Biometrics: Face Recognition

Reyansh Gupta

Topics Covered

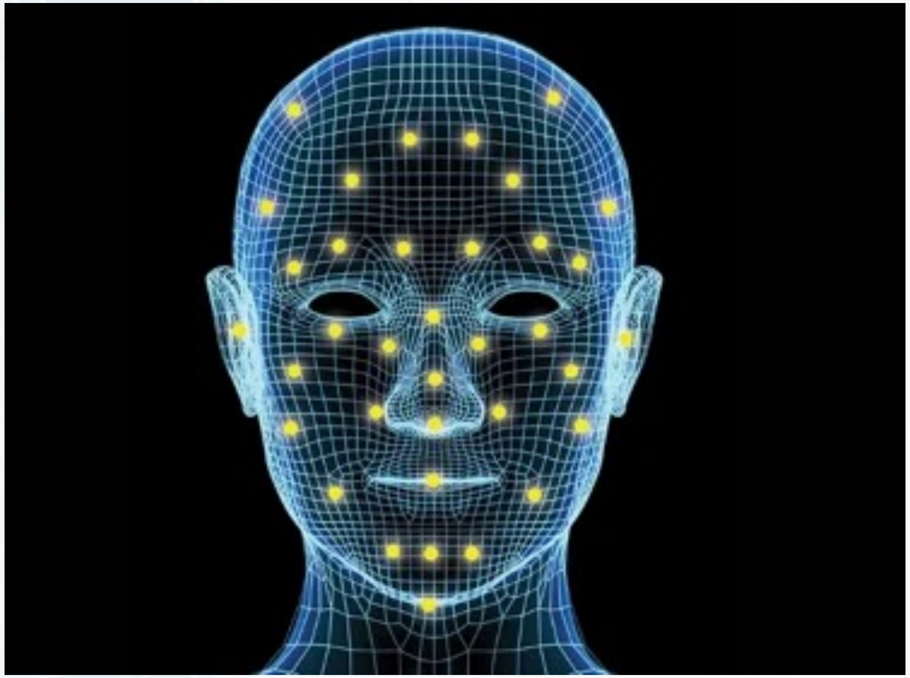
Facial Recognition

- Biometric technology that identifies or verifies a person's identity using facial features
- Use distance between eyes, shape of jawline, contour of cheekbones - can check over 80 nodal points
- High accuracy, no contact, user friendly
- New systems use deep learning to recognise faces
- 3D Face modelling is done to overcome challenges in 2D face recognition.

Traits Used in Facial Recognition

- **Facial Landmarks:** unique points on the face (eyes, nose)
- **Texture and Color:** Skin patterns, moles, complexion
- **2D Geometric Features:** Distance between facial features
- **3D Shape Information:** Depth information for increased accuracy
- **Deep Learning Representations:** Neural networks used for feature extraction
- **Fusion of modalities:** Combines 2D and 3D data for better recognition
- **Temporal Information:** Considers facial expressionns and dynamic patterns

Facial Recognition Traits

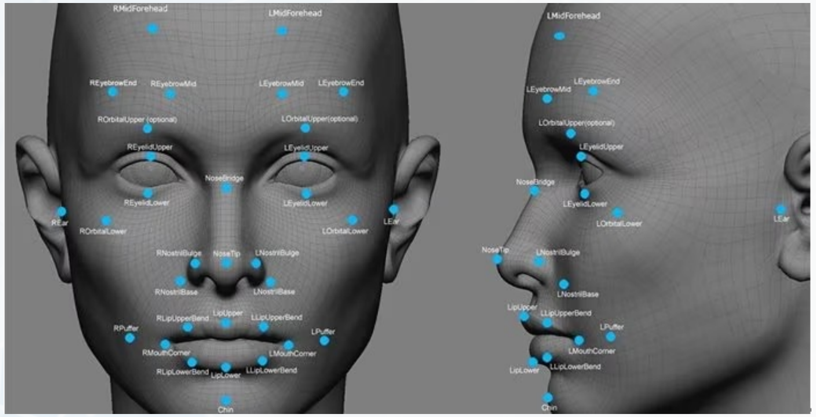


How 3D Sensing Enables Mobile Face Recognition : IEEE Spectrum

- **Time-of-flight sensing**
  - Measures distance by timing the flight of infrared light from the emitter to the user's face and back to a photosensor.
- **Stereo imaging**
  - As in human vision, two spaced photosensors create perspective and depth. Infrared light projectors enable an Active Stereo Vision system to work with no ambient light.
- **Structured light**
  - Algorithms generate depth maps by analyzing the distortions in random patterns of dots projected on the user's face.

Case Study: Apple’s Face ID

Decoding Apple iPhone X's FaceID:
IndiaTimes



IPhone X vs Samsung Face
Recognition

- The flood illuminator gets active - which lights up our face for other sensors to scan.
- The Infrared camera flashes IR lights our face detecting its placement, depth and position. Since IR cameras also work in the dark, it isn’t affected by low-light conditions.
- The Dot projector flashes 30,000 invisible dots on our face which scans facial features and creates a unique 3D map of the face.
- After capturing the 3D data, it compares it to the one stored on the iPhone during the initial setup, and if it matches, we get access to our iPhone. This all takes place in a matter of seconds.

Facial Recognition Traits

Pros & Cons

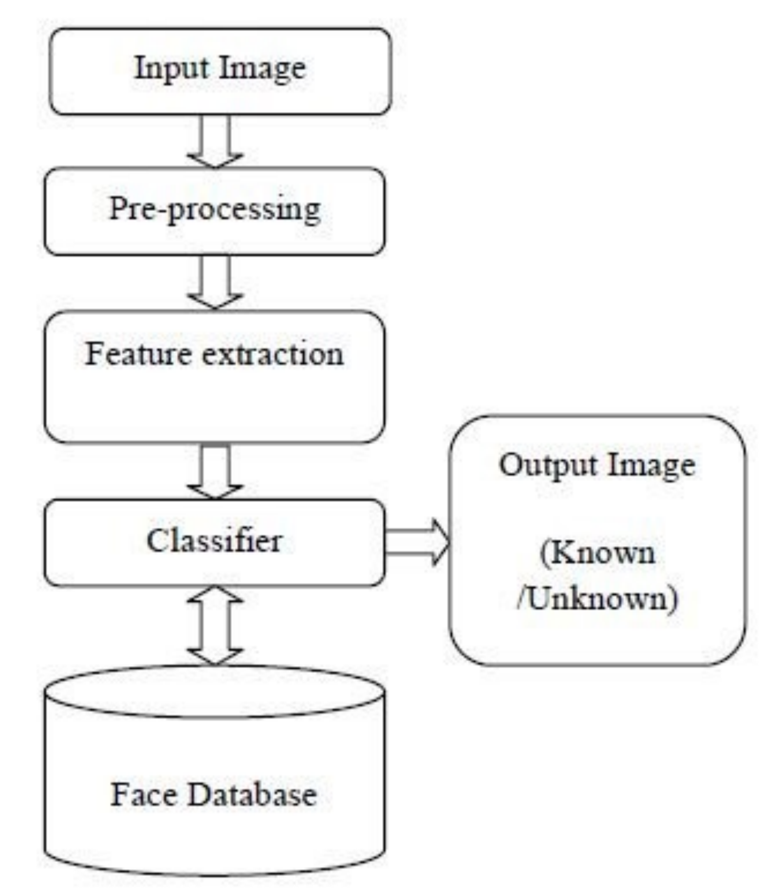
Pros

- **Accuracy:** High accuracy in identifying individuals.
- **Security:** Enhanced security for access control and authentication.
- **Efficiency:** Speeds up processes like smartphone unlocking.
- **Versatility:** Used in diverse applications, from security to healthcare.
- **Continuous Improvement:** Advances in deep learning boost performance.

Cons

- **Privacy Concerns:** Potential misuse of facial data raises privacy issues.
- **Bias and Fairness:** Systems may exhibit biases based on race, gender, etc.
- **Ethical Dilemmas:** Raises ethical questions about surveillance and consent.
- **Lighting and Pose:** Sensitive to lighting conditions and pose variations.
- **Spoofing Risks:** Vulnerable to attacks using photos or videos.

System Representaion



ResearchGate

- Image Capture
- Feature Extraction
- Feature Comparision
- Decision Algorithm
- Result

Operating Modes

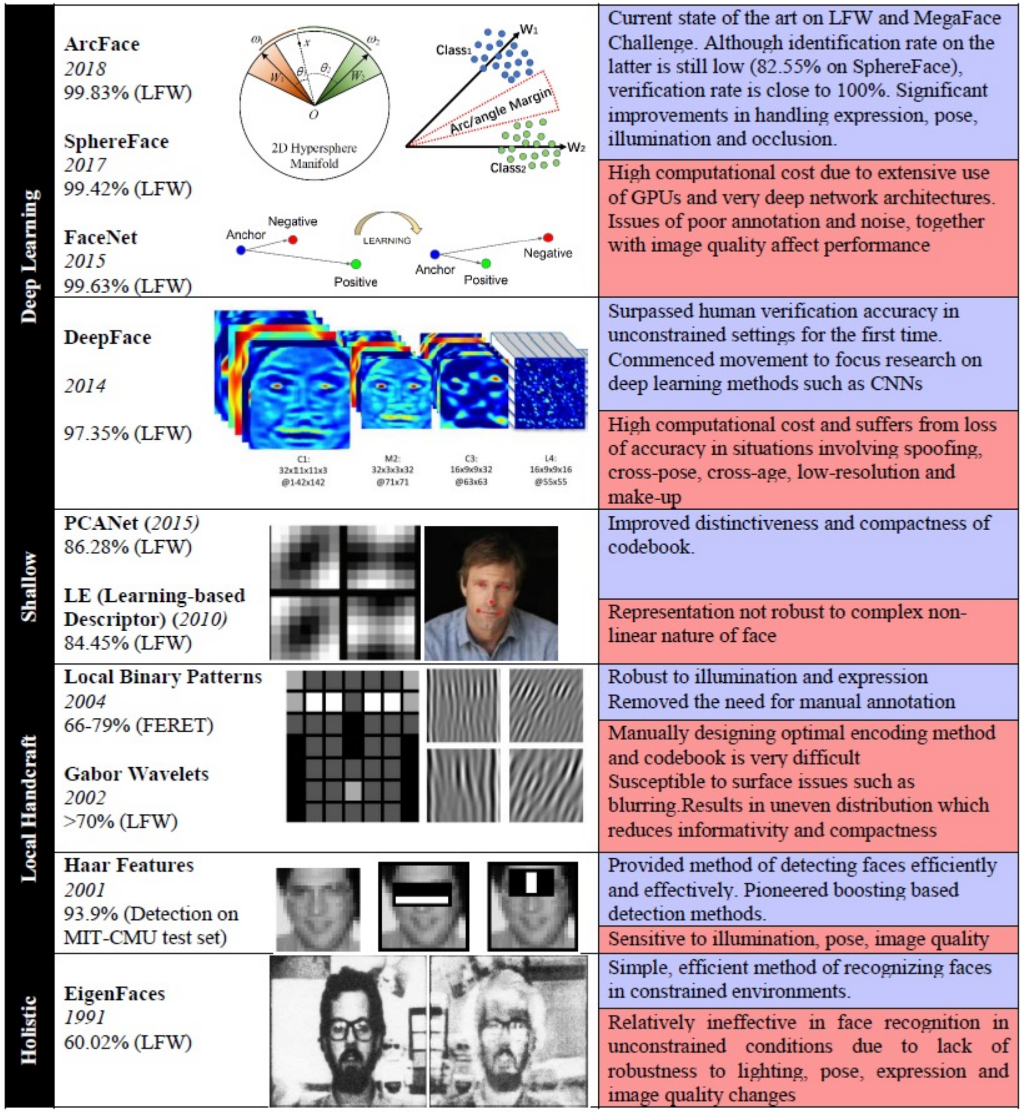
Two types of operating modes:

Verification Mode:

- 1:1 Matching
- System verifies if the presented face matches a specific individual's face.
- Commonly used for authentication and access control, such as unlocking smartphones or granting access to secure areas.
- Example: Confirming if a person's face matches the stored facial template on their ID card.

Identification Mode:

- 1:N Matching
- System compares the presented face against a large database of faces to identify the individual.
- Widely used in scenarios where the identity of an individual is unknown
- Common applications include law enforcement, border security, and airport screening.
- Example: Searching for a suspect's identity by comparing their face against a criminal database.



Category	Method	Strengths	Limitations
Deep Learning	**ArcFace** *2018* 99.83% (LFW); **SphereFace** *2017* 99.42% (LFW); **FaceNet** *2015* 99.63% (LFW)	Current state of the art on LFW and MegaFace Challenge. Although identification rate on the latter is still low (82.55% on SphereFace), verification rate is close to 100%. Significant improvements in handling expression, pose, illumination and occlusion.	High computational cost due to extensive use of GPUs and very deep network architectures. Issues of poor annotation and noise, together with image quality affect performance
Deep Learning	**DeepFace** *2014* 97.35% (LFW)	Surpassed human verification accuracy in unconstrained settings for the first time. Commenced movement to focus research on deep learning methods such as CNNs	High computational cost and suffers from loss of accuracy in situations involving spoofing, cross-pose, cross-age, low-resolution and make-up
Shallow	**PCANet** *(2015)* 86.28% (LFW); **LE (Learning-based Descriptor)** *(2010)* 84.45% (LFW)	Improved distinctiveness and compactness of codebook.	Representation not robust to complex non-linear nature of face
Local Handcraft	**Local Binary Patterns** *2004* 66-79% (FERET); **Gabor Wavelets** *2002* >70% (LFW)	Robust to illumination and expression Removed the need for manual annotation	Manually designing optimal encoding method and codebook is very difficult Susceptible to surface issues such as blurring.Results in uneven distribution which reduces informativity and compactness
Local Handcraft	**Haar Features** *2001* 93.9% (Detection on MIT-CMU test set)	Provided method of detecting faces efficiently and effectively. Pioneered boosting based detection methods.	Sensitive to illumination, pose, image quality
Holistic	**EigenFaces** *1991* 60.02% (LFW)	Simple, efficient method of recognizing faces in constrained environments.	Relatively ineffective in face recognition in unconstrained conditions due to lack of robustness to lighting, pose, expression and image quality changes

Figure 1: *Timeline of developments in facial feature representations and face verification accuracy*

Deep Learning for Face Recognition: A critical Analysis

Timeline of face recognition and its accuracy

Facial Recognition Applications

- Smart Systems:
  - Facial Recognition for access control & surveillance systems
  - Grant / Deny access to individuals
- Smartphones
- Payment Authentication
- Smart Policing
  - Used by law enforcement to track suspects
  - Aids in solving crimes and maintaining public safety

Case Study

The Sunday Guardian

New Delhi Airport

DigiYatra: Revolutionising Air Travel

- DigiYatra is an initiative in that leverages facial recognition for a seamless airport experience.
- Passengers can complete various airport processes, including check-in, security checks, and boarding, using facial verification.
- Paperless and Hassle-Free Travel

Performance Measures

01 Recognition Accuracy:

- System’s ability to correctly identify individuals
- True Positive Rate (TPR) or Sensitivity/True Negative Rate (TNR) or Specificity, Precision and Recall
- High accuracy: crucial for security

02 Processing Time:

- Processing time indicates how quickly the system can verify or identify individuals.
- It's essential for real-time applications
- Faster processing enhances user experience.
- Template Update Time

03 System Robustness:

- Robustness assesses the system's ability to perform well under various challenges: pose variations, facial expressions, and occlusions.
- A robust system maintains accuracy in diverse scenarios.
- Equal Error Rate (EER), Failure to Acquire Rate (FTAR), Failure to Enroll Rate (FTER)

04

Importance of Dataset Diversity:

- Diverse training datasets are critical to ensure the system generalizes well to different demographics, ethnicities, and backgrounds.
- Reduces bias
- Receiver Operating Characteristic (ROC) Curve, Area Under the Curve (AUC)

Algorithm Efficiency:

- Algorithm efficiency impacts both processing time and system resource requirements.
- Efficient algorithms optimize computational resources
- Crossover Error Rate (CER)

Additional Considerations:

Ethical Issues:

- **Consent:**
  - Obtaining informed consent from individuals is crucial before capturing and using their facial data.
- Potential for Bias:
  - Facial recognition systems can exhibit bias, particularly in gender, race, and age.
- Privacy Implications:
  - Facial recognition raises concerns about the collection and storage of biometric data.

Technological Advancements:

- Machine Learning Algorithms:
  - Advances in machine learning and deep learning algorithms continue to enhance recognition accuracy.
- Real-Time Processing:
  - Real-time processing capabilities enable applications like instant access control and live surveillance.
- Anti-Spoofing Techniques:
  - To counter spoofing attempts (e.g., using photos or videos), anti-spoofing techniques are crucial.
  - Multimodal authentication and liveness detection help verify the authenticity of faces.

Conclusion

- Facial recognition technology is widely used in security, access control, and convenience-driven applications.
- It relies on deep learning algorithms and biometric traits for high accuracy.
- Challenges include privacy concerns, potential bias, and the need for robust anti-spoofing measures.

Future Directions:

- **Enhancing Accuracy:** Ongoing research aims to improve accuracy, particularly in challenging scenarios like low-light conditions and pose variations.
- **Privacy-Preserving Techniques:** Developing techniques that protect individual privacy while still enabling facial recognition is crucial.
- **Ethical Regulations:** Governments and organizations must establish clear ethical regulations for facial recognition use.
- **Bias Mitigation:** Addressing bias in facial recognition systems is a critical focus area.

References

- Deep Learning for Face Recognition: a critical analysis
- A Survey On Deep Learning Approaches for Real-Time License Plate, Vehicle Type and Face Recognition
- Press Information Bureau, Government of India - Digi Yatra: A Paperless and Seamless Travel Experience
- Enhancing security and privacy in biometrics-based authentication systems
- How 3D Sensing Enables Mobile Face Recognition : IEEE Spectrum
- IPhone X vs Samsung Face Recognition
- Apple: About Face ID advanced technology
- Decoding Apple iPhone X's FaceID: IndiaTimes

Thank You