FRVT MORPH - Current Vulnerability Assessment and Automated Detection Performance

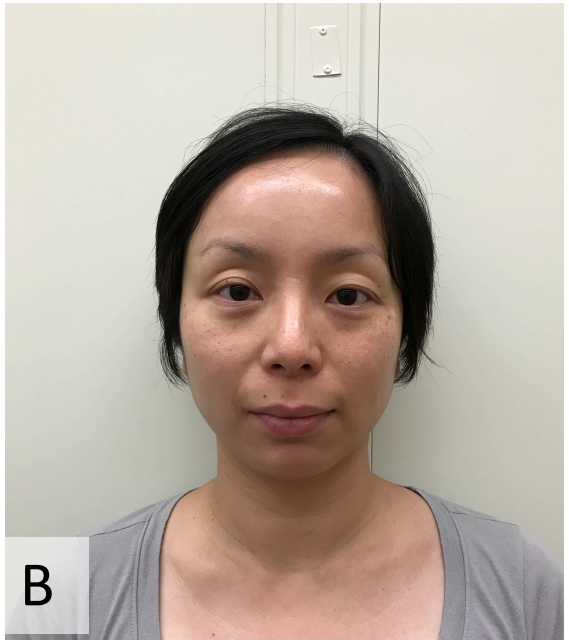
Mei Ngan, Patrick Grother, Kayee Hanaoka
National Institute of Standards and Technology (NIST)
US Department of Commerce

International Face Performance Conference (IFPC) 2022
November 17, 2022

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

Face Morphing

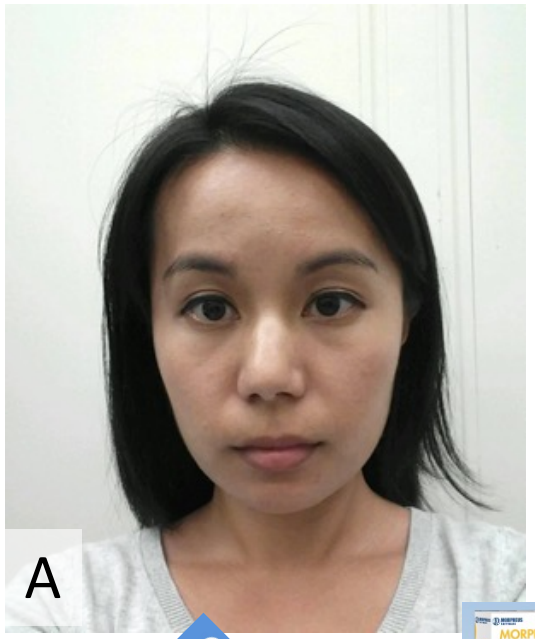
+



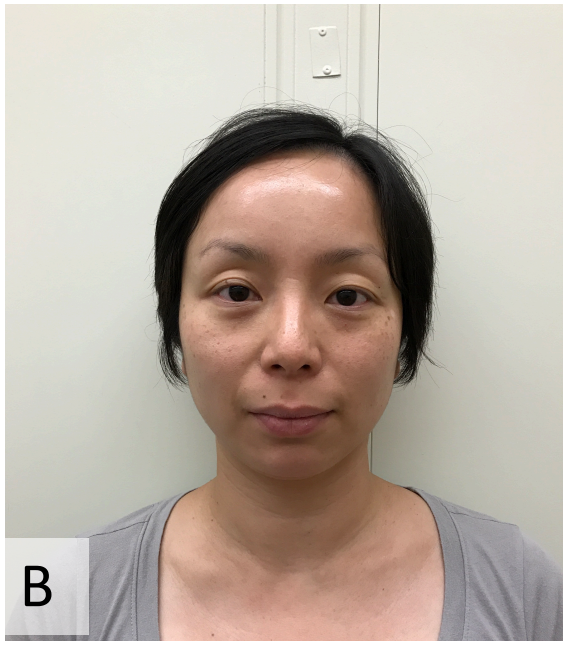
=

Image Source: NIST

Face Morphing



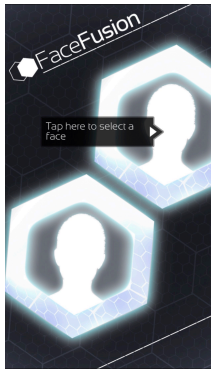
+



=

Image Source: NIST

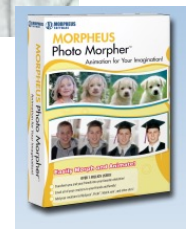
Source: http://www.piviandco.com/apps/mixbooth



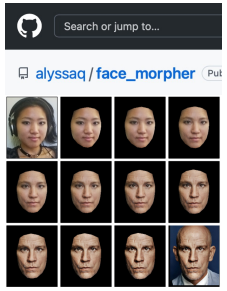
Source: https://en.softonic.com/solutions/apps/facefusion-lite

Source: http://www.morphthing.com

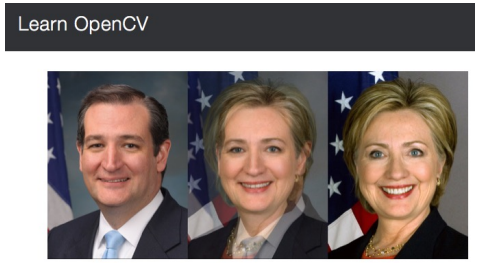
Source: http://www.facemorpher.com



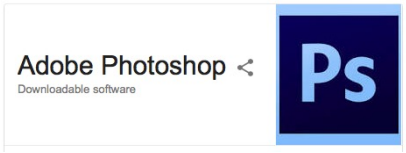
Source: http://www.morpheussoftware.net



Source: https://github.com/alyssaq/face_morpher

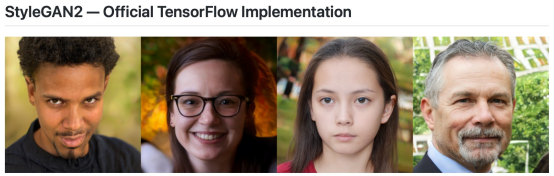


Source: https://www.learnopencv.com/face-morph-using-opencv-cpp-python



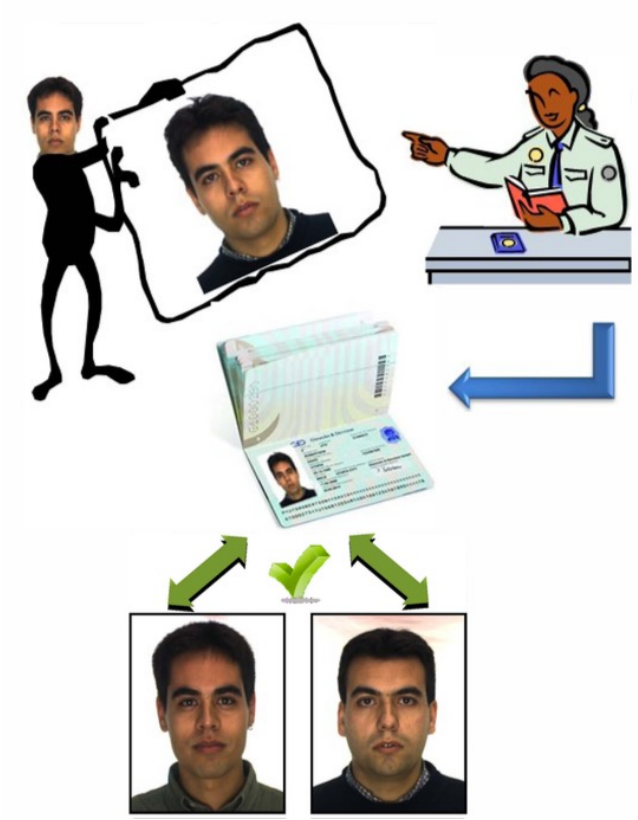
Source: https://www.adobe.com/products/photoshop.html

Source: http://www.fantamorph.com



Source: https://github.com/NVlabs/stylegan2

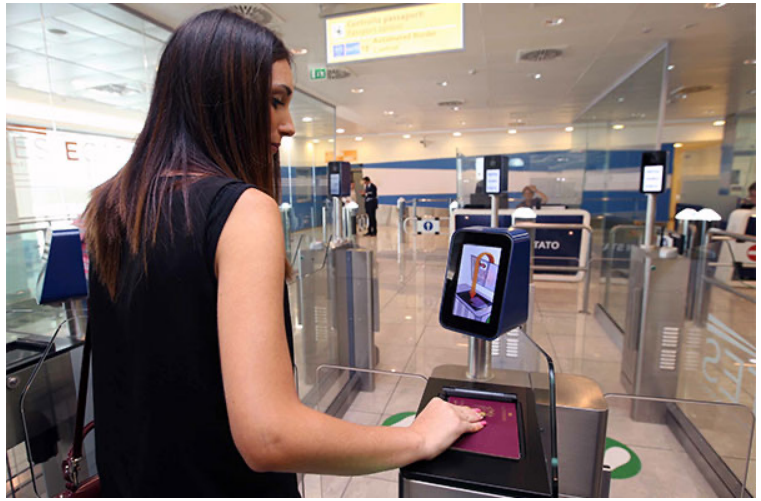
Threats & Consequences



Accomplice Attacker (other identity)

Source: Ferrara, Franco, and Maltoni, ***The Magic Passport***, IEEE International Joint Conference on Biometrics, October 2014, pp. 1-7

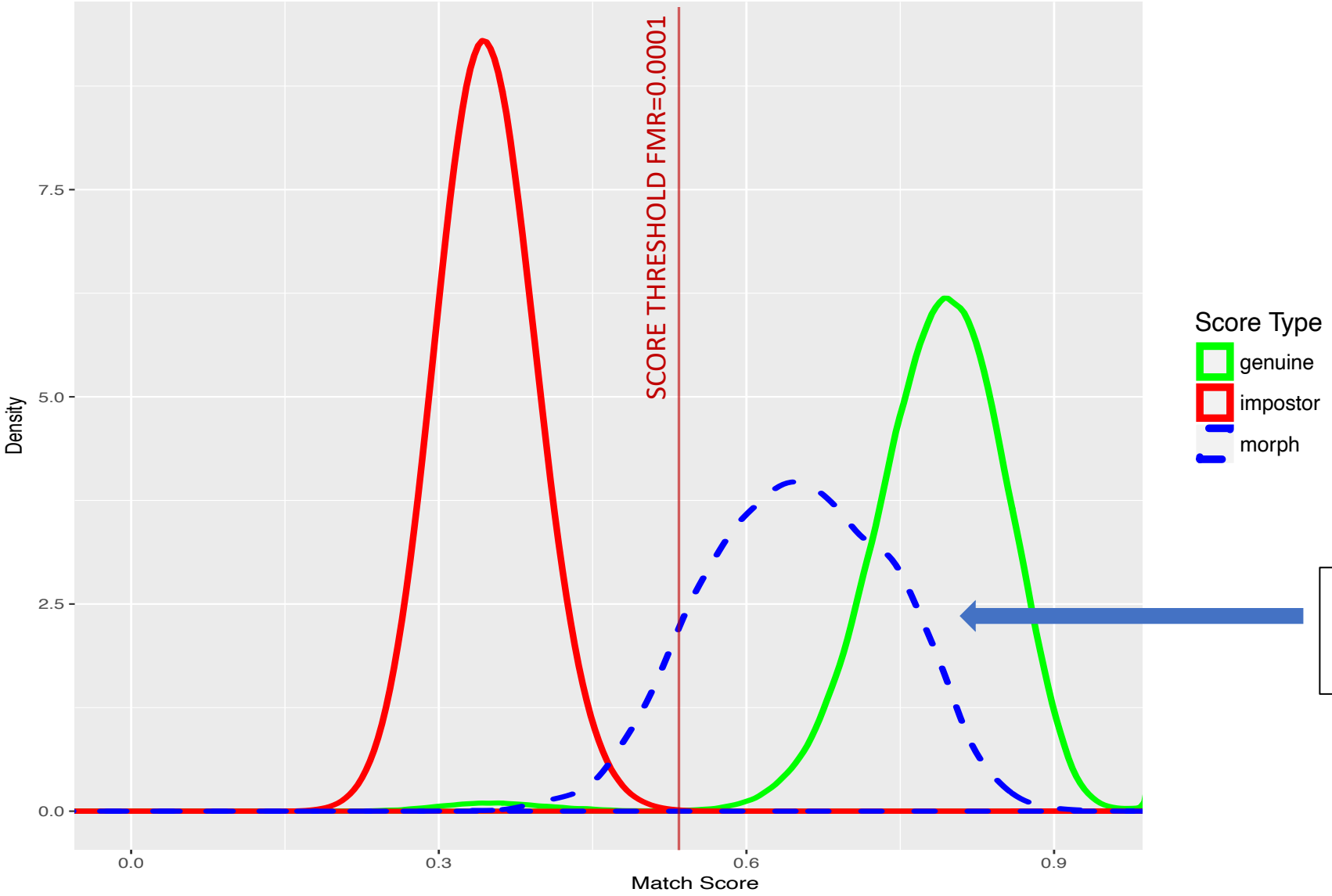
Automated Border Control Gate



Source: http://www.futuretravelexperience.com/2016/01/automated-border-control-e-gates-go-live-at-naples-airport/

Morphing poses a threat to entities that accept user-submitted photos for identity credentials

Automated Face Recognition: Genuines, Impostors, and Morphs



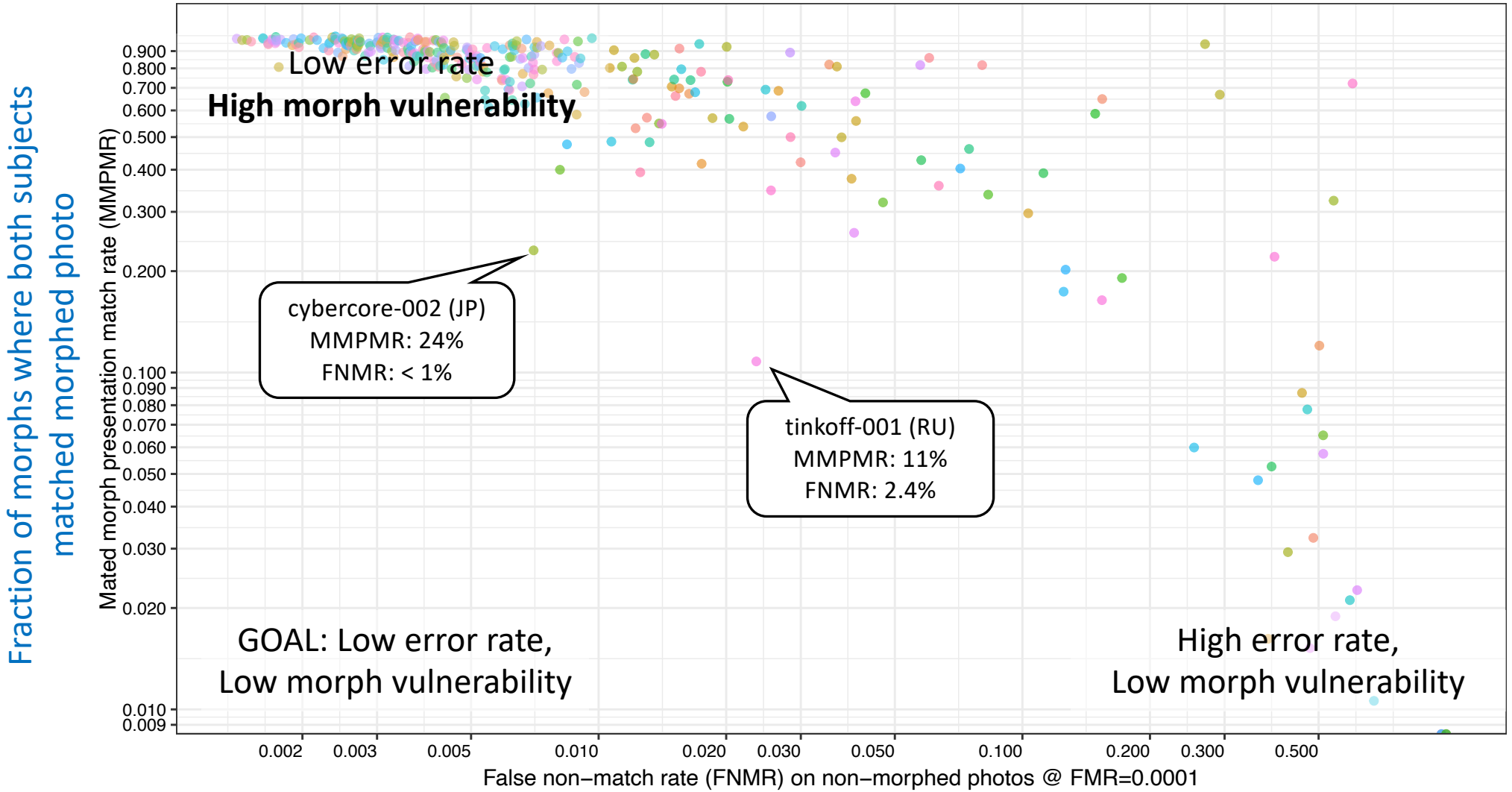
Fraction of morphs where the subject matches morphed photo above threshold

Face morphing: Current face recognition vulnerability

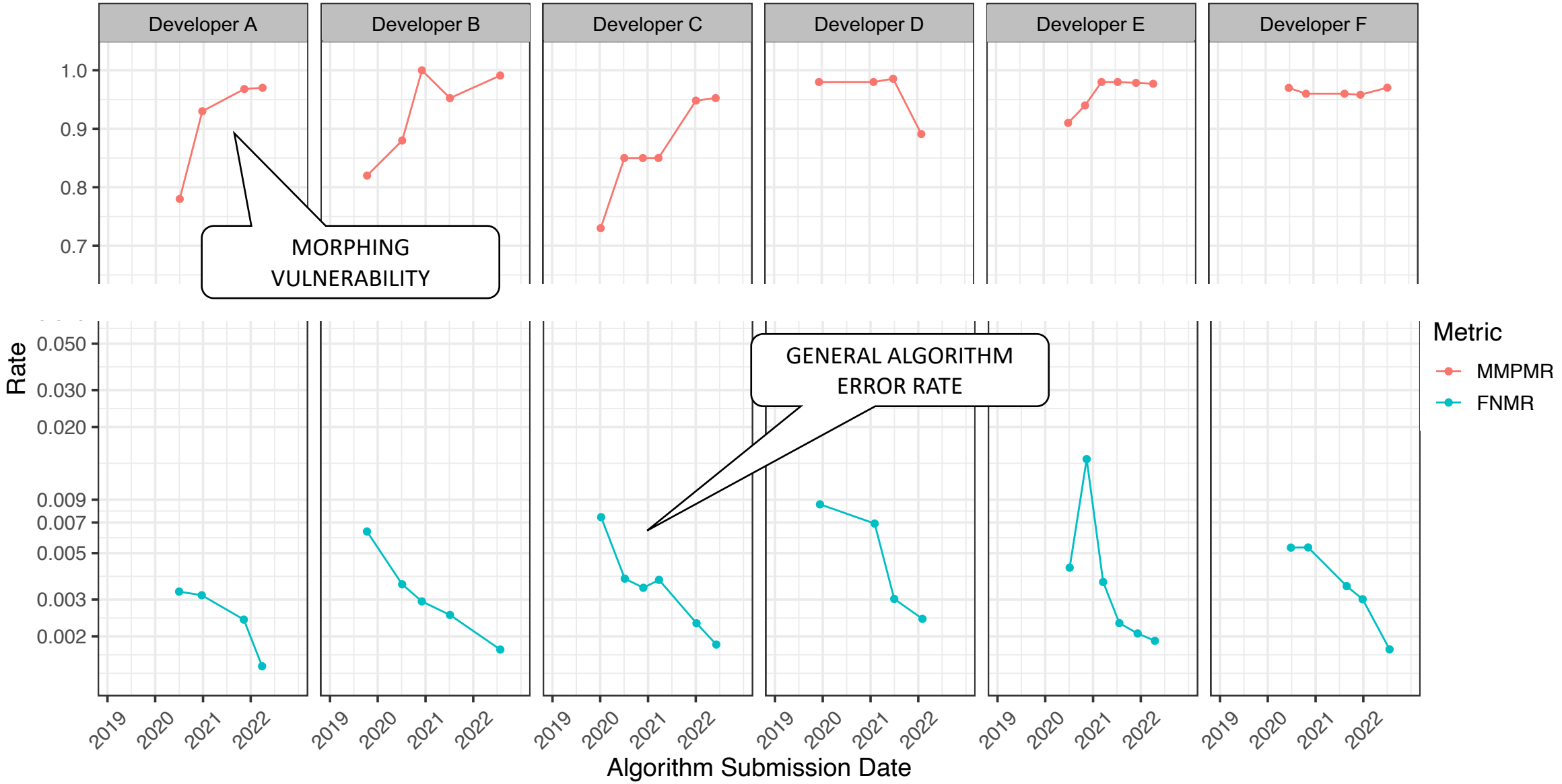
Each dot represents a recent FR algorithm submitted to the NIST Ongoing FRVT 1:1 Verification Test

Face morphing: Current face recognition vulnerability

Each dot represents a recent FR algorithm submitted to the NIST Ongoing FRVT 1:1 Verification Test



Morphing vulnerability trends

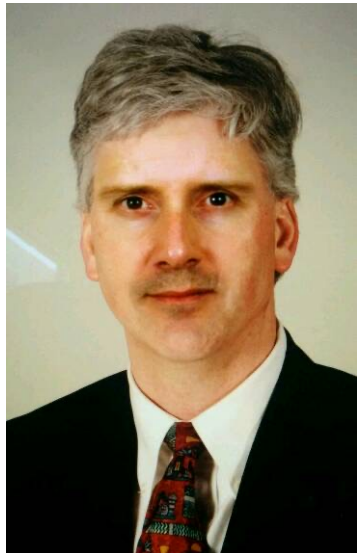


FRVT MORPH Use Case: Morph Detection

Single-image

Morph detection with single image in isolation

(e.g., initial passport application)

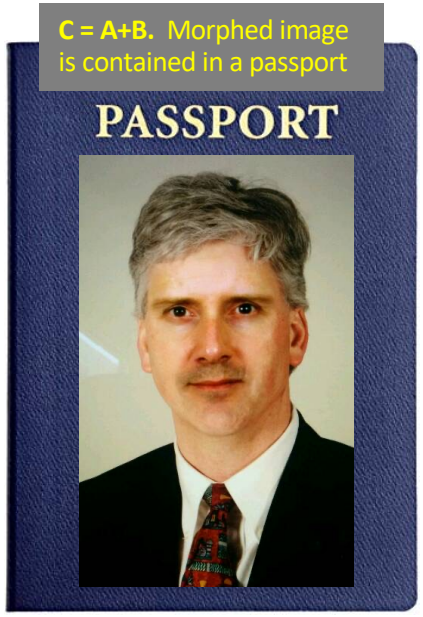


Goal: Determine whether image being submitted is a morph or not.

Differential

Morph detection with additional live capture image

(e.g., morph on passport + eGate webcam photo)



Goal: Determine whether image on passport is morphed by using the additional information available in the live capture image.

Image Source: NIST + USG employee with permission

FRVT MORPH Participation

Academia

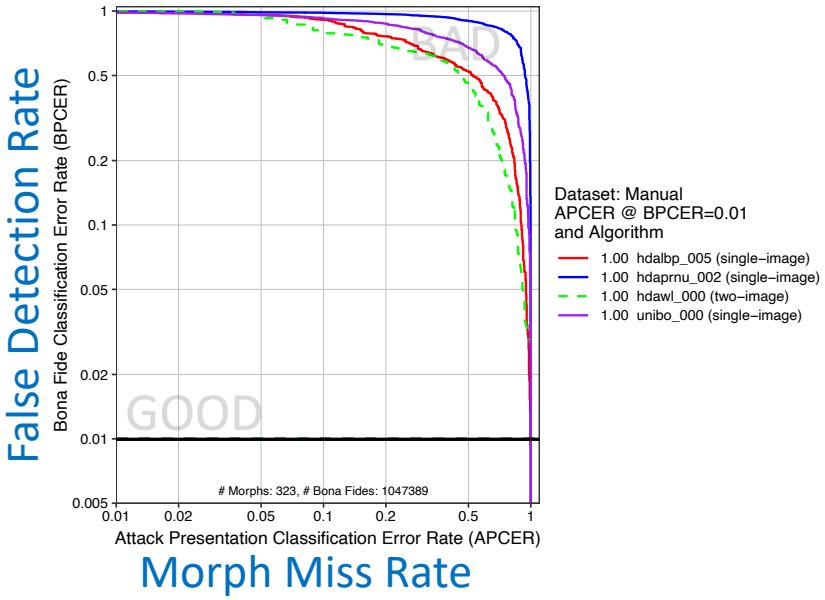
- Hochschule Darmstadt (DE)
- Norwegian University of Science and Technology (NO)
- University of Bologna (IT)
- West Virginia University (US)
- University of Coimbra (PT)

Industry

- secunet (DE)

Morph Detection: Progress

September 2019

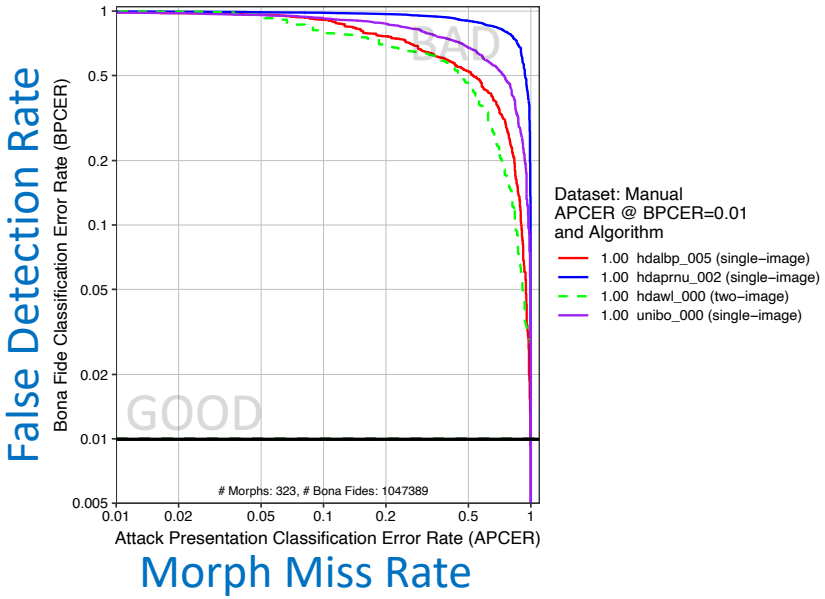


——— single-image

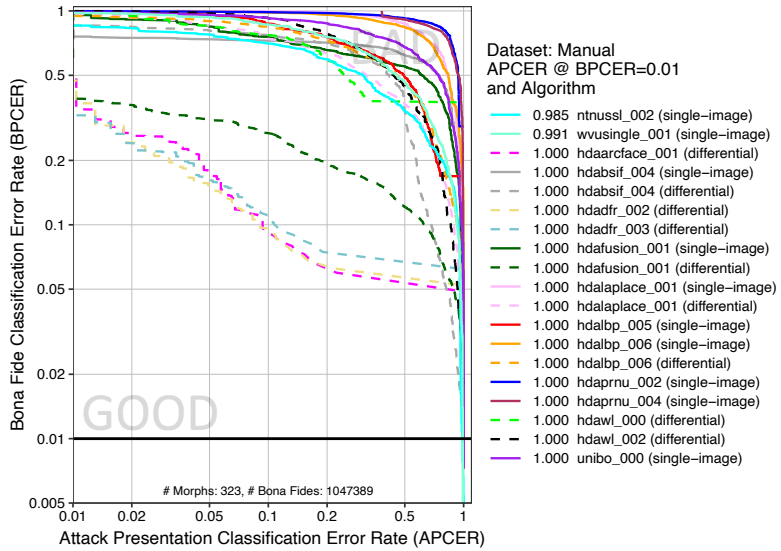
– – – differential (two-image)

Morph Detection: Progress

September 2019



September 2021

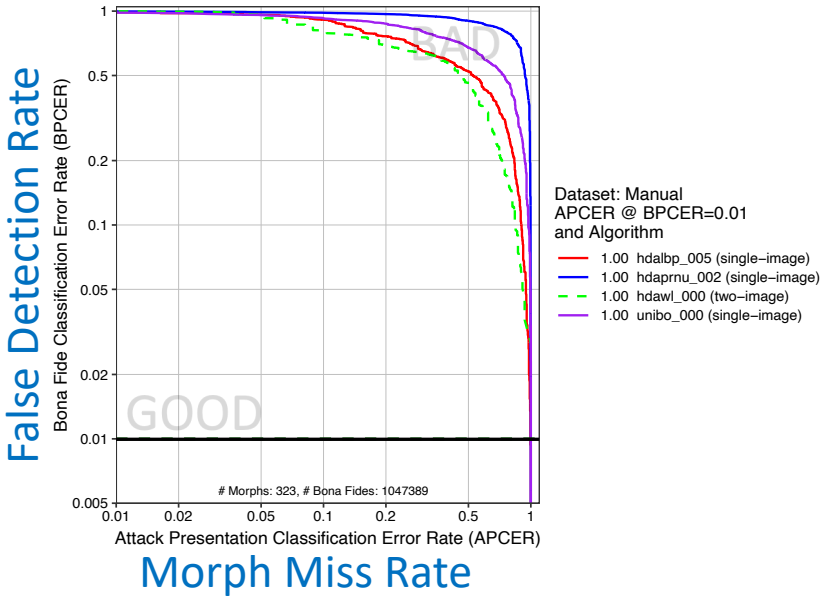


——— single-image

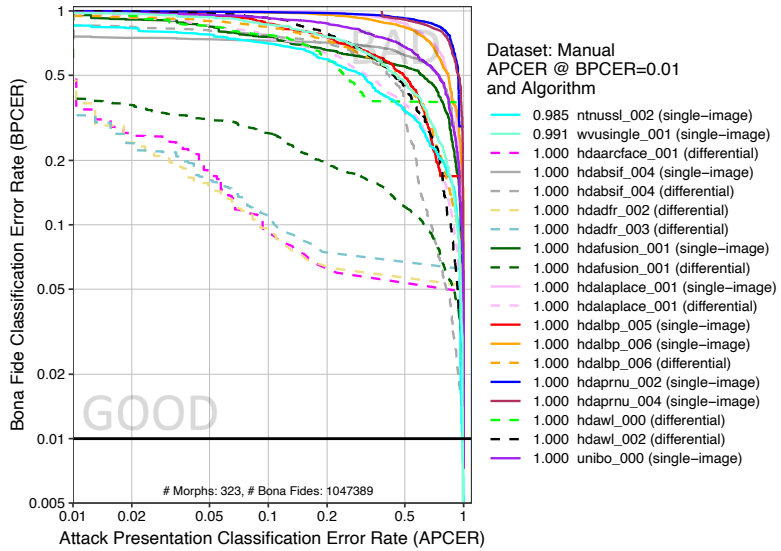
– – – differential (two-image)

Morph Detection: Progress

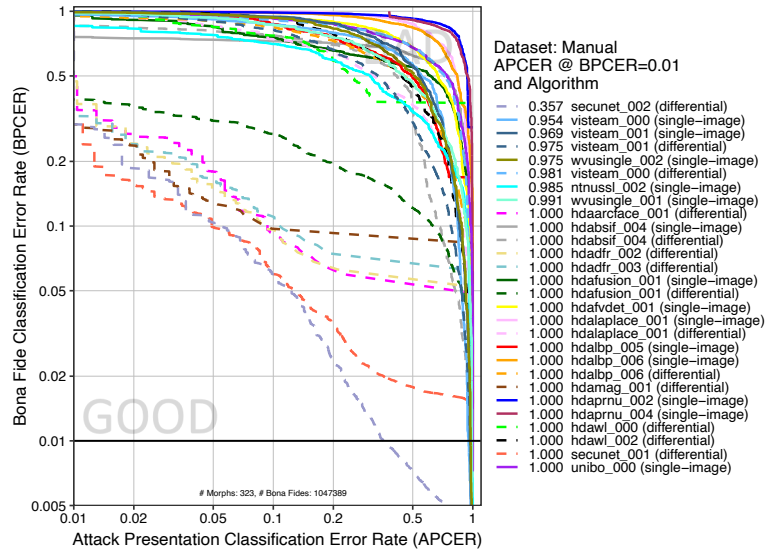
September 2019



September 2021



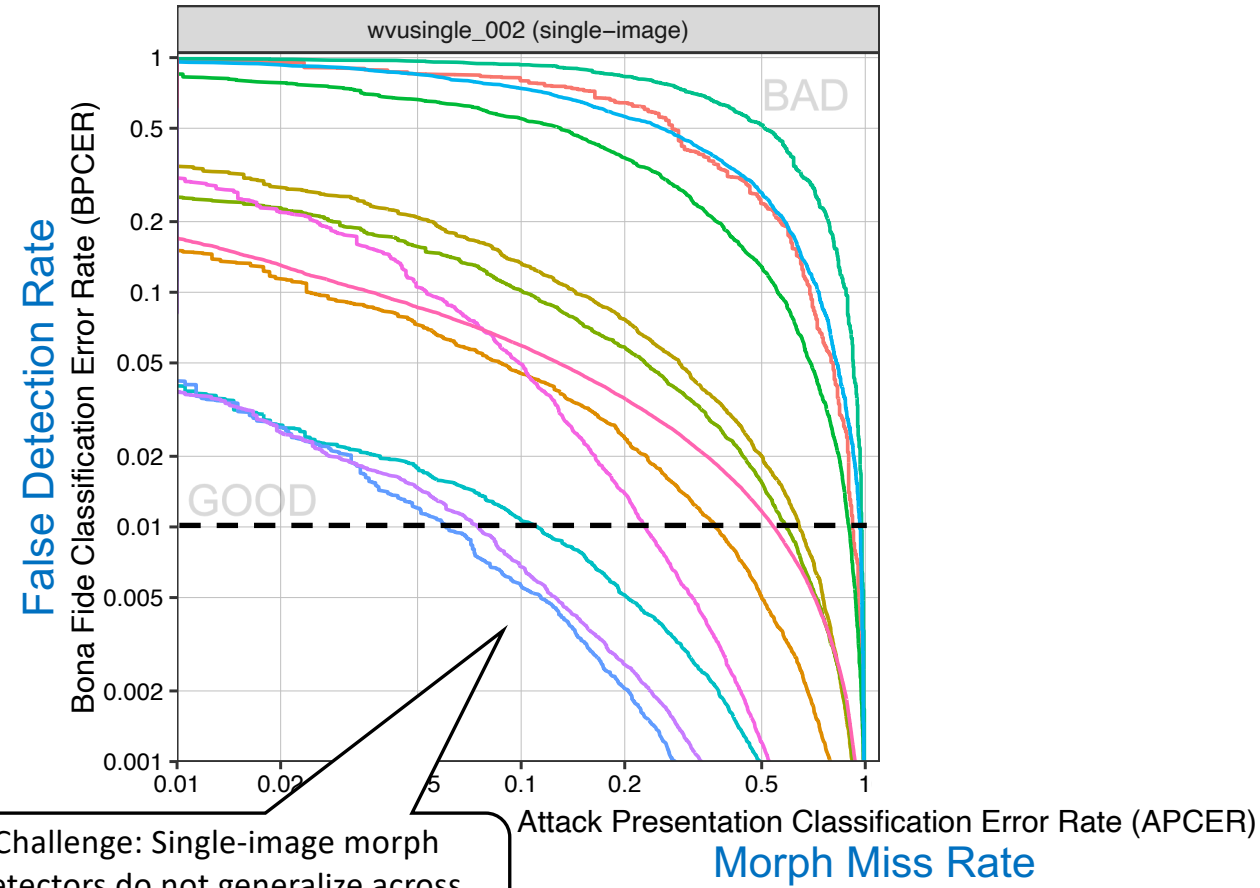
November 2022

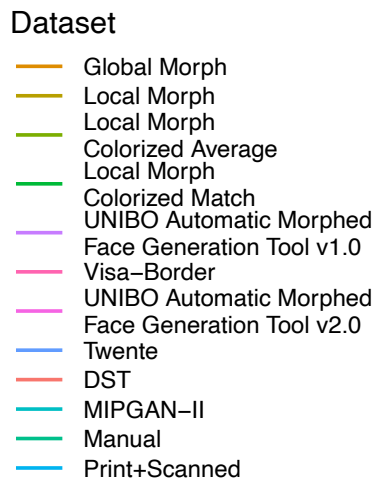


single-image

differential (two-image)

Morph Detection: Challenges and Opportunities

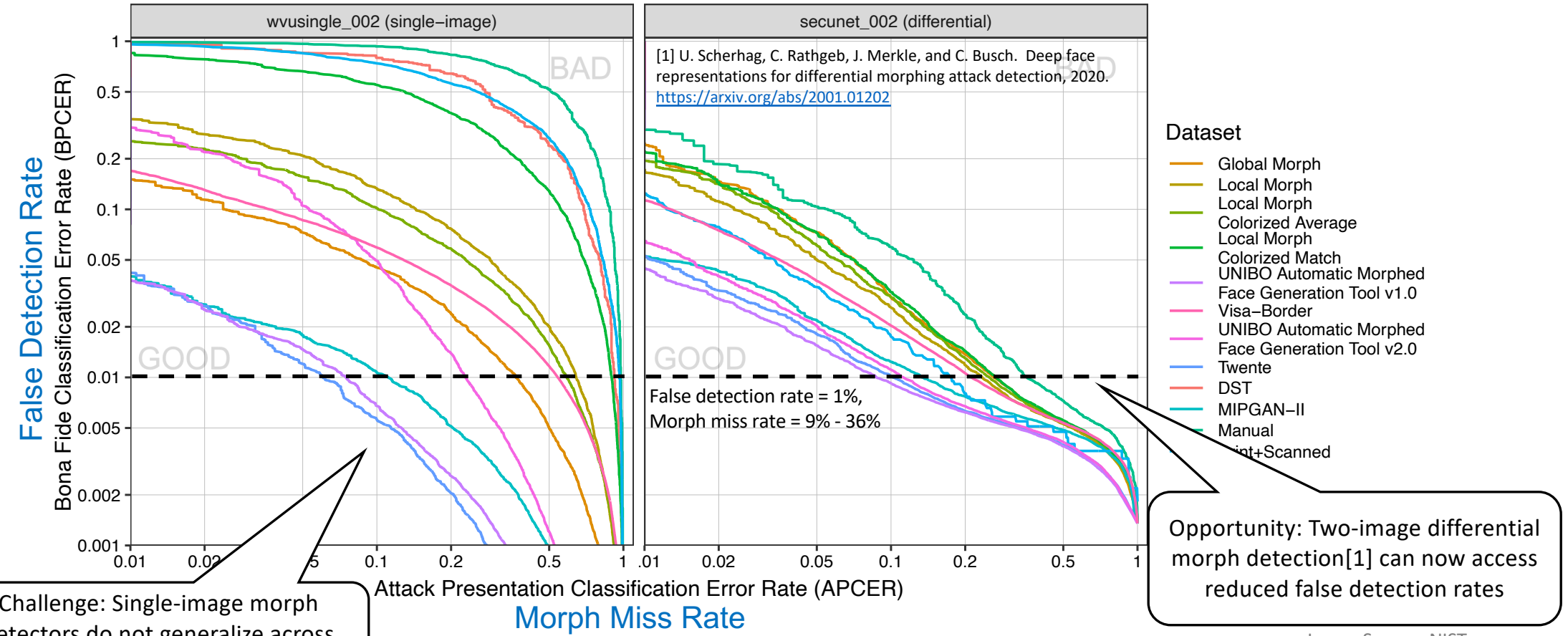




Challenge: Single-image morph detectors do not generalize across different morphing methods

Image Source: NIST

Morph Detection: Challenges and Opportunities

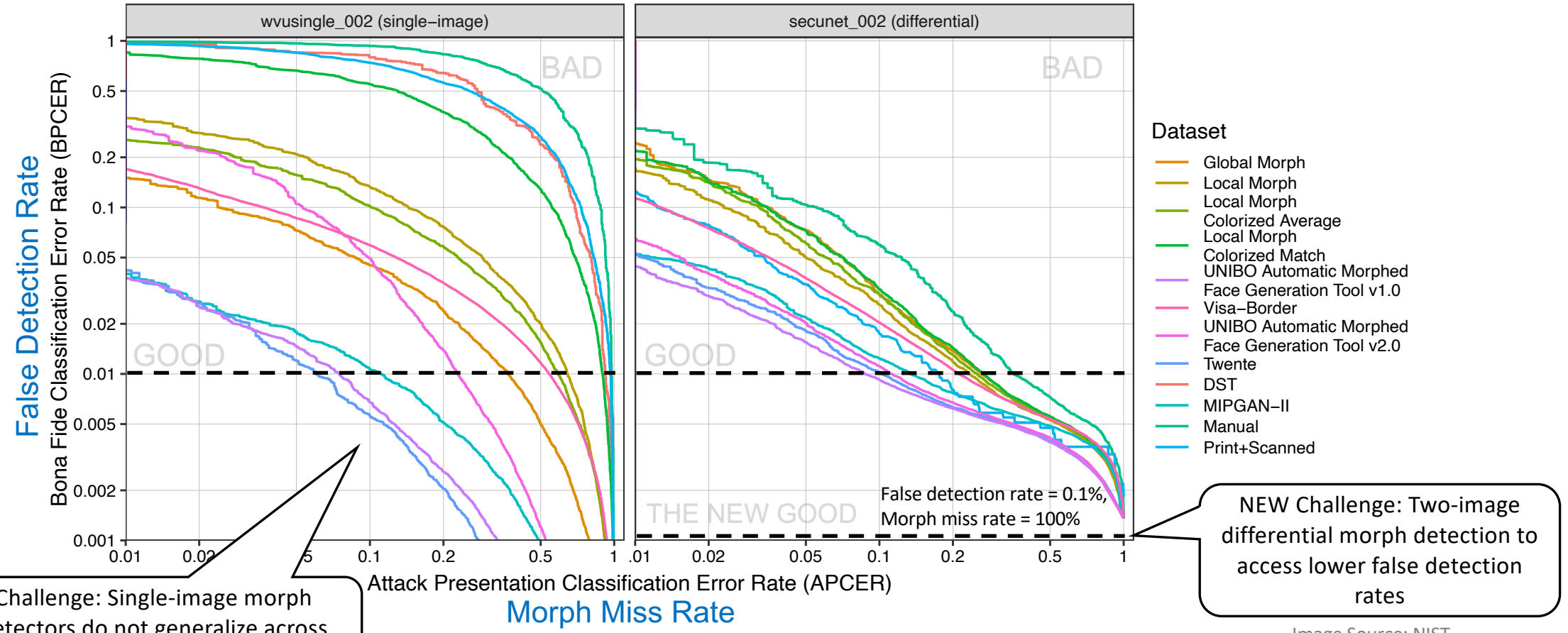


Challenge: Single-image morph detectors do not generalize across different morphing methods

Opportunity: Two-image differential morph detection[1] can now access reduced false detection rates

Image Source: NIST

Morph Detection: Challenges and Opportunities



Challenge: Single-image morph detectors do not generalize across different morphing methods

NEW Challenge: Two-image differential morph detection to access lower false detection rates

Image Source: NIST

FRVT MORPH Use Case:
Morph Resistant Face Recognition

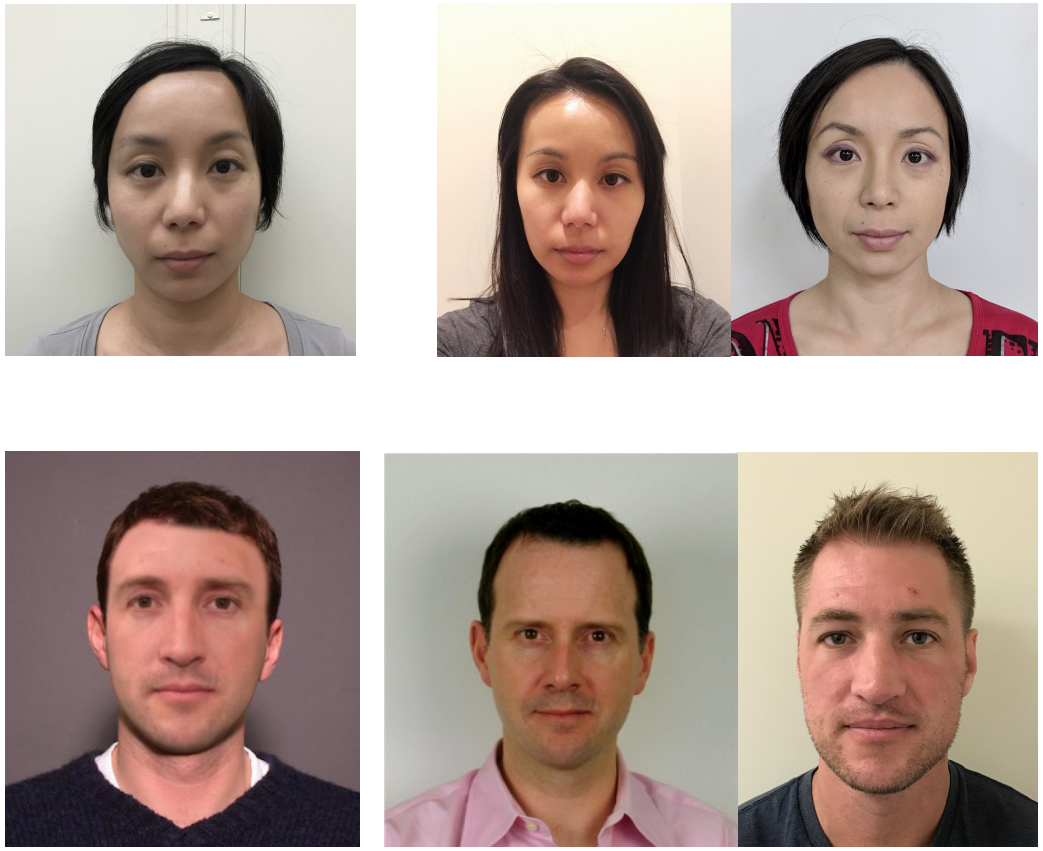


Image Source: NIST

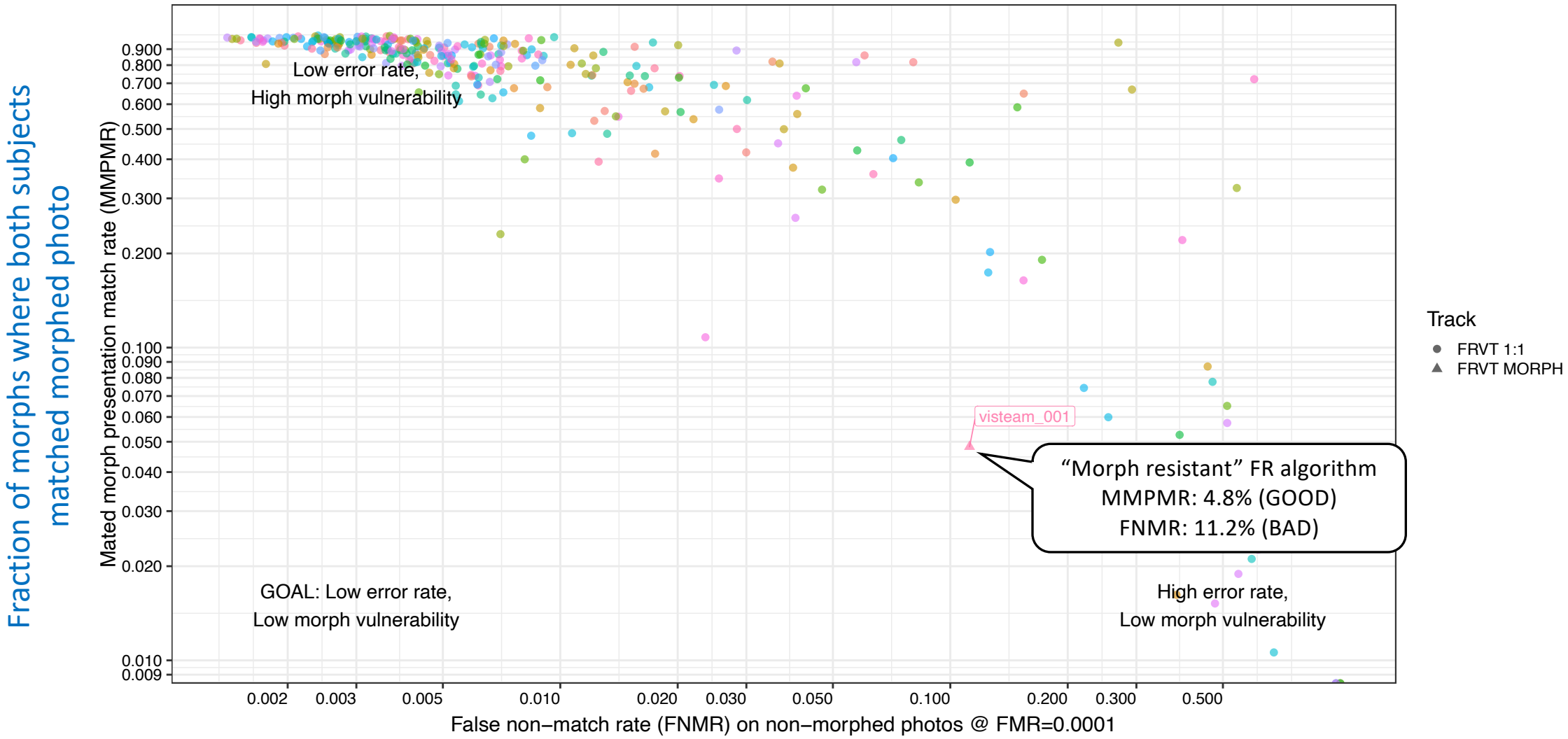
Use Case: Test FR algorithm resistance against morphing

Protocol: Given image X and image Y, produce verification similarity score

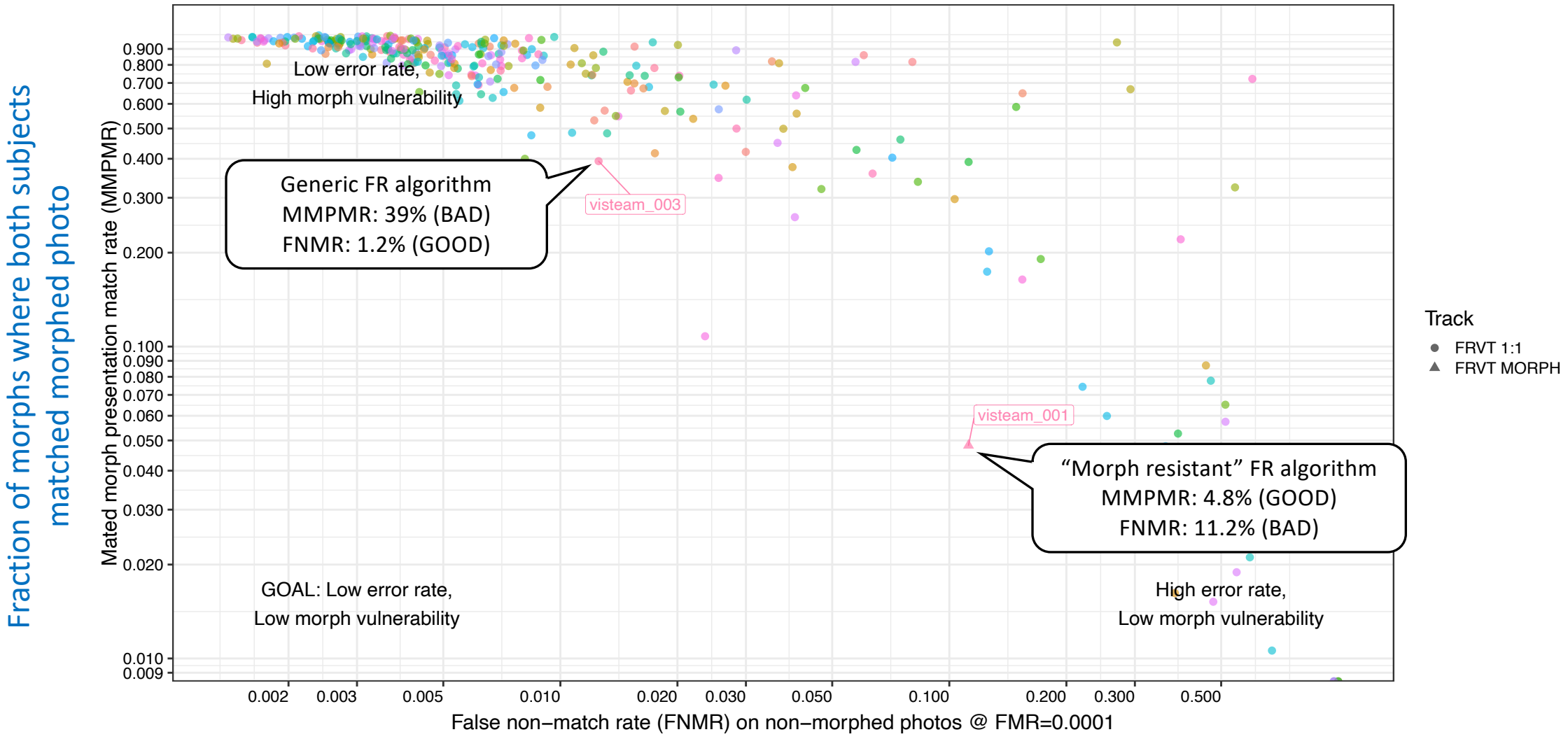
Evaluation: ISO/IEC 30107-3 metrics

- Mated Morph Presentation Match Rate (MMPMR)
- False non-match rate (FNMR)
- False match rate (FMR)
- Others TBD

Morph resistant face recognition performance



Morph resistant face recognition performance

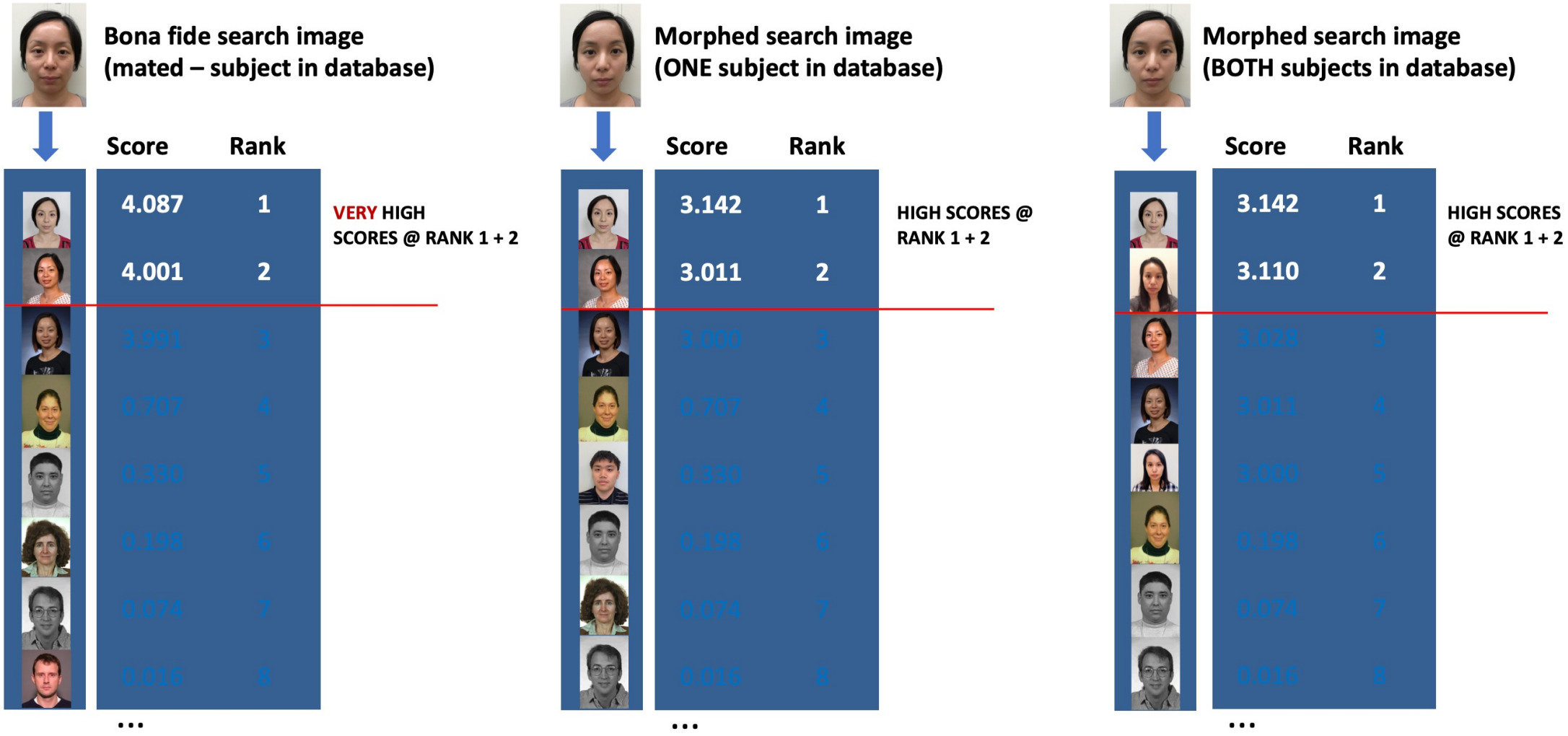


Utility of 1:N search for morph detection

NISTIR 8430: FRVT Part 4A: MORPH – Utility of 1:N Face Recognition Algorithms for Morph Detection, July 27, 2022

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

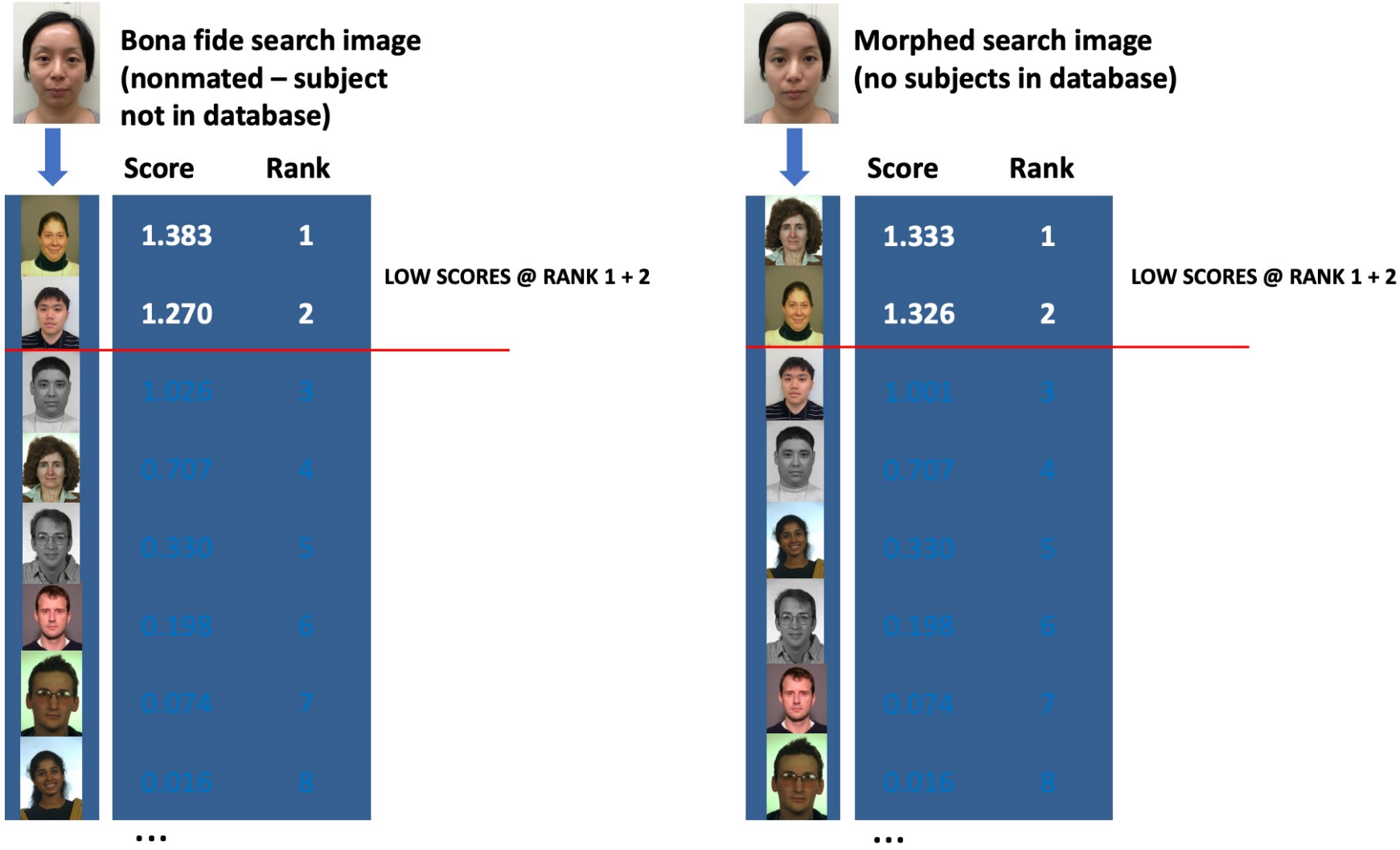
Analysis of rank 1 and 2 similarity scores from 1:N face recognition search for morph detection
SCENARIO: RENEWAL



All databases used in experiments contain bona fide imagery

Image Source: NIST + Public FERET Database

Analysis of rank 1 and 2 similarity scores from 1:N face recognition search for morph detection
SCENARIO: NEW ENROLLMENT

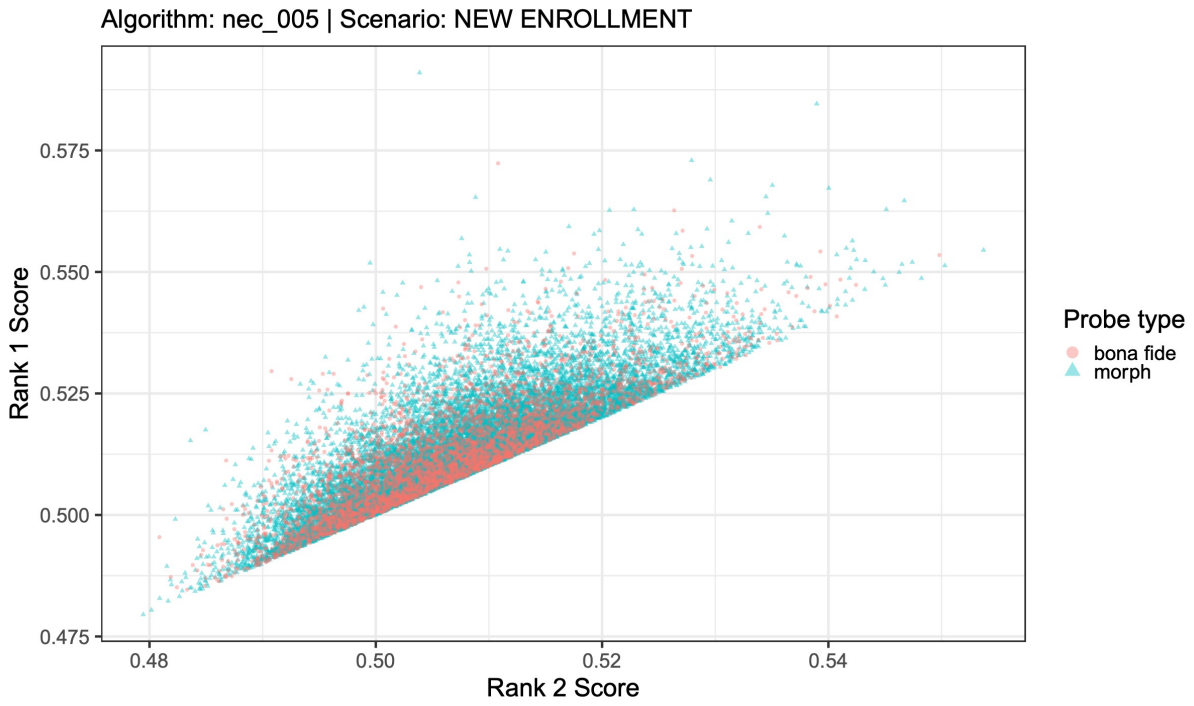


All databases used in experiments contain bona fide imagery

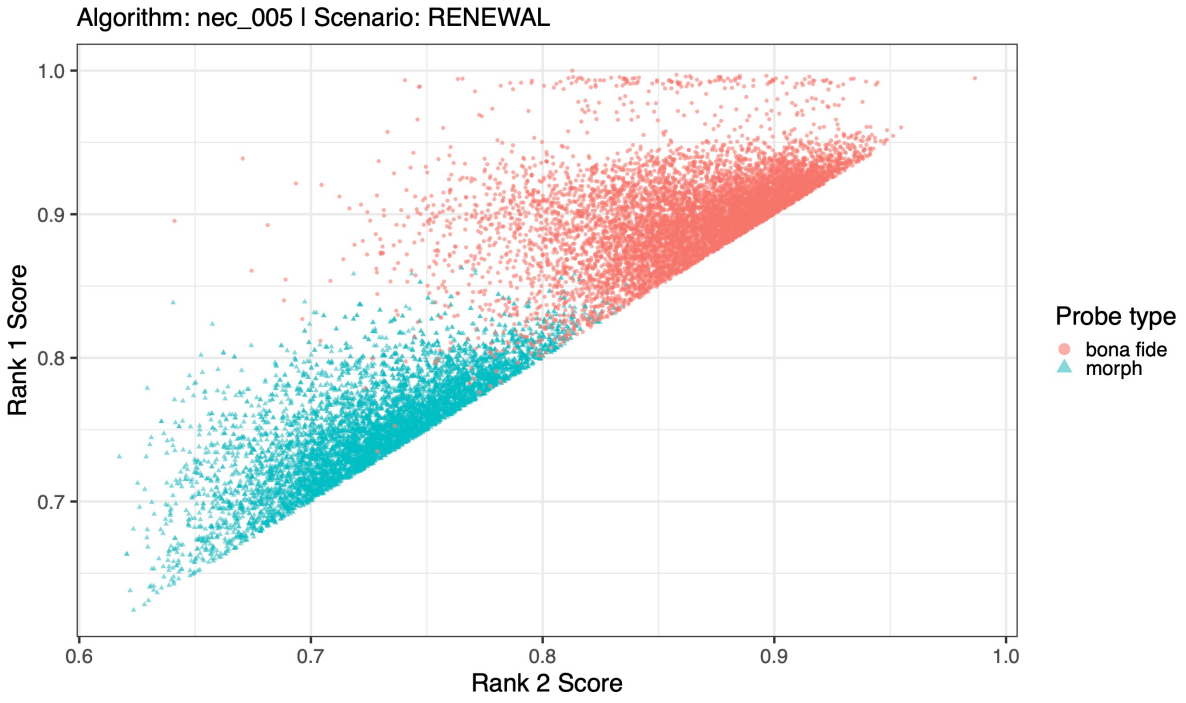
Image Source: NIST + Public FERET Database

Visualization of rank 1 and 2 similarity scores

Scenario: NEW ENROLLMENT
(subjects do not exist in the database)



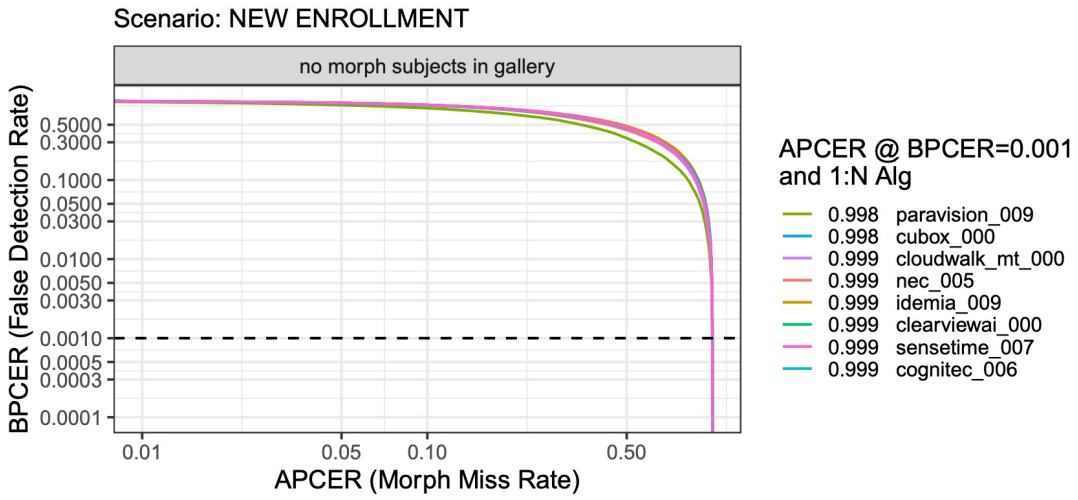
Scenario: RENEWAL
(multiple photos of one or both subjects exist in the database)



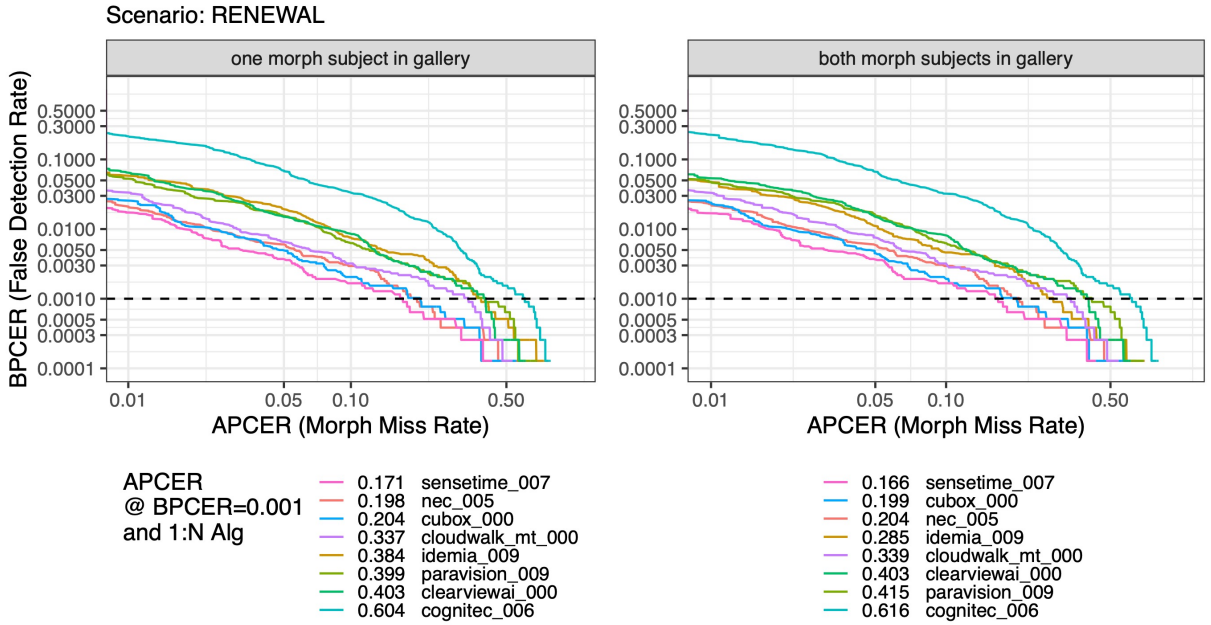
Large separation in score distributions presents detection opportunity!

Proof of concept: Morph detection results from training a morph classifier with rank 1 and 2 scores

Scenario: NEW ENROLLMENT



Scenario: RENEWAL



Morph detection using 1:N face recognition is **not** effective in a new enrollment scenario

Morph detection using 1:N face recognition may be effective in a renewal scenario (low false detection rates attainable)

Source: NISTIR 8430: FRVT Part 4A: MORPH – Utility of 1:N Face Recognition Algorithms for Morph Detection, July 27, 2022

Summary and closing thoughts…

- Modern face recognition is vulnerable to face morphing
- Automated morph detection has made notable progress
- One-to-many face recognition may have utility in morph detection under certain scenarios
- Other potential mitigations
  - Live enrollment (e.g., Norway, Sweden, Germany 2025!)
  - Human involvement remains critical (training + strong secondary verification processes)

Thank you!

Mei Ngan
National Institute of Standards and Technology (NIST)
US Department of Commerce
frvt@nist.gov