Updates on Face Morphing: Risks, Evaluation, and Potential Mitigation

Mei Ngan
Scientist
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce

ICAO Montreal
November 14th, 2024

Face Morphing: Single Image of Two People

Face morphing generates an image that visually resembles both contributing subjects

Image Source: NIST

The problem: face recognition matches *both* persons

Subject A

Morph (A+B)

Face Recognition

SAME PEOPLE

Subject B

Morph (A+B)

Face Recognition

SAME PEOPLE

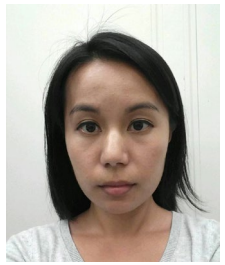
Multiple people can authenticate against a morph

All modern face recognition algorithms tested by NIST and operational matchers tested by parts of the U.S. Government are vulnerable to morphs

Image Source: NIST

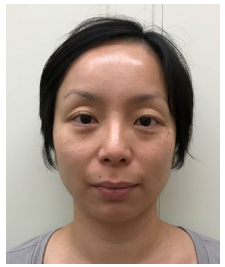
Threat: one document, multiple users

PASSPORT APPLICATION



Accomplice
(passport owner)

+



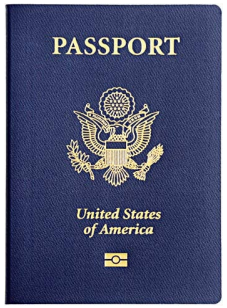
Attacker
(other identity)

Morph = A + B

Printed on
2in x 2in
photo paper and
mailed to passport
office

Passport office scans printed photo, conducts human examination, …

Ultimately, passport gets issued with morphed photo on it



Current U.S. passport application susceptible to manipulation of user-submitted photos.

Many other countries also accept user-submitted photos for identity credential applications.

Risk #1: Organizations that accept user-submitted photos for enrollment are at risk of morphing attack.

Risk #2: Organizations that may have to process ID documents from other countries that are vulnerable to morphs may also be at risk.

Image Source: NIST

NIST FATE MORPH Evaluation [Ongoing]

Automated Face Morph Detection Evaluation

- Independent, **sequestered** evaluation of morph detection capabilities across diverse datasets
- “Black-box” testing
- Ongoing testing + public reporting (report + interactive webpage)

Use Cases

- Single-image morph detection
- Two-image differential morph detection
- 1:1 morph acceptance (FR resistance against morphing)
- Demorphing

Recent participants

- **Academic:** Norwegian University of Science and Technology (NO), Fraunhofer Institute for Telecommunications Heinrich Hertz Institute (DE), Universidade de Coimbra (PT), West Virginia University (US), University of Bologna (IT), Hochschule Darmstadt
- **Commercial:** Idemia (FR), Neurotechnology (LT), Vision-box (PT), Secunet (DE), Kempelen Institute of Intelligent Technologies (SK)

FATE MORPH Report published as NIST Interagency Report 8292
Ongoing morph detection submissions accepted! Google: FATE MORPH

FATE MORPH Track: Morph Detection

Single-image (S-MAD)

Morph detection with single image in isolation

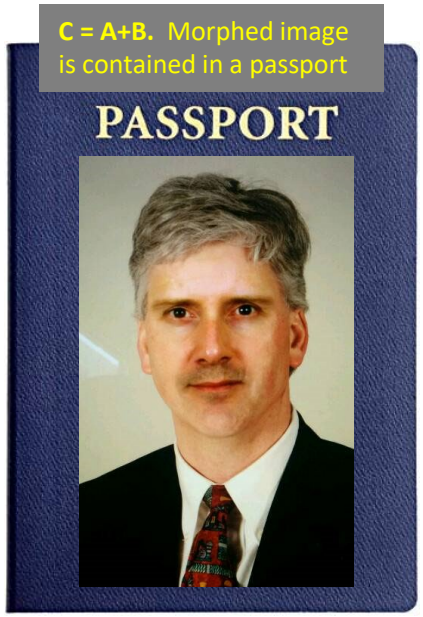
(e.g., document issuance)

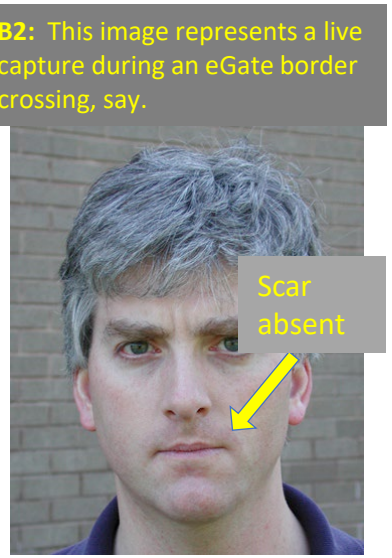
DOCUMENT ISSUANCE: Suspect image in isolation

Differential (D-MAD)

Morph detection with additional live capture image

(e.g., border crossing)





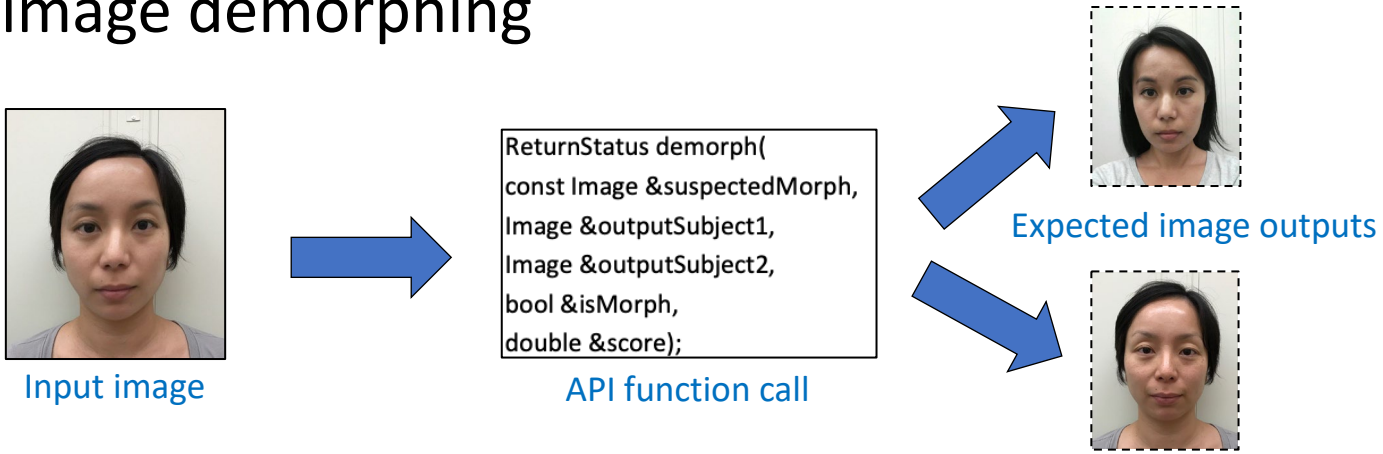
BORDER CROSSING: Suspect image + live image

Image Source: NIST + USG employee with permission

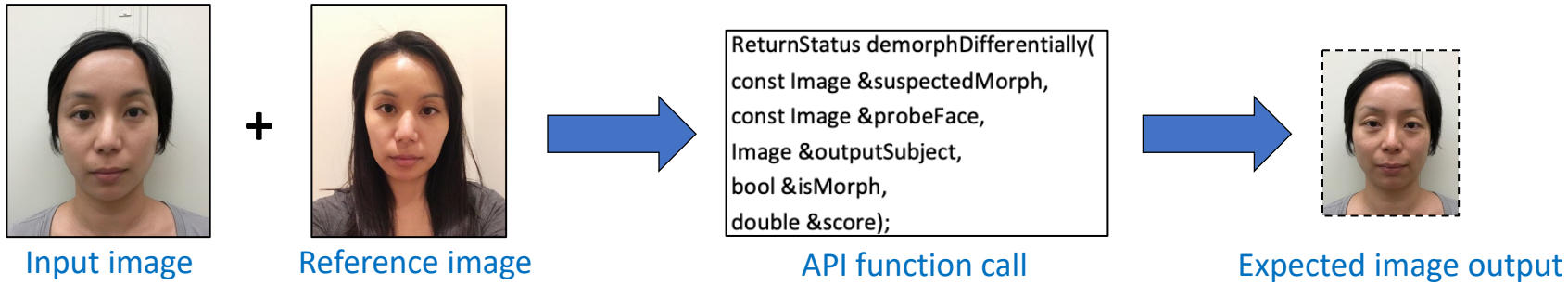
New FATE MORPH Track: Demorphing

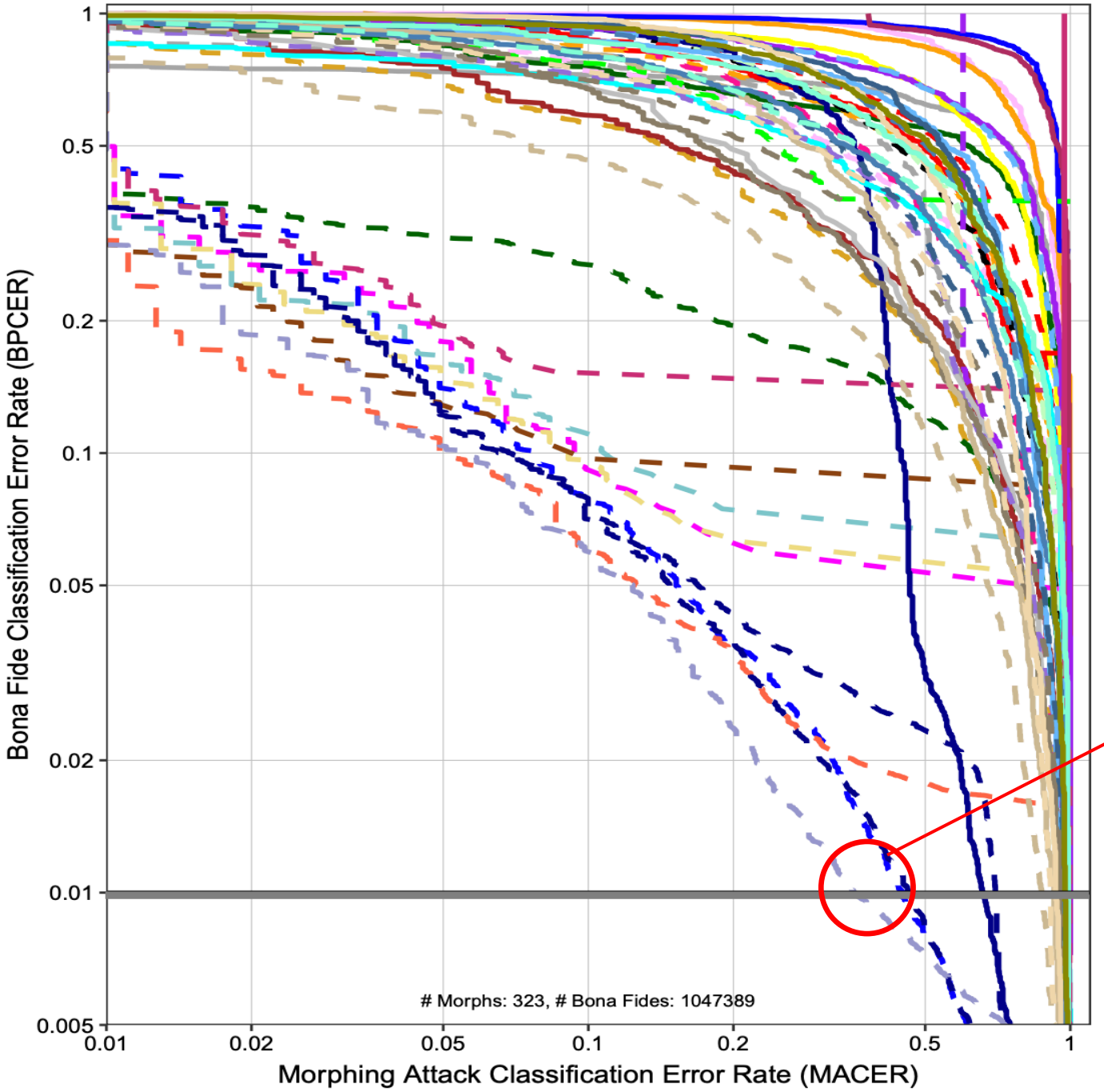
Demorphing is the process of recovering the original faces/identities used to generate a morph

- Single-image demorphing



- Differential demorphing





Differential morph detection capability is close to valuable: Run silent pilots

False Accusation Rate, BPCER = 0.01

Proportion of morphs **not** detected, MACER = 0.36

Potential Detection Strategy: Secondary Immigration

Operational Use of Differential Morph Detection in Border Control (D-MAD)

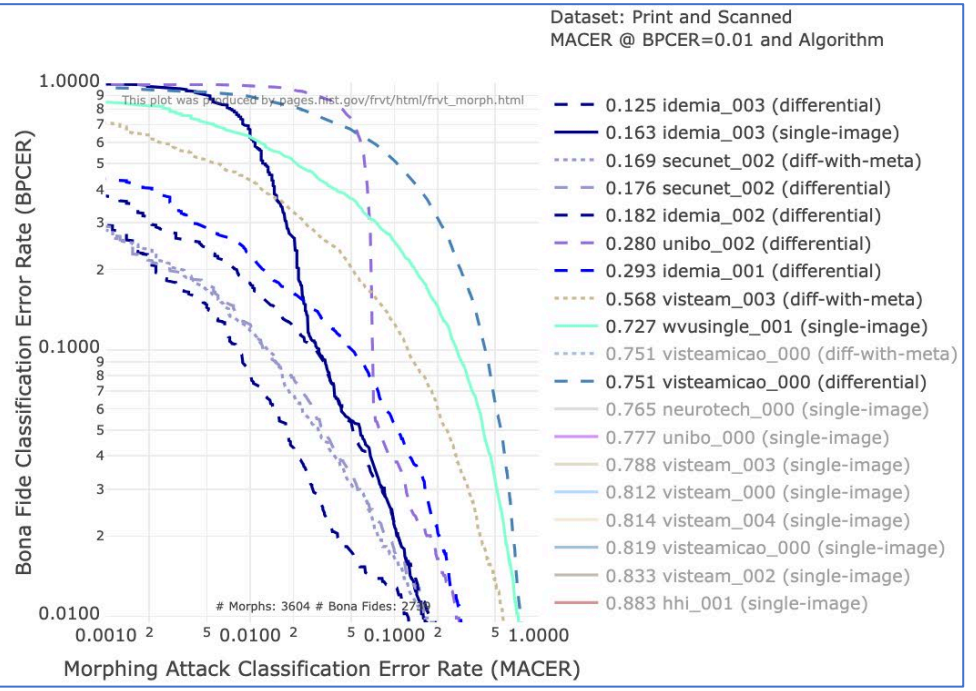
This operates in the following setting

- Suspected morph from passport
  AND
- Live border crossing photo ⟶ not a morph

Document scope

- Algorithm selection
- Algorithm configuration – low BPCER
- Human-led investigative process after a candidate morph detected

Print and Scanned



Possible application of differential morph detection

- In primary immigration eGate, run differential morph detector configured at a ***low*** false detection rate
- When a potential morph is detected, send traveler to secondary
- In secondary review
  - Inspect document, question traveler
  - Retrieve and visually compare
    - Photo(s) of document owner from other sources if available (e.g., ID card, driver's license)
    - Previous passport photos of document owner if available
  - Collect a pristine ICAO compliant portrait of traveler, then
    - Run differential morph detection of portrait against DG2 (to rule out quality-related issues)
    - Run a 1:1 matcher with portrait and 1) previous passport photos and/or 2) photos from other sources
  - Confirm traveler identity with different biometric modality (e.g., DG3, DG4) if available

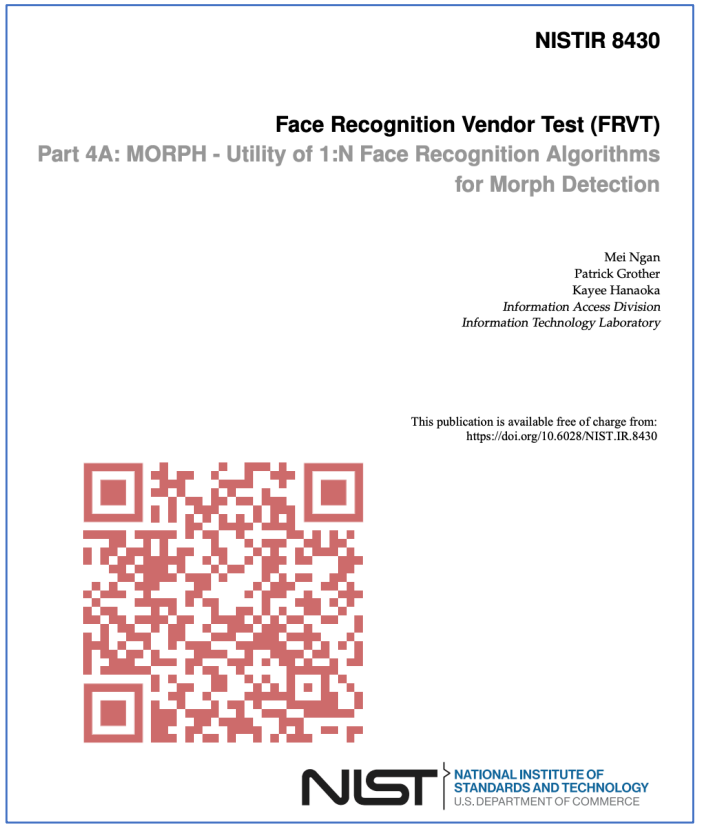
Potential Detection Strategy: 1:N Duplicate Detection

When a face is submitted for, say, passport application, execute a search of the databases of prior applicants.

Expected result: Strong hit, if previously encountered, OR

No hit if not.

But for morphed image: Possible weaker hit.


NISTIR 8430

Face Recognition Vendor Test (FRVT)
Part 4A: MORPH - Utility of 1:N Face Recognition Algorithms for Morph Detection

Mei Ngan
Patrick Grother
Kayee Hanaoka
Information Access Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8430

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8430.pdf

Use of 1:N Face Recognition for Morph Detection

Example Scenario: Passport Renewal

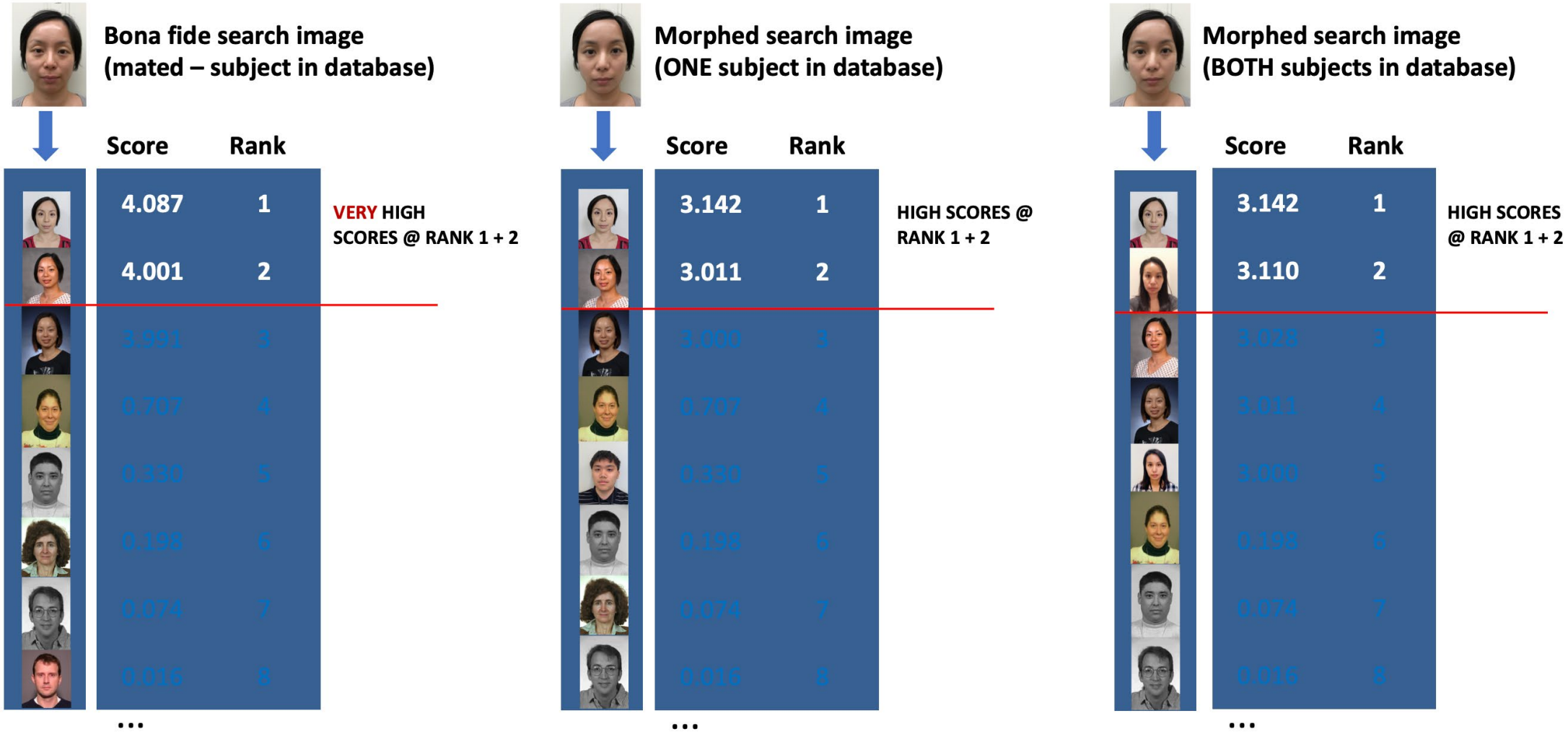


Image Source: NIST + Public FERET Database

Patent Pending: U.S. Patent Application No. US2023/015079

Morphing: possible mitigation

Do live enrollment

- Norway (now), Sweden (now), Germany 2025[1]
- Should be adopted by all countries to be effective
- But some morphs in circulation now

Do trusted external capture

- Signed photobooths
- Certified photographers (e.g., Finland, France)
- Liveness detection in dedicated, secure mobile application

Continue to develop morph detection

- Continue development of automated morph detection (particularly D-MAD, which may be ready for operational piloting)
- Perform 1:N duplicate check; look for suspicious activity [NISTIR 8430]

Build awareness

- Train relevant personnel about morphs
- Can training improve personnel skills on morphed image over time?
- What cues are people good at detecting morphs using and are any of them tangible to document?

Eliminate print + scanned photos

- Avoid printing and scanning
- Require high resolution, digital photos

Establish strong secondary verification processes

- Verify with additional data source (e.g., Slovenia)
- Use another biometric modality

[1] https://www.reuters.com/article/us-germany-tech-morphing/germany-bans-digital-doppelganger-passport-photos-idUSKBN23A1YM

Thank you!

Mei Ngan
National Institute of Standards and Technology
frvt@nist.gov | mei@nist.gov