

Face Recognition: Beyond Performance Statistics

James Alexander
University of Pennsylvania

Talk Overview

- Claim: Serious holes exist in our understanding of face recognition technology
 - Security consequences
 - Privacy consequences
- How might we plug these holes?

The Nature of FR Testing

- Facial Recognition Vendor Test (FVRT)
 - Testing face matching accuracy for a given false accept rate
 - Vast majority of test data are high-quality, frontal facial images taken under controlled conditions
 - See www.fvrt.org for details

Why current testing is not enough

- Systems are being fielded **now**, but very little work exists toward understanding how and why these can systems fail
 - Foolhardy to employ any security tool if we don't understand its limits
 - We don't know how to fight back if this tool is used against us

Why this is a security problem

- You don't know how to deploy your system in a safe way
- The bad guys may be able to find loopholes in your system that you don't know are there
- Biometric technology development lacks the adversarial relationship of the cryptographer and cryptanalyst

How to break some FR systems









Privacy Issues

United Kingdom: King of Video Surveillance

- UK has an estimated 4 million CCTV cameras, 500k in London alone (about 1 camera for every 14 residents)
 - Face recognition software already in use in some areas
 - London Underground stations have 6000 cameras now, with 3000 more planned, plus cameras will be added to trains

U. S. camera networks growing

- Chicago plans to pool video from existing 2000 cameras, plans to add more
- Baltimore plans to install a new camera network that will be monitored live 24/7

Private Camera Networks

- Number of private CCTV cameras in use is largely unknown
 - Selfridges, a London department store, says they use over 4000 cameras
 - Large chains like Wal-Mart and Zellers could easily pool their video

The end of anonymous purchasing

- Once FR technology matures, it is almost inevitable it will become too inexpensive to *not* use
 - It may start coming bundled with cameras
- Using cash and avoiding discount card would no longer be sufficient for anonymous shopping

Private Information Leakage

Familial

|
|

Commercial

Medical

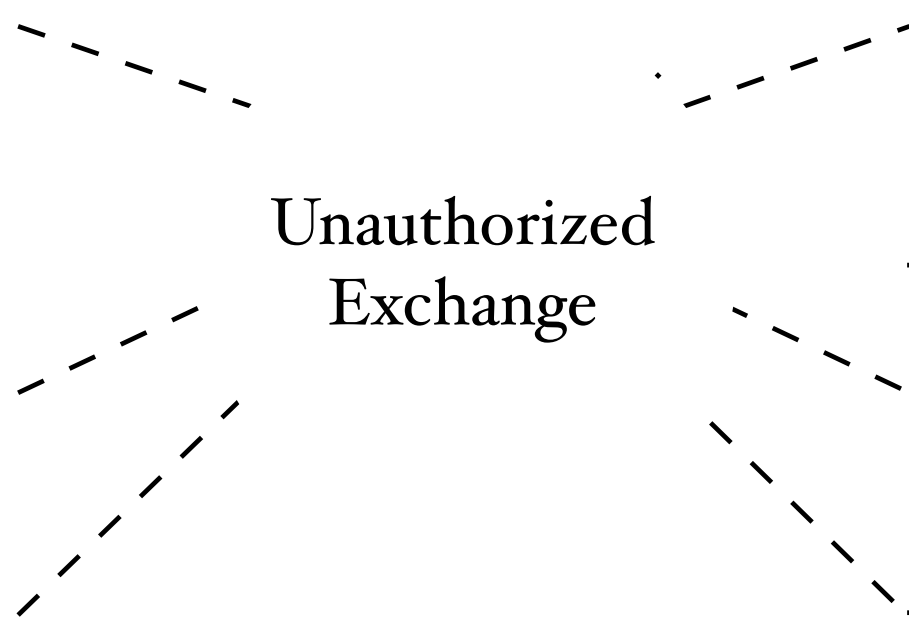
Unauthorized
Exchange

Occupational

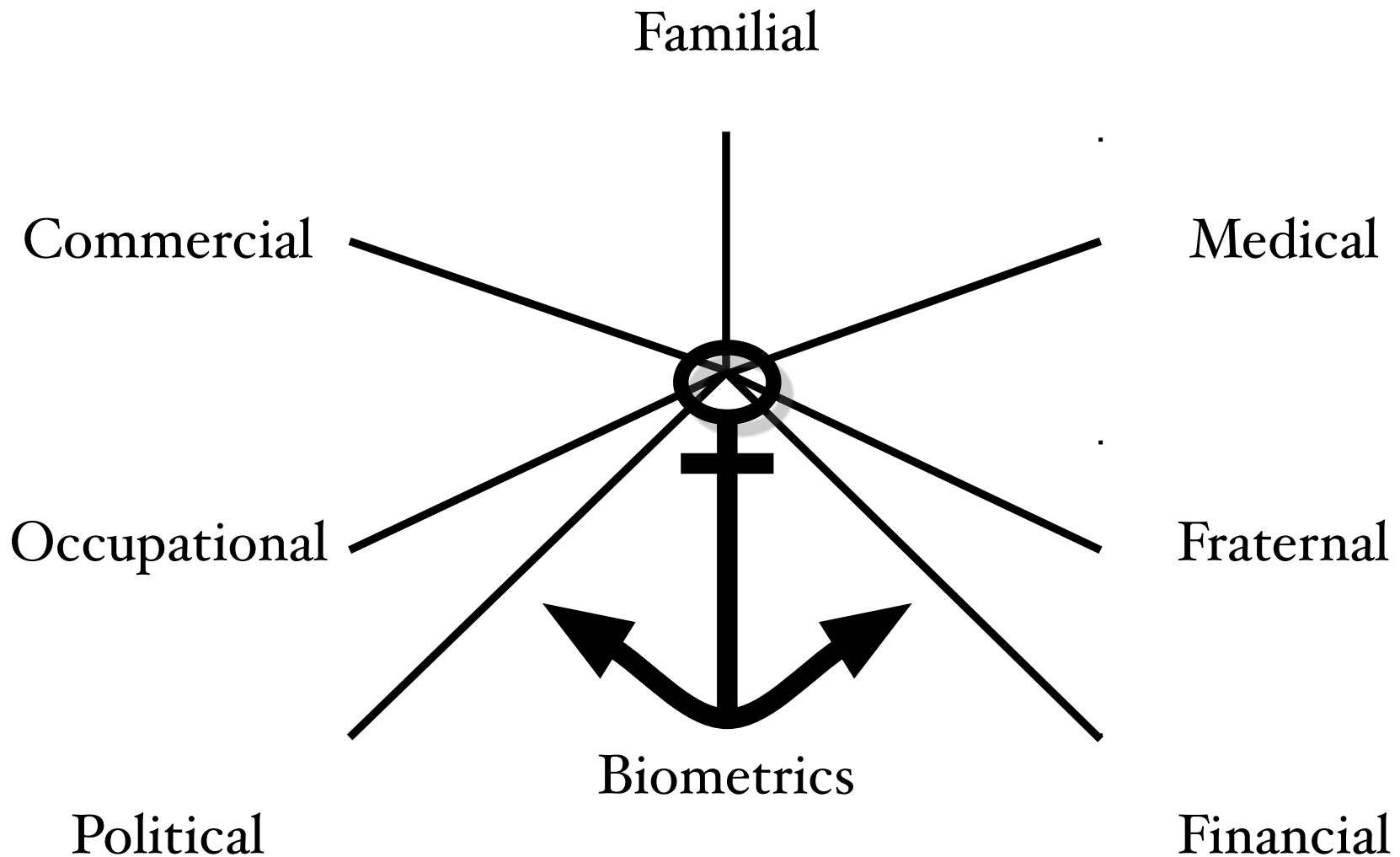
Fraternal

Political

Financial



The Biometric Anchor



Summary

- There are legitimate reasons for understanding how to break facial recognition systems
 - We need to know what the flaws so they can be properly protected against in security applications
 - We need to know how to counteract inappropriate, overreaching uses of the technology

What to do?

- Major roadblock: we don't have good data on the statistical variation of the human face
 - Without that basic research, we don't know which facial features contain the most identifying information
 - We have to just guess what attacks might work best!

Eigenface “features”



Or we could ...

- Roll our sleeves up and do that basic research
 - My lab is working on acquiring a new set of highly controlled facial images, to be hand annotated for facial feature size, shape, position, texture, etc.
 - Disguises will be designed for the most informative features of each individual face

Geometrical Analysis Mock-up



Thank you