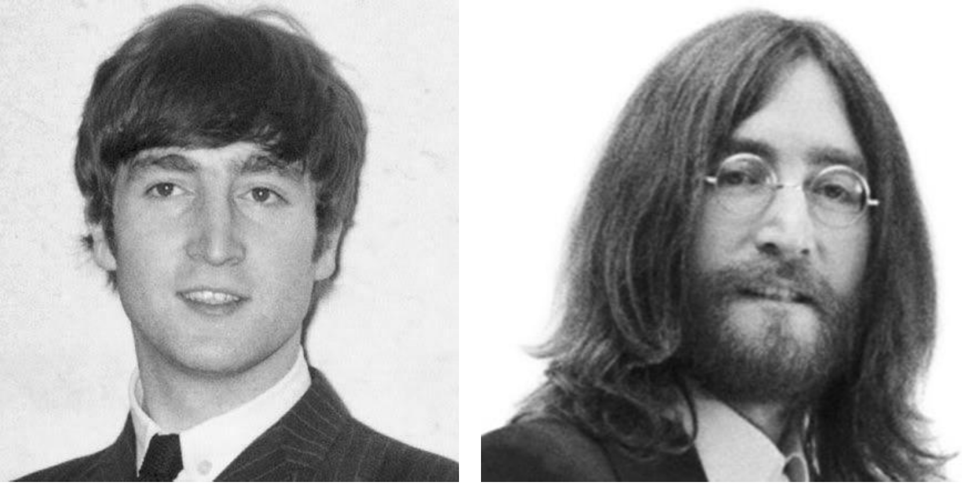
Face Recognition In ID Proofing: Pros and Cons

Patrick Grother
National Institute of Standards and Technology
U. S. Department of Commerce

ENISA-ETSI ID Proofing Conference
May 3, 2022

Appearance change is bad?



Match!

Beatle John Lennon between the release of the Red Album and the Blue Album, ~5 years.

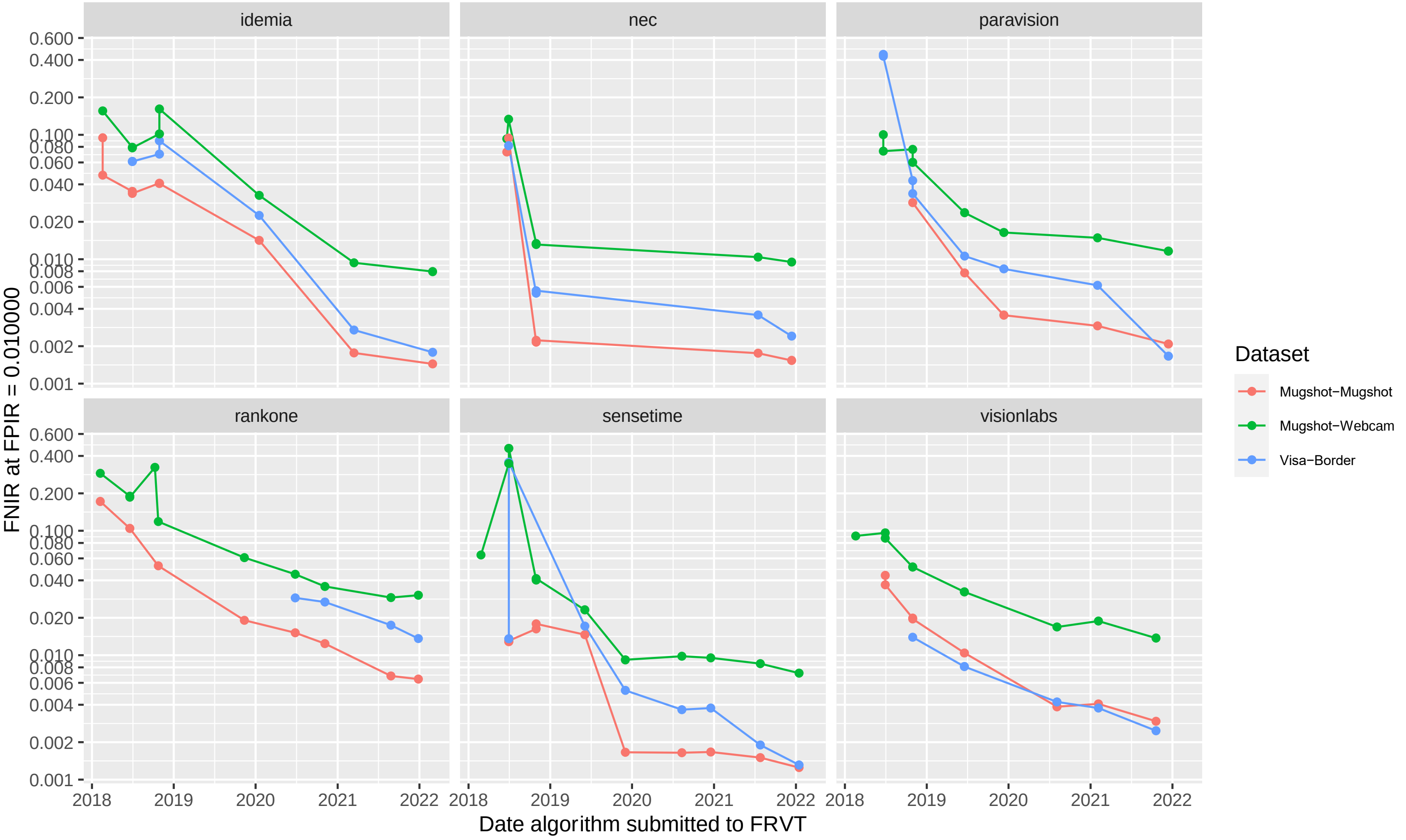
Developer	Algorithm	Score	FMR	Outcome
Idemia	008	7438.78	< 5.049e-07	Correct match
Paravision	010	0.38308	< 5.049e-07	Correct match

Accuracy Gains 2018-2022

- 1:N Search
- N = 1.6 million
- 1 photo per person

- Three cooperative datasets
- Worst photos are apprehensions

- Accuracy gains from ~10% to ~0.1%
- AI Revolution
- Implications



Face Recognition

Pros +

- Photography is social acceptable (from DL and passport)
- Face is present on authoritative ID credentials
  - Often via trusted capture and issuance
- The biometric “sensor” is now very common
  - Phone cameras
  - Fingerprint and iris require specialist hardware
- We have standardized image appearance (ISO)
- Face recognition accuracy now sufficient
  - For “at home” use, with weak lighting controls
  - For 1:N duplicate ID detection

Cons -

- FR algorithms vary in the capability
  - Procurement risk
  - Not commoditized
- Twins give false matches
  - 3% of live births in USA 2015 are a twin, triplet
- FR thresholds are too low
  - Much higher false match rates in certain races, age groups, and women
- Face is not a secret and easily stolen (then replayed, or injected) by an attacker
- We don’t have standard image diagnostic tools
- Inability to cryptographically authenticate the sensor
- Morphing is difficult to detect

ID Proofing: Countermeasures and Testing

Possible countermeasures

- » Trusted devices, trusted capture
- » Random challenge-response
  - Video
  - Facial actions
    - Expression
    - Eyes closed
    - Head orientation
  - Multimodality
    - Speech, speaker ID, secrets
    - Accelerometer
  - Human-interpretable challenges – machine un-interpretable

Testing

- » Tests of ID-Proofing systems
  - Must have human-in-the-loop
    - Bona fide
    - Attacks
- » Component testing is valuable but not sufficient
  - Face Recognition
  - PAD (analog attacks)
  - Test expression classifiers, pose estimators, etc
- » Systems and algorithms, AI-based or not, can vary across demographics

THANKS | MERCI

PATRICK.GROTHER@NIST.GOV

FRVT@NIST.GOV