Computer Vision - 2025

Lecture #07. Face Recognition

Lectures by Alexei Kornaev [1,2,3,4]
Practical sessions by Kirill Yakovlev [2]

[1]AI Institute, Innopolis University (IU), Innopolis
[2]Robotics & CV Master's Program, IU, Innopolis
[3]RC for AI, National RC for Oncology, Moscow
[4]Dept. of M^2R, OSU, Orel

March 3, 2025

Agenda

1. Outcomes
2. Challenges in FR
3. Traditional FR Methods
4. Deep Learning for FR
5. Conclusion & Discussion

Section 1. Outcomes

Outcomes

This week on Face Recognition aims to provide students with a comprehensive understanding of face detection and recognition techniques. By the end of this lecture, students will be able to:

1. Estimate the challenges in the domain, including pose variation, illumination changes, occlusion, ethics, and adversarial attacks.
2. Understand and compare different face recognition architectures.
3. Analyze loss functions like contrastive loss, triplet loss, and ArcFace loss for face recognition models.
4. Implement face recognition systems using deep learning frameworks and estimate the results.

Key Takeaway: Face recognition is a crucial technology in security, authentication, and social applications, but it also raises ethical concerns that must be addressed.

Section 2. Challenges in FR

Challenges in Face Recognition

Overview of Challenges

Face recognition systems face several challenges that can significantly impact their performance. These include pose variation, illumination changes, occlusion, ethical concerns, and adversarial attacks.

- **Pose Variation:** Faces can appear in different orientations, making it difficult to match them.
- **Illumination Changes:** Variations in lighting conditions can alter the appearance of faces.
- **Occlusion:** Parts of the face may be obscured by objects or other faces.
- **Ethics:** Privacy concerns and biases in face recognition systems.
- **Adversarial Attacks:** Deliberate attempts to fool face recognition systems.

Pose Variation

Pose Variation

Pose variation refers to the different orientations of a face relative to the camera. This can include frontal, profile, and oblique views.

- **Impact:** Reduces the accuracy of face recognition systems.
- **Solutions:** Use of 3D models, multi-view training data, and pose-invariant features.

Illumination Changes

Illumination Changes

Illumination changes refer to variations in lighting conditions that can alter the appearance of a face.

- **Impact:** Can cause significant changes in the appearance of facial features.
- **Solutions:** Normalization techniques, use of infrared imaging, and deep learning models trained under various lighting conditions.

Occlusion

Occlusion occurs when parts of a face are obscured by objects (e.g., masks, sunglasses), other people, or environmental factors. It degrades recognition accuracy by hiding critical facial features.

Understanding Occlusion

Figure: Examples of occluded face images from the MAFA dataset [Zeng et al., 2021].

- **Impact:**
  - Loss of key features (e.g., eyes, mouth).
  - State-of-the-art models like DeepFace or ArcFace suffer >30% accuracy drop under heavy occlusion.
- **Common Occlusions:** *Masks* (e.g., medical masks). *Accessories* (e.g., sunglasses, scarves). *Environmental* (e.g., hands, hair).
- **Challenges:**
  - Partial face data limits recognition methods.
  - Dynamic occlusions require real-time adaptation.

Solutions for Occlusion Handling

Technical Approaches

Addressing occlusion requires robust feature extraction and reconstruction techniques.

- **Partial Face Recognition:**
  - Train models on cropped facial regions (e.g., eyes-only, mouth-only). Use *metric learning* to match partial and holistic embeddings.
- **Attention Mechanisms:**
  - Focus on visible regions, e.g. *Transformer Networks*) may prioritize non-occluded areas with attention [Liu et al., 2023].
- **Generative Models:**
  - Reconstruct occluded regions using GANs, Diffusion models.

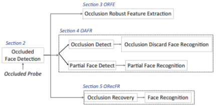


Figure: FR under occlusion [Zeng et al., 2021].

Ethical Challenges in Face Recognition

Ethics: Privacy, Bias, and Misuse

Face recognition systems raise critical ethical concerns, including privacy violations, algorithmic bias, and misuse in surveillance. These challenges undermine trust and fairness.

- **Privacy Violations:**
  - *Issue:* Unauthorized data collection and mass surveillance.
  - *Approach:* Implement strict data governance, anonymization, and user consent mechanisms.
- **Algorithmic Bias:**
  - *Issue:* Higher error rates for minorities, women, and darker-skinned individuals due to imbalanced training data.
  - *Example:* Buolamwini & Gebru (2018) showed 34% error for dark-skinned women vs. 0.8% for light-skinned men.
  - *Approach:* Curate diverse datasets, audit models for fairness, and adopt bias-mitigation techniques (e.g., reweighting losses).

Ethical Challenges: Solutions and Regulations

Regulatory Frameworks

Addressing ethical issues requires technical, legal, and societal interventions.

- **Technical Solutions:**
  - *Fairness-aware training:* Use fairness constraints during model optimization.
  - *Explainability:* Tools like LIME or SHAP to interpret model decisions.
- **Legal Solutions:**
  - *Bans on mass surveillance:* EU's GDPR, proposed U.S. FR Act.
  - *Transparency laws:* Require disclosure of face recognition use cases.
- **Societal Solutions:**
  - Public awareness campaigns and ethical AI certification programs.

Adversarial Attacks: Threat Models

Adversarial Attacks in Face Recognition

Adversarial attacks manipulate inputs to deceive face recognition systems. Common types include:

- **Evasion Attacks:**
  - *Goal:* Fool the system during inference (e.g., adversarial glasses).
- **Poisoning Attacks:**
  - *Goal:* Corrupt training data (e.g. injecting malicious samples).
- **Model Inversion Attacks:**
  - *Goal:* Reconstruct training data from model outputs (privacy breach).

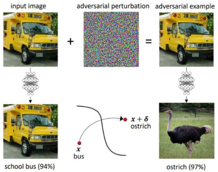


Figure: Adversarial noise attack.

Defending Against Adversarial Attacks

Robustness Strategies

Mitigating adversarial attacks requires proactive defenses and robust model design.

- **Adversarial Training:**
  - Train models on adversarial examples to improve robustness.
  - *Limitation:* Computationally expensive; does not generalize to all attacks.
- **Input Preprocessing:**
  - Apply noise reduction, quantization, or JPEG compression to inputs.
- **Detection Mechanisms:**
  - Deploy detectors to flag adversarial inputs (e.g., using inconsistency in feature space).
- **Certified Defenses:**
  - Use mathematically proven robust models (e.g., randomized smoothing).

Section 3. Traditional FR Methods

Traditional Face Recognition Methods

Early approaches relied on dimensionality reduction and handcrafted features.

Linear Methods

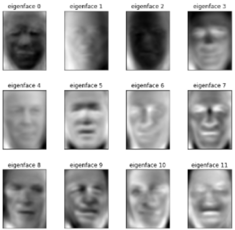


Figure: Eigenfaces [Turk and Pentland, 1991].

- **Eigenfaces [Turk and Pentland, 1991]:**
  - Uses PCA to project faces into a low-dimensional subspace.
  - Maximizes variance to capture dominant facial features.
- **LBPH (Local Binary Patterns Histogram):**
  - Encodes texture patterns using local binary operators.
  - Robust to monotonic illumination changes but struggles with pose/occlusion.

Section 4. Deep Learning for FR

Deep Learning Architectures for Face Recognition

A.Kornaev,
K.Yakovlev

Outcomes
Challenges in FR
Traditional FR Methods
Deep Learning for FR
Conclusion & Discussion

Deep learning models learn discriminative embeddings by optimizing metric-based losses.

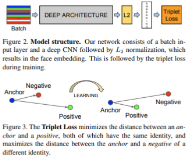


Figure: FaceNet embeddings [Schroff et al., 2015; Deng et al., 2019].

Key Architectures

- **Siamese Networks [Koch et al., 2015]:**
  - Twin nets with shared weights for similarity learning.
  - *Contrastive loss* minimizes distances
- **FaceNet [Schroff et al., 2015]:**
  - Maps faces to a compact 128D Euclidean space.
  - Uses *triplet loss*: $\mathcal{L} = \max(||f(a) - f(p)||^2 - ||f(a) - f(n)||^2 + \alpha, 0)$, where a=anchor, p=positive, n=negative.
- **ArcFace [Deng et al., 2019]:**
  - Adds an *additive angular margin m* to the loss.
  - Enforces compactness and separation.

Loss Functions in Face Recognition

Metric Learning Objective

A loss enforces that embeddings of the same identity are closer than those of different identities.

- **Contrastive Loss :**

$$\mathcal{L} = \frac{1}{2N} \sum_{i=1}^{N} y_i \cdot d_i^2 + (1 - y_i) \cdot \max(\alpha - d_i, 0)^2$$

  where $y_i = 1$ for same-class pairs, d_i=embedding distance, α=margin.
- **Triplet Loss [Schroff et al., 2015]:**

$$\mathcal{L} = \sum_{i=1}^{N} \max\left(||f(a_i) - f(p_i)||^2 - ||f(a_i) - f(n_i)||^2 + \alpha, 0\right)$$

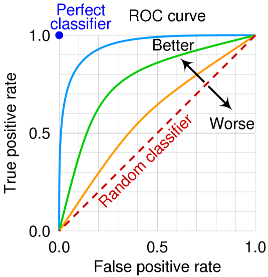
- **ArcFace Loss [Deng et al., 2019]:**

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

  where s=scaling factor, m=angular margin, θ=angle between weight and feature.

Evaluation Metrics

Metrics vary based on the task: verification (1:1) or identification (1:N).



ROC curve [Huang et al., 2008].

Performance Assessment

- **Verification:**
  - *False Acceptance Rate (FAR):* Incorrectly accepting impostors.
  - *False Rejection Rate (FRR):* Incorrectly rejecting genuine users.
  - *Equal Error Rate (EER):* FAR = FRR.
- **Identification:**
  - Rank-1 accuracy: Top-1 match rate.
  - Cumulative Match Curve (CMC).
- **Benchmarks:**
  - LFW (Labeled Faces in the Wild): 99.8% accuracy for ArcFace

Section 5. Conclusion & Discussion

Conclusion & Discussion

Strengths and Limitations

- **Traditional Methods (PCA/LBP):** Interpretable but fail on complex variations
- **Deep Embeddings (FaceNet):** Robust features but need massive labeled data
- **ArcFace:** Superior separation but sensitive to alignment

Future Directions

- Vision Transformers for face recognition
- Federated learning for privacy-preserving biometrics
- Synthetic data generation with diffusion models

Open Challenges

- Ethical deployment: Bias mitigation & fairness
- Robustness to adversarial attacks
- Cross-ethnicity generalization

Key Takeaways & Practical Insights

Student Summary

- **Traditional Methods:**
  - Simple but limited (PCA/LBP struggle with pose/lighting)
  - Foundation for understanding feature engineering
- **Deep Learning:**
  - Embeddings + metric loss = Robustness
  - Automatically learns hierarchical features

The Loss Function Revolution

- Contrastive Loss: Pair-based similarity learning
- Triplet Loss: Relative distance optimization
- ArcFace: Angular margin for better separation

Bibliography

Jiankang Deng, Jia Guo, Niannan Xue, and Stefanos Zafeiriou. Arcface: Additive angular margin loss for deep face recognition. 2019.

Gary B Huang, Marwan Mattar, Tamara Berg, and Eric Learned-Miller. Labeled faces in the wild: A database for studying face recognition in unconstrained environments. 2008.

Gregory Koch, Richard Zemel, and Ruslan Salakhutdinov. Siamese neural networks for one-shot image recognition. 2015.

Chang Liu, Kaoru Hirota, and Yaping Dai. Patch attention convolutional vision transformer for facial expression recognition with occlusion. **Information Sciences**, 619:781–794, 2023.

Florian Schroff, Dmitry Kalenichenko, and James Philbin. Facenet: A unified embedding for face recognition and clustering. 2015.

Matthew Turk and Alex Pentland. Eigenfaces for recognition. **Journal of cognitive neuroscience**, 3(1):71–86, 1991.

Dan Zeng, Raymond Veldhuis, and Luuk Spreeuwers. A survey of face recognition techniques under occlusion. **IET biometrics**, 10 (6):581–606, 2021.