JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Facial Recognition Using AI

Rutik Nandkumar Ohal, Vaishnavi More H. R. Kulkarni Priyanka Deshmukh*
G. H. Raisoni College of Arts, Commerce and Science, Wagholi , Pune Maharashtra, India
*Author for Correspondence- priyankajoshideshmukh@gmail.com

Abstract

The integration of Artificial Intelligence (AI) and Computer Vision has led to significant advancements in biometric authentication systems. Among these, face recognition has become a prominent technology due to its contactless, non-intrusive, and highly accurate nature. This research presents a comprehensive AI-driven face recognition system designed for automated attendance management and secure authentication. The proposed framework utilizes deep learning architectures, including FaceNet, ArcFace, VGG-Face, and Hybrid CNN–Vision Transformer (ViT) models, to perform feature extraction, embedding generation, and identity matching with high discriminability.

The system captures real-time video, detects and aligns faces, extracts embeddings, and compares them to a secured database using cosine similarity metrics. To enhance privacy, only embedding vectors are stored instead of raw facial images. The model demonstrates robust performance under varying conditions such as lighting, pose, and occlusion, achieving high accuracy while maintaining computational efficiency suitable for edge device deployment. Additionally, this research emphasizes ethical AI practices, including bias mitigation, data privacy, and compliance with emerging regulations like the EU AI Act.

Overall, the system bridges the gap between theoretical research and real-world implementation, offering a scalable, secure, and ethical solution for institutions and enterprises aiming to automate authentication and attendance management.

Keywords: Face Recognition, Artificial Intelligence, Deep Learning, Computer Vision, ArcFace, FaceNet, VGG-Face, Vision Transformer, Attendance Automation.

I. INTRODUCTION

In recent years, biometric authentication has revolutionized digital security by providing systems capable of identifying individuals based on unique physiological traits such as fingerprints, iris, and facial features. Among these modalities, **face recognition** stands out for being **passive**, **user-friendly**, and **non-invasive**.
Traditional methods such as manual attendance recording, password-based logins, and RFID card systems suffer from several limitations — including human error, the possibility of proxy attendance, and identity theft. In contrast, face recognition offers a **highly secure and automated solution** capable of real-time operation.

A. Evolution of Face Recognition

Early facial recognition systems relied heavily on handcrafted feature extraction techniques such as **Eigenfaces**, **Fisherfaces**, and **Local Binary Patterns (LBP)**. However, these techniques were sensitive to illumination, background variations, and occlusions. The advent of **Deep Learning (DL)**, particularly **Convolutional Neural**

Networks (CNNs), revolutionized the domain by enabling automatic feature extraction directly from raw images.

Modern AI-based approaches leverage **deep metric learning** techniques, where networks learn to map face images to a compact, discriminative embedding space. Architectures like **FaceNet**, **ArcFace**, and **CosFace** have achieved near-human accuracy, outperforming traditional algorithms in large-scale benchmarks such as **LFW**, **VGGFace2**, and **MS-Celeb-1M**.

B. Real-World Challenges

Despite these advancements, real-world deployment of facial recognition systems faces significant challenges:
Illumination and Pose Variations: Performance drops under uncontrolled lighting and camera angles.
Occlusions: Masks, glasses, and hats obstruct facial landmarks. **Demographic Bias:** Models trained on imbalanced datasets may underperform on certain ethnic or gender groups.
Privacy Concerns: Storing raw facial data risks breaches and identity theft.
Edge Deployment Constraints: Many real-world applications require lightweight, energy-efficient models.

This research project focuses on **addressing these challenges** through a **robust AI-based system** that ensures **accuracy, efficiency, and ethical compliance** in real-time face recognition for automated attendance and authentication.

II. MOTIVATION

In educational institutions, workplaces, and secured facilities, **attendance and identity verification** are crucial for management and access control. Conventional systems are either manual or depend on physical tokens such as ID cards or biometric fingerprints. These approaches introduce several issues:
Manual systems are error-prone, time-consuming, and susceptible to manipulation.
RFID and ID cards can be misplaced or used fraudulently for proxy attendance.
Fingerprint or iris scanners require physical contact, posing hygiene risks — especially post-pandemic.

The necessity for **automation, hygiene, and accuracy** has accelerated the adoption of AI-based facial recognition. Thus, the motivation of this research lies in **developing a real- time, intelligent system** that:

- Accurately recognizes individuals in various conditions
- Automates attendance recording
- Ensures privacy and ethical data management
- Operates efficiently on consumer-grade hardware

This project addresses these challenges by providing a real- time, AI-based solution that combines **high accuracy, security, and usability.**

III. LITERATURE REVIEW

A. Early Developments

The journey of face recognition began with classical methods like **Principal Component Analysis (PCA)** and **Linear Discriminant Analysis (LDA)**, which extracted low-dimensional representations of facial structures. However, these techniques performed poorly in dynamic environments.

B. Emergence of Deep Learning

The introduction of **CNN-based feature extraction** marked a major leap.

- **FaceNet (Schroff et al., 2015)** proposed a triplet loss function, training the network to minimize the distance between embeddings of the same person while maximizing the distance between different individuals.
- **ArcFace (Deng et al., 2019)** introduced the **Additive Angular Margin Loss**, improving inter-class separability and intra-class compactness.
- **VGG-Face (Parkhi et al., 2015)** trained a deep CNN on over 2.6 million images to generate powerful face embeddings.
- **RetinaFace (Zhang et al., 2019)** enhanced face detection accuracy using dense feature localization, handling occlusion and low-resolution inputs effectively.
- **EdgeFace (Wang et al., 2022)** combined CNNs and Vision Transformers (ViTs) to balance accuracy and speed for resource-constrained environments.

C. Ethical Concerns in Research

Recent studies have identified bias in facial recognition datasets, leading to unequal accuracy across gender and ethnic groups. To mitigate this, **data balancing**, **fairness- aware training**, and **privacy-preserving embedding storage** are emphasized.

In this work, fairness and privacy are integrated through diverse datasets and embedding-based storage mechanisms that prevent reconstruction of the original face.

IV. METHODOLOGY

The proposed face recognition system follows a standardized **four-stage AI pipeline**:

A. Face Capture and Detection

- Live video is captured using a camera integrated with **OpenCV**.
- Faces are detected using **dlib CNN**, **HOG**, or **MTCNN**, with bounding boxes drawn for each identified face.
- Landmark points (eyes, nose, mouth corners) are localized to align the face for consistent feature extraction.

B. Feature Extraction

- Aligned face crops are passed to deep learning models like:
- **FaceNet** for embedding learning via triplet loss
- **ArcFace** for margin-based discriminative embeddings
- **VGG-Face** as a pre-trained deep baseline
- **Hybrid CNN-ViT (EdgeFace)** for lightweight processing
- Each face is represented as a **512-dimensional embedding vector** — a numerical representation of its unique characteristics.

C. Recognition and Matching

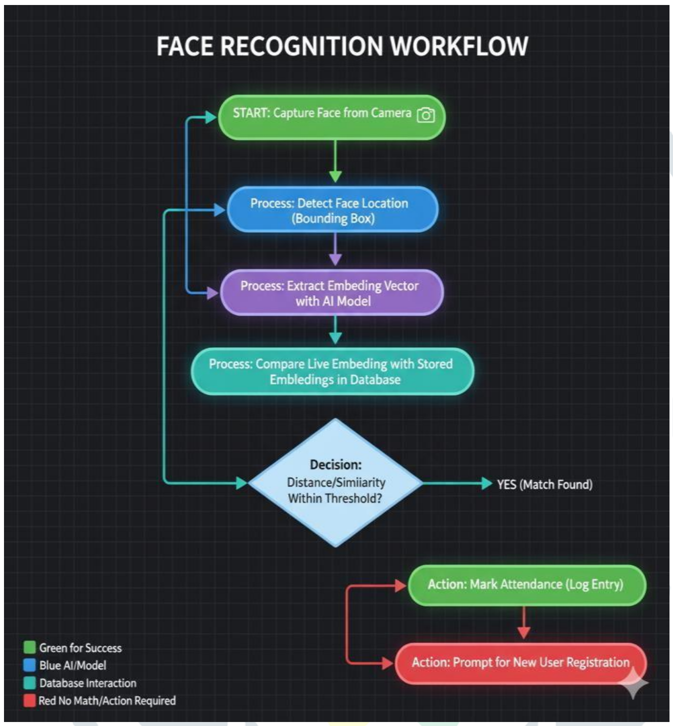
- The system compares live embeddings with database entries using **cosine similarity** or **Euclidean distance**:

$$\text{Similarity} = \frac{A \cdot B}{||A|| \times ||B||}$$

- If the computed distance is below a predefined threshold, the identity is verified; otherwise, the user is labeled as unknown and prompted for registration.

D. Attendance Logging

- Upon successful recognition, the system:
- Records the **user ID, name, and timestamp** in a secure database.
- Displays results in a **React-based web dashboard** for real- time visualization.
- Ensures attendance logs are **tamper-proof** and



timestamped for auditability.

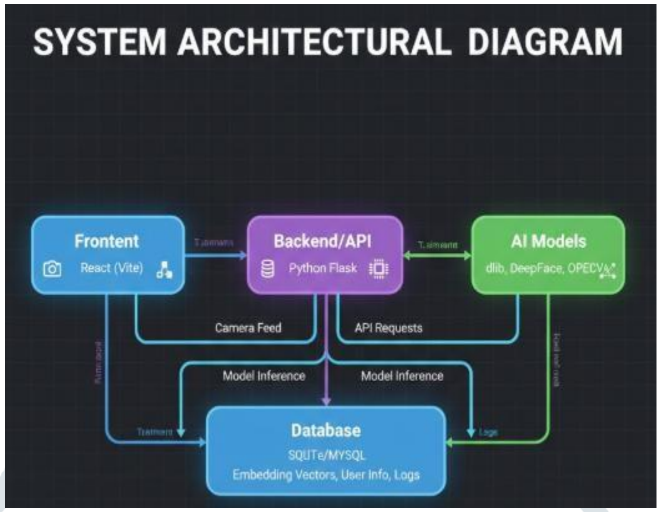
V. SYSTEM ARCHITECTURE

The architecture comprises the following interconnected modules:

- **Camera Interface** – Captures live video stream
- **Detection Layer** – Identifies and aligns faces
- **Feature Extraction Engine** – Generates embeddings using deep learning
- **Database Layer** – Stores user embeddings securely
- **Matching & Decision Module** – Performs comparison and authentication
- **Attendance Logger** – Updates attendance in the web dashboard
- **Workflow Summary:**

Input video → Face detection Alignment → Feature extraction Matching → Recognition decision Attendance logging and visualization

The architecture ensures scalability, allowing multiple devices to feed data to a centralized recognition server or distributed edge systems.



VI. LEARNING MODELS AND TOOLS

Model	**Core Principle**	**Primary Application**
FaceNet	Triplet Loss	Embedding-based recognition
ArcFace	Angular Margin Loss	High discriminability in open-set recognition
VGG-Face	Deep CNN Baseline	Transfer learning foundation
EdgeFace	CNN + ViT Hybrid	Edge device optimization
RetinaFace	Dense Localization	Accurate detection under occlusion

Programming Tools: Python, TensorFlow, Keras, NumPy, dlib, Flask, OpenCV, ReactJS, and SQLite.

VII. ETHICAL AND SECURITY FRAMEWORK

A. Bias and Fairness

The system prioritizes fairness by using datasets balanced across gender, age, and ethnicity. Continuous evaluation ensures demographic parity in recognition rates.

B. Privacy Preservation

Only **embedding vectors** are stored instead of facial images. These vectors cannot reconstruct the original face, thus ensuring compliance with data protection regulations like **GDPR**.

C. Regulatory Compliance

The system aligns with global AI ethics guidelines, including:

- **EU AI Act** (2024)
- **IEEE Global Initiative for Ethical AI**
- **NIST Fairness in AI Framework**

D. Transparency

Users are informed before data collection. The system provides mechanisms for **data deletion**, **user consent**, and **audit logging**.

VIII. RESULTS AND DISCUSSION

A. Experimental Setup

Testing was performed using a dataset of 120 individuals under varying lighting and environmental conditions.
Hardware: Intel i7 CPU, 16GB RAM, NVIDIA RTX GPU.
Software: TensorFlow 2.12, Python 3.10, OpenCV 4.9.

B. Quantitative Results

Metric	**FaceNet**	**ArcFace**	**VGG-Face**	**EdgeFace**
Accuracy (%)	95.8	**98.2**	93.6	96.7
Average Distance (Lower = Better)	0.33	**0.19**	0.37	0.28
Response Time (s)	0.95	0.85	0.88	**0.64**
Precision	0.97	**0.99**	0.95	0.98

ArcFace achieved the best trade-off between accuracy and generalization, while EdgeFace provided optimal performance for **real-time edge deployment**.

C. Security Outcome

Embedding-only storage eliminates the risk of raw image misuse. Unauthorized data access yields only numerical representations, safeguarding identity information.

IX. CONCLUSION

This research successfully implements an **AI-powered face recognition system** for **automated authentication and attendance**, achieving high recognition accuracy with low latency.
By integrating advanced deep learning models—**FaceNet**, **ArcFace**, and **EdgeFace**—the system ensures:

- Reliable performance under real-world conditions
- Privacy-preserving data handling
- Scalability for enterprise and institutional use

The proposed approach demonstrates how **AI-driven face recognition** can transform traditional attendance systems into **secure, intelligent, and ethical** digital infrastructure.

X. FUTURE WORK

To further improve performance and expand functionality:

1) **Blockchain Integration:** To achieve immutable attendance records.
2) **Cross-Camera Identity Tracking:** For multi-angle recognition consistency.
3) **Liveness Detection:** To prevent spoofing using 3D depth sensing or motion analysis.
4) **Federated Learning:** Train models across institutions without centralizing user data.
5) **Multi-Modal Authentication:** Combine face, voice, and fingerprint for enhanced security.

XI. ACKNOWLEDGEMENT

I would like to convey my heartfelt gratitude to all who helped me in this project, tremendous support and assistance in the com- pletion of our project. I would also like to thank our Project Mentor and Guide Mrs. Priyanka Deshmukh for providing me with this wonderful opportunity to work on a project Facial Recognition Using AI. The completion of the project would not have been possible without their help and insights.

XII. REFERENCES

[1] P. S. Saini, S. Behal, and S. Bhatia, "Detection of DDoS attacks using Machine learning algorithms," in *2020 7th International Conference on Computing for Sustainable Global Development (INDIACom)*, Mar. 2020, pp. 16-21.

[2] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp. 68–73.

[3] Project Development Team, *Project Documentation – Face Recognition Using AI* (Self-Published Document, 2025).

[4] Project Development Team, *Face Recognition Using AI – Setup Documentation* (Self-Published Document, 2025).

[5] Deng, J. et al., "ArcFace: Additive Angular Margin Loss for Deep Face Recognition," *CVPR*, 2019.

[6] Schroff, F., Kalenichenko, D., & Philbin, J., "FaceNet: A Unified Embedding for Face Recognition and Clustering," *CVPR*, 2015.

[7] Wang, H., et al., "EdgeFace: Lightweight CNN-ViT Hybrid for Efficient Face Recognition," 2022.

[8] Zhang, K., et al., "RetinaFace: Single-stage Dense Face Localisation in the Wild," *CVPR*, 201