Face Morphing – Threats, Technology, and What's Next

Mei Ngan
Patrick Grother
Kayee Hanaoka
Jason Kuo

National Institute of Standards & Technology (NIST), US Department of Commerce

International Face Performance Conference (IFPC) 2020
October 28, 2020

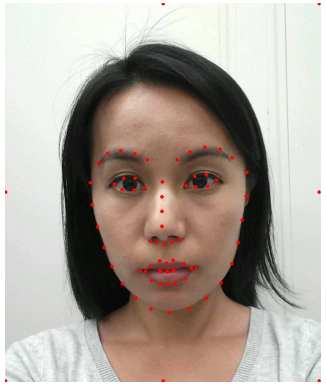
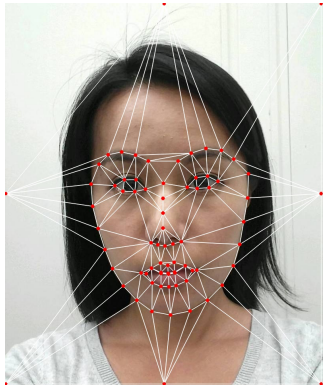
NIST National Institute of Standards and Technology U.S. Department of Commerce

INFORMATION TECHNOLOGY LABORATORY

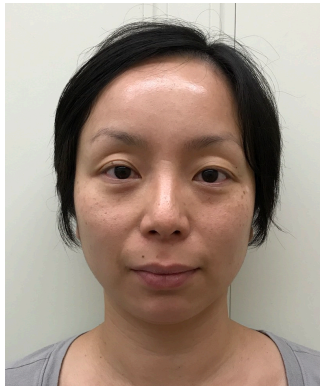
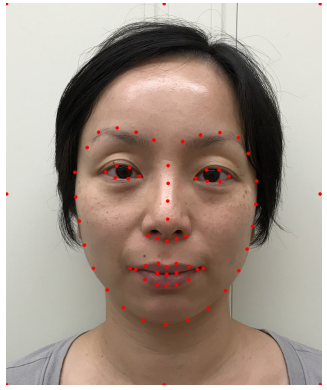
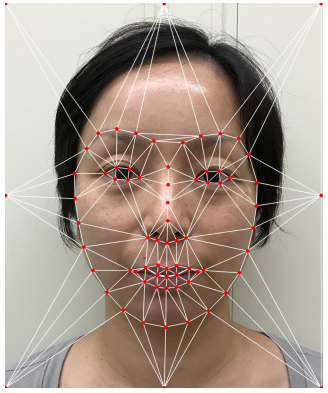
Agenda

- WHAT IS FACE MORPHING
- THREATS & CONSEQUENCES
- NIST FRVT MORPH EVALUATION

Face Morphing

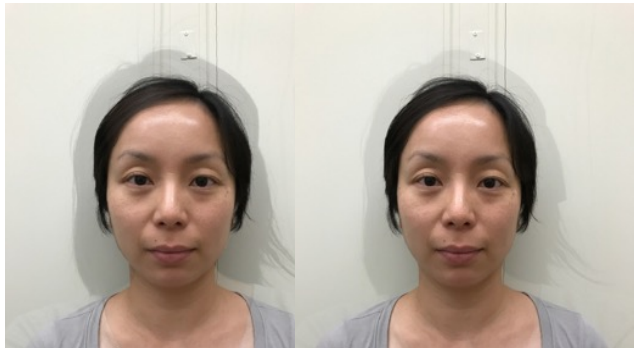
Subject A

Subject B

Subject A contribution (%) | Subject B contribution (%)

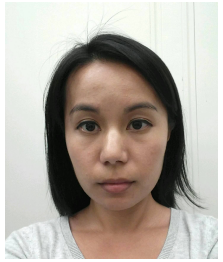
90% | 10% 70% | 30% 50% | 50%



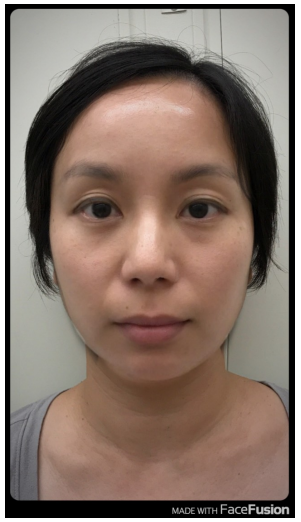
30% | 70% 10% | 90%

Source: NIST

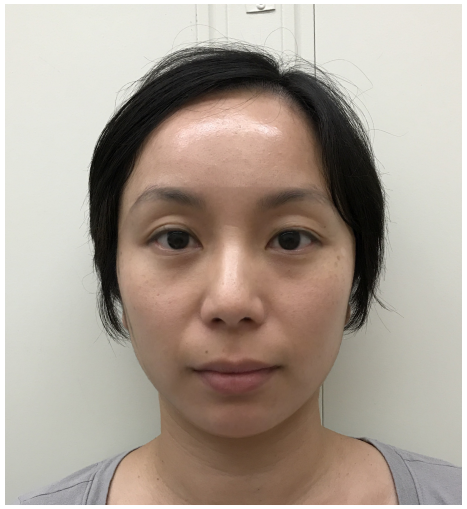
Morph Examples


+


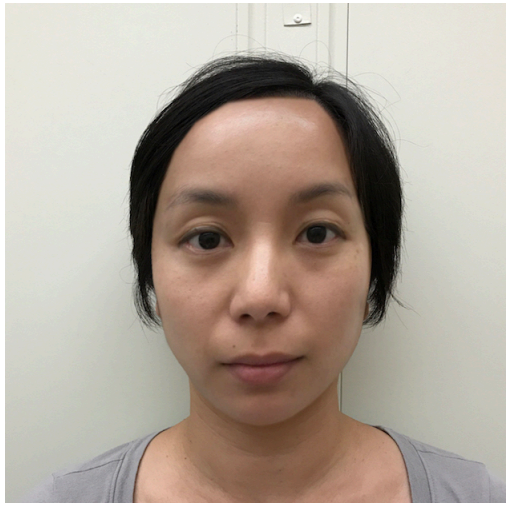
www.MorphThing.com



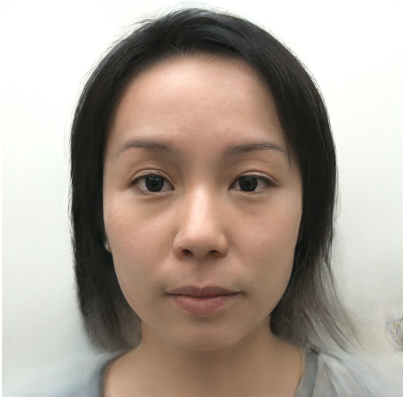
FaceFusion Mobile App



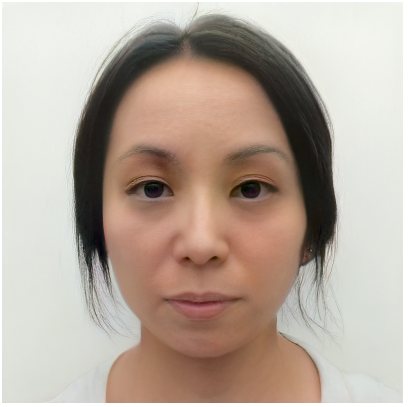
Automated Method (UNIBO v1) [1-3]



FantaMorph + Photoshop



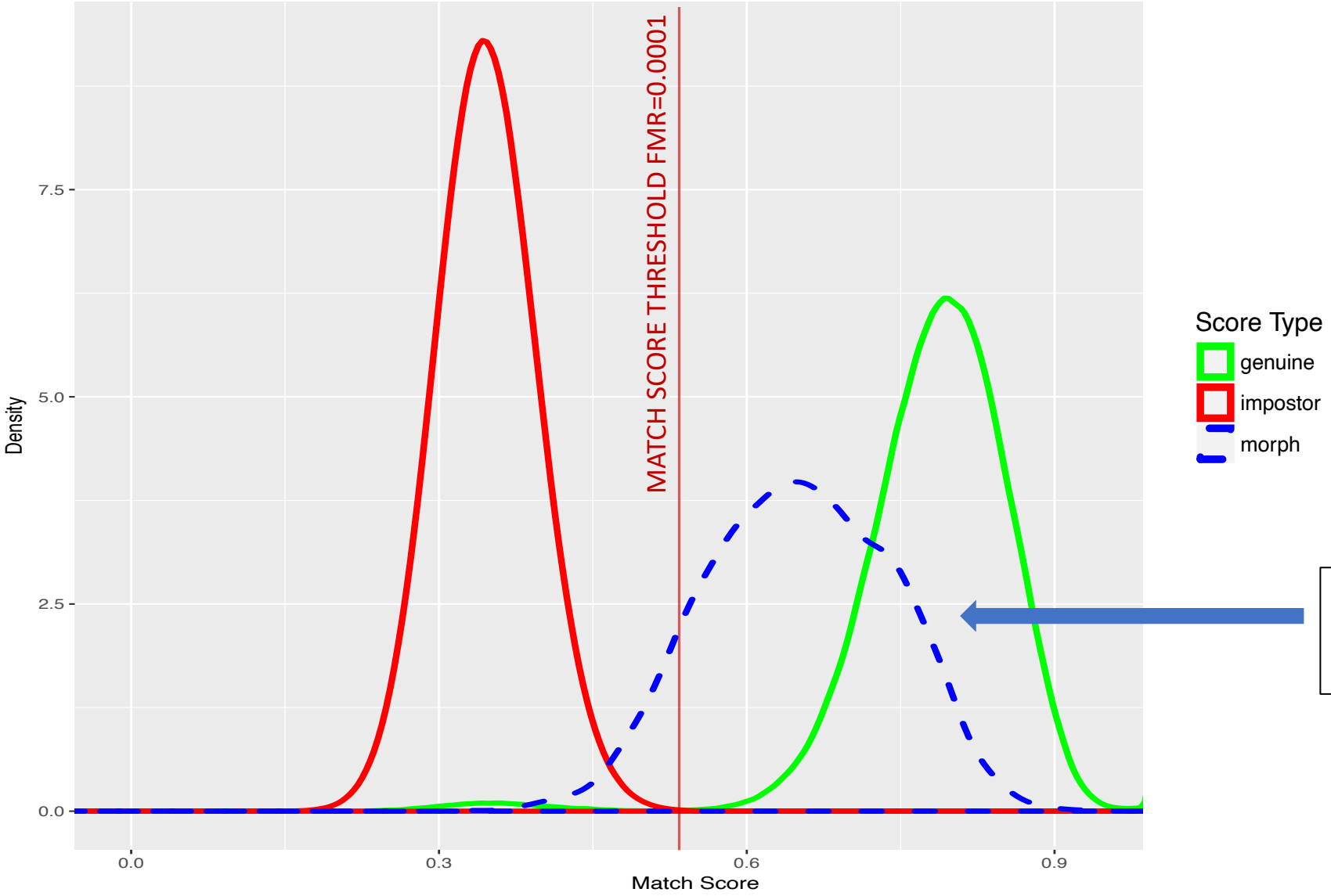
StyleGAN



StyleGAN2

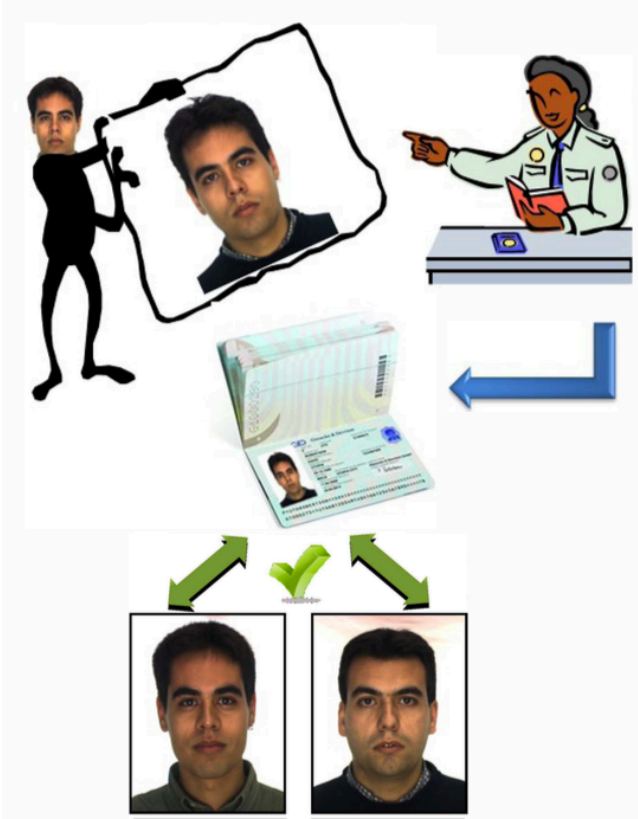
[1] M. Ferrara, A. Franco, and D. Maltoni, "Face Demorphing," IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 1008-1017, April 2018.
[2] M. Ferrara, A. Franco, and D. Maltoni, "The Magic Passport," in IEEE International Joint Conference on Biometrics (IJCB), Clearwater, Florida, USA, 2014, pp. 1-7.
[3] M. Ferrara, A. Franco, and D. Maltoni, "On the Effects of Image Alterations on Face Recognition Accuracy," in Face Recognition Across the Electromagnetic Spectrum. Switzerland: Springer International Publishing, 2016, pp. 195-222.

Automated FR: Genuines, Impostors, and Morphs



Fraction of morphs where the subject matches morphed photo above threshold

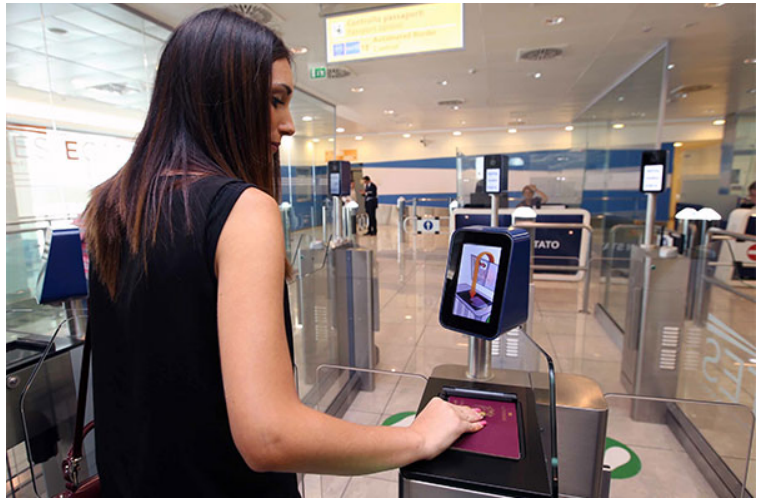
Threats & Consequences



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

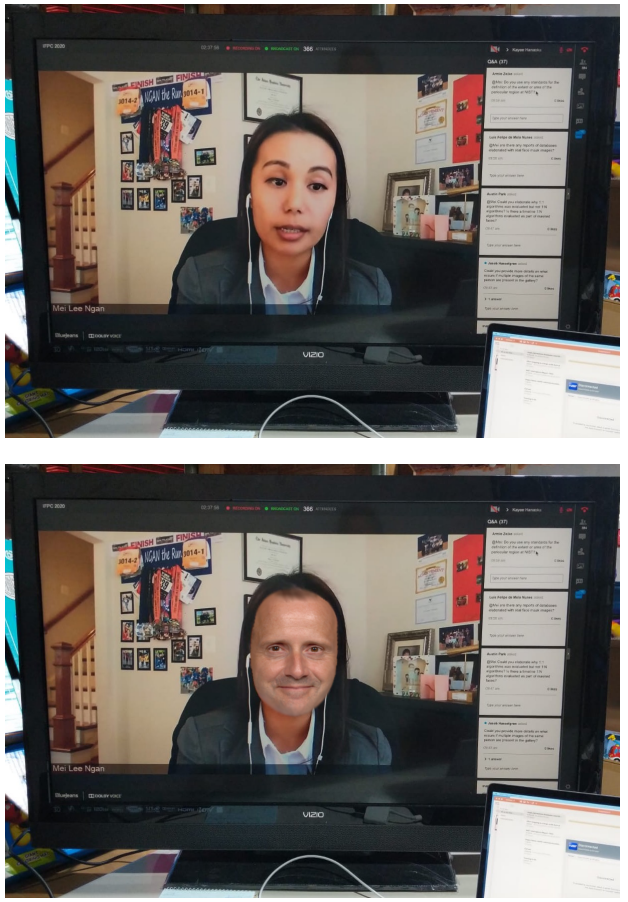


Source: http://www.futuretravelexperience.com/2016/01/automated-border-control-e-gates-go-live-at-naples-airport/

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

Morphs are different from deepfakes

Morphs merge different faces together

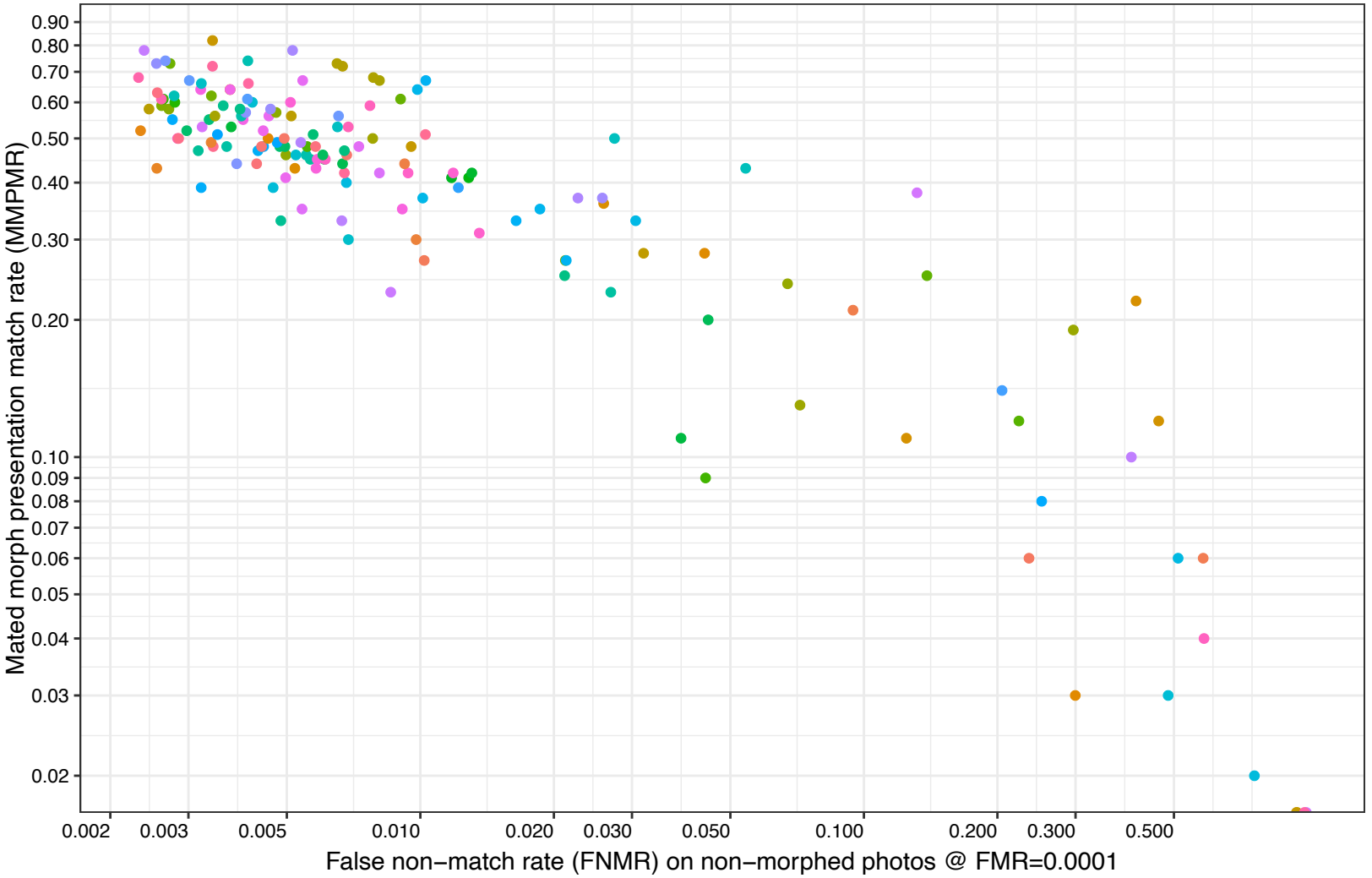


Deepfakes generally replace a person in an existing image or video with someone else's face

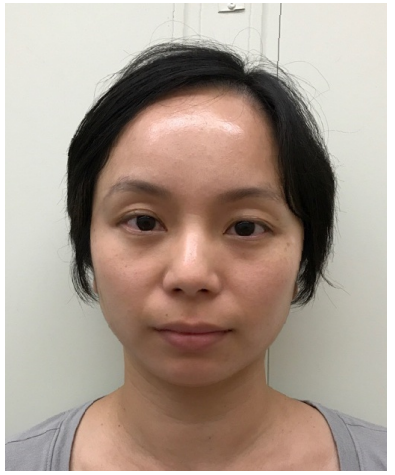
Current face recognition vulnerability

Each dot represents an FR algorithm from NIST Ongoing FRVT 1:1 Verification Test

Fraction of morphs where both subjects matched morphed photo



Miss Rate on non-morphed photos

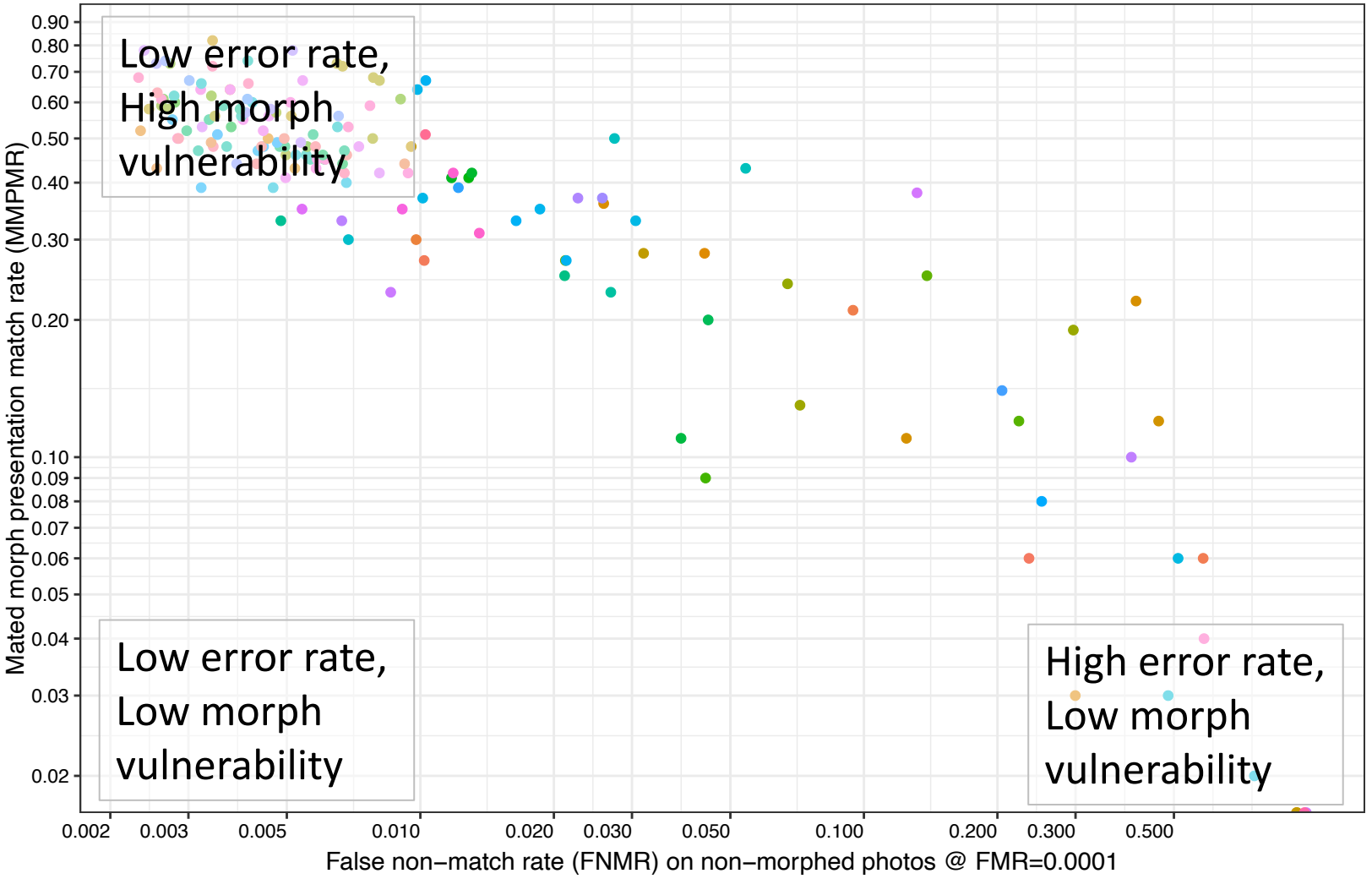


- 2-person morphs
- Subject alpha: 50% each
- Morphed within sex and ethnicity label groups
- Morphing Method:
  Local Colorized Match – Face area is averaged after alignment and feature warping. Subject A provides the periphery and face area is adjusted to match Subject A's color histogram.

- 2 692 comparisons of morphs w/ other portrait photos of constituents
- 90 million non-morphed comparisons on mugshot photos

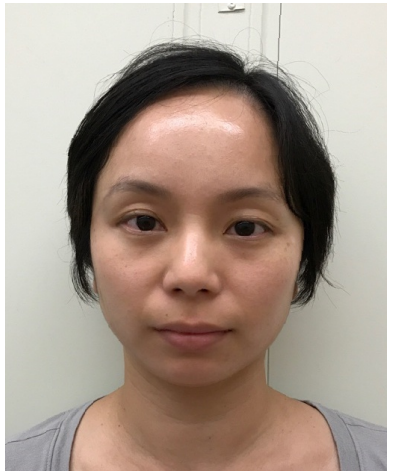
Current face recognition vulnerability

Each dot represents an FR algorithm from NIST Ongoing FRVT 1:1 Verification Test



Fraction of morphs where both subjects matched morphed photo

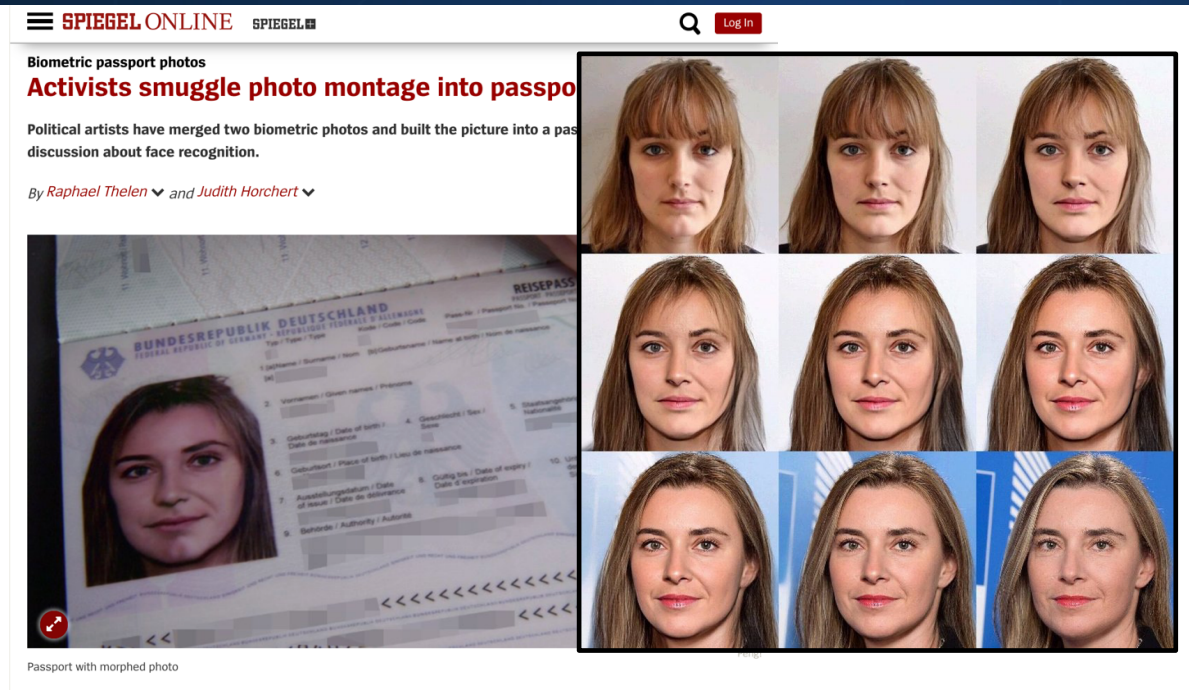
Miss Rate on non-morphed photos



- 2-person morphs
- Subject alpha: 50% each
- Morphed within sex and ethnicity label groups
- Morphing Method:
  Local Colorized Match – Face area is averaged after alignment and feature warping. Subject A provides the periphery and face area is adjusted to match Subject A's color histogram.

- 2 692 comparisons of morphs w/ other portrait photos of constituents
- 90 million non-morphed comparisons on mugshot photos

Morphing in the wild

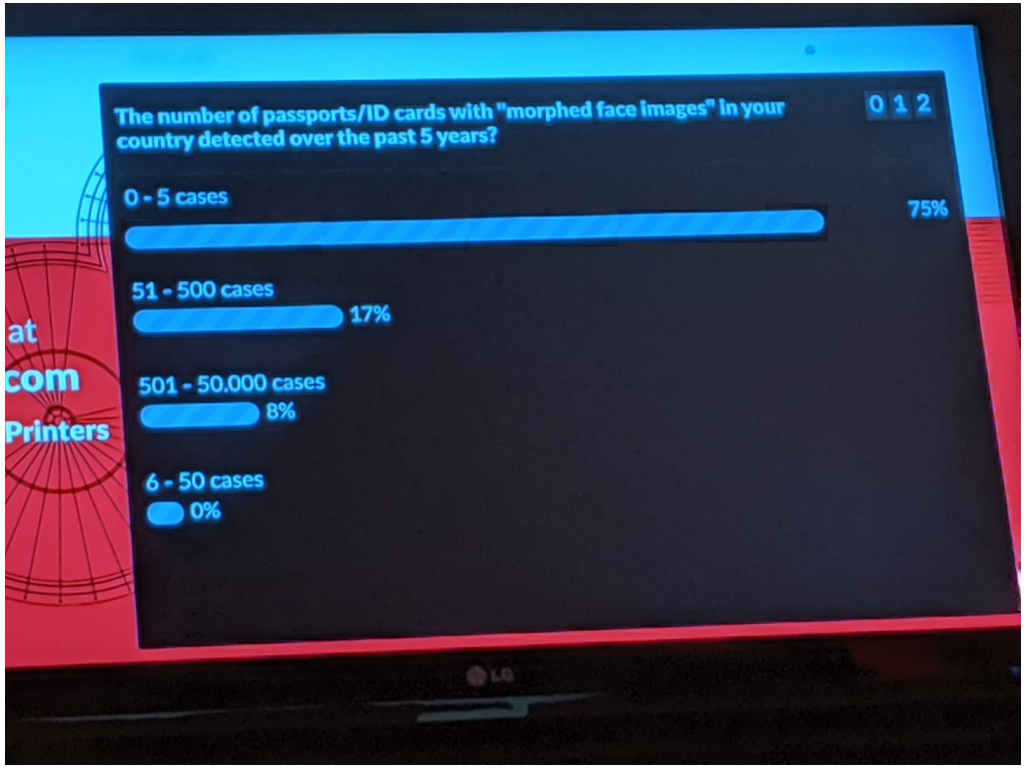


Passport with morphed photo

Sept. 22, 2018: Member of German activist group successfully applies for a passport with a morphed image (containing Federica Mogherini, High Representative of the Union for Foreign Affairs and Security Policy)

Source (9/22/2018): http://www.spiegel.de/netzwelt/netzpolitik/biometrie-im-reisepass-peng-kollektiv-schmuggelt-fotomontage-in-ausweis-a-1229418.html via Google Translate

How many morphed face images has your country detected over the past 5 years?



October 25, 2019: A poll from the Security Printers 2019 Conference, Copenhagen

NIST FRVT MORPH Evaluation [June 2018 – current]

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

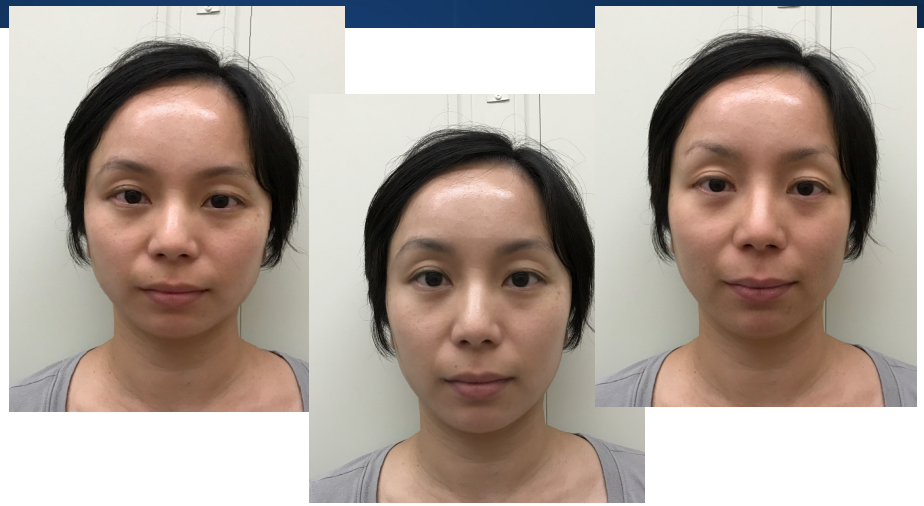
- Single-image morph detection
- Two-image differential morph detection
- 1:1 morph acceptance (FR resistance against morphing)

Collaborators

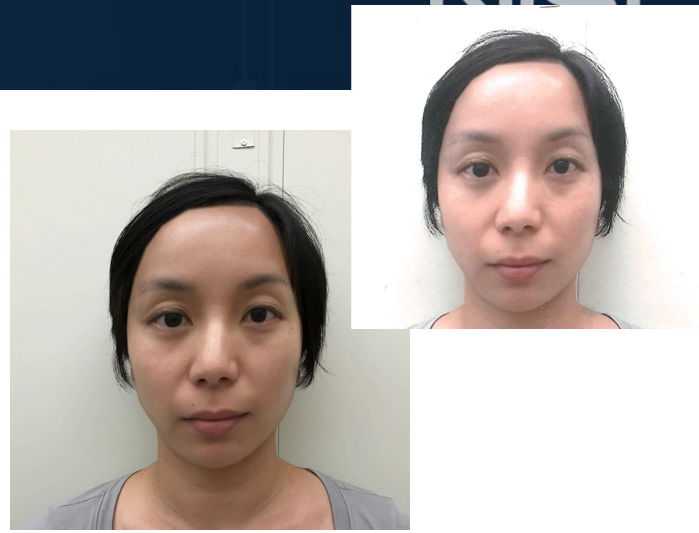
- Department of State, USA
- Otto von Guericke University of Magdeburg, Germany
- Australian Defence Science and Technology Group
- University of Lincoln, United Kingdom
- University of Bologna, Italy
- Hochschule Darmstadt
- Norwegian University of Science and Technology
- FBI and DHS S&T, USA

FRVT MORPH Report published as NIST Interagency Report 8292 (last updated July 2020)
Ongoing morph detection submissions accepted! Google: FRVT MORPH

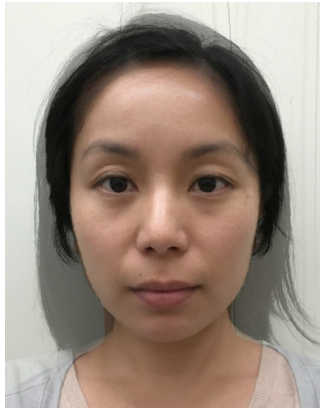
FRVT MORPH Test Data



From non-expert
tools + apps
Visible artifacts

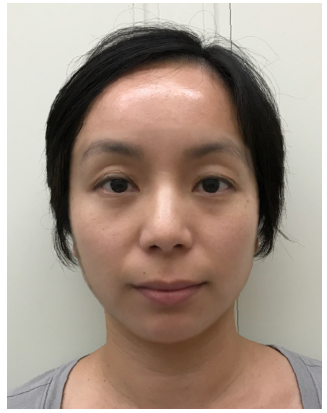


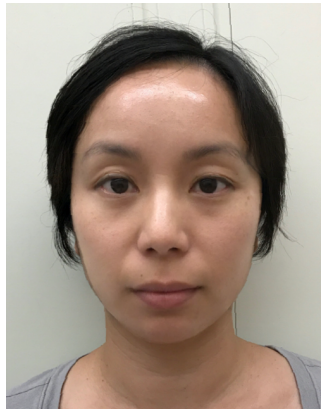
"Less sophisticated" morphs — *"More Sophisticated" morphs*



Source: NIST

From automated methods
Moderate to minimal artifacts





From commercial-graphics tools
Print + scanned
Very minimal artifacts

[1] Makrushin, A., Neubert, T., Dittmann, J., 2017. Automatic generation and detection of visually faultless facial morphs, In Proc. 12th Int. Joint Conf. on Computer Vision, Imaging and Computer Graphics Theory and Applications - Volume 6: VISAPP, pp. 39-50.

[2] Neubert, T., Makrushin, A., Hildebrandt, M., Kraetzer, C., Dittmann, J., 2018. Extended StirTrace Benchmarking of Biometric and Forensic Qualities of Morphed Face Images, IET Biometrics, Vol. 7, Issue 4, pp. 325-332.

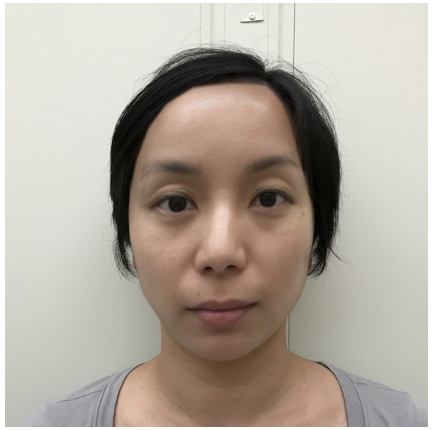
[3] M. Ferrara, A. Franco, and D. Maltoni, "Face Demorphing," IEEE Transactions on Information Forensics and Security, vol. 13, no. 4, pp. 1008-1017, April 2018.

[4] M. Ferrara, A. Franco, and D. Maltoni, "The Magic Passport," in IEEE International Joint Conference on Biometrics (IJCB), Clearwater, Florida, USA, 2014, pp. 1-7.

[5] M. Ferrara, A. Franco, and D. Maltoni, "On the Effects of Image Alterations on Face Recognition Accuracy," in Face Recognition Across the Electromagnetic Spectrum. Switzerland: Springer International Publishing, 2016, pp. 195-222.

[6] Robin S. S. Kramer, Michael O. Mireku, Tessa R. Flack, and Kay L. Ritchie. Face morphing attacks: Investigating detection with humans and computers. *Cognitive Research: Principles and Implications*, 4(1):28, 2019.

Use case #1: Single-Image Morph Detection
Morphed image or not?



Source: NIST

Use Case: Attack on enrollment

- Untrusted capture
- Upload to server

Protocol: Given **single image** X in isolation, produce

1) Morph decision => APCER, BPCER
2) "morphiness" score => DET analysis

Morphiness = F(X)

Evaluation: ISO/IEC 30107-3 metrics

- Attack Presentation Classification Error Rate (APCER): proportion of morph attack samples incorrectly classified as bona fide presentation (missed detection rate over morphed images) => **System Insecurity**
- Bona Fide Presentation Classification Error Rate (BPCER): proportion of bona fide samples incorrectly classified as morphed samples (false detection rate over non-morphed images) => **User Inconvenience**

Use case #2: Two-Image Differential Morph Detection
Morph detection given live image?

Use Case: Attack during verification (e.g., at eGate)

- Prior morph enrolled e.g. on identity document

Source: NIST

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

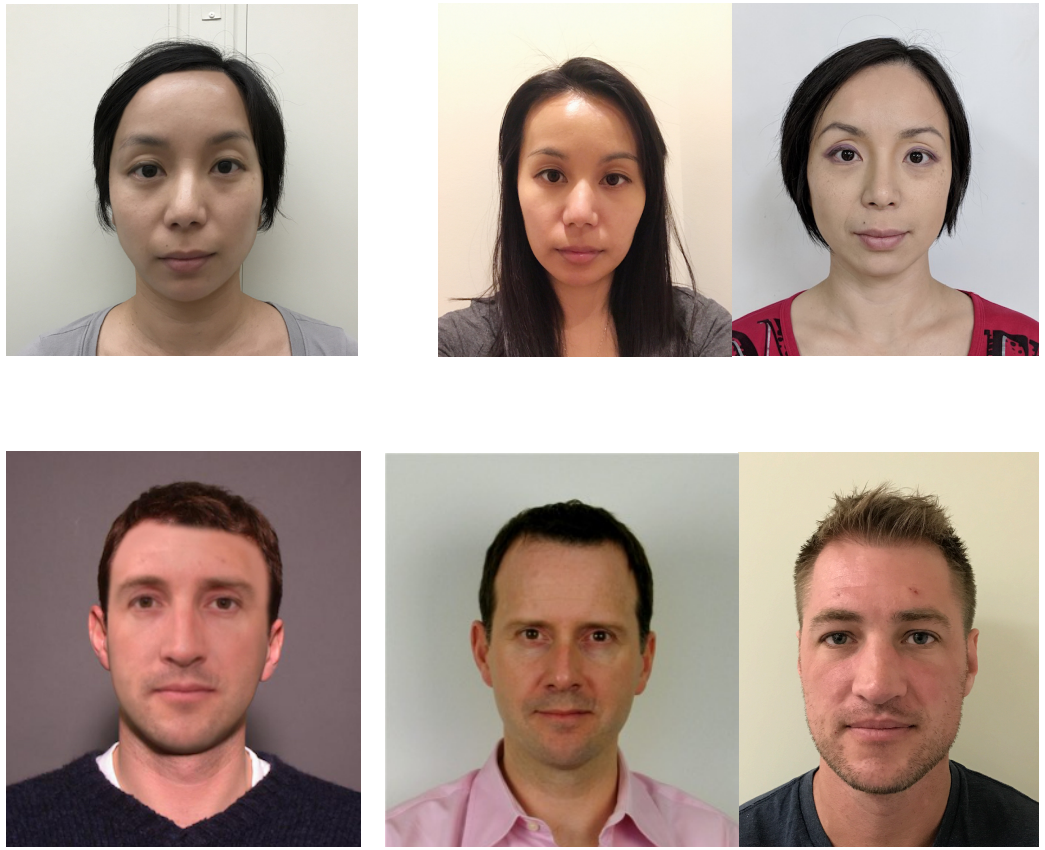
Protocol: Given suspected morph X and live image Y, produce

1) Morph decision
2) "morphiness" score

Evaluation: ISO/IEC 30107-3 metrics

- BPCER/False Detection Rate
- APCER/Morph Miss Rate

Use case #3: One-to-one Morph Acceptance
Do subjects verify against morphed 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
- False match rate

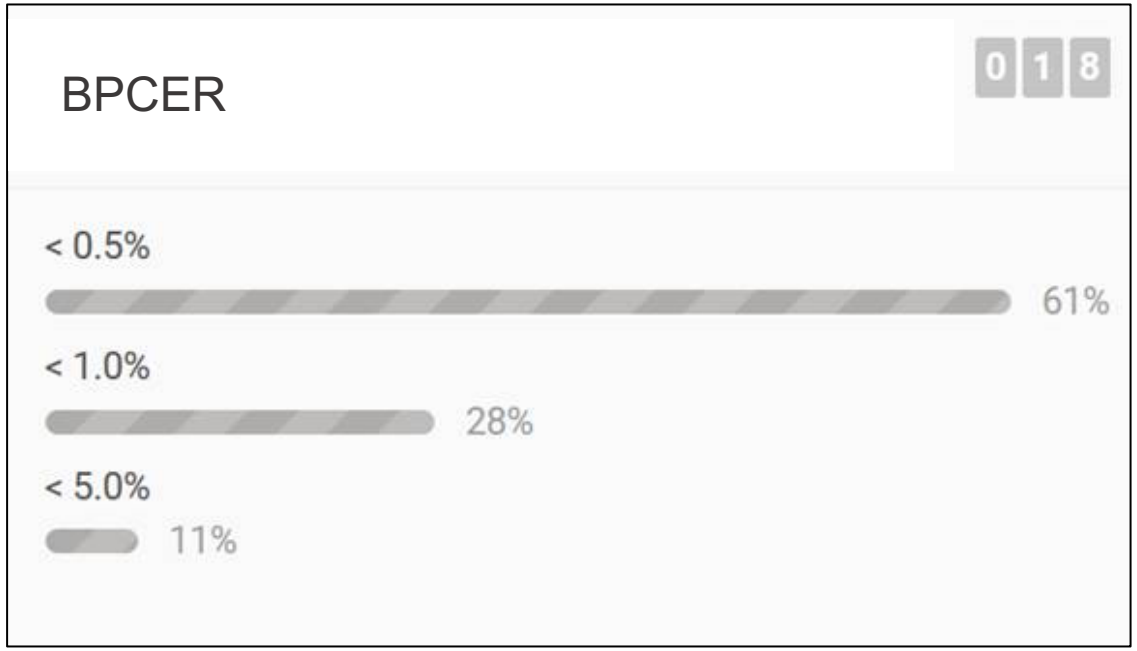
Involvement from commercial face recognition community!

FRVT MORPH Participation [June 2018 – current]

- Single-image morph detection – *9 submissions*
  - Hochschule Darmstadt
  - Norwegian University of Science and Technology
  - University of Bologna
- Two-image differential morph detection – *8 submissions*
  - Hochschule Darmstadt
- Currently all prototypes from European academic entities
- US DHS S&T sponsored CITeR research efforts
  - Clarkson University
  - West Virginia University
  - University at Buffalo

Measuring BPCER (false detection rates)

What false detection rates are operationally acceptable?



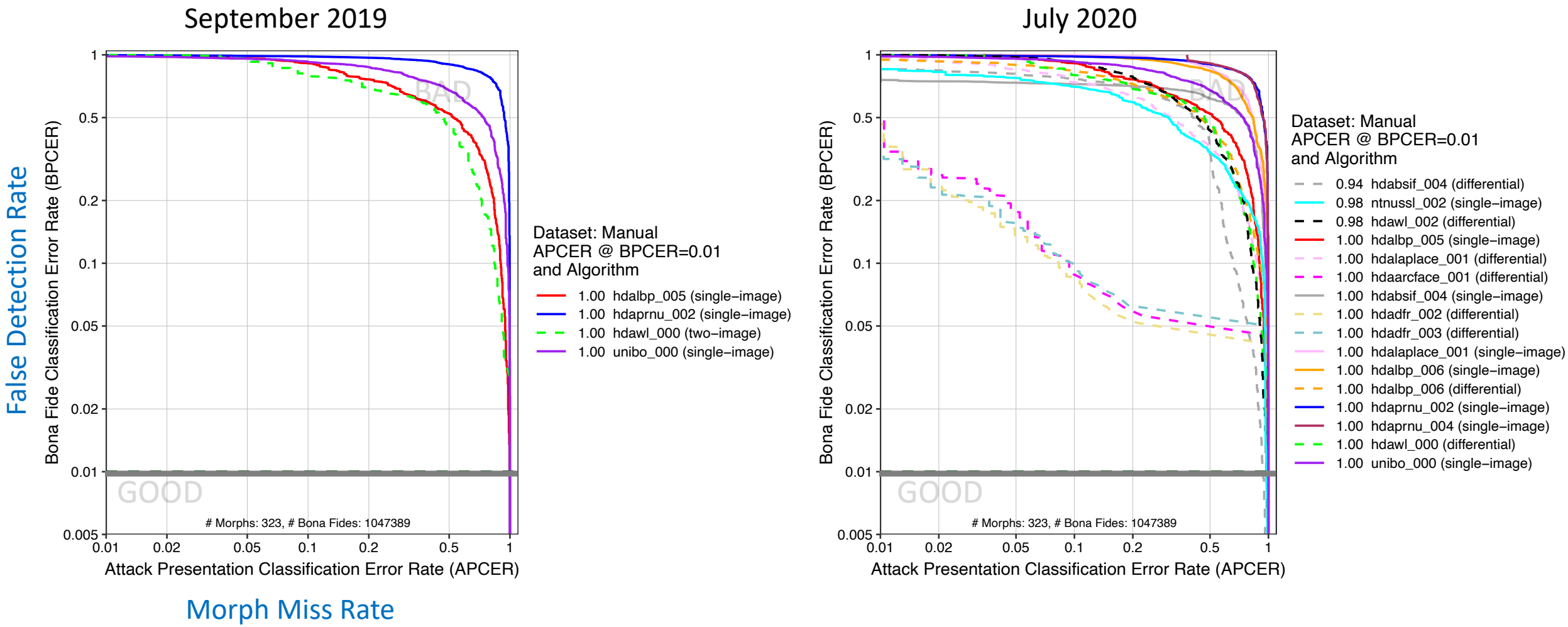
Source: Survey from participants of the ICBB 2019: Morphing and Morphing Attack Detection Methods Conference

Method: Use large sets of live-capture photos

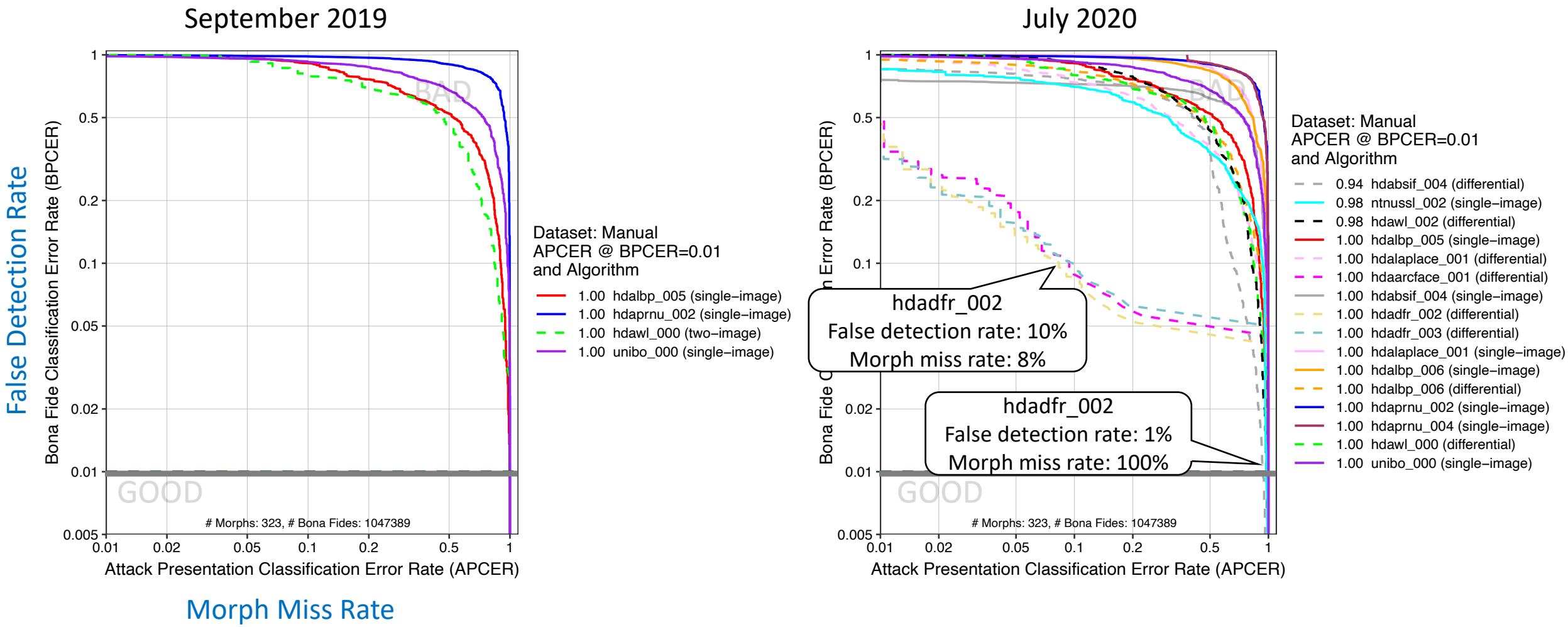
- Enables measurement of accuracy at low BPCER
- Bona fide datasets of
  - 1 047 389 live-capture mugshot photos
  - 871 984 live-capture visa photos

Goal: HIGH morph detection rates with LOW false detection rates

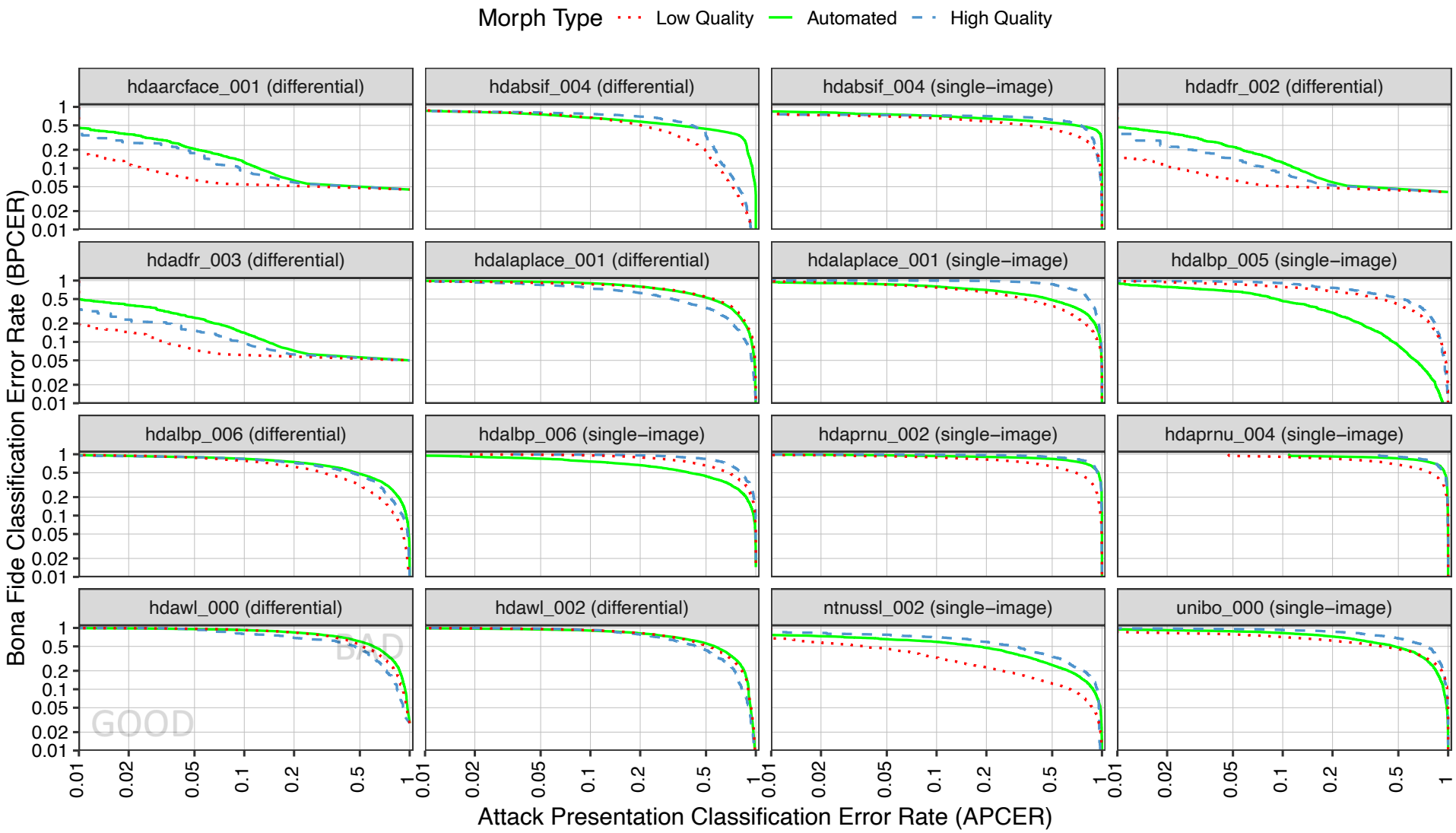
Accuracy gains since 2019



Accuracy gains since 2019



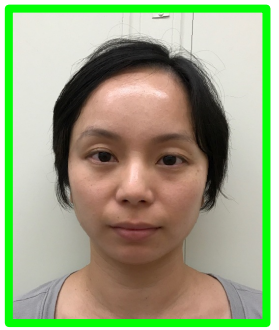
Are “less sophisticated” morphs easier to detect by algorithms?



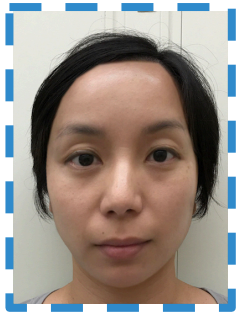
False Detection Rate

Morph Miss Rate

Low Quality

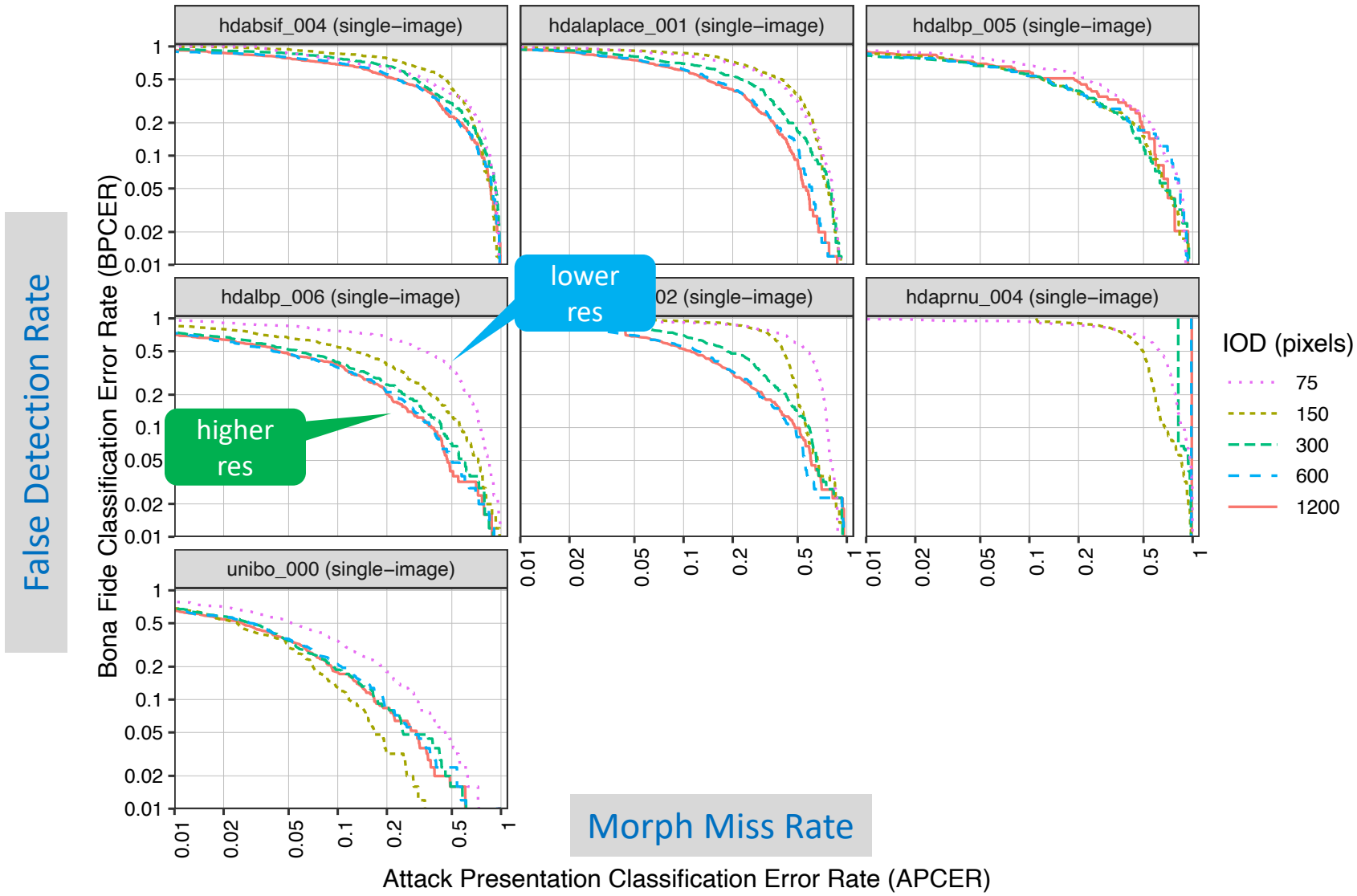


Automated



High Quality

Impact of Image Resolution - is bigger better?



Other Potential Mitigations

1 Live Enrollment

- E.g., Norway, Sweden
- Is it politically tenable in large countries?
- Doesn't address morphs that are already in circulation

2 Trusted external capture

- Signed photobooths
- Certified photographers (e.g., Ireland, France)

3 Eliminate print + scanned photos

Community consensus that print and scanned photos introduces artifacts that make it more difficult for humans and algorithms to do morph detection

4 Use FR on centralized database

- Perform 1:N duplicate check; look for multiple high scoring candidates
- Ineffective unless multiple subjects have been previously encountered

5 Awareness

Train relevant personnel about morphs!

Thank you!

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

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

FRVT 1:1 Verification: https://pages.nist.gov/frvt/html/frvt11.html
FRVT 1:N Identification: https://pages.nist.gov/frvt/html/frvt1N.html
FRVT MORPH: https://pages.nist.gov/frvt/html/frvt_morph.html
FRVT Quality Assessment: https://pages.nist.gov/frvt/html/frvt_quality.html
FRVT Face Masks: https://pages.nist.gov/frvt/html/frvt_facemask.html