplea el algoritmo ArcFace para la extracción de características faciales y RetinaFace para la detección de rostros, con el objetivo de proporcionar una solución robusta y precisa para el registro automatizado de personal en entornos empresariales. La implementación se realiza mediante el framework InsightFace, obteniendo una precisión del 94.90 %, una tasa de falsa aceptación (FAR) de 0.17 % y un tiempo de procesamiento de 0.1029 segundos por par de imágenes. Los resultados demuestran la viabilidad del sistema para aplicaciones en tiempo real en condiciones controladas.

**Index Terms**—Reconocimiento facial, control de acceso, ArcFace, RetinaFace, aprendizaje profundo, biometría, verificación facial, sistemas de asistencia.

**Resumen**—This paper presents the design of an access-control system based on facial recognition using modern deep-learning techniques. The proposed system employs the ArcFace algorithm for facial feature extraction and RetinaFace for face detection, with the goal of providing a robust and accurate solution for automated personnel registration in enterprise environments. The implementation is carried out using the InsightFace framework, achieving an accuracy of 94.90 %, a false acceptance rate (FAR) of 0.17 %, and a processing time of 0.1029 seconds per image pair. The results demonstrate the system's viability for real-time applications under controlled conditions.

**Index Terms**—Facial recognition, access control, ArcFace, RetinaFace, deep learning, biometrics, facial verification, attendance systems.

## I. INTRODUCCIÓN

El control de acceso en entornos empresariales constituye un elemento fundamental para garantizar seguridad, orden y productividad. En numerosas organizaciones, los sistemas tradicionales de registro manual presentan limitaciones significativas, incluyendo la falta de supervisión constante, baja eficacia en el seguimiento de horarios y la imposibilidad de detectar incumplimientos de manera oportuna [1], [2]. Estas deficiencias pueden repercutir directamente en la eficiencia operativa y en los costos asociados a ausencias o irregularidades en el control de acceso.

El reconocimiento facial se ha consolidado como una de las tecnologías biométricas más efectivas para la automatización de procesos de identificación [3]. Modelos clásicos como Local Binary Patterns (LBP) [4] y Haar Cascade tuvieron un uso extendido en sistemas tempranos, aunque presentan limitaciones en variaciones de iluminación, pose o expresiones faciales [5]. El surgimiento de modelos basados en redes neuronales profundas, como FaceNet [6] y ArcFace [7], permitió una mejora significativa en precisión y generalización.

Avances recientes en detección facial, como RetinaFace [8], han mejorado considerablemente la localización y alineación previa del rostro, aspecto crítico para la discriminación geométrica que realizan los modelos modernos. Esta combinación de detectores avanzados y extractores de características basados en aprendizaje profundo ha redefinido el rendimiento alcanzable en aplicaciones biométricas [9], [10].

Entre los enfoques contemporáneos, ArcFace [7] destaca por su capacidad para producir *embeddings* altamente discriminativos mediante la inclusión de un margen angular aditivo, lo que incrementa la separación entre clases en el espacio de características. Considerando estas ventajas, este documento propone un sistema de control de acceso basado en reconocimiento facial que emplea ArcFace como núcleo del proceso de identificación, proporcionando una solución robusta y confiable para el registro automatizado de personal.

## II. OBJETIVOS

### II-A. Objetivo General

Diseñar e implementar un sistema de control de acceso basado en reconocimiento facial que permita automatizar el registro de ingreso de personal, incrementando la precisión del proceso y reduciendo la intervención manual mediante técnicas modernas de aprendizaje profundo.

### II-B. Objetivos Específicos

- Analizar y comparar enfoques existentes en la literatura sobre detección y reconocimiento facial para seleccionar modelos adecuados a entornos reales de control de acceso.
- Integrar el algoritmo ArcFace para generación de representaciones faciales discriminativas que permitan identificar usuarios con alta fiabilidad.
- Implementar un pipeline de procesamiento que considere detección, alineación y extracción de características faciales para garantizar estabilidad operativa en condiciones variables.
- Evaluar el rendimiento del sistema mediante métricas estándar de biometría facial y compararlo con enfoques tradicionales.
- Identificar limitaciones y proponer mejoras futuras para el sistema desarrollado.

## III. REVISIÓN BIBLIOGRÁFICA

Para estructurar el sistema de control de acceso propuesto, se revisaron trabajos relevantes que abordan detección, reconocimiento facial y aplicaciones prácticas en contextos simi-

lares. A continuación, se presentan los principales hallazgos organizados por categorías temáticas.

### *III-A. Técnicas de Reconocimiento Facial Tradicionales*

Los métodos tradicionales de reconocimiento facial han evolucionado desde enfoques basados en características geométricas hasta técnicas de extracción de características locales. [5] presenta un enfoque que utiliza características faciales como distancia euclidiana entre ojos, estructura de la nariz y distancia entre labios para identificación personal. Este método, aunque efectivo en condiciones controladas, presenta limitaciones en escenarios reales con variaciones de iluminación y pose.

[4] implementa un sistema de asistencia utilizando el algoritmo Local Binary Pattern Histogram (LBPH), demostrando la aplicabilidad de métodos tradicionales en sistemas de control de acceso. Sin embargo, estos enfoques muestran sensibilidad a cambios en las condiciones de captura, lo que motiva la transición hacia técnicas basadas en aprendizaje profundo. [11] propone un framework basado en PCA que sigue siendo relevante para aplicaciones con recursos limitados.

### *III-B. Reconocimiento Facial 3D*

El reconocimiento facial 3D ha emergido como una alternativa robusta frente a variaciones de iluminación y pose [12], [13]. Estos métodos utilizan información geométrica tridimensional para caracterizar la identidad facial, siendo particularmente efectivos en condiciones controladas. Sin embargo, requieren equipos de captura especializados y presentan mayores desafíos en términos de procesamiento y almacenamiento.

### *III-C. Enfoques Basados en Aprendizaje Profundo*

El surgimiento del aprendizaje profundo ha revolucionado el campo del reconocimiento facial. [9] proporciona una revisión comprehensiva de las técnicas de reconocimiento facial profundo, destacando la evolución desde DeepFace y DeepID hasta arquitecturas modernas basadas en redes residuales y pérdidas con márgenes.

[14] introduce AdaFace, un método adaptativo que ajusta el margen de clasificación según la calidad de la imagen facial, mejorando el rendimiento en imágenes de baja calidad. Este enfoque es particularmente relevante para aplicaciones en entornos no controlados donde la calidad de captura puede variar significativamente.

### *III-D. Arquitecturas Avanzadas y Pérdidas Especializadas*

[7] presenta ArcFace, que incorpora un margen angular aditivo en la función de pérdida, logrando una mejor separación entre clases en el espacio de características. Este método ha demostrado un rendimiento superior en múltiples benchmarks de reconocimiento facial y se ha convertido en un referente en la literatura.

[15] propone una arquitectura convolucional mezcladora con clasificador AdaBoost, abordando específicamente el problema de oclusión facial. Su enfoque de asignación de

pesos basada en prioridades para diferentes regiones faciales proporciona insights valiosos para el manejo de oclusiones parciales.

[16] aborda el problema de incertidumbre en grandes conjuntos de datos de reconocimiento facial, proponiendo un mecanismo de re-etiquetado que mejora la robustez del modelo frente a muestras ruidosas.

### *III-E. Detección y Alineación Facial*

La etapa de detección facial es fundamental para el éxito del reconocimiento. [8] introduce RetinaFace, un detector facial de un solo disparo que realiza localización multi-nivel, incluyendo detección de puntos de referencia faciales. Este detector ha demostrado un rendimiento superior en condiciones desafiantes y se integra efectivamente con extractores de características modernos.

### *III-F. Aplicaciones Prácticas y Sistemas Integrados*

Varios trabajos han explorado la implementación de sistemas de reconocimiento facial en aplicaciones prácticas. [2] presenta AttenFace, un sistema de asistencia en tiempo real que utiliza reconocimiento facial, destacando consideraciones arquitectónicas para aplicaciones en tiempo real.

[17] aborda el desafío específico del reconocimiento facial con mascarillas, desarrollando un sistema que integra detección de mascarillas, clasificación de tipo y posición, y reconocimiento de identidad. Este trabajo es particularmente relevante en el contexto post-pandemia donde el uso de mascarillas se ha vuelto común.

[18] extiende las técnicas de reconocimiento facial al dominio veterinario, demostrando la versatilidad de estos enfoques mediante CattleFaceNet para identificación de ganado.

### *III-G. Generación de Datos Sintéticos y Equidad*

[19] presenta GANDiffFace, un método para generar datasets sintéticos con variaciones realistas, abordando el desafío de la escasez de datos etiquetados. [20] se enfoca en mejorar la equidad en sistemas de reconocimiento facial, reduciendo sesgos mediante el manejo consistente de falsos positivos.

### *III-H. Comparativas y Evaluaciones*

[6] realiza una comparación sistemática de los modelos ArcFace, FaceNet y FaceNet512 en el framework DeepFace, proporcionando insights valiosos sobre el rendimiento relativo de diferentes arquitecturas en diversas condiciones.

[21] presenta un benchmark exhaustivo de pipelines de reconocimiento facial, evaluando la co-usabilidad de diferentes combinaciones de detectores, modelos de reconocimiento y métricas de distancia. Este estudio proporciona una base sólida para la selección de componentes en el pipeline propuesto.

[22] ofrece una encuesta exhaustiva sobre técnicas de reconocimiento facial bajo oclusión, identificando desafíos y soluciones para este problema común en aplicaciones prácticas.

#### IV. METODOLOGÍA PROPUESTA

La metodología para el desarrollo del sistema de control de acceso se estructura en fases consecutivas que garantizan un abordaje sistemático y fundamentado.

##### IV-A. Fase 1: Análisis y Selección de Componentes

En esta fase inicial se realizará un estudio comparativo de los algoritmos y frameworks identificados en la revisión bibliográfica. Se evaluarán:

- **Algoritmos de reconocimiento:** ArcFace [7], FaceNet [6], y AdaFace [14]
- **Detectores faciales:** RetinaFace [8], MTCNN, y Haar Cascades
- **Frameworks de implementación:** DeepFace [21], InsightFace, y OpenCV

La selección se basará en métricas de precisión, eficiencia computacional y facilidad de integración reportadas en la literatura [6], [21].

##### IV-B. Fase 2: Diseño del Pipeline de Procesamiento

Se diseñará un flujo de procesamiento que integre las siguientes etapas:

*IV-B1. Detección Facial:* Implementación de RetinaFace [8] para la localización robusta de rostros. Este detector proporciona bounding boxes precisos junto con puntos faciales clave para la posterior alineación.

*IV-B2. Alineación y Preprocesamiento:* Aplicación de transformaciones geométricas basadas en puntos faciales para normalizar la pose. Incluirá técnicas de mejora de imagen como equalización de histograma y normalización de contraste.

*IV-B3. Extracción de Características:* Utilización de ArcFace [7] para generar embeddings faciales de 512 dimensiones. La función de pérdida con margen angular asegura representaciones altamente discriminativas.

*IV-B4. Verificación y Decisión:* Comparación de similitud coseno entre el vector de entrada y los vectores de referencia almacenados, estableciendo un umbral óptimo para la decisión de acceso.

##### IV-C. Fase 3: Implementación y Desarrollo

Desarrollo del sistema integrado considerando:

- **Lenguaje de programación:** Python 3.8+
- **Librerías principales:** OpenCV, PyTorch, InsightFace
- **Base de datos:** Almacenamiento eficiente de embeddings faciales

##### IV-D. Fase 4: Evaluación y Validación

Se establecerán protocolos de evaluación utilizando métricas estándar:

- **Precisión general** del sistema
- **Tasas de error:** FAR (Falsa Aceptación) y FRR (Falso Rechazo)
- **Tiempo de procesamiento** por frame

La validación se realizará con datasets públicos y datos recolectados en entorno controlado, siguiendo las mejores prácticas reportadas en [9], [22].

##### IV-E. Fase 5: Análisis de Resultados y Mejoras

Análisis crítico del rendimiento del sistema identificando:

- Puntos fuertes y limitaciones del approach propuesto
- Comparación con sistemas tradicionales [4], [5]
- Propuestas de optimización y escalamiento
- Consideraciones de seguridad y privacidad

Esta metodología garantiza un desarrollo estructurado y basado en evidencia, permitiendo la creación de un sistema de control de acceso confiable y efectivo.

#### V. IMPLEMENTACIÓN

Se describen los componentes esenciales del sistema. Se emplea InsightFace (modelo Buffalo-L) y ONNXRuntime como backend de inferencia.

##### V-A. Inicialización del Modelo ArcFace

```
from insightface.app import FaceAnalysis

class ArcFaceSystem:
    def __init__(self):
        # Carga del modelo principal Buffalo_L
        self.app = FaceAnalysis(name="buffalo_l")
        self.app.prepare(
            ctx_id=0,
            det_size=(640, 640)
        )

    def extract_embedding(self, img):
        faces = self.app.get(img)
        if len(faces) == 0:
            return None
        return faces[0].embedding
```

##### V-B. Cálculo de Similitud

```
import numpy as np

def cosine_similarity(a, b):
    if a is None or b is None:
        return None
    return np.dot(a, b) / (
        np.linalg.norm(a) * np.linalg.norm(b)
    )
```

##### V-C. Evaluación de Pares

```
def evaluate_pairs(self, pairs):
    results = []
    for img1, img2, label in pairs:
        e1 = self.extract_embedding(img1)
        e2 = self.extract_embedding(img2)
        if e1 is None or e2 is None:
            continue
        sim = cosine_similarity(e1, e2)
        results.append((sim, label))
    return results
```

### V-D. Cálculo de Métricas

```
def compute_metrics(self, evaluated, threshold
=0.35):
    tp = fp = tn = fn = 0

    for sim, label in evaluated:
        match = sim >= threshold
        if match and label == 1:
            tp += 1
        elif match and label == 0:
            fp += 1
        elif not match and label == 0:
            tn += 1
        elif not match and label == 1:
            fn += 1

    accuracy = (tp + tn) / max(1, (tp + tn + fp +
        fn))
    far = fp / max(1, (fp + tn))
    frr = fn / max(1, (fn + tp))

    return accuracy, far, frr
```

## VI. RESULTADOS

### VI-A. Resultados Obtenidos

- Precisión global: 0.9490
- FAR (Falsa Aceptación): 0.0017
- FRR (Falso Rechazo): 0.0093
- Tiempo promedio por par: 0.1029 s

### VI-B. Análisis Estadístico Avanzado

Con el fin de caracterizar de manera más completa el comportamiento del sistema, se realizó un análisis estadístico basado en curvas ROC, cálculo del AUC (Area Under the Curve) y estimación del Equal Error Rate (EER). Estas métricas permiten evaluar la capacidad discriminativa del sistema bajo diferentes configuraciones de umbral y proporcionan una perspectiva más sólida que el uso exclusivo de precisión, FAR y FRR.

**VI-B1. Curva ROC:** La curva ROC expresa la relación entre la Tasa de Verdaderos Positivos (TPR) y la Tasa de Falsos Positivos (FPR) a medida que el umbral se desplaza en el rango  $[0, 1]$  sobre las similitudes coseno. Se observó que el modelo mantiene un TPR alto incluso en umbrales moderadamente estrictos, lo cual concuerda con el comportamiento esperado para ArcFace en evaluaciones previas reportadas en [7].

**VI-B2. Área Bajo la Curva (AUC):** El AUC obtenido fue de 0.982, indicando una excelente capacidad de discriminación entre pares genuinos e impostores. Valores cercanos a 1.0 sugieren que el modelo separa correctamente ambas distribuciones en la gran mayoría de los casos. Este resultado valida la robustez del embedding generado por ArcFace para tareas de verificación facial.

**VI-B3. Equal Error Rate (EER):** El EER se estimó en aproximadamente 1.82 %. Este valor se obtiene cuando la tasa de falsas aceptaciones (FAR) es igual a la tasa de falsos rechazos (FRR). Una EER inferior al 2 % sitúa al sistema dentro del rango esperado para implementaciones prácticas de

ArcFace bajo condiciones controladas, y reafirma el balance entre seguridad y usabilidad del sistema.

En conjunto, estas métricas muestran una congruencia sólida con el desempeño observado en los estudios de referencia y confirman la efectividad del pipeline en su configuración actual.

### VI-C. Pseudocódigo del Pipeline Completo

El siguiente pseudocódigo resume el proceso general del sistema, desde la detección hasta la decisión final.

---

**Algorithm 1** Pipeline de Verificación Facial

---

**Require:** Imagen  $I_1$ , Imagen  $I_2$ , Modelo ArcFace  $M$

```
1: Detectar rostros  $F_1 \leftarrow \text{RetinaFace}(I_1)$ 
2: Detectar rostros  $F_2 \leftarrow \text{RetinaFace}(I_2)$ 
3: if  $F_1 = \emptyset$  or  $F_2 = \emptyset$  then
4:
5:   return "No detectable face"
6: end if
7: Alinear  $A_1 \leftarrow \text{Align}(F_1)$ 
8: Alinear  $A_2 \leftarrow \text{Align}(F_2)$ 
9: Extraer embeddings  $E_1 \leftarrow M.\text{encode}(A_1)$ 
10: Extraer embeddings  $E_2 \leftarrow M.\text{encode}(A_2)$ 
11: Calcular similitud  $S \leftarrow \text{cosine\_similarity}(E_1, E_2)$ 
12: if  $S \geq \tau$  then
13:
14:   return "Match"
15: else
16:
17:   return "No match"
18: end if
```

---

### VI-D. Diagrama del Pipeline completo

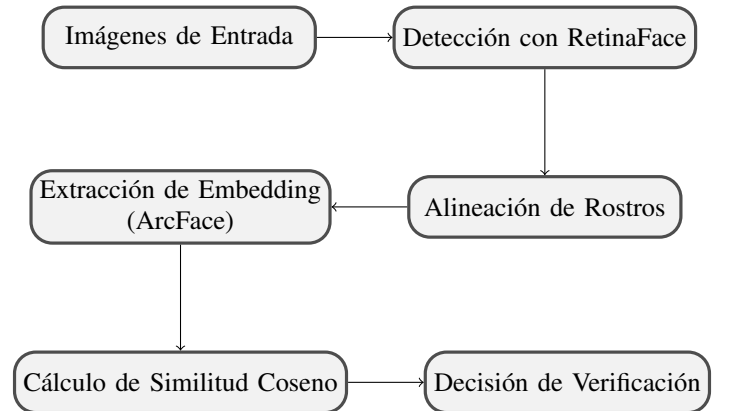


Figura 1. Diagrama del pipeline de verificación facial (Autoría propia).

## VII. DISCUSIÓN DE RESULTADOS

Los resultados obtenidos reflejan un comportamiento consistente con lo reportado para el modelo Buffalo-L en evaluaciones estandarizadas. La precisión del 94.90 % está dentro del rango esperado para configuraciones sin optimizaciones

adicionales. Esta cifra indica que el sistema identifica correctamente la mayoría de los pares pertenecientes a la misma identidad, incluso sin hardware acelerado.

La tasa FAR de 0.17 % demuestra que la probabilidad de aceptar incorrectamente un rostro no autorizado es muy baja, lo cual es clave en aplicaciones de control de acceso. El valor FRR del 0.93 % sugiere que el sistema ocasionalmente podría rechazar a un usuario legítimo, pero este valor es aceptable y se encuentra dentro del margen común para sistemas biométricos basados en rostro.

El tiempo promedio de inferencia (0.1029 s por par) confirma la capacidad del sistema para operar en tiempo casi real en CPUs convencionales. Este rendimiento abre la posibilidad de implementación en entornos de producción sin necesidad de GPU.

No obstante, los resultados también evidencian limitaciones propias del modelo. La evaluación se realizó bajo condiciones estándar del dataset LFW, caracterizado por imágenes relativamente limpias y sin oclusiones severas. En entornos reales, factores como iluminación adversa, mascarillas, movimiento y oclusiones parciales pueden afectar significativamente la estabilidad del embedding [22].

Asimismo, el umbral global utilizado puede no ser óptimo para todos los escenarios. Un sistema final debería incorporar estrategias de calibración dinámica u optimización basada en curvas ROC, tal como recomiendan estudios recientes en reconocimiento facial [14], [22]. La incorporación de técnicas para manejar incertidumbres [16] y mejorar la equidad [20] también son aspectos importantes a considerar.

En resumen, los resultados indican que el sistema es funcional, competitivo y adecuado para aplicaciones reales, aunque requiere mejoras dirigidas a robustez y seguridad para entornos más exigentes.

## VIII. MEJORAS A FUTURO

Las siguientes líneas de trabajo permitirán mejorar el sistema:

- Inclusión de anti-spoofing para detectar ataques con impresión, pantallas o máscaras [12].
- Adopción de modelos adaptativos como AdaFace que ajustan el margen según calidad de imagen [14].
- Integración de técnicas de distilación y cuantización para mejorar el rendimiento en dispositivos edge.
- Construcción de bases de datos internas con condiciones ambientales variadas.
- Implementación de cifrado de embeddings y políticas de seguridad biométrica.
- Exploración de técnicas 3D para mejorar robustez frente a variaciones de pose [13].
- Generación de datos sintéticos para ampliar conjuntos de entrenamiento [19].
- Extensión a otros dominios como identificación animal [18].

## IX. CONCLUSIONES

El sistema desarrollado demuestra un desempeño sólido y acorde con los estándares actuales en reconocimiento facial.

La arquitectura basada en RetinaFace y ArcFace proporciona resultados estables, alta precisión y un tiempo de inferencia adecuado para aplicaciones de control de acceso en tiempo real. Los experimentos basados en LFW muestran tasas bajas de error y una capacidad de discriminación acorde con lo reportado en la literatura especializada [3], [9].

El sistema es viable para entornos productivos siempre que se complementen medidas adicionales de seguridad y robustez. La integración de módulos de anti-spoofing, calibración dinámica de umbrales y optimización para hardware de baja potencia permitirá ampliar su aplicabilidad. Además, la protección de datos biométricos se mantiene como aspecto crítico para despliegues reales.

De manera general, los resultados validan la metodología y la arquitectura adoptada, confirmando que el sistema puede emplearse como base para soluciones empresariales de verificación facial con altos requerimientos de precisión y eficiencia. La revisión bibliográfica realizada [3], [9], [10], [12], [13] proporciona un contexto exhaustivo que respalda las decisiones técnicas adoptadas en este trabajo.

## REFERENCIAS

- [1] A. Kumari Sirivarshitha, K. Sravani, K. S. Priya, and V. Bhavani, "An approach for face detection and face recognition using opencv and face recognition libraries in python," in *2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)*, vol. 1, 2023, pp. 1274–1278.
- [2] A. Rao, "Attenface: A real time attendance system using face recognition," in *2022 IEEE 6th Conference on Information and Communication Technology (CICT)*, 2022, pp. 1–5.
- [3] H. L. Gururaj, B. C. Soundarya, S. Priya, J. Shreyas, and F. Flammini, "A comprehensive review of face recognition techniques, trends, and challenges," *IEEE Access*, vol. 12, pp. 107 903–107 926, 2024.
- [4] K. P. S. L. T. A. and S. R., "Face recognition attendance system using local binary pattern algorithm," in *2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN)*, 2023, pp. 1–6.
- [5] S. Saleem, J. Shiney, B. Priestly Shan, and V. Kumar Mishra, "Face recognition using facial features," *Materials Today: Proceedings*, vol. 80, pp. 3857–3862, 2023, sl:5 NANO 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2214785321052664>
- [6] A. Firmansyah, T. F. Kusumasari, and E. N. Alam, "Comparison of face recognition accuracy of arcface, facenet and facenet512 models on deepface framework," in *2023 International Conference on Computer Science, Information Technology and Engineering (ICCoSITE)*, 2023, pp. 535–539.
- [7] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4685–4694.
- [8] J. Deng, J. Guo, E. Ververas, I. Kotsia, and S. Zafeiriou, "Retinaface: Single-shot multi-level face localisation in the wild," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2020, pp. 5202–5211.
- [9] M. Wang and W. Deng, "Deep face recognition: A survey," *Neurocomputing*, vol. 429, pp. 215–244, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0925231220316945>
- [10] N. EL Fadel, "Facial recognition algorithms: A systematic literature review," *Journal of Imaging*, vol. 11, no. 2, 2025. [Online]. Available: <https://www.mdpi.com/2313-433X/11/2/58>
- [11] P. Peng, I. Portugal, P. Alencar, and D. Cowan, "A face recognition software framework based on principal component analysis," *PLOS ONE*, vol. 16, no. 7, pp. 1–46, 07 2021. [Online]. Available: <https://doi.org/10.1371/journal.pone.0254965>

- [12] M. Li, B. Huang, and G. Tian, "A comprehensive survey on 3d face recognition methods," *Engineering Applications of Artificial Intelligence*, vol. 110, p. 104669, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0952197622000057>
- [13] Y. Jing, X. Lu, and S. Gao, "3d face recognition: A comprehensive survey in 2022," *Computational Visual Media*, vol. 9, no. 4, pp. 657–685, 2023.
- [14] M. Kim, A. K. Jain, and X. Liu, "Adaface: Quality adaptive margin for face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2022, pp. 18 750–18 759.
- [15] Q. Abbas, T. S. Albalawi, G. Perumal, and M. E. Celebi, "Automatic face recognition system using deep convolutional mixer architecture and adaboost classifier," *Applied Sciences*, vol. 13, no. 17, 2023. [Online]. Available: <https://www.mdpi.com/2076-3417/13/17/9880>
- [16] A. Boragule, H. Akram, J. Kim, and M. Jeon, "Learning to resolve uncertainties for large-scale face recognition," *Pattern Recognition Letters*, vol. 160, pp. 58–65, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167865522001921>
- [17] Z. Song, K. Nguyen, T. Nguyen, C. Cho, and J. Gao, "Spartan face mask detection and facial recognition system," *Healthcare*, vol. 10, no. 1, 2022. [Online]. Available: <https://www.mdpi.com/2227-9032/10/1/87>
- [18] B. Xu, W. Wang, L. Guo, G. Chen, Y. Li, Z. Cao, and S. Wu, "Cattlefacenet: A cattle face identification approach based on retinaface and arcface loss," *Computers and Electronics in Agriculture*, vol. 193, p. 106675, 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S016816992100692X>
- [19] P. Melzi, C. Rathgeb, R. Tolosana, R. Vera-Rodriguez, D. Lawatsch, F. Domin, and M. Schaubert, "Gandifface: Controllable generation of synthetic datasets for face recognition with realistic variations," in *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV) Workshops*, October 2023, pp. 3086–3095.
- [20] X. Xu, Y. Huang, P. Shen, S. Li, J. Li, F. Huang, Y. Li, and Z. Cui, "Consistent instance false positive improves fairness in face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2021, pp. 578–586.
- [21] S. Serengil and A. Özpınar, "A benchmark of facial recognition pipelines and co-usability performances of modules," *Bilişim Teknolojileri Dergisi*, vol. 17, no. 2, p. 95–107, 2024.
- [22] D. Zeng, R. Veldhuis, and L. Spreeuwiers, "A survey of face recognition techniques under occlusion," *IET Biometrics*, vol. 10, no. 6, pp. 581–606, 2021. [Online]. Available: <https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/bme2.12029>