IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 6, Ser. 4 (Nov. – Dec. 2025), PP 49-63
www.iosrjournals.org

Deep Learning Techniques For Unconstrained Face Identification And Verification In IoT Applications

Samadhan S. Ghodke, Prapti D. Deshmukh, Shalini R. Bakal, Anand D. Kadam
(Dr. G. Y. Pathrikar College Of Computer Science And IT, MGM University (MH), Chhatrapati Sambhajinagar, India).

Abstract:
Face recognition technology has evolved significantly with the integration of Internet of Things (IoT) and machine learning approaches, enabling real-time identification and verification in unconstrained environments. This comprehensive review examines recent advancements in IoT-based face recognition systems, focusing on methodologies that address challenges in unconstrained conditions including variations in pose, illumination, occlusion, and resolution. We analyze the progression from traditional handcrafted methods to deep learning architectures, exploring their implementation on resource-constrained edge devices such as Raspberry Pi. The paper systematically reviews face detection algorithms (MTCNN, RetinaFace, Haar Cascade), recognition models (FaceNet, ArcFace, VGG-16, ResNet-50), and their deployment strategies in IoT environments. Additionally, we examine critical aspects including privacy preservation, edge computing paradigms, and performance optimization techniques. Our analysis reveals that deep learning-based approaches, particularly CNNs with margin-based loss functions, achieve superior accuracy (95-97%) compared to traditional methods, even on edge devices. However, challenges remain in ensuring robustness under extreme unconstrained conditions, balancing computational efficiency with accuracy, and maintaining privacy in distributed IoT systems. This review provides insights into current state-of-the-art methodologies and identifies promising directions for future research in developing robust, efficient, and privacy-preserving IoT-based face recognition systems.

Key Word: *Face Recognition, Face Verification, IoT, Edge Computing, Deep Learning, Unconstrained Environment, Raspberry Pi, Privacy Preservation.*

Date of Submission: 18-12-2025 Date of Acceptance: 28-12-2025

I. Introduction

Face recognition technology represents one of the most successful applications of artificial intelligence and computer vision, providing non-intrusive biometric identification capabilities that have transformed security, authentication, and surveillance systems [1]. Unlike other biometric modalities such as fingerprints or iris scanning, face recognition offers contactless operation, making it particularly suitable for modern applications where hygiene and user convenience are paramount [2]. The integration of face recognition with Internet of Things (IoT) infrastructure has further expanded its applicability, enabling distributed, real-time processing across networked edge devices[3].

The distinction between face identification (1:N matching) and face verification (1:1 matching) is fundamental to understanding face recognition systems[4]. Face identification involves searching through a database of known faces to determine an individual's identity, while face verification confirms whether a captured face matches a claimed identity. Both tasks become significantly more challenging in unconstrained environments, where uncontrolled factors such as varying illumination, arbitrary pose angles, partial occlusions, diverse facial expressions, and low resolution severely impact recognition performance[5].

Traditional face recognition approaches relied on handcrafted features such as Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), and Principal Component Analysis (PCA)[6]. While these methods demonstrated acceptable performance under controlled conditions, they exhibited substantial accuracy degradation when deployed in real-world unconstrained scenarios[5]. The emergence of deep learning, particularly Convolutional Neural Networks (CNNs), has revolutionized the field by enabling automatic feature learning from large-scale datasets, resulting in recognition systems that surpass human performance on benchmark datasets[7].

The integration of face recognition with IoT architectures presents unique opportunities and challenges. IoT-based systems enable distributed data collection, real-time processing at the edge, and seamless integration with smart environments[8]. However, deploying sophisticated deep learning models on resource-constrained devices such as Raspberry Pi requires careful optimization of computational complexity, memory consumption,

and energy efficiency[9]. Additionally, privacy concerns associated with collecting and processing biometric data necessitate robust security mechanisms and privacy-preserving techniques[10].

Recent face biometric research has focused on addressing these challenges through various approaches: developing lightweight architectures suitable for edge deployment, implementing privacy-preserving protocols, optimizing detection and recognition pipelines, and enhancing robustness to unconstrained conditions[11][12]. This review systematically analyzes these developments, providing a comprehensive overview of methodologies, architectures, and implementation strategies for IoT-based face recognition systems operating in unconstrained environments.

II. Methodology

The IoT-based face recognition methodology captures images and preprocesses them to improve quality. After detecting and aligning the face, deep learning extracts key features. These are matched with stored templates to verify identity, and the system performs actions such as marking attendance or updating records, more info refer

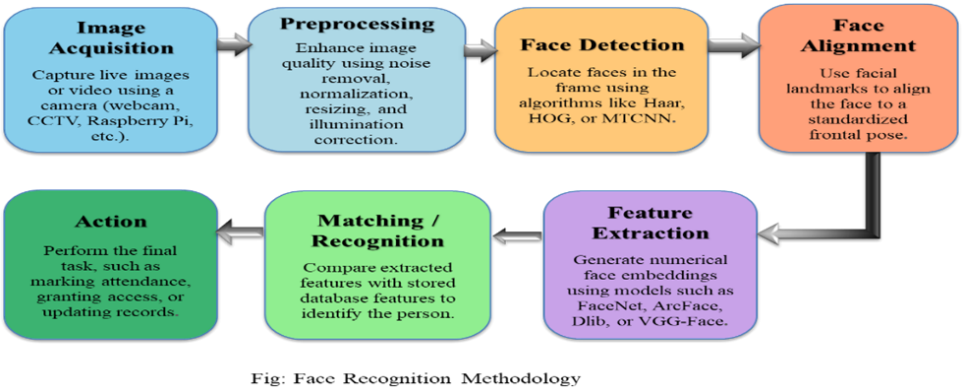

Fig: Face Recognition Methodology

(Fig.1) Methodology.

III. Unconstrained Face Recognition: Challenges And Definition

Definition of Unconstrained Conditions

Unconstrained face recognition refers to the identification or verification of individuals under real-world conditions where environmental factors are not controlled [5]. Unlike constrained scenarios where subjects cooperate with standardized imaging protocols (frontal pose, neutral expression, uniform illumination), unconstrained conditions present multiple simultaneous challenges that degrade recognition performance. Key characteristics of unconstrained environments include [5][13]:

Table.1: Characteristics of Unconstrained Environments

Environmental Factor	Description	Performance Impact
Pose Variation	Arbitrary head orientations from frontal to extreme profile (±90°)	30-40% accuracy drop at extreme angles
Illumination Variation	Uncontrolled lighting, shadows, directional light, low-light scenarios	Significant appearance changes
Occlusion	Glasses, masks, scarves, objects obstructing facial regions	40-60% accuracy drop with >50% occlusion
Expression Variation	Non-neutral facial expressions causing geometric deformations	Moderate impact on traditional methods
Resolution & Quality	Low-resolution, motion blur, compression artifacts	50-70% accuracy drop below 32×32 pixels
Aging & Appearance	Long-term variations from aging, weight changes, hairstyles	15-20% accuracy degradation
Environmental Degradation	Weather conditions, atmospheric effects, camera artifacts	Variable impact depending on severity

Fig .2: Sample Unconstrained Faces (Own Dataset).

Shepley (2019) conducted a systematic review revealing a consistent increase in research interest in unconstrained face recognition between 2012 and 2018, driven by improvements in hardware capabilities, availability of large-scale datasets, and the emergence of powerful deep learning architectures [5]. The review identified that 39% of studies addressed unconstrained conditions generally rather than focusing on specific environmental factors, indicating that modern deep learning approaches learn to handle multiple unconstrained features simultaneously during training.

Performance Degradation in Unconstrained Scenarios

Traditional feature-based methods degrade severely under unconstrained conditions because they depend on geometric and texture patterns that become unstable with appearance variations [5]. Research by Hoermann shows occlusions cause major drops in accuracy, proportional to the size and location of the occluded regions [14]. When multiple unconstrained factors occur together—common in real-world surveillance—pose, resolution, and illumination variations create recognition challenges that simple algorithms cannot handle [15]. Recent benchmarks such as WiderFace and UFDD evaluate performance under these conditions and show that traditional methods still perform poorly, especially for small-scale and heavily occluded faces, with significant drops in detection rates [16].

Table.2: Performance Degradation in Unconstrained Scenarios

Method Type	Robustness	Accuracy (Controlled)	Accuracy (Unconstrained)	Degradation
Traditional Feature-Based	Low	85-90%	40-60%	25-50%
Handcrafted Features (LBP, HOG)	Low	80-85%	35-55%	25-50%
Early CNNs	Moderate	90-95%	70-80%	10-25%
Modern Deep Learning	High	95-99%	85-96%	3-14%

Evolution from Constrained to Unconstrained Recognition

Face recognition has progressed from controlled laboratory systems to deep learning models achieving near-human accuracy [1][2][7]. Despite major gains, extreme unconstrained conditions and adversarial attacks remain ongoing challenges [5]

Table. 3: Evolution of Face Recognition Technology

Era	Period	Methods	Accuracy	Environment	Key Development
Laboratory Era	1960s-1990s	Eigenfaces, Fisherfaces	60-70%	Controlled only	Foundational algorithms
Transition Era	2000s	Viola-Jones, AdaBoost	75-85%	Mostly controlled	First practical deployments
Deep Learning Era	2014-2015	DeepFace, FaceNet	97-99%	Both	Superhuman performance
Modern Edge Era	2018-2025	Optimized CNNs, Transformers	92-98%	Unconstrained	Real-time edge deployment

IV. Deep Learning Architectures For Face Recognition

Convolutional Neural Networks (CNNs)

CNNs dominate face recognition because they automatically learn hierarchical features directly from pixel data, removing the need for manual feature engineering [17]. Successive layers extract low-, mid-, and high-level identity features for robust recognition [18].

The general CNN architecture for face recognition consists of[19]:

1. **Input Layer:** Accepts preprocessed face images, typically normalized to fixed dimensions (e.g., 224×224 or 160×160 pixels)
2. **Convolutional Layers:** Apply learned filters to extract spatial features while preserving spatial relationships
3. **Activation Functions:** Introduce non-linearity, commonly using ReLU (Rectified Linear Unit) activation
4. **Pooling Layers:** Reduce spatial dimensions while retaining important features, providing translation invariance
5. **Fully Connected Layers:** Aggregate features for final classification or embedding generation
6. **Output Layer:** Produces identity classification (for closed-set recognition) or feature embeddings (for open-set recognition)

Transfer Learning and Pretrained Models

Transfer learning has become essential for deploying face recognition on resource-constrained IoT devices, allowing models pretrained on large datasets to be fine-tuned for specific applications with limited training data[20]. Ahmed Ali Aboluhom et al. (2024) investigated transfer learning feasibility for facial

recognition on Raspberry Pi, evaluating multiple pretrained architectures including VGG-16, ResNet-50, and MobileNetV2[9].

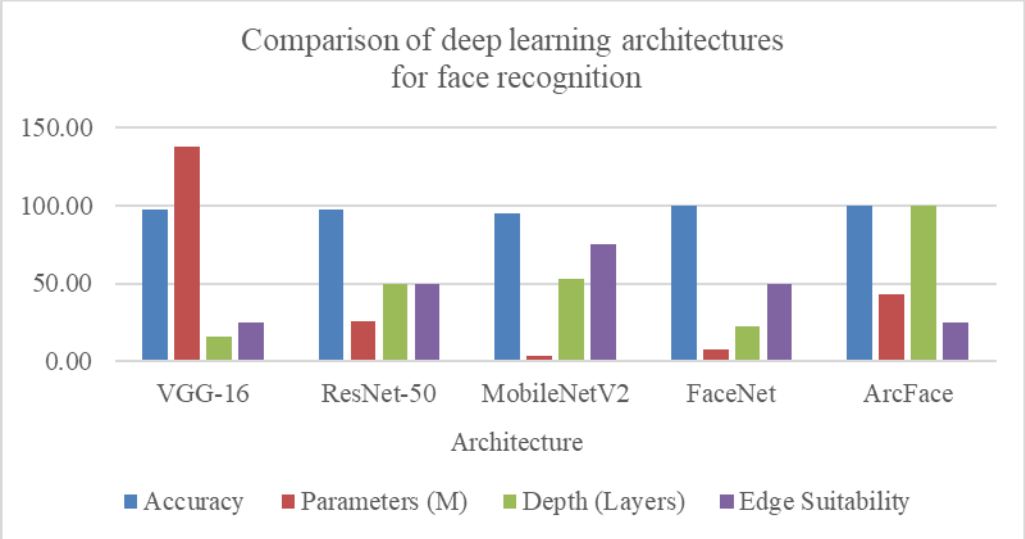

Fig 3: Comparison of deep learning architectures for face recognition

VGG-16 offers strong feature extraction using 3×3 filters but is computationally heavy, though works like Hussain et al. reported 97% accuracy with SVM in IoT access control [2]. **ResNet-50** uses skip connections to train deeper networks effectively and performs well in face recognition when resources allow [2][9]. **MobileNetV2** is lightweight and ideal for edge devices, with studies showing it outperforms VGG-16 and ResNet-50 on Raspberry Pi using transfer learning [9].

Landmark Architectures: FaceNet, DeepFace, and ArcFace

FaceNet (2015) learns a 128-D embedding where face similarity is measured by Euclidean distance using triplet loss, achieving over 99% accuracy on LFW [21][22].

$$L = \sum_{i}^{N} [\|f(x_i^a) - f(x_i^p)\|_2^2 - \|f(x_i^a) - f(x_i^n)\|_2^2 + \alpha]_+$$

Fig 4.3: FaceNet Pertained model

DeepFace (2014) reached **97.35% accuracy on LFW** using 3D alignment and a deep CNN trained on 4M facial images [7].

ArcFace (2019) improves discrimination with Additive Angular Margin Loss, achieving 99.83% on LFW and outperforming FaceNet in real-world deployments [23][24].

$$L_{ArcFace} = -\frac{1}{N}\sum_{i=1}^{N} \log \frac{e^{s\cos(\theta_{y_i}+m)}}{e^{s\cos(\theta_{y_i}+m)} + \sum_{j=1,j\neq y_i}^{C} e^{s\cos\theta_j}}$$

Loss Functions for Discriminative Learning

Loss function evolution has played a major role in improving face recognition. Early CNN systems relied on **softmax**, which was insufficient for learning highly discriminative features at large scale [1]. Metric learning methods such as **Contrastive Loss** and **Triplet Loss** optimized embedding distances to cluster same-identity faces and separate different identities, but required careful sample selection [1][22]. Modern margin-based losses now dominate, including **SphereFace** (angular margin on a hypersphere), **CosFace** (cosine margin), and **ArcFace** (additive angular margin in arc-cosine space) [1][23]. These methods enforce stronger class separation and yield improved generalization under challenging real-world conditions.

V. Face Detection Algorithms

Traditional Methods: Haar Cascade and Viola-Jones

Haar Cascade, based on the Viola-Jones framework, is one of the earliest practical face detection algorithms [25]. It uses Haar-like features with integral images for fast computation, AdaBoost for feature selection, and a cascade of classifiers for rapidly rejecting non-face regions [2][26]. Hussain et al. (2022) used Haar Cascade in an IoT medical facility system, citing high detection accuracy, fast processing, and low false positives on devices like Raspberry Pi [2]. However, Haar Cascade performs poorly under unconstrained conditions, struggling with pose changes, occlusion, and non-frontal faces [27].

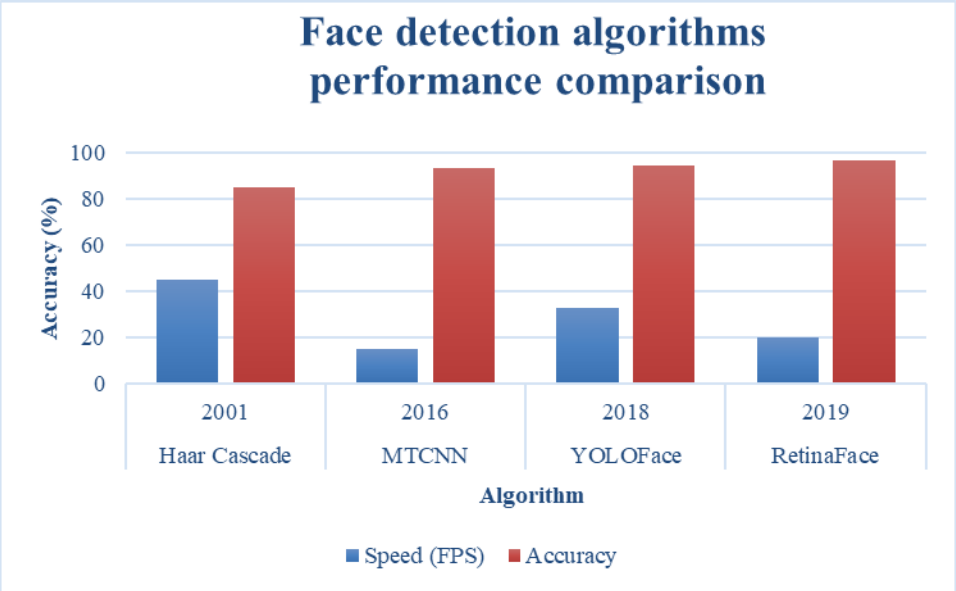

Fig 4: Face detection algorithms performance comparison

Fig 4.: Features using Haar Cascade to localize the Region of Interest (ROI).

Comparative studies by Ananda et al. (2024) demonstrate that while Haar Cascade performs adequately for frontal faces in controlled conditions, it fails substantially when faces are occluded or captured at extreme angles [27]. This performance gap has driven the adoption of deep learning-based detection methods for modern unconstrained applications.

Multi-task Cascaded Convolutional Networks (MTCNN)

MTCNN represents a significant advancement in face detection, employing a three-stage cascaded architecture that simultaneously performs face detection and facial landmark localization[28]. The cascade consists of:

1. **Proposal Network (P-Net):** Rapidly generates candidate facial regions through a fully convolutional network
2. **Refine Network (R-Net):** Refines candidate boxes and rejects false positives
3. **Output Network (O-Net):** Produces final face boxes with high precision and detects five facial landmarks (eyes, nose, mouth corners)

MTCNN uses a multi-task learning framework to jointly optimize face classification, bounding box regression, and landmark localization, improving detection accuracy and enabling reliable face alignment [24][28]. Asmara et al. reported MTCNN is effective as a backend detector, though RetinaFace performed better in comparison [24]. MTCNN can detect multiple faces with landmark output, making it useful for IoT surveillance, but its computational load is higher than Haar Cascade and requires optimization for edge devices [29].

RetinaFace: State-of-the-Art Single-Stage Detection

RetinaFace is a state-of-the-art face detector based on the single-stage RetinaNet architecture, enhanced with multi-task learning (detection + landmarks + 3D alignment), Feature Pyramid Networks for multi-scale detection, context modules for small faces, and dense regression with deformable convolutions [30]. Ren et al. (2025) reported **96.12% accuracy on WiderFace**, showing strong performance on small and distant faces [30]. Studies consistently find RetinaFace outperforms Haar Cascade and MTCNN under occlusion, pose variation, and varying scales, and Asmara et al. recommend pairing RetinaFace detection with ArcFace recognition for highest accuracy despite higher computational cost [24][27][30].

Comparative Performance Analysis

Recent comparative studies provide clear guidance on detector selection based on application requirements. Ananda et al. (2024) conducted comprehensive analysis across four detection algorithms (Haar Cascade, MTCNN, YOLOFace, RetinaFace) under various unconstrained conditions[27]:

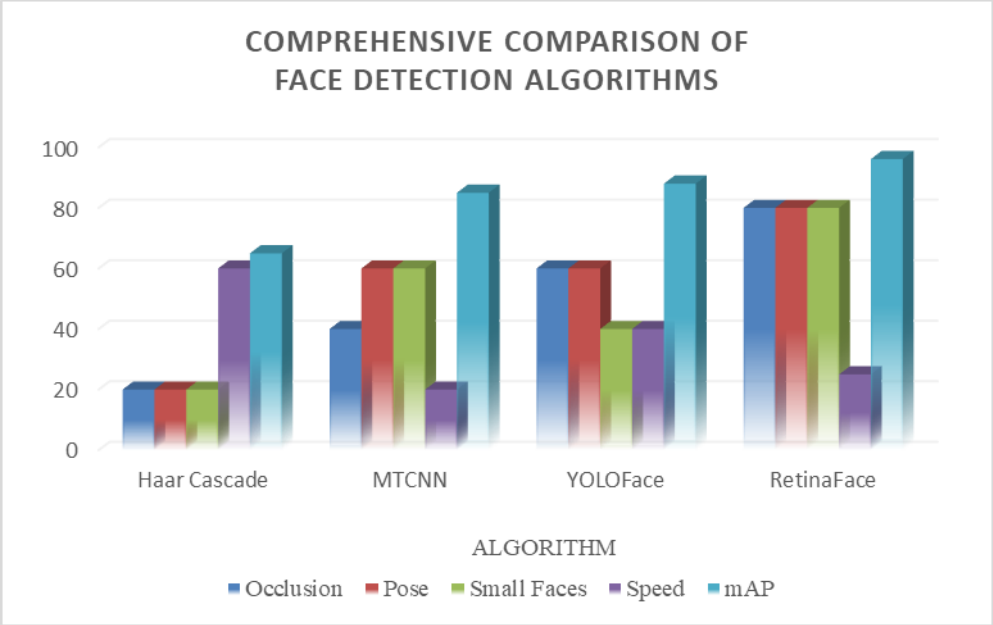

Fig 5: Comprehensive comparison of face detection algorithms

For IoT edge deployments, balancing accuracy and computational efficiency is crucial. RetinaFace offers top accuracy, but lightweight options such as MTCNN or optimized YOLOFace are often better suited for resource-limited devices [31]. Detector choice should reflect application needs, hardware capacity, and the expected level of unconstrained conditions.

VI. IoT-Based Face Recognition Systems

IoT Architecture for Face Recognition

IoT-based face recognition typically uses a **three-tier architecture**: a **Device Layer** for image capture, an **Edge Computing Layer** for detection and feature extraction, and a **Cloud Layer** for large-scale storage and model training [2][9][32]. Xiang et al. (2025) demonstrated adaptive edge systems enabling sustainable, unmanned operation in real-world environments [33].

Table.4: Three-Tier IoT Architecture

Tier	Layer Name	Components	Functions	Output
1	Device Layer	Cameras, sensors	Image capture, basic preprocessing	Raw/filtered images

Tier	Layer Name	Components	Functions	Output
2	Edge Computing	RPi/Jetson, local processors	Detection, feature extraction, recognition	Results, embeddings
3	Cloud Layer	Centralized servers	Database management, model training, analytics	Logs, insights, models

Raspberry Pi as Edge Platform

Raspberry Pi has emerged as a popular platform for deploying face recognition at the edge due to its low cost, moderate computational capability, compact form factor, and extensive community support[9][22][34]. Multiple studies have demonstrated successful implementation of deep learning-based face recognition on Raspberry Pi platforms:

Table.5: Edge computing platforms for face recognition

Platform	CPU	RAM	FPS	Accuracy
RPi 3 Model B	1.4GHz 4-core	1GB	2[35]	97%[35]
RPi 4 Model B	1.8GHz 4-core	2-8GB	5-10[9]	95%[9]
RPi 4 (8GB)	1.8GHz 4-core	8GB	8-12[37]	94.6%[37]
Jetson Nano	1.43GHz 4-core	4GB	15-20	96-97%

Real-time Processing and Performance Optimization

Real-time edge performance requires multi-level optimization. **Rana et al. (2023)** showed practical Raspberry Pi deployment by balancing accuracy and speed through preprocessing (resolution reduction, fast detection, frame skipping) [28][37], efficient model choices like depthwise separable convolutions and inverted residual blocks (MobileNetV2) [9], and inference techniques such as quantization, pruning, and hardware acceleration [22][37]. Pipeline strategies include multi-threading, frame buffering, and adaptive quality control [33][37]. **Sumathi et al. (2022)** demonstrated that careful IoT system design can achieve low-latency face detection even on constrained devices [8].

Table.6: Real-Time Processing Optimization Strategies

Strategy	Technique	Speed Improvement	Accuracy Impact
Image Preprocessing	Lower resolution, frame skipping	20-30% faster	<2% loss
Model Selection	MobileNet over VGG-16	3-5x faster	2-3% loss
Quantization	Float32 → Int8	2-4x faster	1-2% loss
Pruning	Remove redundant weights	1.5-3x faster	<1% loss
Multi-threading	Parallel detection-recognition	30-50% faster	No loss
Frame Buffering	Process queue smoothing	Consistent speed	No loss
Hardware Acceleration	NEON instructions (ARM)	1.5-2x faster	No loss

Integration with Access Control and Security Systems

IoT-based face recognition is widely used in **smart door locks**, **attendance systems**, **surveillance**, and **multi-factor authentication** [2][38]. Hussain et al. (2022) implemented Raspberry Pi–based door access control [2], while Warman et al. (2023) used FaceNet for real-time attendance synchronization across facilities [40]. Integrating edge processing with CCTV and additional factors like RFID improves security and reduces bandwidth needs [39][41].

VII. Privacy And Security In IoT Face Recognition

Privacy Challenges in Biometric Systems

Face recognition in IoT environments presents major privacy risks due to sensitive biometric data and distributed system vulnerabilities to multiple attack vectors [10][42].

Data collection and consent: Facial biometrics can be captured without user awareness, and compromised faces cannot be changed [5].

Storage and transmission security: Raw images and templates moving between edge and cloud are vulnerable to interception and identity theft [43].

Inference and linkage attacks: Facial data can reveal sensitive attributes and allow cross-system tracking without consent [10].

Model extraction and inversion: Attackers may steal models or reconstruct faces from embeddings through repeated queries [42].

Table.7: Privacy threats and mitigation strategies in IoT face recognition systems

Privacy Threat	Attack Vector	Severity	Detection Difficulty	Mitigation Cost	Best Mitigation
Unauthorized Capture	Hidden cameras	High	High	Medium	Consent frameworks
Data Interception	Network sniffing	Critical	Low	Low	AES-256 encryption
Database Breach	Server compromise	Critical	High	Medium	Encrypted storage
Attribute Inference	ML analysis of embeddings	Medium	High	High	Differential privacy
Cross-DB Linkage	Feature matching across systems	Medium	Medium	High	Template protection
Model Inversion	Gradient attacks	Medium	Very High	Very High	Federated learning
Presentation Attack	Photo/video spoofing	High	Medium	Medium	Liveness detection

Privacy-Preserving Techniques

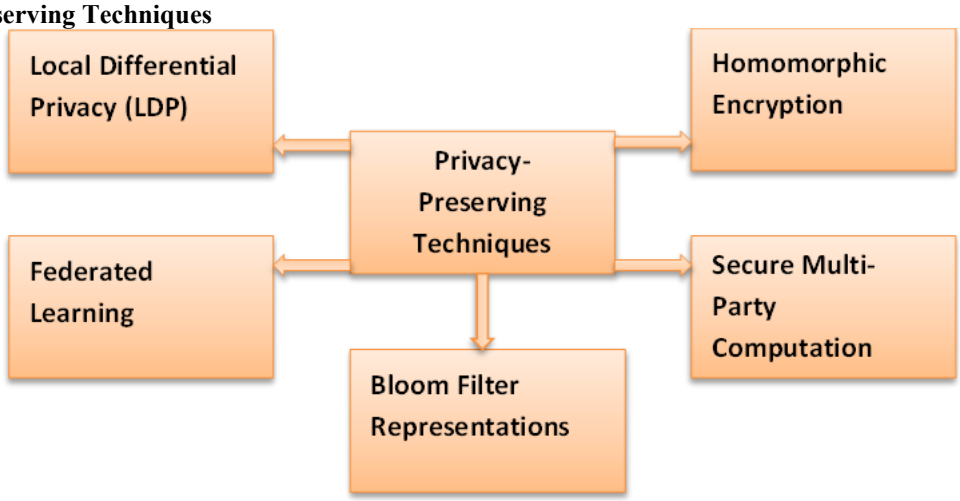

Fig 6: protect privacy while maintaining recognition performance in IoT environments

Recent research has developed multiple approaches to protect privacy while maintaining recognition performance in IoT environments:

Local Differential Privacy (LDP): Adds calibrated noise to facial features at the edge to protect cloud-transmitted data [10].

Homomorphic Encryption: Performs recognition on encrypted biometrics without exposing raw data [43].

Secure Multi-Party Computation: Splits processing across non-colluding servers to prevent full data exposure [43].

Bloom Filter Representations: Converts features into irreversible encodings for safe matching in IoT systems [44].

Federated Learning: Trains models locally and shares only aggregated updates, not raw biometric data [33].

Authentication and Encrypted Communication

Ensuring data integrity and authenticity throughout the IoT face recognition pipeline requires robust cryptographic protocols [10][43]. **Device registration & authentication**: Only verified devices can submit or receive face data, preventing unauthorized access [10]. **End-to-end encryption**: AES encryption and hash checks protect image transmission and data integrity [10]. **Blockchain integration:** Enables immutable logs and decentralized biometric access control, but currently faces scalability and latency challenges [45].

Table.8: Encryption Standards for IoT Systems

Standard	Key Size	Speed	Security Level	Suitable for RPi
AES-128	128-bit	Fast	Good	Yes
AES-256	256-bit	Fast	Excellent	Yes
RSA-2048	2048-bit	Slow	Good	Yes (limited)
RSA-4096	4096-bit	Very Slow	Excellent	No

Standard	Key Size	Speed	Security Level	Suitable for RPi
ECC-256	256-bit	Fast	Excellent	Yes

Liveness Detection and Anti-Spoofing

Beyond privacy preservation, security requires protecting against presentation attacks where adversaries attempt to spoof face recognition systems using photographs, videos, masks, or 3D reconstructions [46]:

Table.9: Anti-Spoofing/Liveness Detection Methods

Method	Detection Type	Computation	Accuracy	Speed	Hardware Required	Citation
Challenge-Response	Interactive	Low	98%+	Slow (1–2s)	None	[47]
Multi-Spectral	Passive	High	95%+	Medium (200–500 ms)	Multi-sensor	[46]
Depth Sensing	Passive	Medium	96%+	Fast (100 ms)	Depth camera	[47]
Motion Analysis	Passive	Medium	93%+	Medium (200 ms)	Standard camera	[46]
Texture Analysis	Passive	Low–Medium	90%+	Fast (100 ms)	Standard camera	[46]
Combined Approach	Active+ Passive	High	99%+	Medium (300–500 ms)	Multiple sensors	–

VIII. Performance Evaluation And Benchmarks

Evaluation Metrics

Face recognition performance is measured using various metrics that capture accuracy, error rates, and overall system reliability.

Hussain et al. (2022) achieved optimal performance at a 90% threshold with **FAR=26.67%, FRR=9.33%, and EER=21.33%**, highlighting the security–convenience trade-off [2]. For IoT edge devices, **processing time, throughput, memory use, and energy consumption** are critical efficiency metrics alongside accuracy [9][37].

Table.10: Performance Evaluation Metrics

Metric	Definition	Formula	Ideal Value	Acceptable Range	Critical For	Measurement Method
Accuracy	Overall correctness	(TP+TN)/ (TP+TN+FP+FN)	100%	>95%	General performance	Confusion matrix
True Positive Rate (TPR)	Correct positive identifications	TP/(TP+FN)	100%	>98%	Security (catch intruders)	Positive samples
False Positive Rate (FPR)	Incorrect positive identifications	FP/(FP+TN)	0%	<1%	User experience	Negative samples
False Negative Rate (FNR)	Missed positive identifications	FN/(TP+FN)	0%	<2%	Security (authorized access)	Positive samples
Precision	Positive prediction accuracy	TP/(TP+FP)	100%	>95%	Minimize false alarms	Predicted positives
Recall (Sensitivity)	Actual positive detection	TP/(TP+FN)	100%	>98%	Comprehensive detection	Actual positives
F1 Score	Harmonic mean of precision/recall	2×(P×R)/(P+R)	1.0	>0.96	Balanced performance	Combined metric
Equal Error Rate (EER)	FPR = FNR point	Intersection point	0%	<3%	System threshold tuning	ROC curve
Inference Time	Processing speed	Time per image	<50ms	<200ms	Real-time applications	Benchmark
Throughput	Images per second	FPS	>30	>10	Video processing	Continuous feed

Standard Datasets for Unconstrained Face Recognition

The table compares major face recognition datasets commonly used in benchmarking, including LFW with 13,233 unconstrained images achieving over 99% accuracy 7, WiderFace featuring 32,203 images with multi-scale difficulty levels 1630, UFDD focusing on extreme conditions like weather and blur 16, MegaFace providing over one million faces for large-scale identification 23, and IJB-C offering unconstrained images and video with significant pose and illumination variations 48.

Table.11: Face Recognition Datasets Comparison

Dataset	Images	Identities	Primary Focus	Difficulty	Unconstrained Variations
LFW	13,233	5,749	Verification	Medium	Pose, lighting, expression **[7]**
WiderFace	32,203	–	Detection	Easy / Medium / Hard	Scale, pose, occlusion, illumination **[16][30]**
UFDD	6,424	–	Extreme conditions	Hard	Weather, blur, degradation **[16]**
MegaFace	1M+	690K+	Large-scale identification	Medium–Hard	Scale variation **[23]**
IJB-C	31,334	3,531	Unconstrained video	Hard	Pose + illumination variations **[48]**
CASIA-WebFace	494,414	10,575	Training	Medium	Web-sourced variations
MS-Celeb-1M	10M+	100K+	Large-scale training	Medium	Celebrity image variations

Reported Performance in Recent Studies

Recent implementations demonstrate the progression of face recognition performance on IoT platforms:

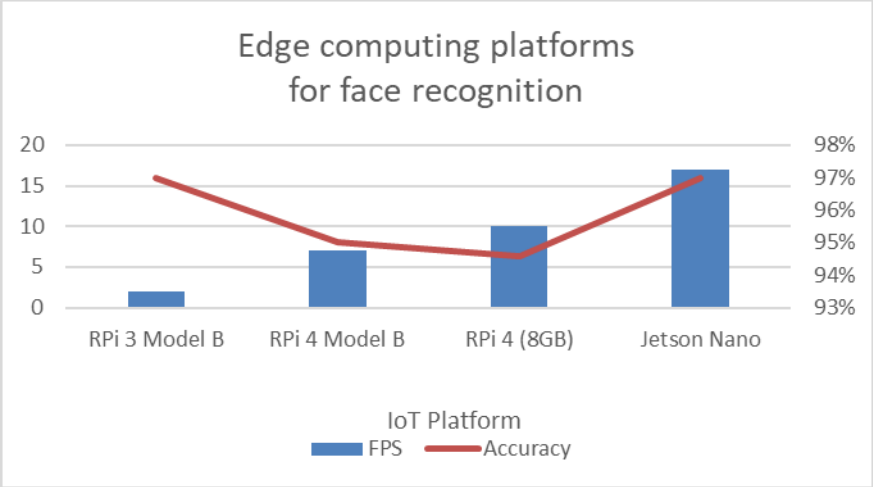

Fig 7: Recognition accuracy and processing speed in recent IoT implementations

Accuracy varies due to differences in datasets and conditions, reaching 95–97% in controlled settings and 84–96% in real-world scenarios **[2][9][30]**. Processing speed on Raspberry Pi has improved from 2 FPS on early boards to near real-time on RPi 4 with optimized models **[35][37]**.

Factors Affecting Real-World Performance

Studies consistently identify several factors impacting deployed system performance, **Fig.7:**

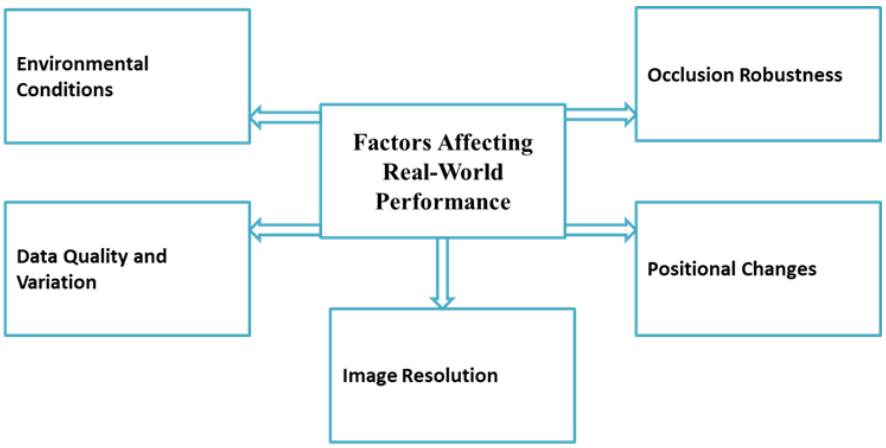

Fig: Identify several factors impacting deployed system performance

Environmental Conditions: Lighting variation reduces recognition accuracy; standardized lighting improves performance [2][50].
Data Quality & Variation: Diverse and large training datasets are essential for robust recognition in real-world conditions [2][9].
Image Resolution: Low-resolution or distant faces require specialized models for reliable recognition [30].
Positional Changes: Capturing multiple facial poses or using pose-invariant methods improves matching accuracy [2].
Occlusion Robustness: Techniques like face completion or partial face matching help handle masks, glasses, and occlusions [14].
Training with Augmentation: Synthetic data augmentation strengthens model performance under unconstrained environments [50].

Table.12: Impact of Unconstrained Conditions on Accuracy

Condition	Severity	Traditional	Deep Learning (pre-2015)	Modern CNN	ArcFace
Frontal, Controlled	None	95%	97%	99%	99.80%
Pose ±45° *(Positional Changes [2])*	Moderate	70%	80%	92%	96%
Pose >75° *(Positional Changes [2])*	Severe	40%	55%	75%	85%
Partial Occlusion (30%) *(Occlusion Robustness [14])*	Moderate	65%	75%	90%	94%
Heavy Occlusion (50%) *(Occlusion Robustness [14])*	Severe	25%	35%	70%	80%
Low Light *(Environmental Conditions [2][50])*	Moderate	60%	70%	85%	90%
Low Resolution (32×32) *(Image Resolution [30])*	Severe	30%	40%	60%	72%
Combined Challenges *(Training + Variation [2][50][9])*	Extreme	20%	30%	50%	65%

IX. Current Challenges And Future Directions

Remaining Technical Challenges

Despite significant advances, several challenges persist in IoT-based face recognition for unconstrained environments:

Table.13: Current challenges and their impact on face recognition performance

Challenge	Description	Impact Level	Current Solutions	Limitations of Solutions	Future Research Directions	Timeline
Extreme Pose Variations	Profile views (>60°)	High	3D face reconstruction, multi-view training	Computational cost, limited datasets	GAN-based frontal view synthesis	2-3 years
Low-light Conditions	Poor illumination (<10 lux)	High	NIR cameras, image enhancement	Hardware cost, noise amplification	Thermal imaging fusion	1-2 years
Adversarial Attacks	Printed photos, masks, deepfakes	Very High	Liveness detection, 3D sensing	Sophisticated attacks evolving	Multi-modal biometrics	Ongoing
Privacy Regulations	GDPR, CCPA compliance	High	On-device processing, encryption	Performance trade-offs	Federated learning, homomorphic encryption	2-4 years
Computational Constraints	Limited edge device resources	Medium	Model compression, quantization	Accuracy degradation	Neural architecture search, efficient designs	1-3 years
Dataset Bias	Demographic imbalances	High	Balanced datasets, fairness-aware training	Limited diverse data	Synthetic data generation	2-3 years
Real-time Processing	Latency requirements (<100ms)	Medium	Hardware acceleration, optimization	Cost, power consumption	Neuromorphic computing	3-5 years
Scalability	Millions of identities	Medium	Distributed databases, indexing	Memory, search complexity	Approximate nearest neighbor search	1-2 years

Extreme Pose & Occlusion: Severe pose (>75°) and heavy occlusion (>50%) still reduce accuracy despite modern methods [14][50].
Cross-Domain Generalization: Models trained on one dataset often fail in new environments due to domain shift [51].
Adversarial Robustness: Systems remain vulnerable to adversarial patches, makeup attacks, and deepfake presentations [46].
Resource–Accuracy Trade-off: Lightweight edge models can lose accuracy, while high-accuracy models exceed device limits [9][33].
Privacy–Utility Balance: Strong privacy protections often reduce recognition accuracy, making balance challenging [10][42].

Scalability and System Integration
Large-Scale Deployment: Managing thousands of IoT devices requires strong orchestration, model updates, and consistency across hardware [33].
Continuous Learning: Systems must adapt to user appearance changes without forgetting previous knowledge [52].
Multi-Modal Integration: Combining face data with other biometrics or contextual cues improves recognition robustness [53].
Interoperability Standards: Common APIs, data formats, and benchmarks are needed to ensure system compatibility and evaluation [54].

Table.14: Scalability and System Integration Needs

Requirement	Current Status	Gap	Solution Approach	Priority
Large-Scale Deployment	Limited to 10-100s devices	Managing 1000s of devices	Robust orchestration, model versioning	High
Continuous Learning	Static models	Cannot handle long-term drift	Continual learning at edge	High
Multi-Modal Integration	Single modality (face only)	No fusion capability	Multi-modal architectures	Medium
Standardization	No common standards	Interoperability issues	API/format standardization	Medium
Model Updates	Manual deployment	Time-consuming rollouts	Automated OTA updates	High

Emerging Technologies and Approaches
Transformer Architectures: Vision Transformers (ViT) show promises for face recognition; efficient edge variants are an active research area [55].
Federated Learning: Enables collaborative training without sharing raw data; ongoing work focuses on communication efficiency and non-IID edge data [33][56].
Neural Architecture Search (NAS): Automatically discovers optimized models for latency, memory, and energy constraints on IoT devices [57].
Synthetic Data / Generative Models: GANs and diffusion models provide realistic training data without exposing real biometrics [1][58].
3D Face Recognition: Depth-based approaches improve robustness to pose and spoofing; efficient edge deployment is a key challenge [5].
Quantum Machine Learning: Quantum neural networks are being explored as future high-accuracy biometric recognition methods [59].

Ethical and Regulatory Considerations
Bias & Fairness: Systems can perform unevenly across age, gender, and ethnicity; fairness mechanisms are needed for equal error rates [60].
Regulatory Compliance: Laws such as GDPR and BIPA require secure biometric data handling, deletion options, and audit capabilities [10].
Transparency & Explainability: Deep models are often black boxes; interpretable systems can improve trust and error analysis [61].
Social Acceptance: Public trust varies by region and context; deployments must ensure transparency and offer opt-out options [62].

Table.15: Ethical and Regulatory Landscape

Concern	Current Status	Regulatory Pressure	Required Actions	Timeline
Demographic Bias	Exists (higher errors for minorities)	Increasing	Fairness audits, balanced datasets	Immediate
GDPR Compliance	Many systems non-compliant	Critical	Data deletion, consent, audit trails	Immediate
Surveillance Ethics	Controversial deployments	High	Transparency, oversight, limits	Ongoing
Accuracy Standards	No mandatory thresholds	Emerging	Performance certifications	1-2 years
Consent Frameworks	Weakly defined	Increasing	Clear consent mechanisms	1-2 years
Explainability	Limited transparency	Growing demand	Interpretable AI research	2-3 years

X. Conclusion

From 2019 to 2025 Year, IoT-based face recognition has progressed rapidly, supported by deep learning and edge computing that now allow small devices like the Raspberry Pi 3,4,5 to achieve about 95–97% accuracy. Modern systems most of the use pretrained CNN models such as VGG-16, ResNet-50, and MobileNetV2, along with reliable face detectors like RetinaFace and MTCNN and powerful loss functions such as ArcFace. Processing data directly on edge devices helps reduce delays, saves network bandwidth, and protects sensitive Face biometric information, with techniques like differential privacy and federated learning adding further security. Even with these improvements, the field still faces several challenges, including performance drops under occlusion or extreme angles(different poses), limited computational resources, adversarial attacks, domain shifts, demographic bias, and issues that emerge when scaling systems in real environments. Looking ahead, research is moving toward transformer-based models, better federated learning approaches, neural architecture search tailored for edge hardware, 3D sensing, and the use of privacy-preserving synthetic data. In this paper, we focused on understanding the key concepts, challenges, and requirements of unconstrained face recognition system. In the next phase of our work, we will perform IoT-based image acquisition to create a robust unconstrained face dataset and apply detailed preprocessing and hybrid preprocessing techniques to the captured images.

References

[1]. 50 Years Of Automated Face Recognition. Https://Arxiv.Org/Html/2505.24247v1/. Accessed 4 Dec. 2025.

[2]. Hussain, Tahir, Et Al. "Internet Of Things With Deep Learning-Based Face Recognition Approach For Authentication In Control Medical Systems." Computational And Mathematical Methods In Medicine, Vol. 2022, Feb. 2022, P. 5137513. Pubmed Central, Https://Doi.Org/10.1155/2022/5137513.

[3]. Singh, Raghubir, And Sukhpal Singh Gill. "Edge AI: A Survey." Internet Of Things And Cyber-Physical Systems, Vol. 3, Jan. 2023, Pp. 71–92. Sciencedirect, Https://Doi.Org/10.1016/J.Iotcps.2023.02.004.

[4]. "Face Recognition Vs. Face Verification For ID Verification." Regula, Https://Regulaforensics.Com/Blog/Face-Recognition-Vs-Face-Verification/. Accessed 4 Dec. 2025.

[5]. Shepley, Andrew Jason. "Face Recognition In Unconstrained Conditions: A Systematic Review." Arxiv:1908.04404, Arxiv, 12 July 2019. Arxiv.Org, Https://Doi.Org/10.48550/Arxiv.1908.04404.

[6]. Zhou, Liping, Et Al. "Study On Face Recognition Under Unconstrained Conditions Based On LBP And Deep Learning." Journal Of Computational Methods In Sciences And Engineering, Vol. 21, No. 2, May 2021, Pp. 497–508. DOI.Org (Crossref), Https://Doi.Org/10.3233/JCM-204595.

[7]. Asmara, Rosa Andrie, And Brian Et Al Sayudha . "Face Recognition Using Arcface And Facenet In Google Cloud Platform For Attendance System Mobile Application." 2022, ATASEC 2022, Https://Doi.Org/10.2991/978-94-6463-106-7_13.

[8]. Sumathi, K., Et Al. "Iot Based Novel Face Detection Scheme Using Machine Learning Scheme." 2022 International Conference On Advances In Computing, Communication And Applied Informatics (ACCAI), 2022, Pp. 1–5. IEEE Xplore, Https://Doi.Org/10.1109/ACCAI53970.2022.9752504.

[9]. Ahmed Ali Aboluhom, Abdulatif, And Ismet Kandilli. "Face Recognition Using Deep Learning On Raspberry Pi." The Computer Journal, Vol. 67, No. 10, Oct. 2024, Pp. 3020–30. DOI.Org (Crossref), Https://Doi.Org/10.1093/Comjnl/Bxae066.

[10]. Xie, Yun, Et Al. "Privacy Protection Framework For Face Recognition In Edge-Based Internet Of Things." Cluster Computing, Nov. 2022, Pp. 1–19. Pubmed Central, Https://Doi.Org/10.1007/S10586-022-03808-8.

[11]. Ibrahim, Safa Ismael, Et Al. "Unconstrained Face Identification Using Machine Learning Classification." [Baghdad, Iraq], 2024, P. 020056. DOI.Org (Crossref), Https://Doi.Org/10.1063/5.0236373.

[12]. Karanwal, Shekhar. "Robust Face Descriptor In Unconstrained Environments." Expert Systems With Applications, Vol. 247, Aug. 2024, P. 123302. DOI.Org (Crossref), Https://Doi.Org/10.1016/J.Eswa.2024.123302.

[13]. Varun. What Is Face Detection? Ultimate Guide 2025 + Model Comparison. 6 Sept. 2022, Https://Learnopencv.Com/What-Is-Face-Detection-The-Ultimate-Guide/.

[14]. Stefan, H¨Ormann. Robust Face Recognition Under Adverse Conditions. 2023, Https://Mediatum.Ub.Tum.De/Doc/1712921/I7o9c8cu0yf5usvq1kdlmhxd0.Hoermann.Dis.Pdf.

[15]. Chethana, H. T., Et Al. "Face Recognition In Unconstrained Images Using Deep Learning Model For Forensics." SECURITY AND PRIVACY, Vol. 8, No. 2, Mar. 2025, P. E70012. DOI.Org (Crossref), Https://Doi.Org/10.1002/Spy2.70012.

[16]. Nada, Hajime, Et Al. "Pushing The Limits Of Unconstrained Face Detection: A Challenge Dataset And Baseline Results." 2018 IEEE 9th International Conference On Biometrics Theory, Applications And Systems (BTAS) [Redondo Beach, CA, USA], 2018, Pp. 1–10. DOI.Org (Crossref), Https://Doi.Org/10.1109/BTAS.2018.8698561.

[17]. Gill, Baldeep Singh And Abhivardhan, Editors. Artificial Intelligence And Policy In India. First Edition., Indian Society Of Artificial Intelligence And Law, 2020. Open Worldcat.

[18]. Wan, Yan, Et Al. "Research On Unconstrained Face Recognition Based On Deep Learning." 2020 International Conference On Big Data & Artificial Intelligence & Software Engineering (ICBASE), 2020, Pp. 219–27. IEEE Xplore,

Https://Doi.Org/10.1109/ICBASE51474.2020.00054.
[19]. Ben Fredj, Hana, Et Al. "Face Recognition In Unconstrained Environment With CNN." The Visual Computer, Vol. 37, No. 2, Feb. 2021, Pp. 217–26. DOI.Org (Crossref), Https://Doi.Org/10.1007/S00371-020-01794-9.
[20]. "Facial Recognition - Innovatrics - How It Works." Innovatrics, Https://Www.Innovatrics.Com/Facial-Recognition-Technology/. Accessed 4 Dec. 2025.
[21]. "Demystifying The Face Recognition Process: Algorithms And Models." Text. Embien, Https://Www.Embien.Com/Blog/Demystifying-The-Face-Recognition-Process-Algorithms-And-Models. Accessed 4 Dec. 2025.
[22]. Wang, Wenjun, Et Al. "An Implementation Of Face Recognition System With Face Presentation Attack Detection On Raspberry Pi." 2021 IEEE International Conference On E-Business Engineering (ICEBE) [Guangzhou, China], 2021, Pp. 70–75. DOI.Org (Crossref), Https://Doi.Org/10.1109/ICEBE52470.2021.00031.
[23]. The Evolution Of Face Recognition With Neural Networks: From Deepface To Arcface And Beyond | Insightface Blog. Https://Www.Insightface.Ai/Blog/The-Evolution-Of-Face-Recognition-With-Neural-Networks-From-Deepface-To-Arcface-And-Beyond. Accessed 4 Dec. 2025.
[24]. Asmara, Rosa Andrie, Et Al. "Face Recognition Using Arcface And Facenet In Google Cloud Platform For Attendance System Mobile Application." 2022, Pp. 134–44. Www.Atlantis-Press.Com, Https://Doi.Org/10.2991/978-94-6463-106-7_13.
[25]. "Github - Shreeparab1890/Face-Detection-Using-MTCNN-And-Opencv: Face Detection Using MTCNN And Opencv." Github, Https://Github.Com/Shreeparab1890/Face-Detection-Using-MTCNN-And-Opencv. Accessed 4 Dec. 2025.
[26]. Room Security System Using Machine Learning With Face Recognition Verification | IIETA. Https://Doi.Org/10.18280/Ria.370510. Accessed 4 Dec. 2025.
[27]. Ananda, Gheri Febri, Et Al. "Comparative Analysis Of Multi-Face Detection Methods In Classroom Environments: Haar Cascade, MTCNN, Yoloface, And Retinaface." 2024 Seventh International Conference On Vocational Education And Electrical Engineering (ICVEE) [Malang, Indonesia], 2024, Pp. 268–73. DOI.Org (Crossref), Https://Doi.Org/10.1109/ICVEE63912.2024.10823781.
[28]. Checking Your Browser - Recaptcha. Https://Www.Kaggle.Com/Code/Payamamanat/Facerecognition-Sface-Yunet-Mtcnn-Retinaface. Accessed 4 Dec. 2025.
[29]. Muslim, Nasif, And Salekul Islam. "Face Recognition In The Edge Cloud." Proceedings Of The International Conference On Imaging, Signal Processing And Communication [Penang Malaysia], 2017, Pp. 5–9. DOI.Org (Crossref), Https://Doi.Org/10.1145/3132300.3132310.
[30]. Ren, Zhengwei, Et Al. "Littlefacenet: A Small-Sized Face Recognition Method Based On Retinaface And Adaface." Journal Of Imaging, Vol. 11, No. 1, Jan. 2025, P. 24. Pubmed Central, Https://Doi.Org/10.3390/Jimaging11010024.
[31]. B, Venkata Kranthi, And Surekha Borra. "Real-Time Face Detection And Recognition On Raspberry Pi Using LBP And Deep Learning." Proceedings Of The International Conference On Data Science, Machine Learning And Artificial Intelligence [Windhoek Namibia], 2021, Pp. 124–29. DOI.Org (Crossref), Https://Doi.Org/10.1145/3484824.3484903.
[32]. Infisim. "Revolutionising Security: Iot-Empowered Facial Recognition." Infisim, 28 July 2023, Https://Infisim.Com/Blog/Iot-Empowered-Facial-Recognition.
[33]. Xiang, Zhengzhe. Enabling Sustainable And Unmanned Facial Detection And Recognition Services With Adaptive Edge Resource. 2025, Https://Dsg.Tuwien.Ac.At/Team/Sd/Papers/Journal_Paper_2025_S_Dustdar_Enabling.Pdf.
[34]. "Face Recognition With Raspberry Pi And Opencv - Tutorial Australia." Core Electronics, Https://Core-Electronics.Com.Au/Guides/Raspberry-Pi/Face-Identify-Raspberry-Pi/. Accessed 4 Dec. 2025.
[35]. Dürr, Oliver, Et Al. Deep Learning On A Raspberry Pi For Real Time Face Recognition. 2015. Diglib.Eg.Org, Https://Doi.Org/10.2312/Egp.20151036.
[36]. Aboluhom, A.A.A. Real-Time Facial Recognition Via Multitask Learning On Raspberry Pi. 2025, Https://Www.Nature.Com/Articles/S41598-025-97490-6.
[37]. Rana, Md. Shohel, Et Al. "Real Time Deep Learning Based Face Recognition System Using Raspberry PI." 2023 26th International Conference On Computer And Information Technology (ICCIT), 2023, Pp. 1–5. IEEE Xplore, Https://Doi.Org/10.1109/ICCIT60459.2023.10508526.
[38]. Zhou, Xihao, And Sye Loong Keoh. "Deployment Of Facial Recognition Models At The Edge: A Feasibility Study." 2020 21st Asia-Pacific Network Operations And Management Symposium (APNOMS), 2020, Pp. 214–19. IEEE Xplore, Https://Doi.Org/10.23919/APNOMS50412.2020.9236972.
[39]. Warman, G.P. "Face Recognition For Smart Attendance System Using Deep Learning." Communications In Mathematical Biology And Neuroscience, 2023. DOI.Org (Crossref), Https://Doi.Org/10.28919/Cmbn/7872.
[40]. J V, Srivaishnavi, Et Al. "An Investigational Study On Face Recognitionbased Attendance Tracking System For Educational Institutions." 2024 International Conference On Inventive Computation Technologies (ICICT) [Lalitpur, Nepal], 2024, Pp. 900–06. DOI.Org (Crossref), Https://Doi.Org/10.1109/ICICT60155.2024.10544419.
[41]. Rahman, Shafin, Et Al. "Performance Of MPEG-7 Edge Histogram Descriptor In Face Recognition Using Principal Component Analysis." 2010 13th International Conference On Computer And Information Technology (ICCIT) [Dhaka, Bangladesh], 2010, Pp. 476–81. DOI.Org (Crossref), Https://Doi.Org/10.1109/ICCITECHN.2010.5723904.
[42]. Laishram, Lamyanba, Et Al. "Toward A Privacy-Preserving Face Recognition System: A Survey Of Leakages And Solutions." ACM Computing Surveys, Vol. 57, No. 6, June 2025, Pp. 1–38. DOI.Org (Crossref), Https://Doi.Org/10.1145/3673224.
[43]. CSDL | IEEE Computer Society. Https://Www.Computer.Org/Csdl/Proceedings-Article/Etseciot/2020/09097758/1k0pclqbqr2. Accessed 4 Dec. 2025.
[44]. Xue, Wanli, Et Al. "An Efficient Privacy-Preserving Iot System For Face Recognition." 2020 Workshop On Emerging Technologies For Security In Iot (Etseciot), 2020, Pp. 7–11. IEEE Xplore, Https://Doi.Org/10.1109/Etseciot50046.2020.00006.
[45]. Wang, Haoming, Et Al. "Privacy-Enhanced Facial Recognition For Iot Based On Homomorphic Encryption." Internet Of Things, Vol. 34, Nov. 2025, P. 101757. Sciencedirect, Https://Doi.Org/10.1016/J.Iot.2025.101757.
[46]. Biometric Identification. Https://Shuftipro.Com/Knowledgebase/Biometric-Identification/. Accessed 4 Dec. 2025.
[47]. "Amazon Rekognition Identity Verification." Amazon Web Services, Inc., Https://Aws.Amazon.Com/Rekognition/Identity-Verification/. Accessed 4 Dec. 2025.
[48]. Serengil, Sefik, And Alper Ozpinar. A Benchmark Of Facial Recognition Pipelines And Co-Usability Performances Of Modules. 8 Feb. 2020, Python. Version 1.0.0, 2024. Github, Https://Dergipark.Org.Tr/En/Pub/Gazibtd/Issue/84331/1399077.
[49]. Aboluhom, Abdulatif Ahmed Ali, And Ismet Kandilli. "Real-Time Facial Recognition Via Multitask Learning On Raspberry Pi." Scientific Reports, Vol. 15, No. 1, Aug. 2025, P. 28467. Www.Nature.Com, Https://Doi.Org/10.1038/S41598-025-97490-6.
[50]. Ben Fredj, Hana, Et Al. "Face Recognition In Unconstrained Environment With CNN." The Visual Computer, Vol. 37, No. 2, Feb. 2021, Pp. 217–26. DOI.Org (Crossref), Https://Doi.Org/10.1007/S00371-020-01794-9.

[51]. Guo, Yuxiang, Et Al. "Distillation-Guided Representation Learning For Unconstrained Gait Recognition." 2024 IEEE International Joint Conference On Biometrics (IJCB) [Buffalo, NY, USA], 2024, Pp. 1–11. DOI.Org (Crossref), Https://Doi.Org/10.1109/IJCB62174.2024.10744527.
[52]. Lombardi, Marco. "Biometric Verification And Identification Explained." Biometrics Institute, 13 May 2024, Https://Www.Biometricsinstitute.Org/Biometric-Verification-And-Identification-Explained/.
[53]. Passwordless Authentication Platform For Frontline Workers | OLOID. Https://Www.Oloid.Com. Accessed 4 Dec. 2025.
[54]. Abed, Sawsan S., Et Al. "Optical Information Verification And Authentication: Exploring Sparsity Constraints And Optical Encryption For Enhanced Security." [Erbil, Iraq], 2025, P. 030013. DOI.Org (Crossref), Https://Doi.Org/10.1063/5.0258878.
[55]. Correia, Diogo, And Sandra Jardim. "A Deep Learning Approach For Face Detection." Procedia Computer Science, International Conference On Industry Sciences And Computer Science Innovation (Iscsi'24), Vol. 263, Jan. 2025, Pp. 34–41. Sciencedirect, Https://Doi.Org/10.1016/J.Procs.2025.07.005.
[56]. "2025 Edge AI Technology Report." Ceva, Https://Www.Ceva-Ip.Com/2025-Edge-Ai-Technology-Report/. Accessed 4 Dec. 2025.
[57]. Skirelis, Julius, And Dalius Navakauskas. "Performance Analysis Of Edge Computing In Iot." Elektronika Ir Elektrotechnika, Vol. 26, No. 1, Feb. 2020, Pp. 72–77. DOI.Org (Crossref), Https://Doi.Org/10.5755/J01.Eie.26.1.23235.
[58]. Checking Your Browser - Recaptcha. Https://Www.Kaggle.Com/Code/Samiraalipour/Facerecognition-Facenet-Arcface-Vggface-Dlib. Accessed 4 Dec. 2025.
[59]. Jadhav, Abhishek. The Difference Between Biometric Verification, Identification, And Authentication | Biometric Update. 16 June 2024, Https://Www.Biometricupdate.Com/202406/The-Difference-Between-Biometric-Verification-Identification-And-Authentication.
[60]. Telo. "Face Verification Vs. Face Recognition." Alice Biometrics, 23 Feb. 2023, Https://Alicebiometrics.Com/En/Face-Verification-Vs-Face-Recognition/.
[61]. Kontaev, Ilya. Face Recognition With Arcface Machine Learning Model | Learnopencv. 1 Feb. 2021, Https://Learnopencv.Com/Face-Recognition-With-Arcface/.
[62]. Edge Computing In Iot Devices: Everything You Need To Know | Synaptics. Https://Www.Synaptics.Com/Company/Blog/Iot-Edge-Computing-Ml. Accessed 4 Dec. 2025.