“Face Recognition Technology Today”

before the
NTIA Multi-Stakeholder Process To Develop Consumer Data Privacy Code of Conduct Concerning Facial Recognition Technology

February 25, 2014
Facial Recognition Applications in Use Today

Examples

• **Commercial:**
  - Employers for Time and Attendance Verification
  - Physical Access Control Security (Buildings)
  - Logical Access Control (Computer/Device Access)
  - Document Authentication

• **Government:**
  - Drivers Licenses to reduce duplication and fraud
  - Passport Verification
  - Jail Management Systems and Booking
  - Law Enforcement Investigations

• **Social/consumer:**
  - Photo Organizing Google’s Picassa, Facebook
  - Smartphone and App Access Control
Defining Face Recognition

Computer Facial Recognition is the determination of an anonymous or unknown identity of a human being based on the facial characteristics and features derived from camera or digital photo.

Methods: 1:1 Verify and 1:Many Search

Other Applications often called Facial Recognition but are not:

- **Face Detection** - finding the FACES, not identifying who in the photo
- **Gender Determination**
- **Age Range Determination**
Face Recognition is based on Face Biometric Templates

<table>
<thead>
<tr>
<th>Face Biometric Template is...</th>
<th>Versus an Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Not the actual facial image</td>
<td>• Social Security No., Drivers License No., Passport No.</td>
</tr>
<tr>
<td>• A vector of numbers which represent the facial image’s characteristics including measurements, color, lighting, 2D/3D</td>
<td>• Binary match or no match</td>
</tr>
<tr>
<td>• Created by a Face Biometric Algorithm</td>
<td>• Biometric Template (face, fingerprint, or iris) + Name and Meta Data together is an Identifier</td>
</tr>
<tr>
<td>• Not standard format and varies between different algorithms. Usually proprietary.</td>
<td></td>
</tr>
<tr>
<td>• Different for each photo even of the Same Person</td>
<td></td>
</tr>
<tr>
<td>• Not a match between two templates, only a degree of statistical closeness</td>
<td></td>
</tr>
</tbody>
</table>
Why wasn’t Dzhokhar Tsarnaev identified by the Massachusetts Department of Motor Vehicles system from the video surveillance images?
Today’s FR technology will reliably find this photo in a mugshot database of controlled facial images.
Confounding Variables in Uncontrolled Facial Photos

Problematic variables:
1. Resolution (not enough pixels)
2. Facial Pose – angulated
3. Illumination
4. Occluded facial areas

What happens:
- Facial Feature Points (eyes, etc.) not found or distorted
- Algorithm Measurements in Error
- Not Enough Data to Process
Defining a Facial Recognition MATCH

Degree of Similarity

A statistical score between two face biometric templates

Based on a facial characteristics algorithm determines degrees of SIMILARITY or a Score

If the Score meets a certain threshold, then it is considered a Match

Thresholds are determined by the operating parameters required

Operating Parameters are defined by an acceptable error rate for the applications use
Defining Error Rates

*False Accept:* System claims a pair of pictures are a match, when they are actually pictures of different individuals.

*False Accept Rate (FAR):* Frequency that the system makes False Accepts

Example: FAR of 0.1% system will make 1 false accept for every 1000 imposter attempts

*False Reject:* System claims a pair of pictures are a mismatch, when they are actually pictures of the same individual

*False Reject Rate (FRR):* Frequency that the system makes False Rejects

*ID Rate = 100% minus FRR*

E.g.: FRR of 2% or Identification rate of 98% system will reject 2 matches for every 100 authorized attempts

*As FAR is lowered, expect ID Rates to lower*
Error Rates in Practice

Operation implications
  • Control ID Rate by selecting the FAR operating point
  • Desire FAR to be as low as possible..... Minimize imposters
  • If ID Rate is too low, then forcing the subject to try again, and again

No standards exist for “acceptable” error rates, or a rating system, meaning “success” is deemed different within every vendor product, and in every application purpose.
Useable Error Rates Vary by App

<table>
<thead>
<tr>
<th>App Examples</th>
<th>ID RATE</th>
<th>FAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control Normal</td>
<td>90%</td>
<td>0.10%</td>
</tr>
<tr>
<td>Access Control High Security</td>
<td>80%</td>
<td>0.01%</td>
</tr>
<tr>
<td>Time and Attendance</td>
<td>85%</td>
<td>0.10%</td>
</tr>
<tr>
<td>Drivers License/Passport Deduplication</td>
<td>97%</td>
<td>1.00%</td>
</tr>
<tr>
<td>Mobile Phone Authentication</td>
<td>75%</td>
<td>0.20%</td>
</tr>
<tr>
<td>Facebook Private Photo Search</td>
<td>75%</td>
<td>1.00%</td>
</tr>
</tbody>
</table>
Even mugshots will reduce id rates if not “controlled”

Mugshots are subject to control standards, the “Uncontrolled Face Use Standards ISO/IEC 19794-5 “for Enrollments.

Variables like lighting, glasses, background, slight pose, face proportion can cause errors.
Uncontrolled Facial Imagery = High Error Rates

NIST Multiple-Biometric Evaluation (MBE)

2010

Dependence of accuracy on face yaw angle

False Accept Rate Set 0.1%

FNMR (at FMR=0.001)

0% 20% 40% 60% 80% 100%

ID RATE

Yaw Angle (Degrees)
Can a controlled photo find a match in LinkedIn?
LinkedIn Facial Search: Possible but dependent on the input photo and the database enrollment

• LinkedIn are Faces in the Wild
  • Assuming you can scoop all the faces for enrollment into a DB
  • Very low chances in matching

• Conjecture: If LinkedIn forced an IEC/ISO Mugshot standard then you’d have a searchable database
Will new facial technologies solve these problems?

Pose Correction with 3D Model Estimation
Summary

• **Fact:** As of today, facial recognition technology *cannot reliably match* face templates to identities based on photo harvesting of *uncontrolled* images from social networks, let alone in a video surveillance environment, without forensic support.

• **Fact:** *Controlled images* are key to *reliable matching*, and thus the success of current facial recognition technologies.