Morphing Attack Detection

- Obstacles for Research to Deployment

On Behalf of EU H2020-ISF SOTAMD and iMARS Project

INTERNATIONAL FACE PERFORMANCE CONFERENCE
Oct 28, 2020

National Office for Identity Data
Ministry of the Interior and Kingdom Relations

Bundeskriminalamt

UNIVERSITY OF TWENTE.

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

NTNU

Acknowledgements (and Disclaimer)

Funded by the
European Union

This presentation was partially funded by the European Union's Internal Security Fund — Borders and Visa under the project SOTAMD and iMARS (Grant agreement ID: 883356).

The content of this presentation represents the views of the author only and is his sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

Threats on Face Recognition Systems (FRS) through Morphing

Morphing - Introduction

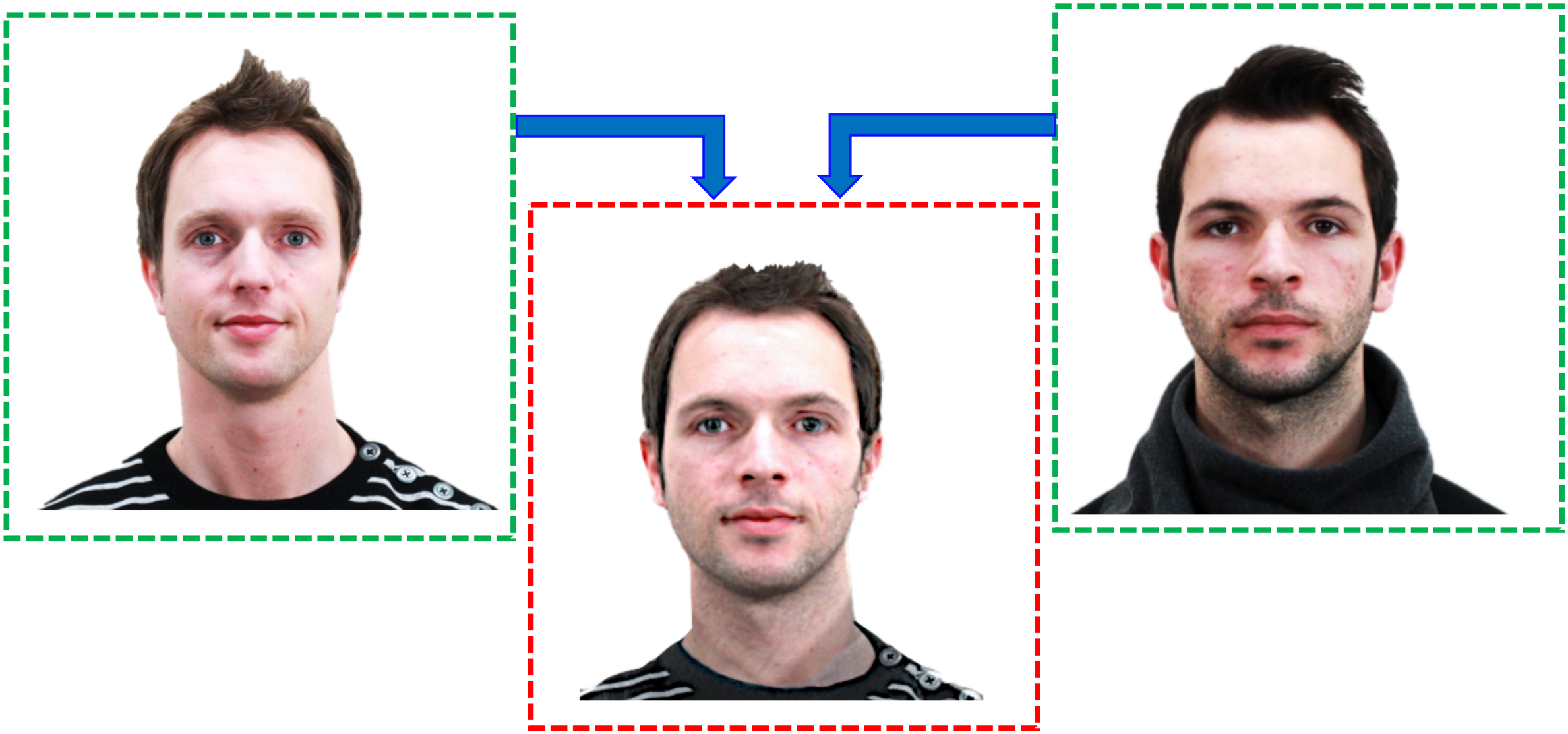
FRS

Score < Threshold

Verified -> Accept

Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Raghavendra, R., Kiran Raja, and Christoph Busch. "Detecting morphed face images." In 2016 IEEE BTAS, pp. 1-7. IEEE, 2016.

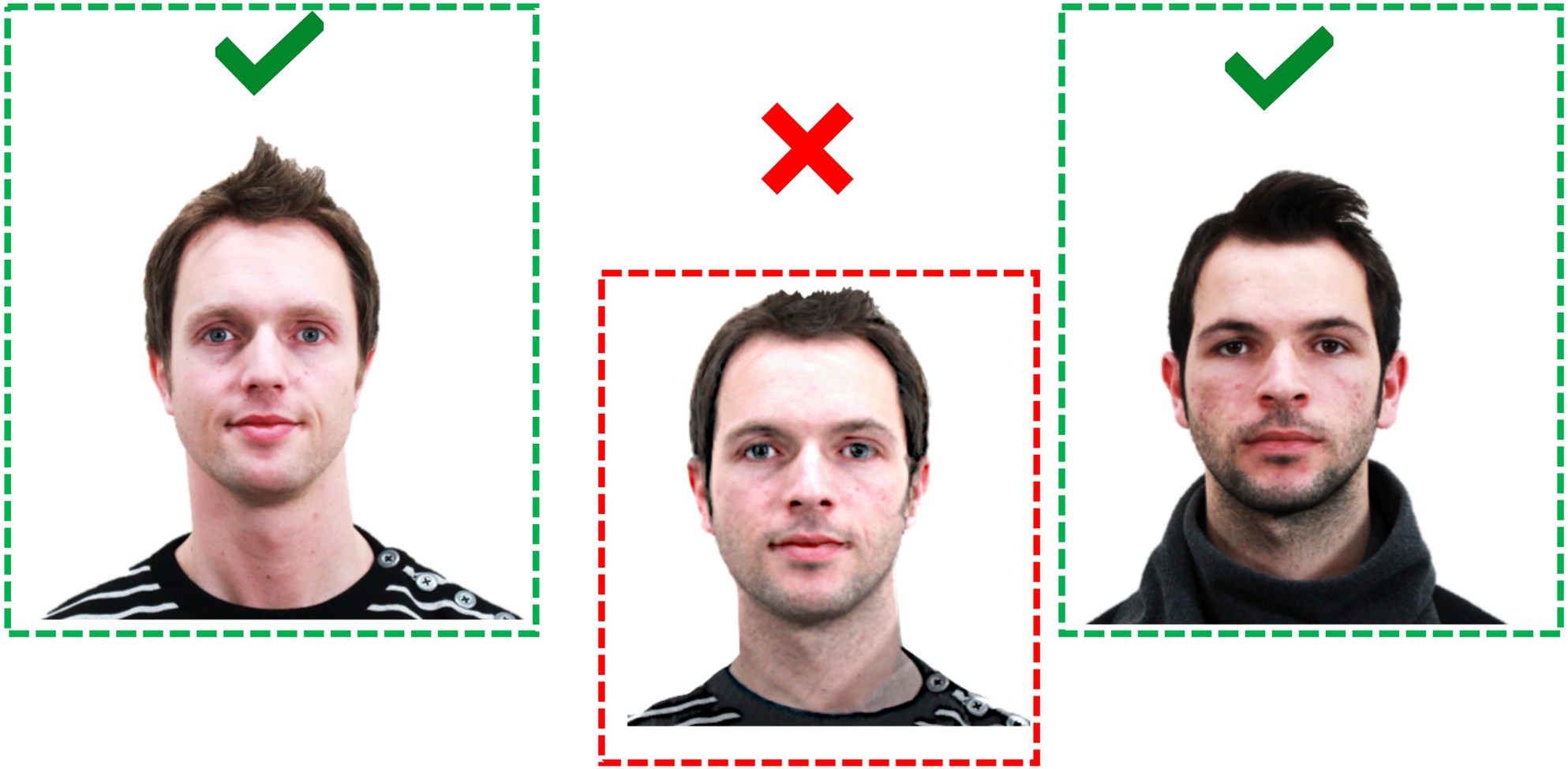
Morphing - Introduction



Morphing - Introduction

Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Raghavendra, R., Kiran Raja, and Christoph Busch. "Detecting morphed face images." In 2016 IEEE BTAS, pp. 1-7. IEEE, 2016.

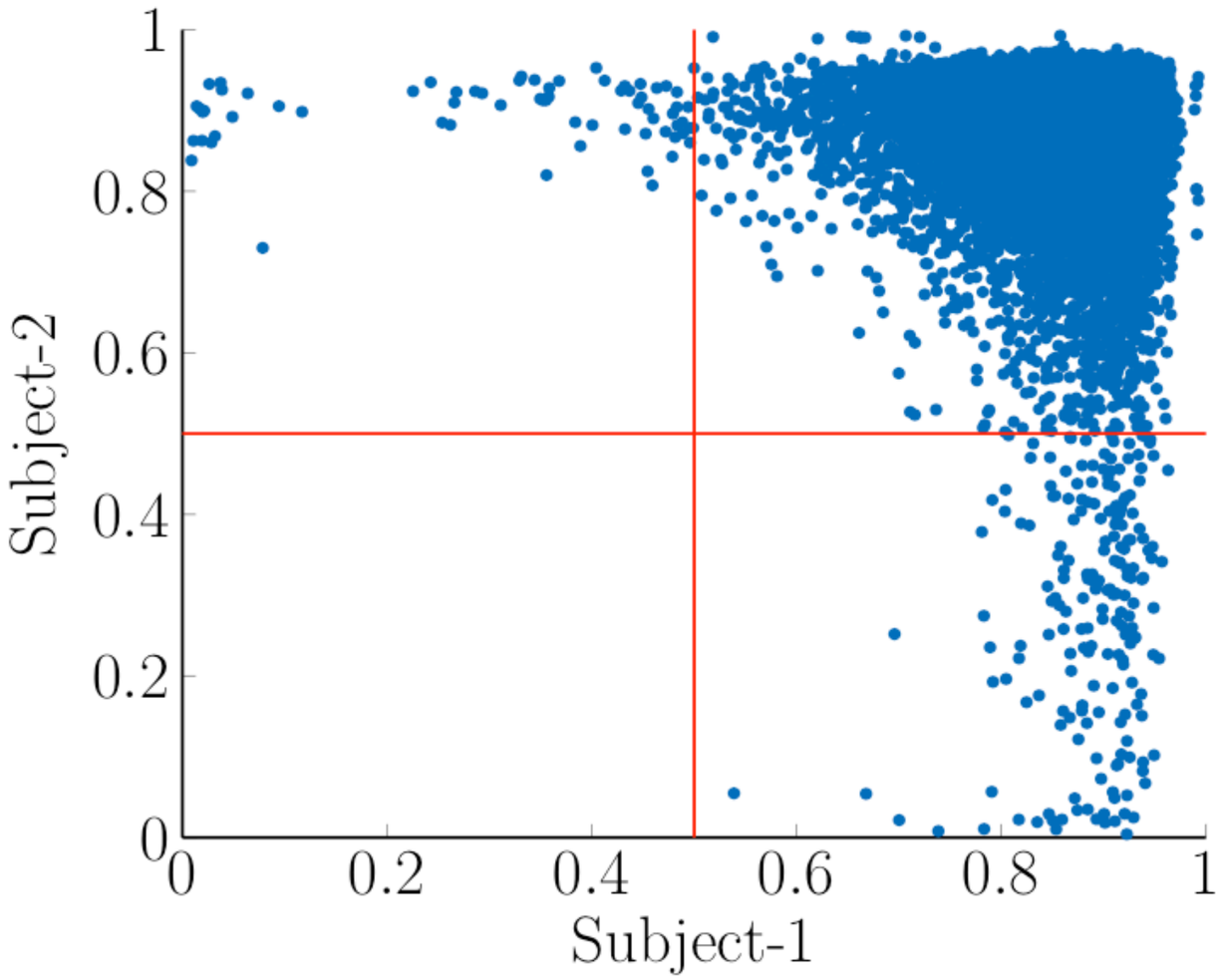
Impact of Morphing on FRS



FRS should accept the genuine and reject the morphed image

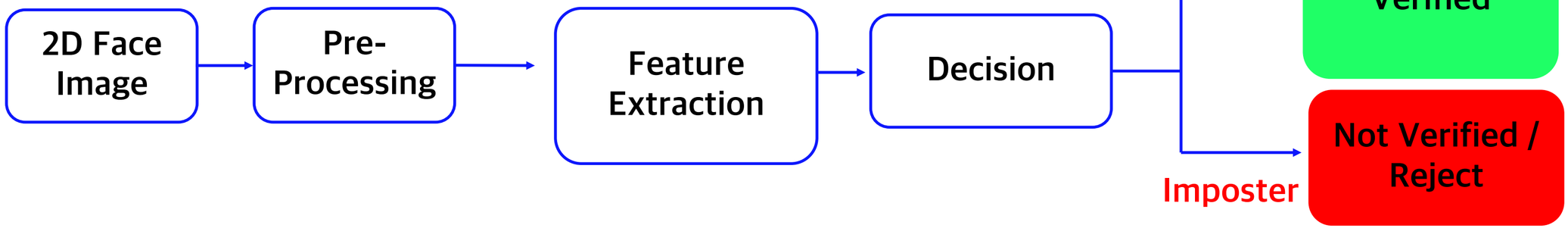
Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Raghavendra, R., Kiran Raja, and Christoph Busch. "Detecting morphed face images." In 2016 IEEE BTAS, pp. 1-7. IEEE, 2016.

Impact of Morphing on FRS



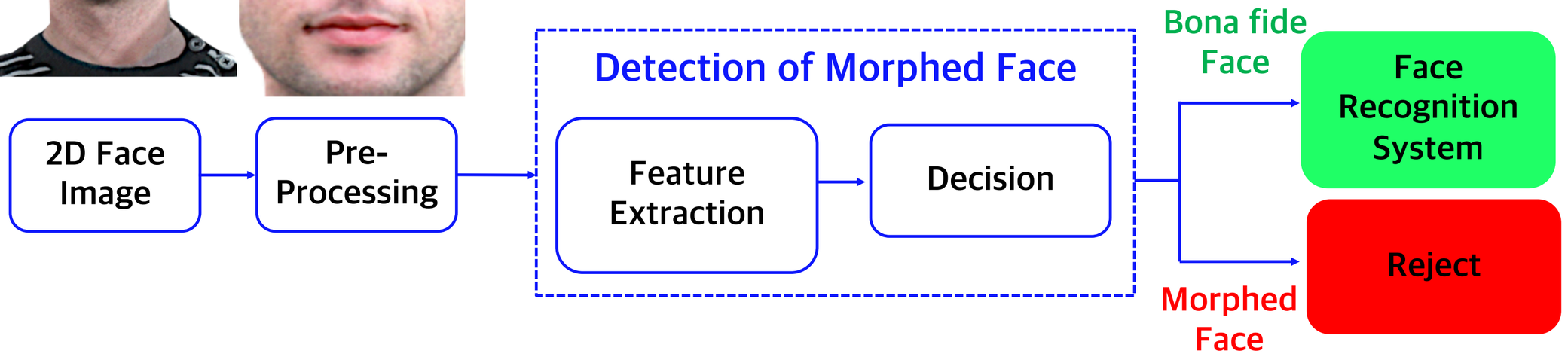
COTS FRS - Accepts both subjects equally, crosses the threshold at operating points of FAR=0.01%.

FRS



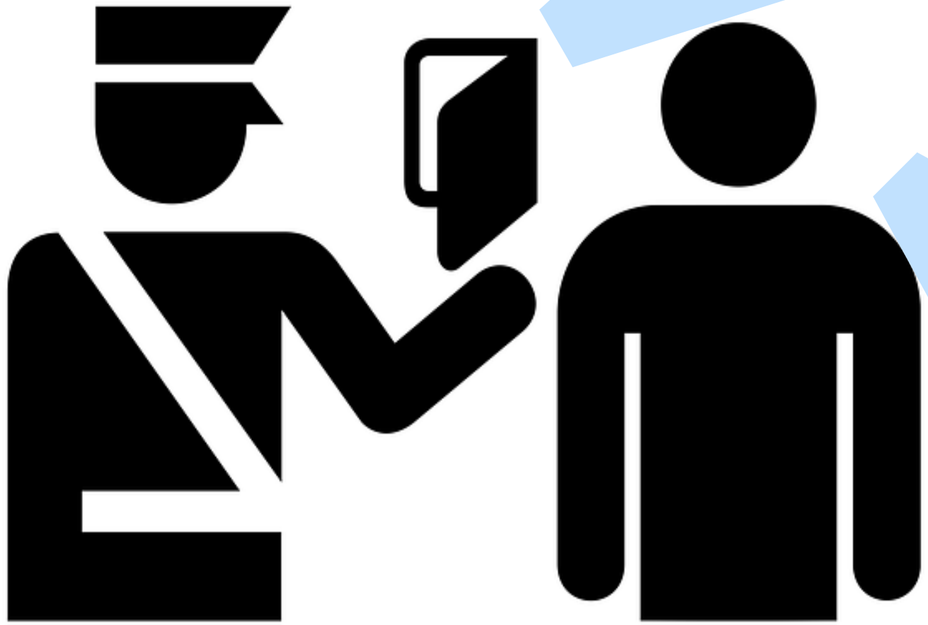
Ulrich Scherhag, Christian Rathgeb, Johannes Merkle, Ralph Breithaupt, Christoph Busch, Face Recognition Systems under Morphing Attacks: A Survey, in IEEE Access, 2019.
R. Raghavendra, K. B. Raja, and C. Busch. Detecting Morphed Face Images. In 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2016.

FRS - With MAD



Ulrich Scherhag, Christian Rathgeb, Johannes Merkle, Ralph Breithaupt, Christoph Busch, Face Recognition Systems under Morphing Attacks: A Survey, in IEEE Access, 2019.
R. Raghavendra, K. B. Raja, and C. Busch. Detecting Morphed Face Images. In 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2016.

Differential MAD (D-MAD) - Scenario



Detection of Morphed Face

Bona fide Face

Face Verified

Morphed Face

Face Not Verified

Differential MAD (D-MAD) - Operations

Detection of Morphed Face

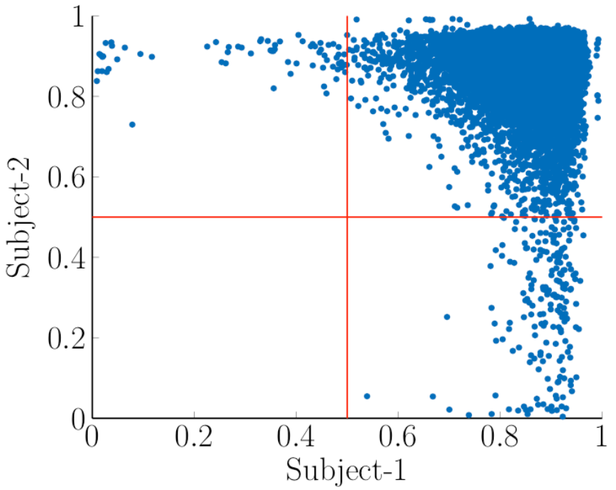
Bona fide Face

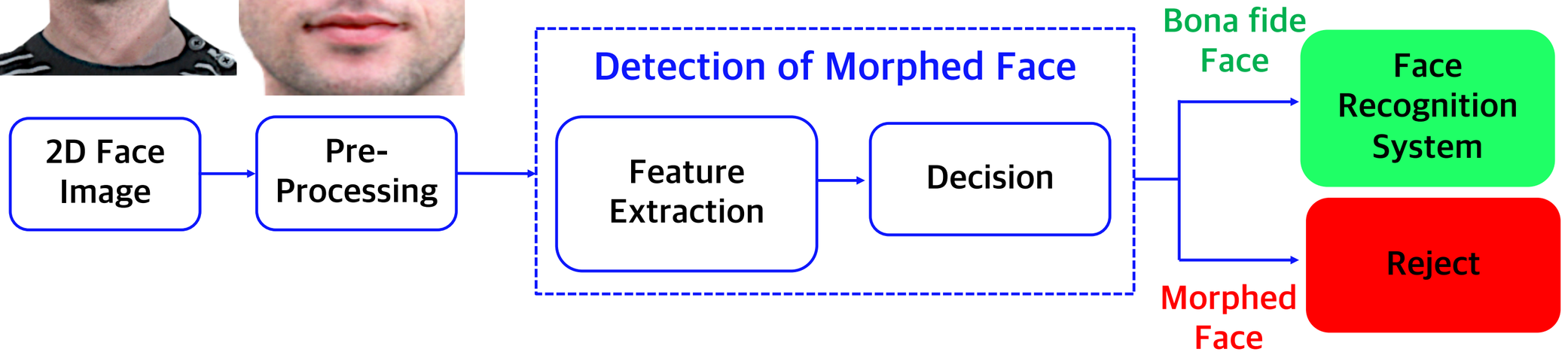
Face Recognition System

Morphed Face

Reject

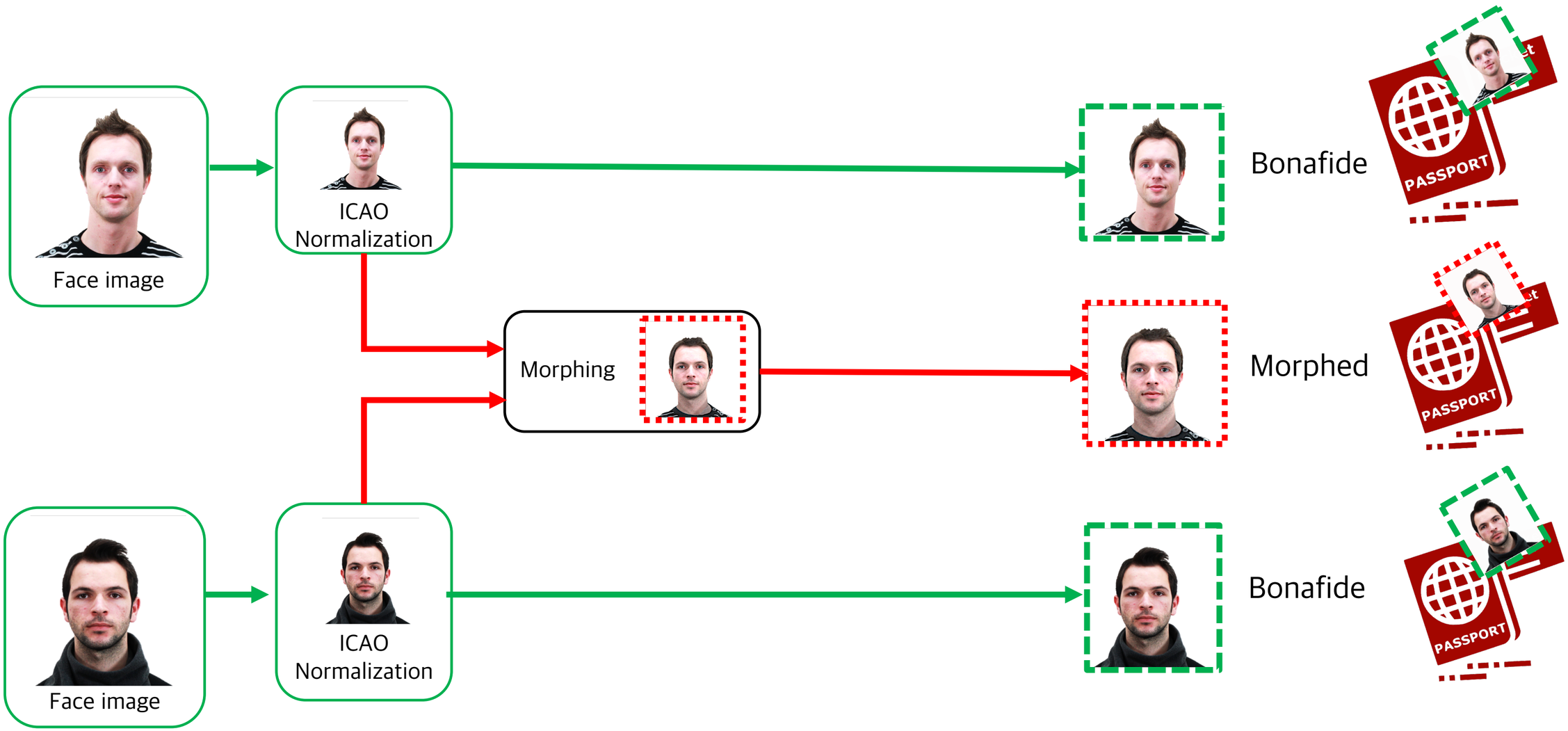
Morphing Attack Detection (MAD)





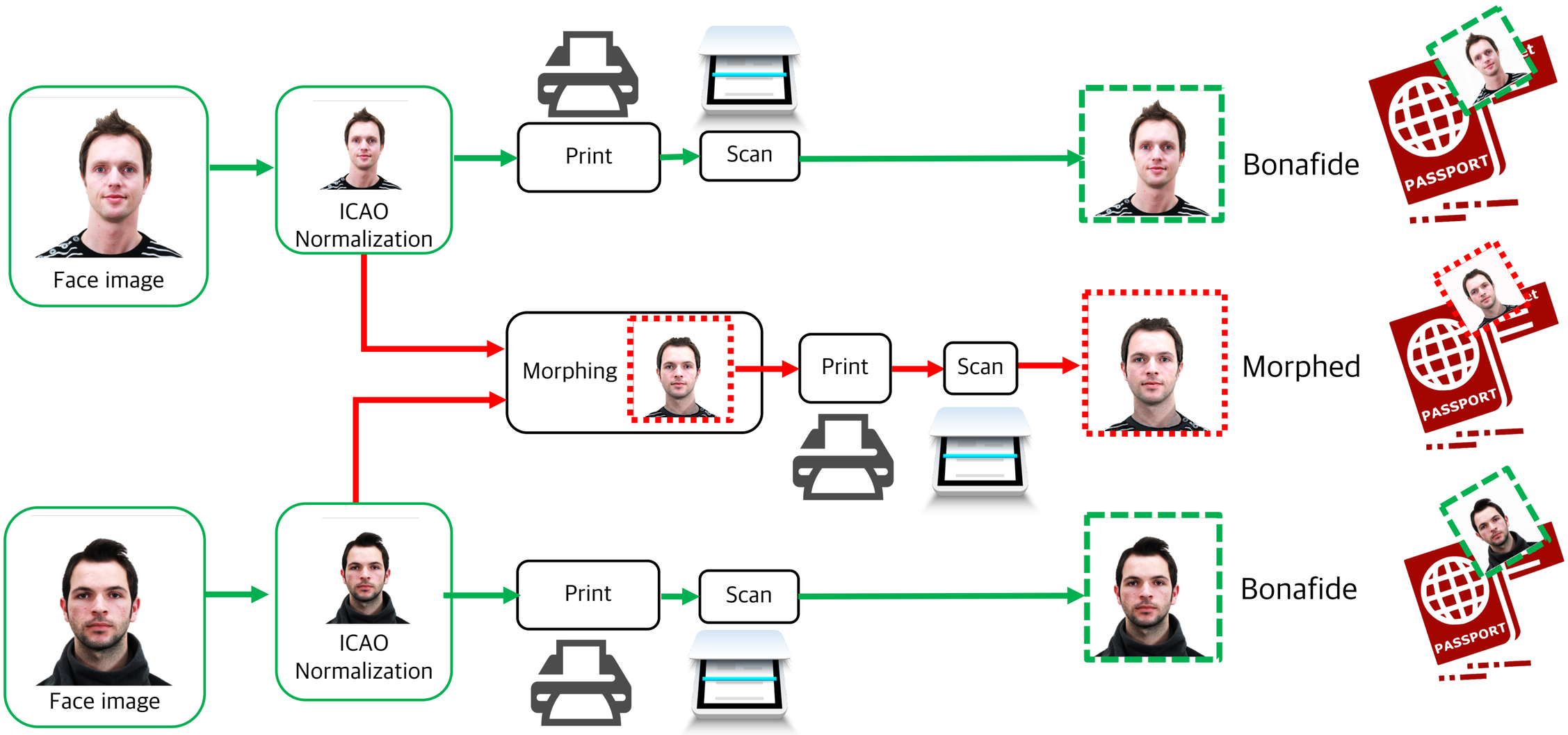
Ulrich Scherhag, Christian Rathgeb, Johannes Merkle, Ralph Breithaupt, Christoph Busch, Face Recognition Systems under Morphing Attacks: A Survey, in IEEE Access, 2019.
R. Raghavendra, K. B. Raja, and C. Busch. Detecting Morphed Face Images. In 8th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 2016.

Morphing Attacks - Challenges – Digital



Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Raghavendra, R., Kiran Raja, and Christoph Busch. "Detecting morphed face images." In 2016 IEEE BTAS, pp. 1-7. IEEE, 2016.

Morphing Attacks - Challenges - Re-digitized

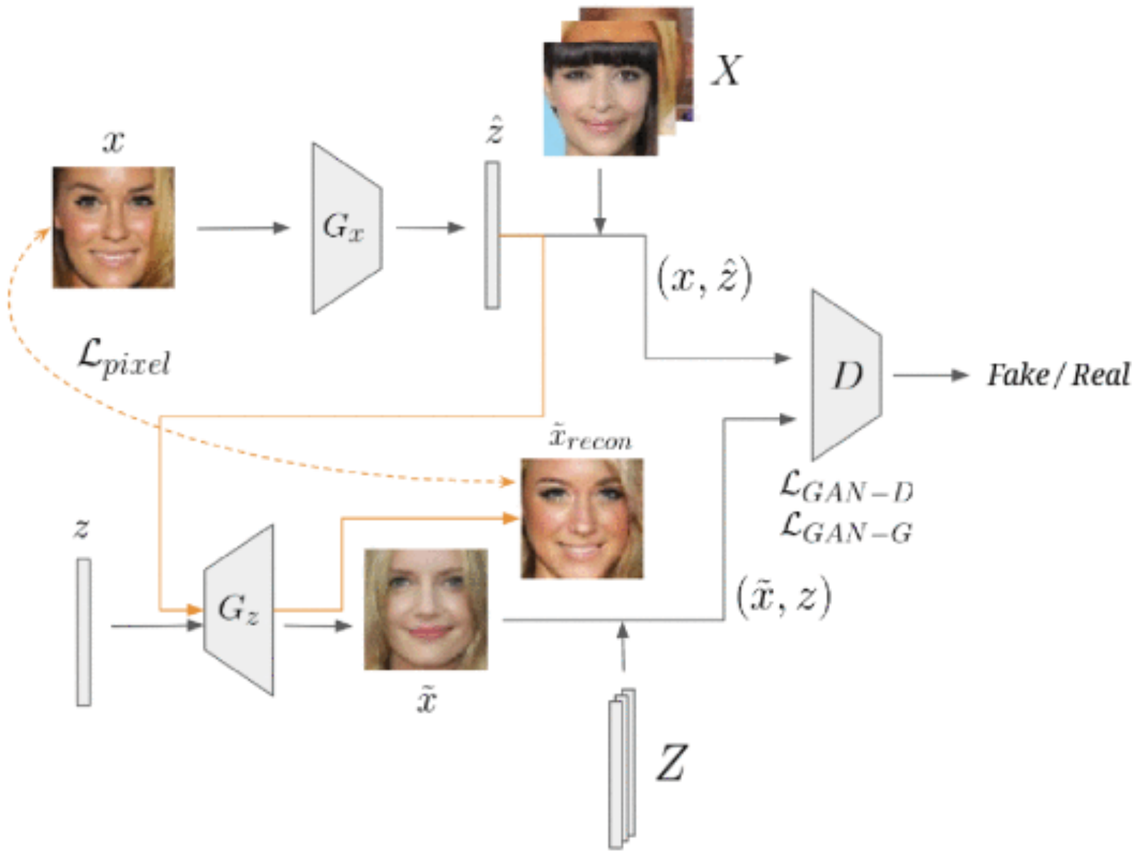


Raghavendra, R., Kiran Raja, Venkatesh, S., & Busch, C. (2017, October). Face morphing versus face averaging: Vulnerability and detection. In 2017 IEEE International Joint Conference on Biometrics (IJCB) (pp. 555-563). IEEE.

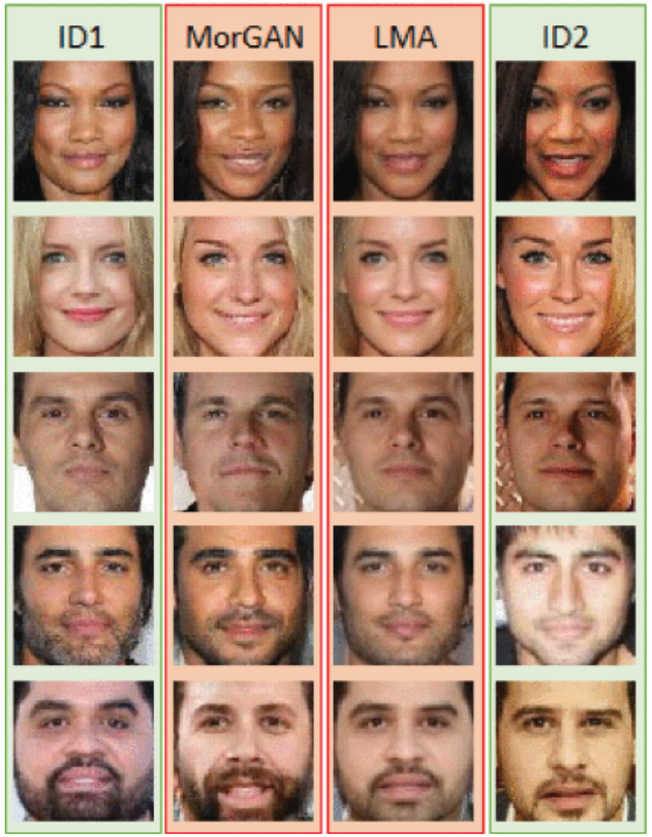
Obstacles for deployment

- Low cost, but effective attacks

GAN - Minimal Effort and Superior Attacks



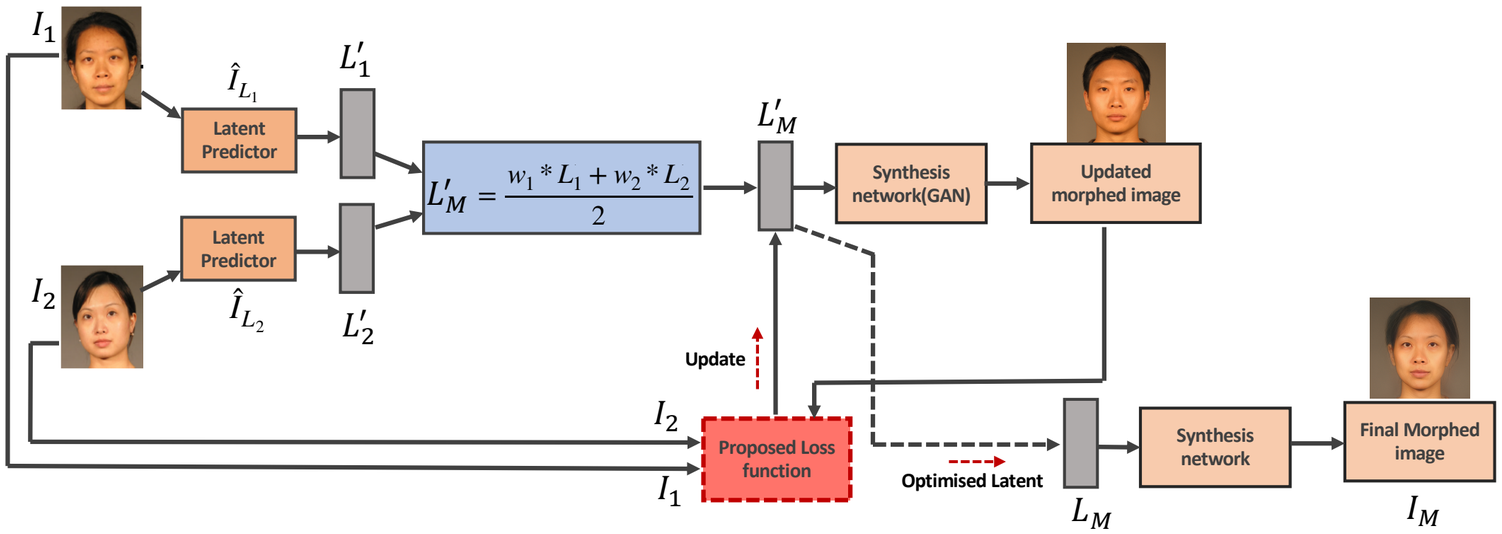
Morphing Process

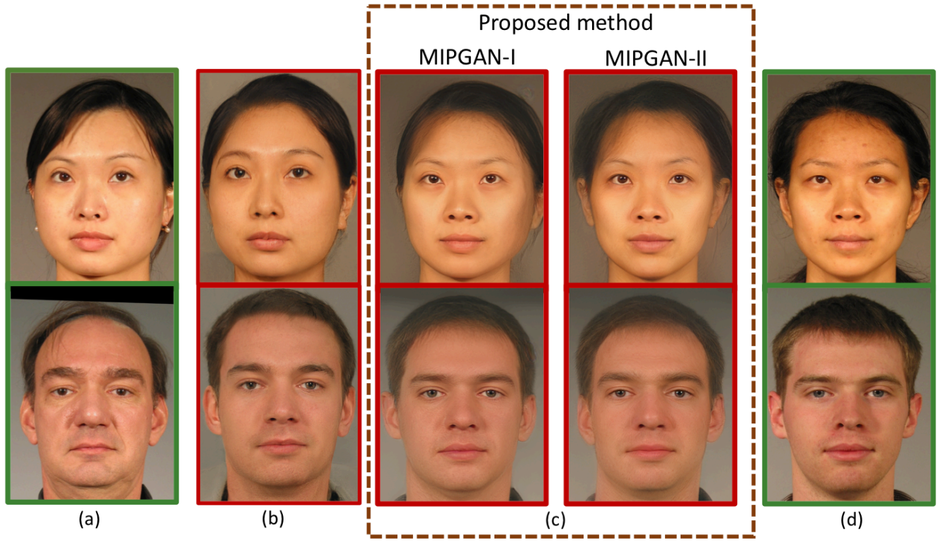


Example Morphed Images

Damer, N., Saladié, A. M., Braun, A., & Kuijper, A. (2018, October). MorGAN: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network. In 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1-10). IEEE.

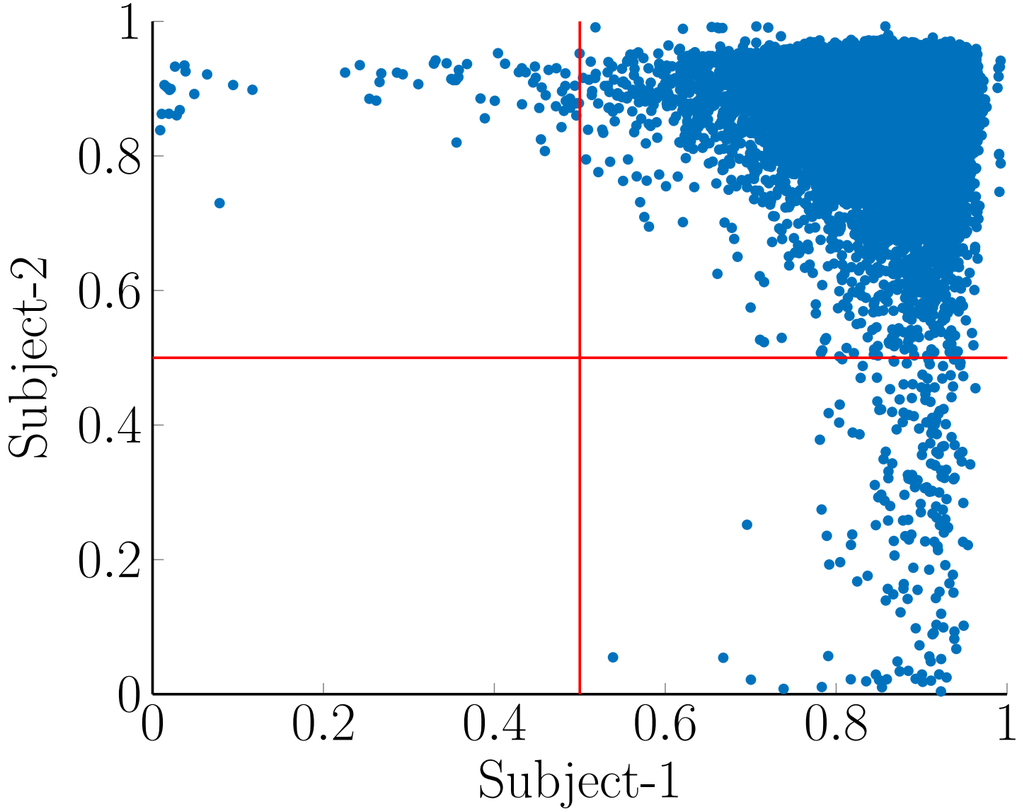
GAN - Minimal Effort and Superior Attacks



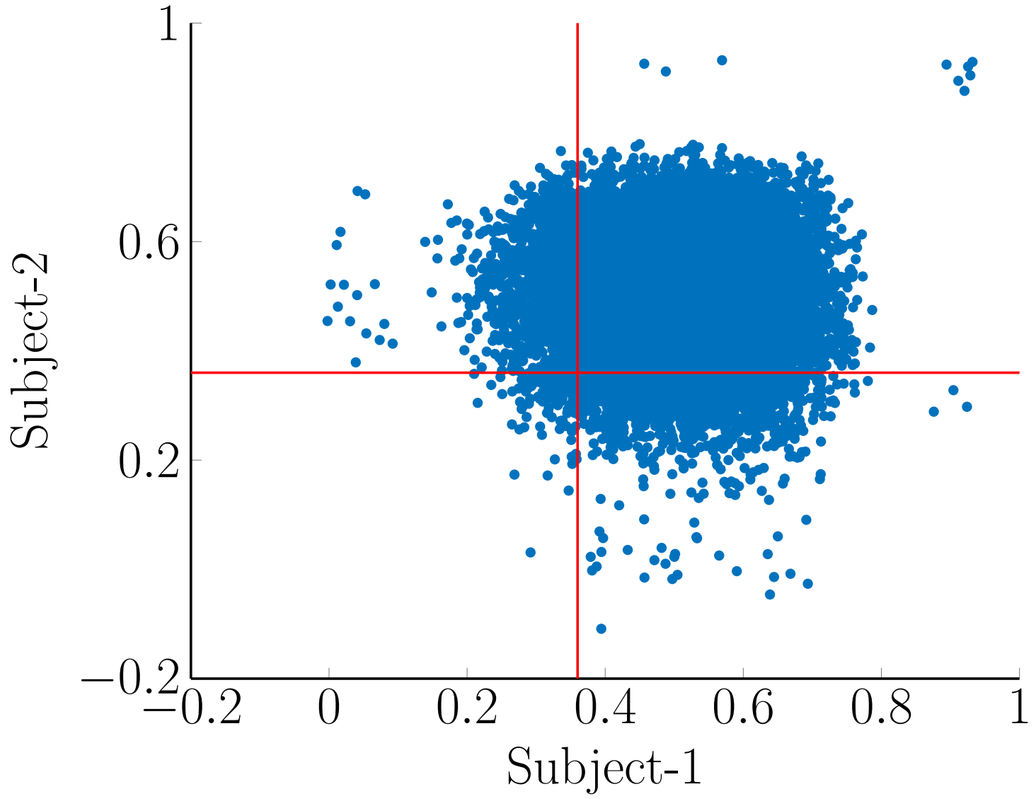


Zhang, Haoyu, Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, Naser Damer, and Christoph Busch. "MIPGAN--Generating Robust and High Quality Morph Attacks Using Identity Prior Driven GAN." arXiv e-prints(2020): arXiv-2009.

GAN - Minimal Effort and Superior Attacks



Landmark Based Morph Attacks

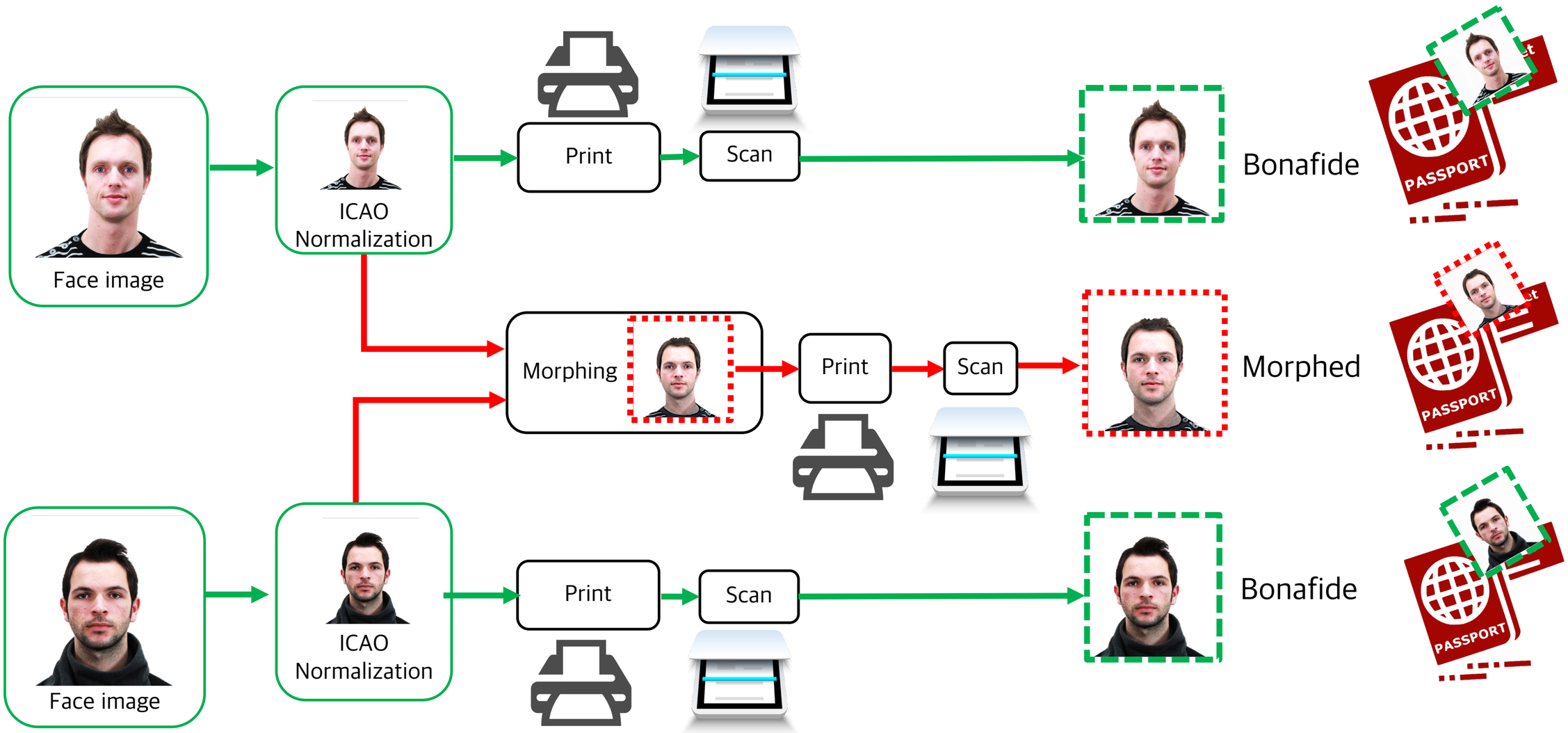


GAN Based Morph Attacks

Zhang, Haoyu, Sushma Venkatesh, Raghavendra Ramachandra, Kiran Raja, Naser Damer, and Christoph Busch. "MIPGAN--Generating Robust and High Quality Morph Attacks Using Identity Prior Driven GAN." arXiv e-prints(2020): arXiv-2009.

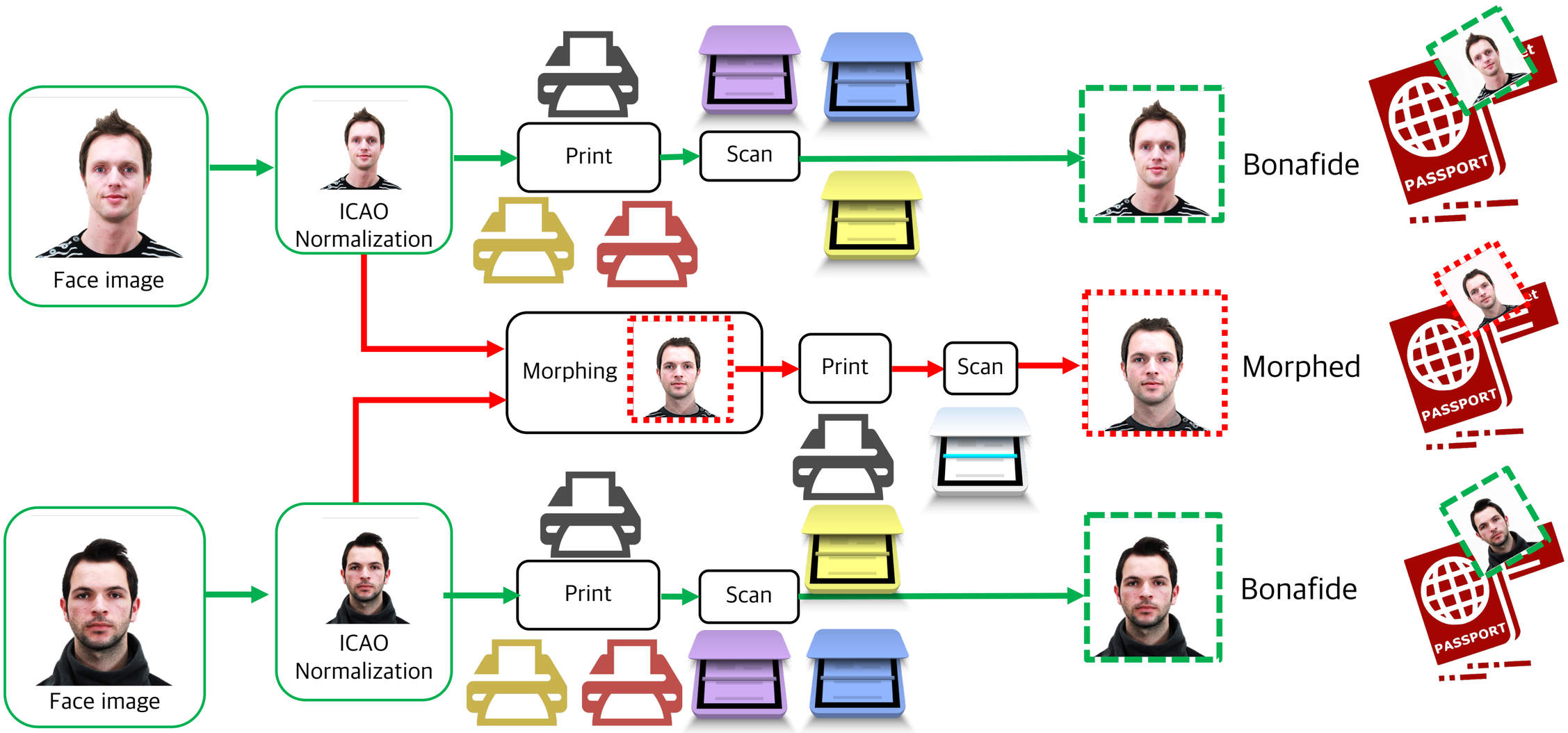
Obstacles for deployment
– Multiplicity of variates

Morphing Attacks - Challenges - Re-digitized



Raghavendra, R., Kiran Raja, Venkatesh, S., & Busch, C. (2017, October). Face morphing versus face averaging: Vulnerability and detection. In 2017 IEEE International Joint Conference on Biometrics (IJCB) (pp. 555-563). IEEE.

Morphing Attacks - Challenges - Re-digitized



Raghavendra, R., Kiran Raja, Venkatesh, S., & Busch, C. (2017, October). Face morphing versus face averaging: Vulnerability and detection. In 2017 IEEE International Joint Conference on Biometrics (IJCB) (pp. 555-563). IEEE.

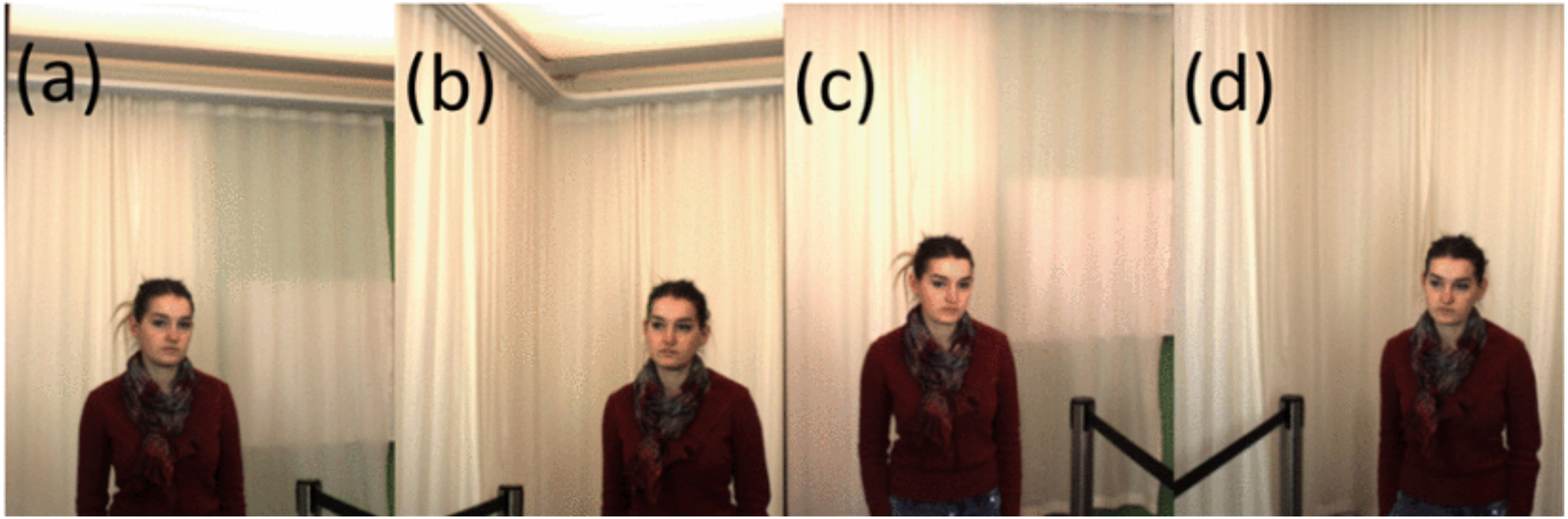
Obstacles for deployment
– Scenario challenges

Morphing Threats - Operational Constraints

ABC Gate operational scenario testing

Raghavendra, Ramachandra, Kiran B. Raja, Bian Yang, and Christoph Busch. "Automatic face quality assessment from video using gray level co-occurrence matrix: An empirical study on automatic border control system." In 2014 22nd International Conference on Pattern Recognition, pp. 438-443. IEEE, 2014.

MAD in Operational Scenario



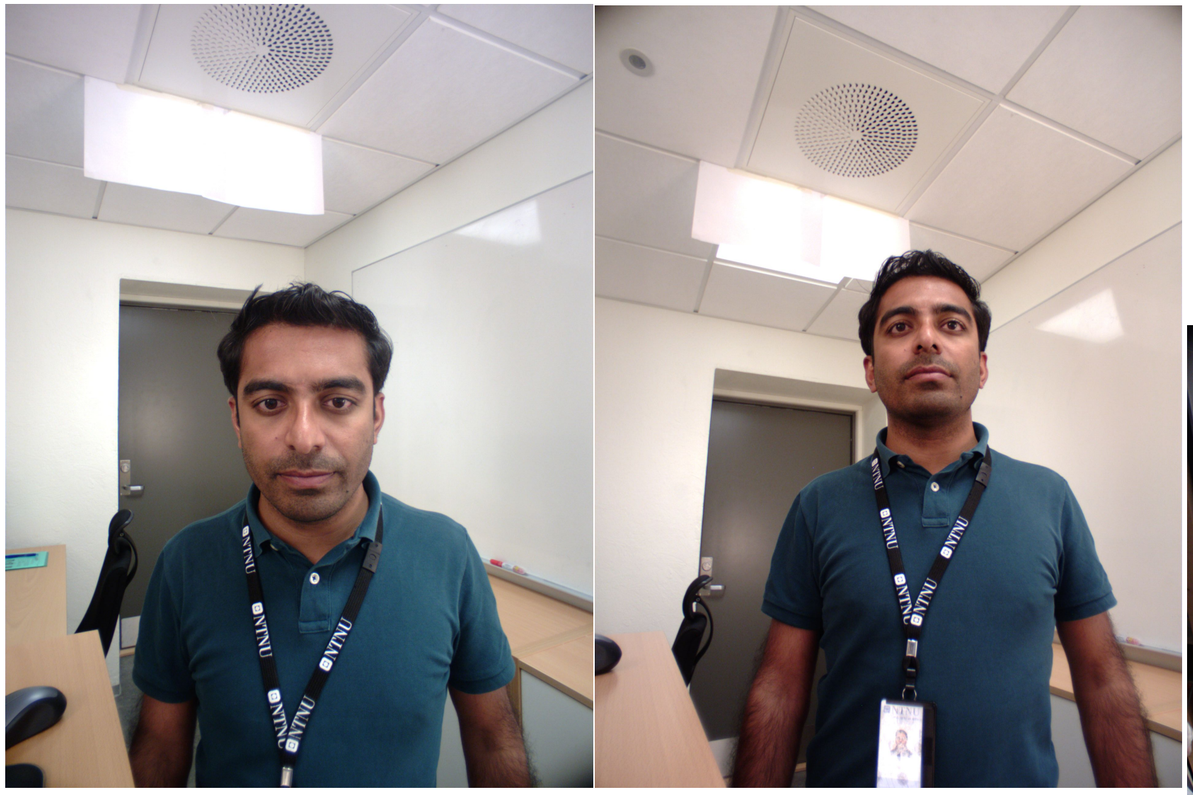
Images acquired from different cameras of ABC system

Raghavendra, Ramachandra, Kiran B. Raja, Bian Yang, and Christoph Busch. "Automatic face quality assessment from video using gray level co-occurrence matrix: An empirical study on automatic border control system." In 2014 22nd International Conference on Pattern Recognition, pp. 438-443. IEEE, 2014.

MAD in Operational Scenario - Unsolved

Top camera

Bottom camera

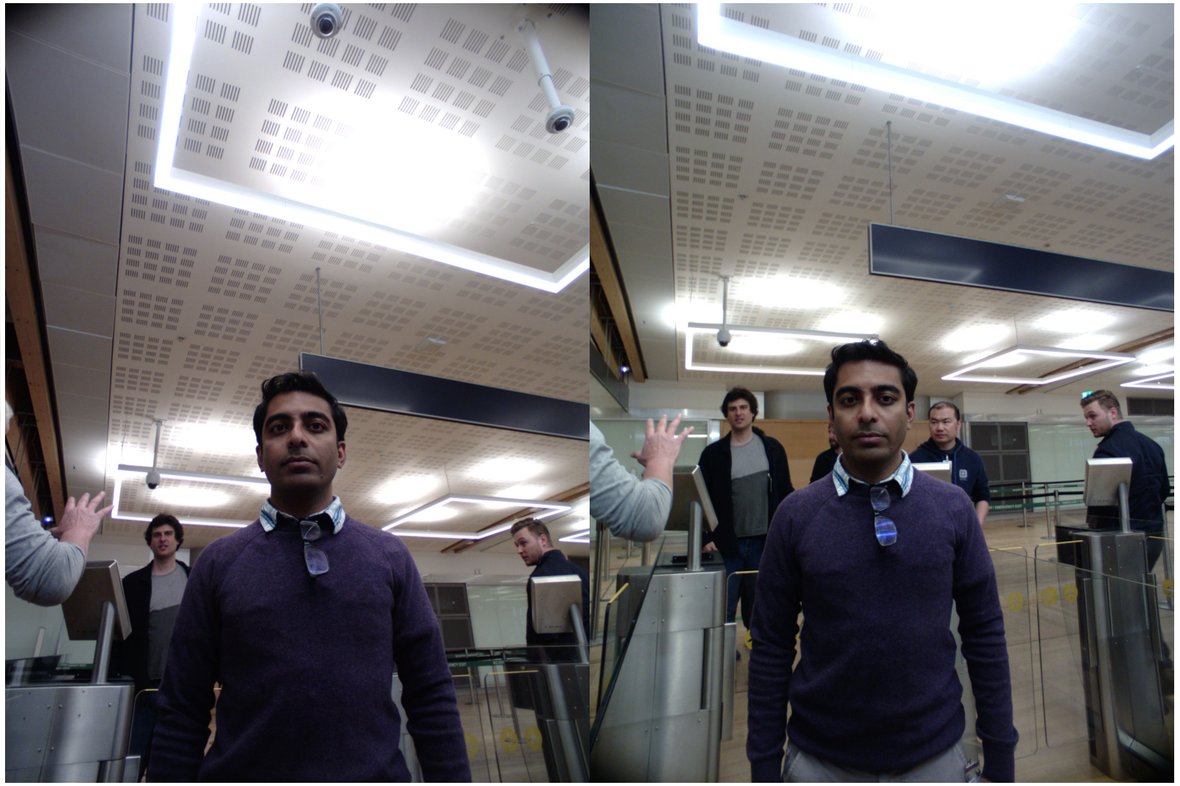


Laboratory Set-up

Realistic Operational Scenario

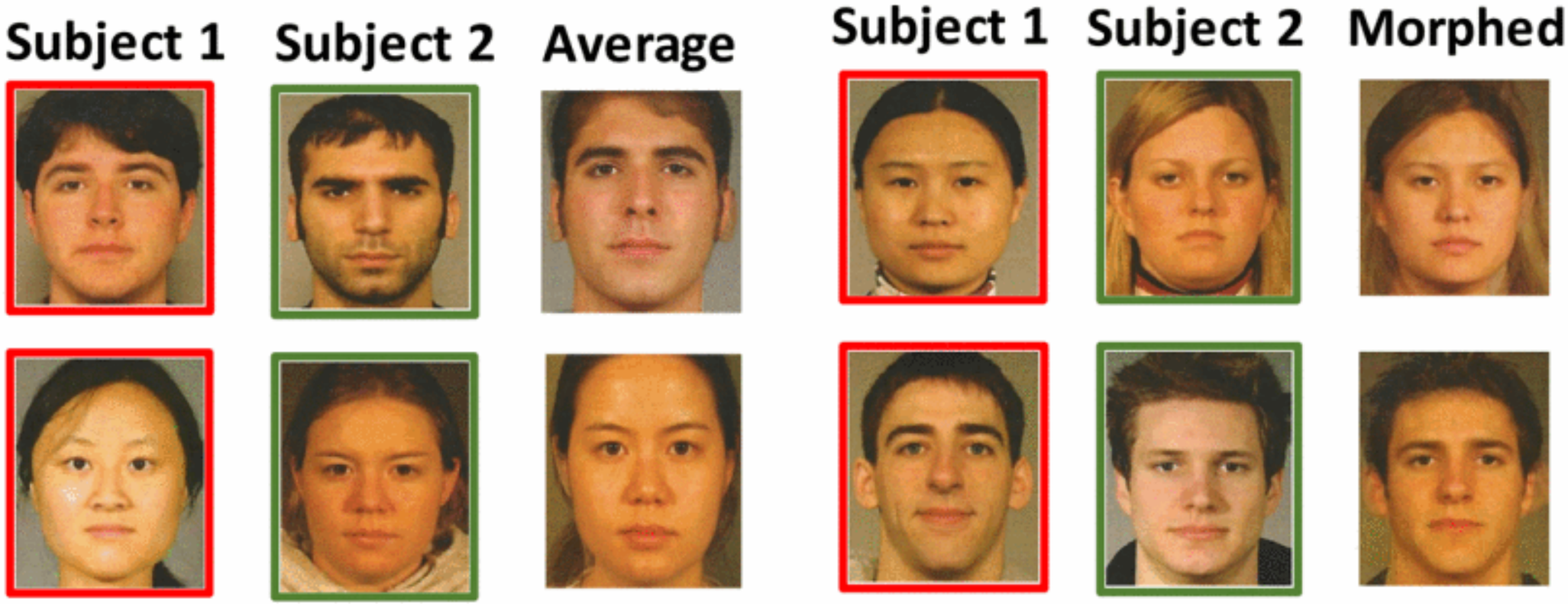
Bottom camera

Top camera



Obstacles for deployment
– Ethnicity, Age and Gender Challenges

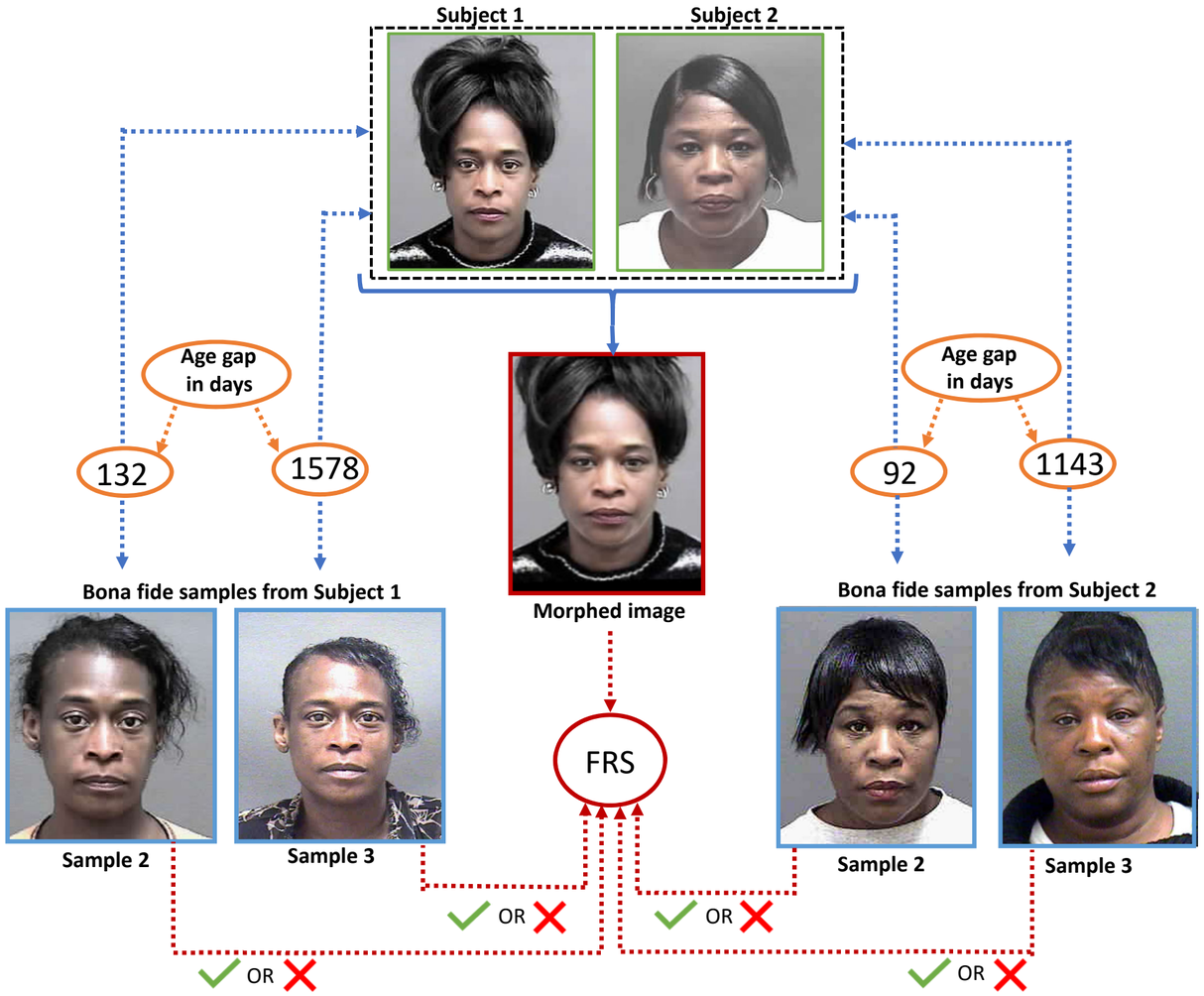
Ethnicity, Age and Gender

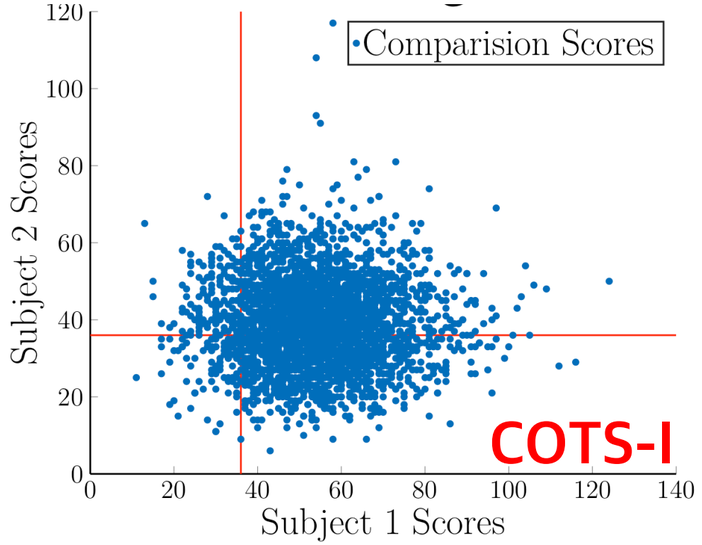


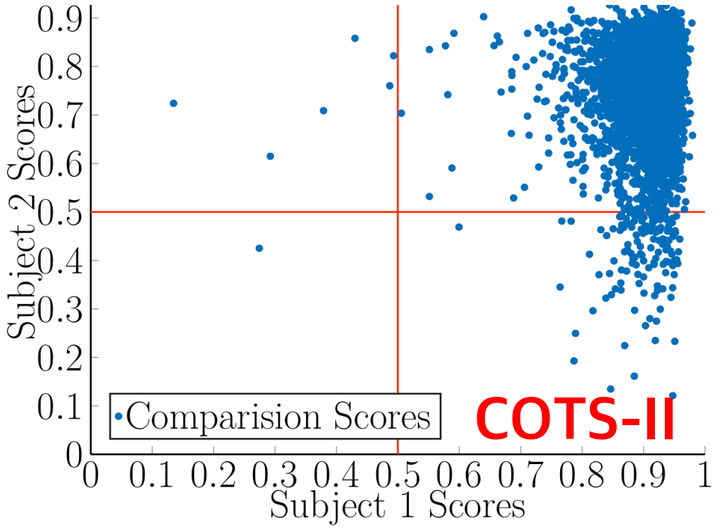
Impact of Ethnicity and Age on Morphing Creation

Raghavendra, R., Kiran Raja, Sushma Venkatesh, and Christoph Busch. "Face morphing versus face averaging: Vulnerability and detection." In 2017 IEEE International Joint Conference on Biometrics (IJCB), pp. 555-563. IEEE, 2017.

Ageing and Passport Lifecycle

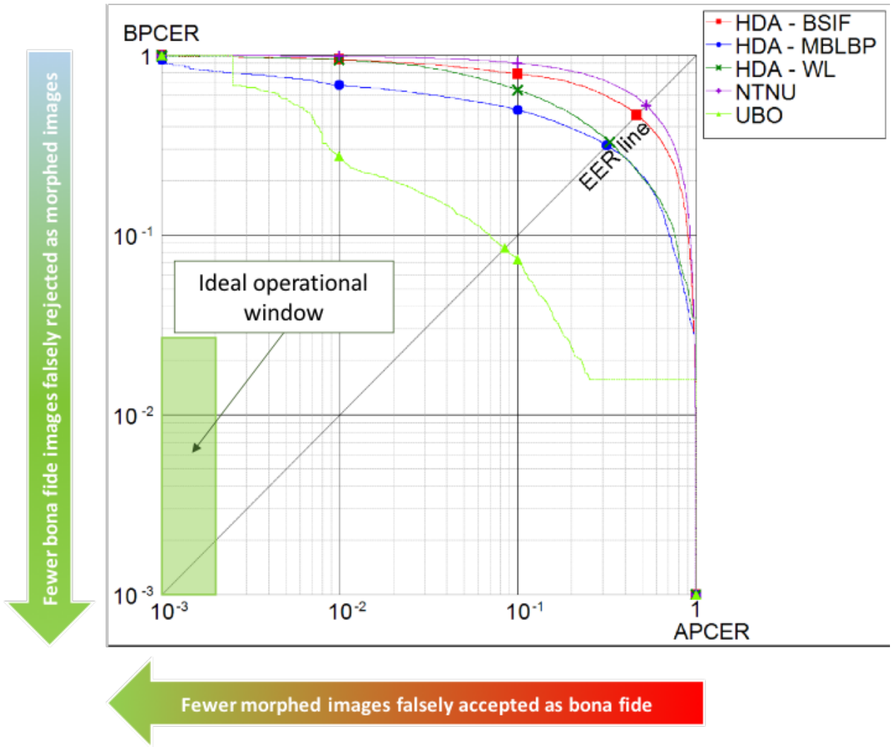




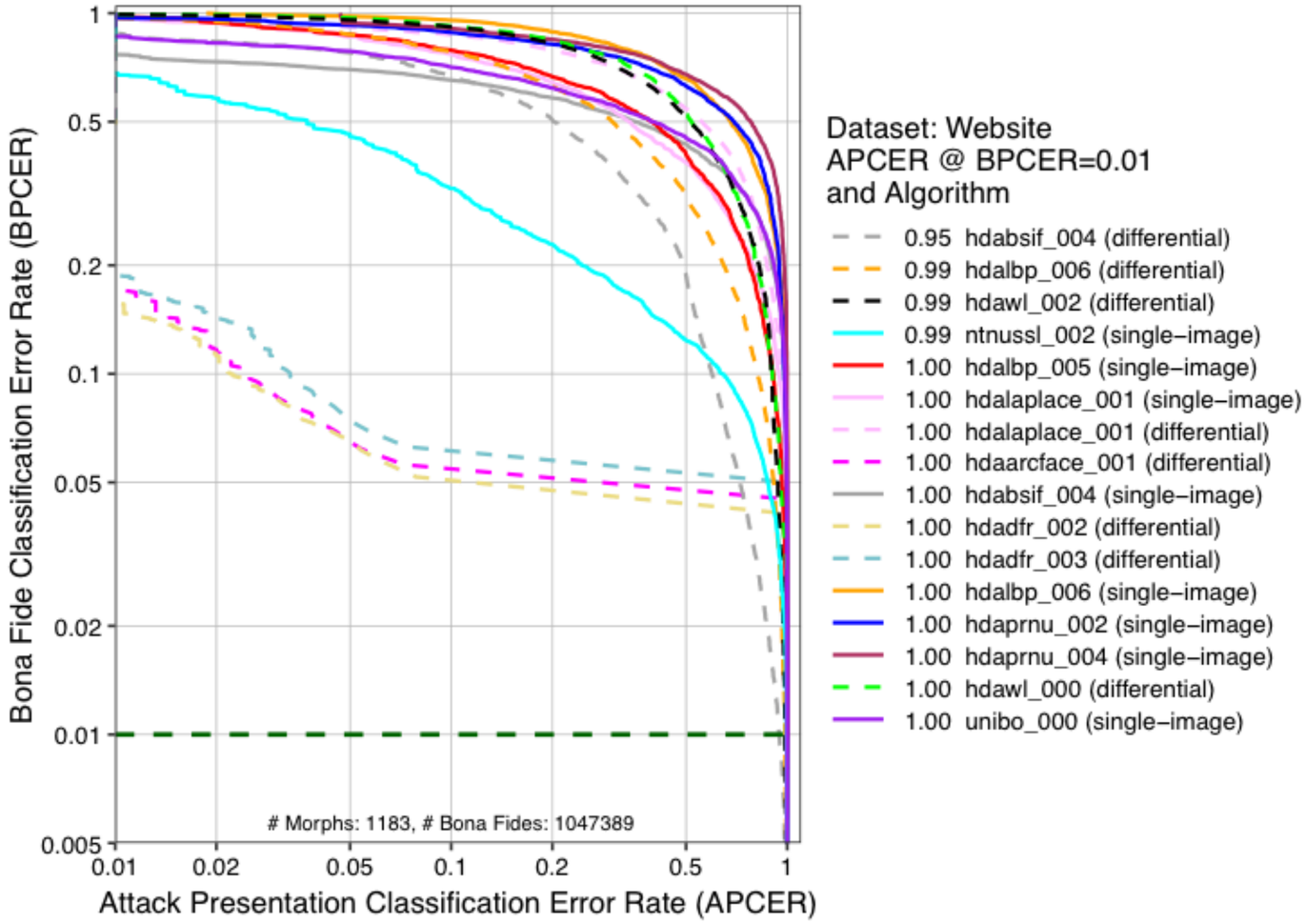


Obstacles for deployment
– Generalization Challenges

NIST - Tier 1 – Low Quality Morphs - S-MAD

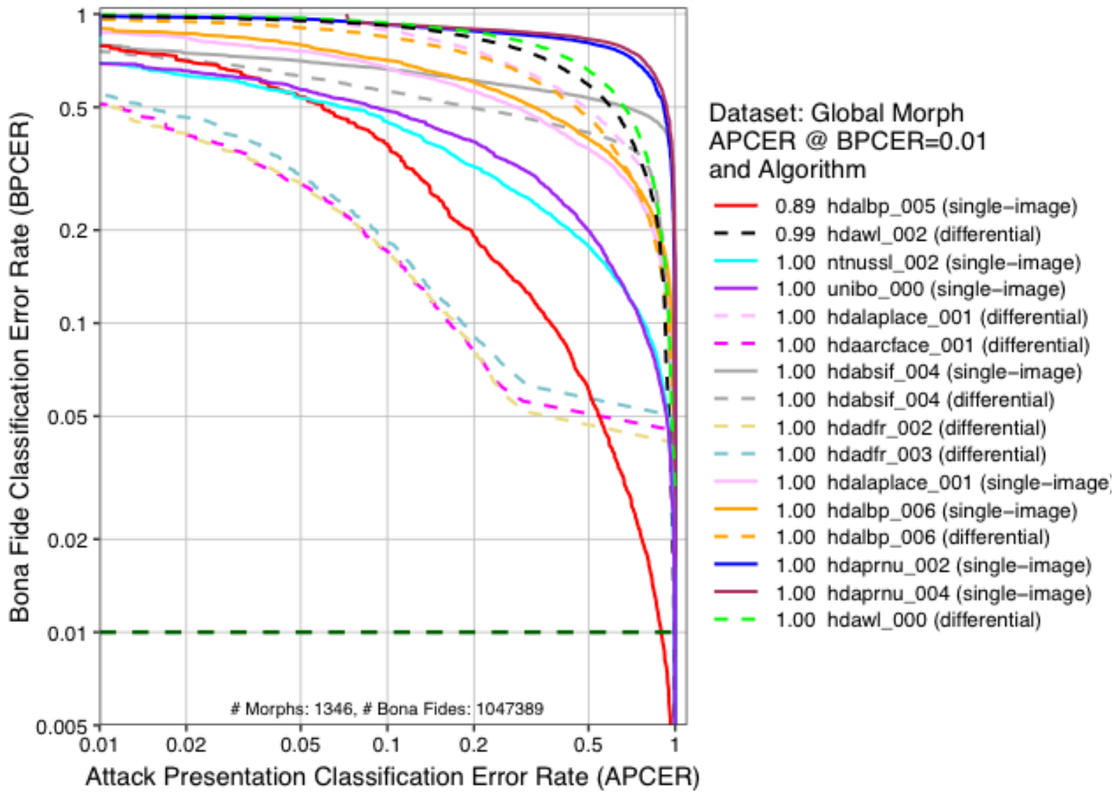


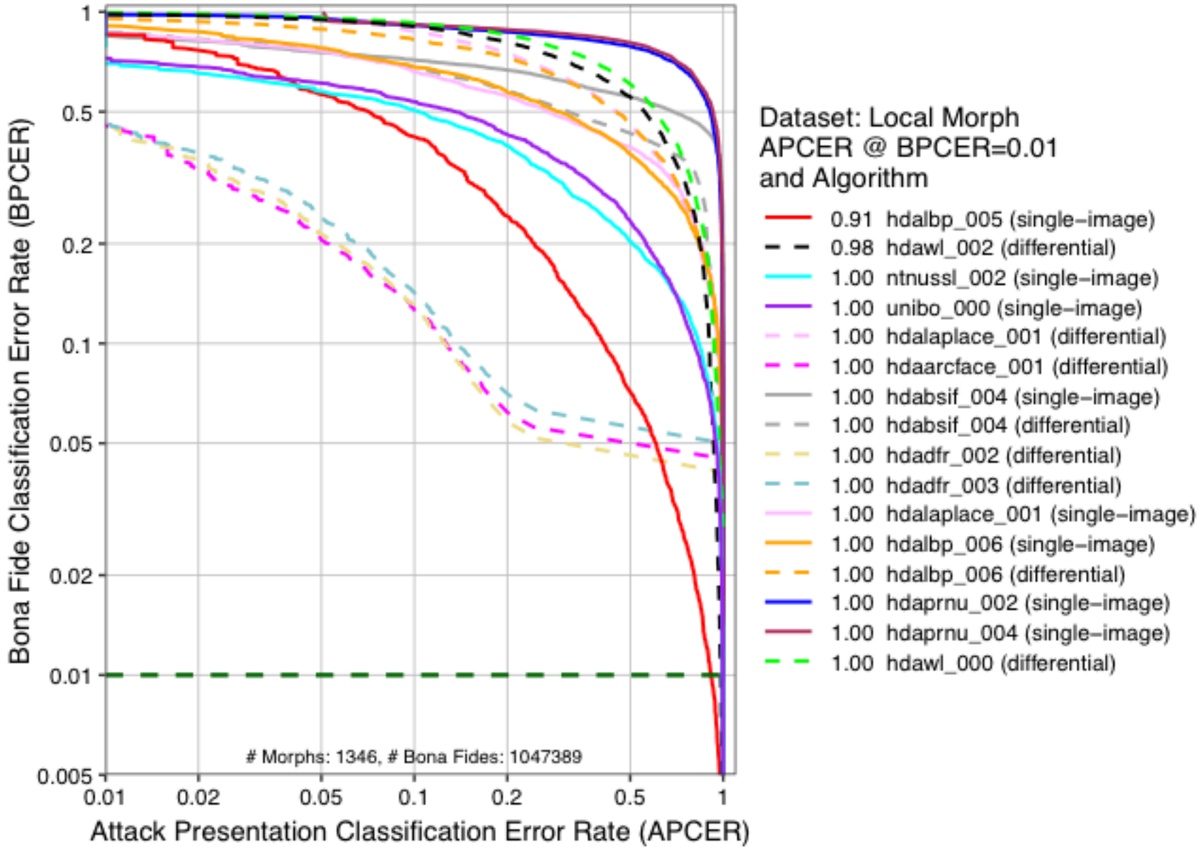
Operational Needs



https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf

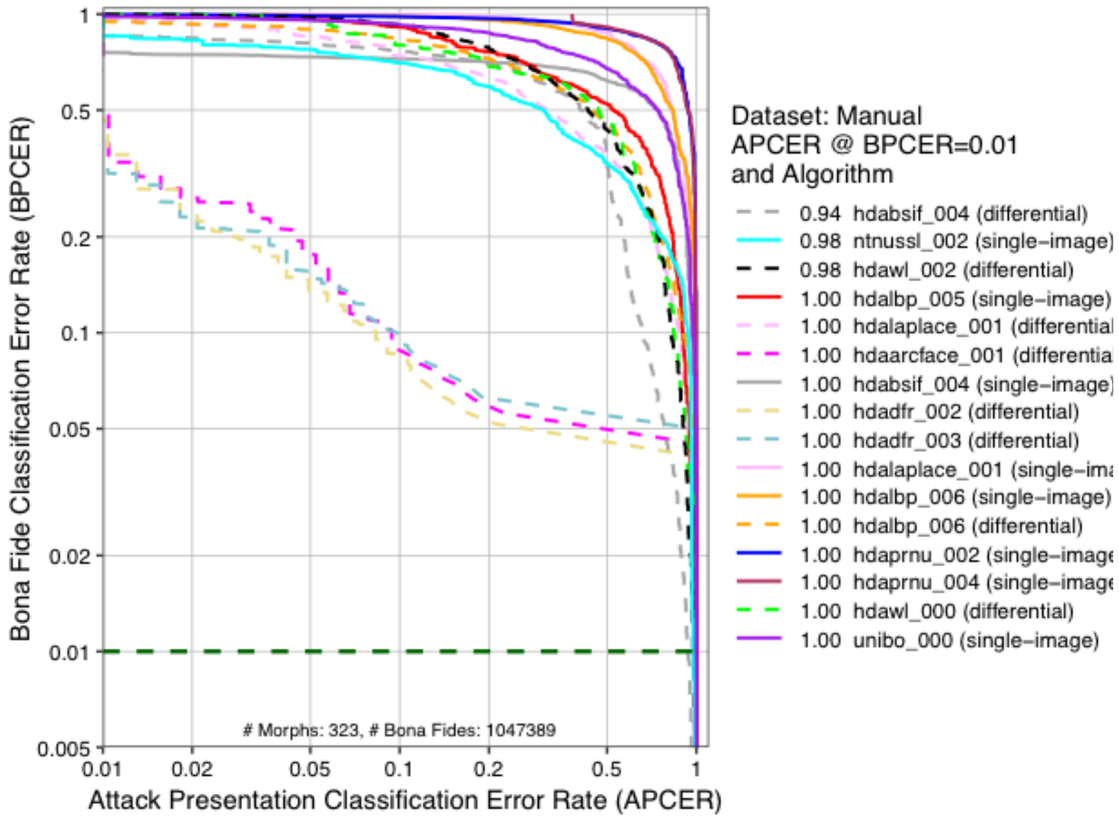
NIST - Tier 2 – Automated Morphs - S-MAD

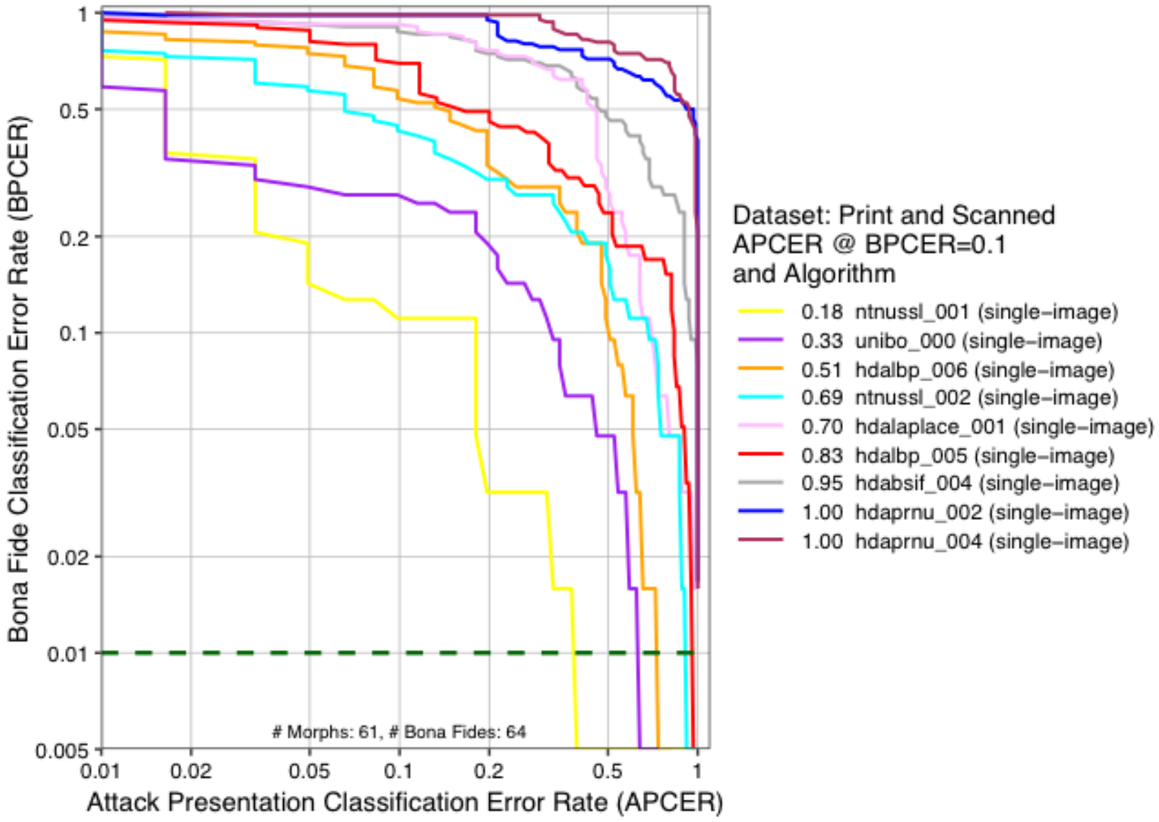




https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf

NIST - Tier 3 – High Quality Morphs

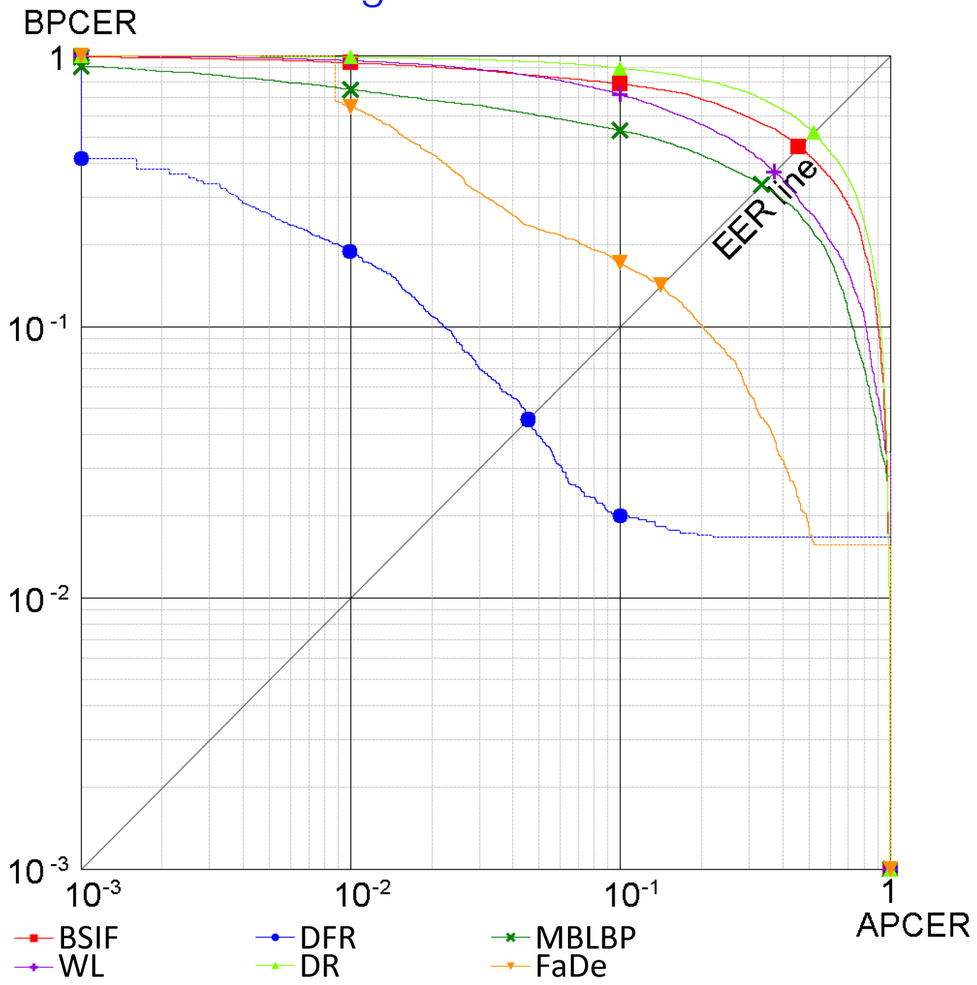




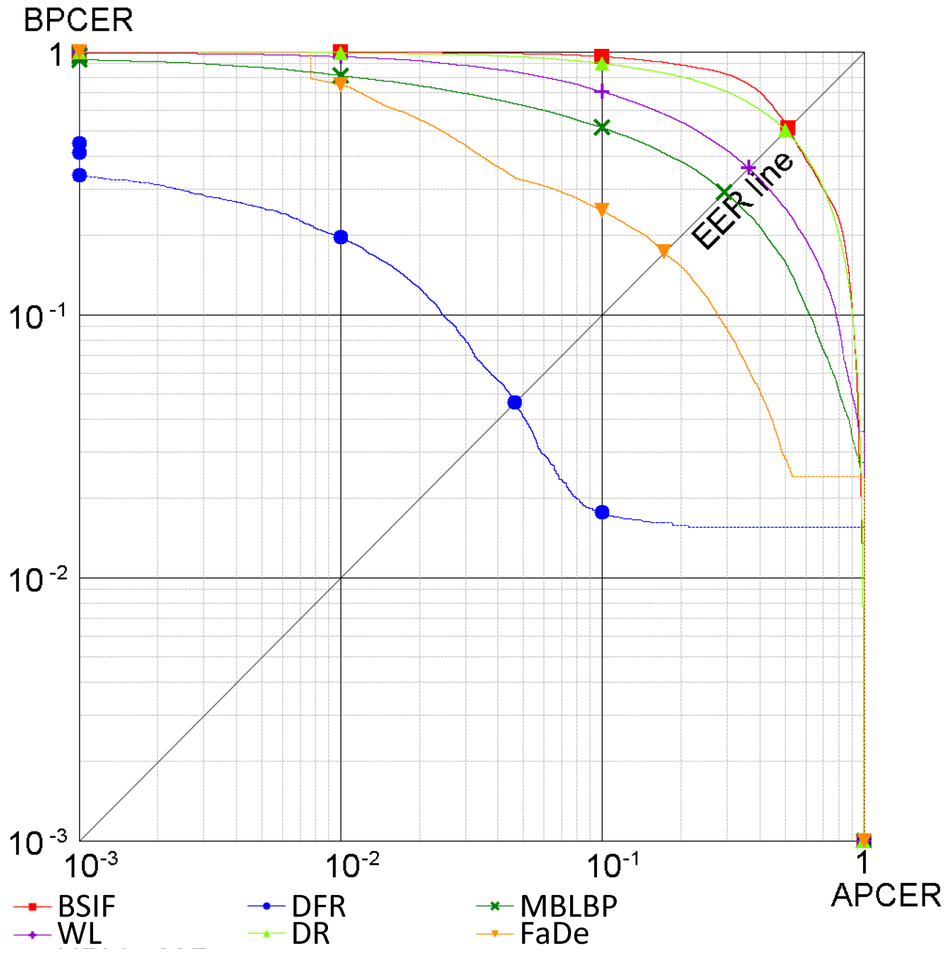
https://pages.nist.gov/frvt/reports/morph/frvt_morph_report.pdf

SOTAMD - State-Of-The-Art Results

Digital Attacks



Print and scan (Re-digitized) Attacks



Raja, K., Ferrara, M., Franco, A., Spreeuwers, L., Batskos, I., Gomez-Barrero, F.D.W.M., Scherhag, U., Fischer, D., Venkatesh, S., Singh, J.M. and Li, G., 2020. Morphing Attack Detection--Database, Evaluation Platform and Benchmarking. arXiv preprint arXiv:2006.06458.

Obstacles for deployment
– Challenge for Human Face Experts

Morphing Threats – Human Observer

Fig. 1 *Top:* An example of the images used in previous work (adapted from Robertson et al., 2018). *Bottom:* An example of the images used in the current work (Experiment 3[1]). The three faces depict two individuals (*left*, *right*) and a morph created using these images (*center*). The individuals pictured have given permission for their images to be reproduced here

Observing better quality morphing by human observers

Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Kramer, Robin SS, 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, no. 1 (2019): 28.

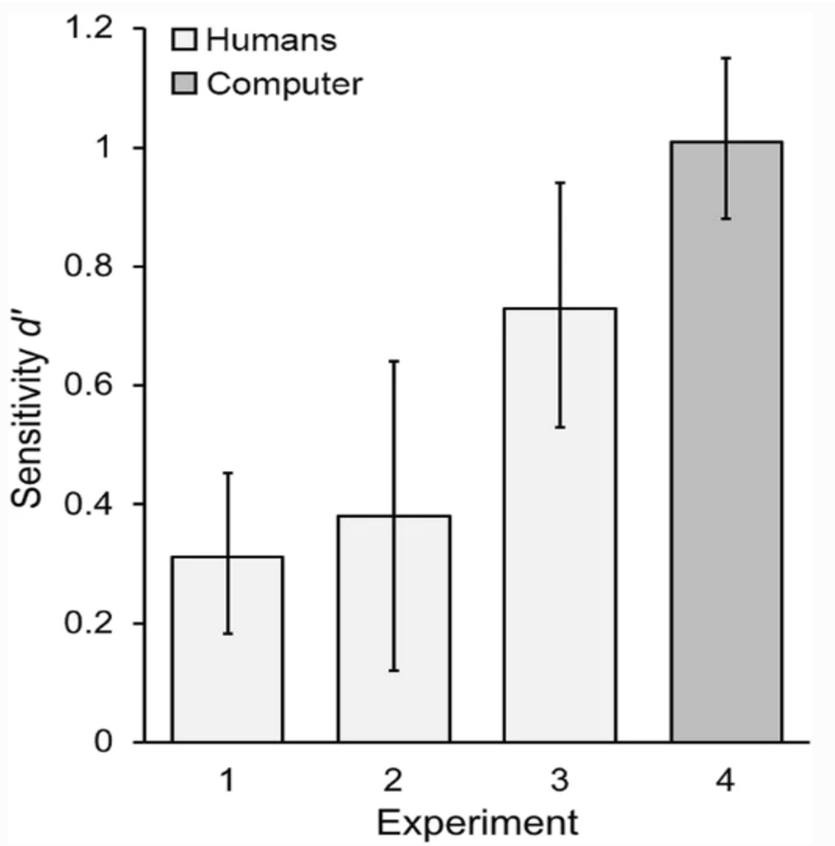
Morphing Threats – Human Observer

Fig. 1 *Top:* An example of the images used in previous work (adapted from Robertson et al., 2018). *Bottom:* An example of the images used in the current work (Experiment 3[1]). The three faces depict two individuals (*left*, *right*) and a morph created using these images (*center*). The individuals pictured have given permission for their images to be reproduced here

Observing better quality morphing by human observers

Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Kramer, Robin SS, 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, no. 1 (2019): 28.

Morphing Threats - Human Observer



Sensitivity = True positive / (True positive + False negative)

	Number of pairs	Error rate	Number of participant
Experiment 1	80	48.5	80
Experiment 2	120	44.6	49
Experiment 3	49	16.8	1410

Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Kramer, Robin SS, 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, no. 1 (2019): 28.

Morphing Threats – Human Observer

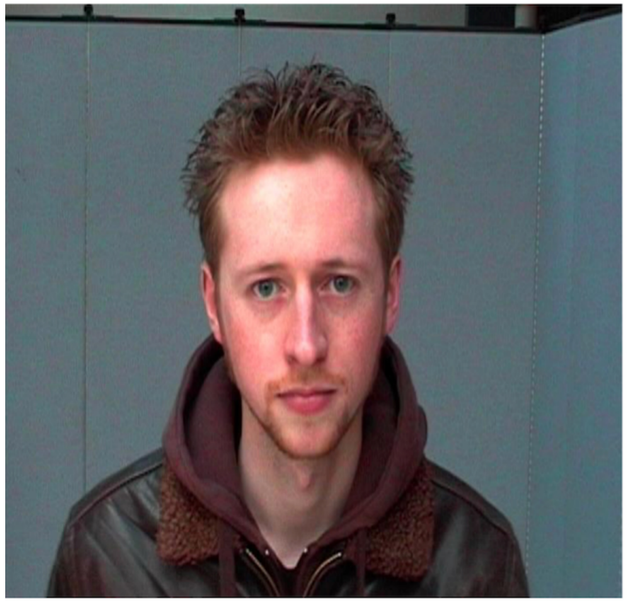
Press 1 for Match (Experiment 1 & 2)
Press 2 for Mismatch (Experiment 1 & 2)
Press 3 for Morph (Experiment 2)

Original person left side. 50/50 morphed image in right side

	Number of images	Error rate	Participant
Experiment 1	49	68%	49
Experiment 2	49	21%	42

Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Robertson, D. J., Kramer, R. S., & Burton, A. M. 2017. Fraudulent id using face morphs: Experiments on human and automatic recognition.PLoS One, 12(3), e0173319.

Morphing Threats - Human Observer



Press 1 for Match (Experiment 1 & 2)
Press 2 for Mismatch (Experiment 1 & 2)
Press 3 for Morph (Experiment 2)

- Original person left side.
- 50/50 morphed image in right side

Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Robertson, D. J., Kramer, R. S., & Burton, A. M. 2017. Fraudulent id using face morphs: Experiments on human and automatic recognition.PLoS One, 12(3), e0173319.

Human Observer Accuracy - Benchmark

Proposed benchmarking tool for iMARS

Instruction

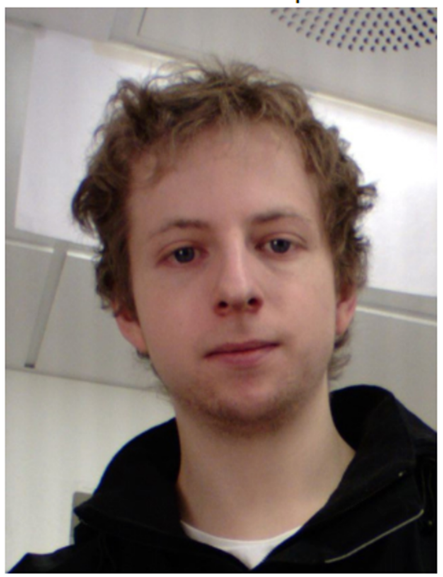
Image 1 out of 100 images

Same Subject

Morph

Unknown Capture

Trusted Live Capture

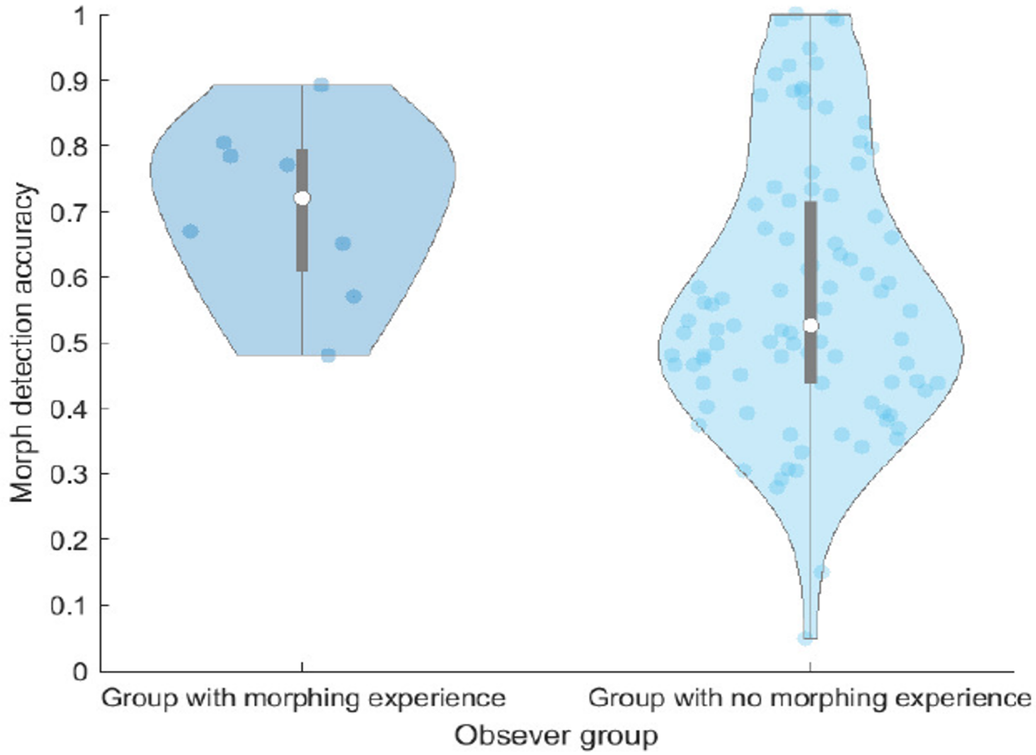


* You can take a break at any time during this experiment by clicking 'Continue later' button. You can continue this experiment using the following URL: http://folk.ntnu.no/sankinir/experiment/index.php/Continue
*Please remember to save your personal code. **aMi8C**

Ferrara, Matteo, Annalisa Franco, and Davide Maltoni. "The magic passport." In IEEE International Joint Conference on Biometrics, pp. 1-7. IEEE, 2014.
Robertson, D. J., Kramer, R. S., & Burton, A. M. 2017. Fraudulent id using face morphs: Experiments on human and automatic recognition.PLoS One, 12(3), e0173319.

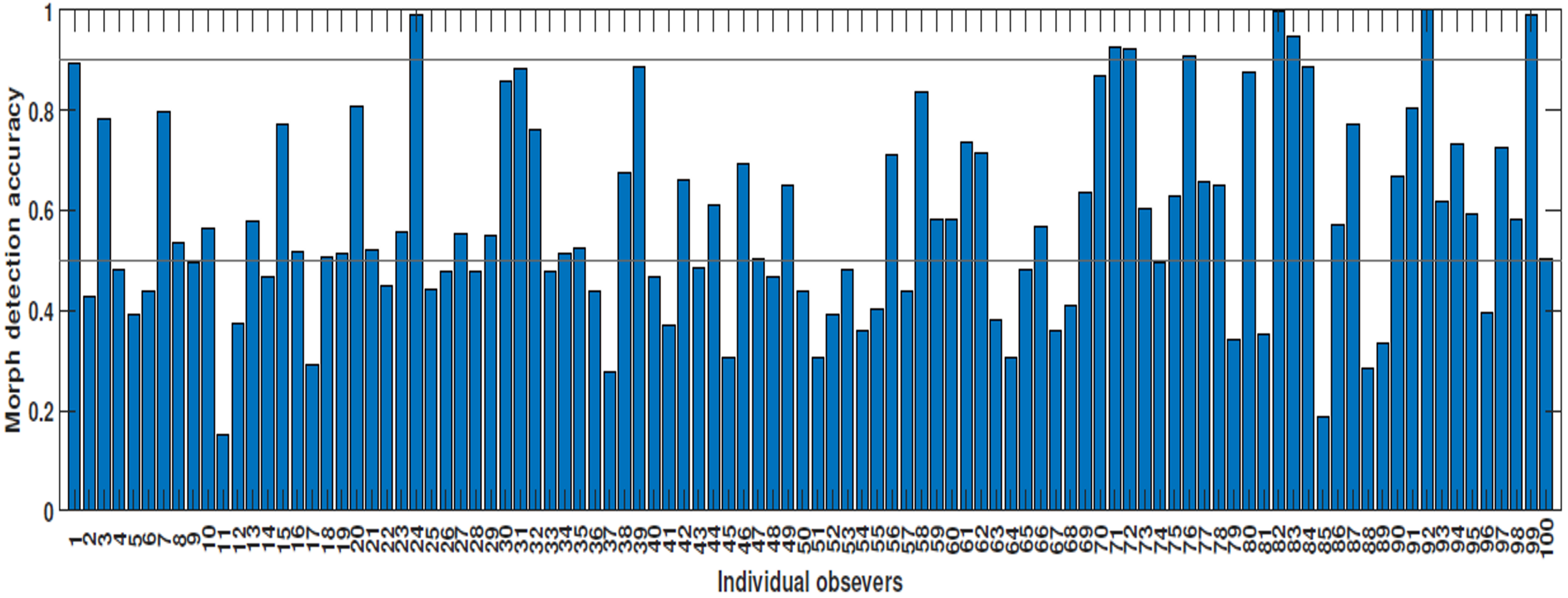
Human Observer Accuracy - Benchmark

	Digital images	Print and scanned
Morph image vs Bona-fide	48	48
Morph image vs ABC gate image	48	48
Post processed morph image vs Bona-fide	48	48
Post processed morph image vs ABC gate image	48	48
Bona-fide vs Bona-fide	*20	0
Total	222	192



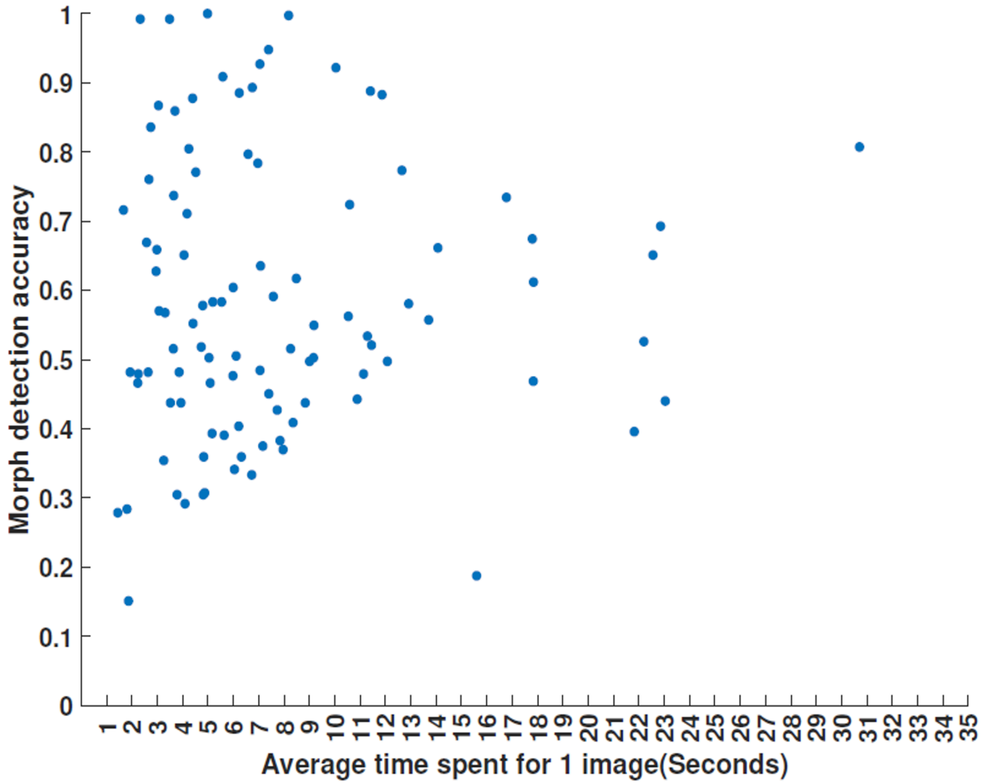
RANCHA GODAGE Sankini, Investigating and Analyzing Human Observer Ability in Detecting Face Morph Attacks, Master Thesis NTNU, 2020

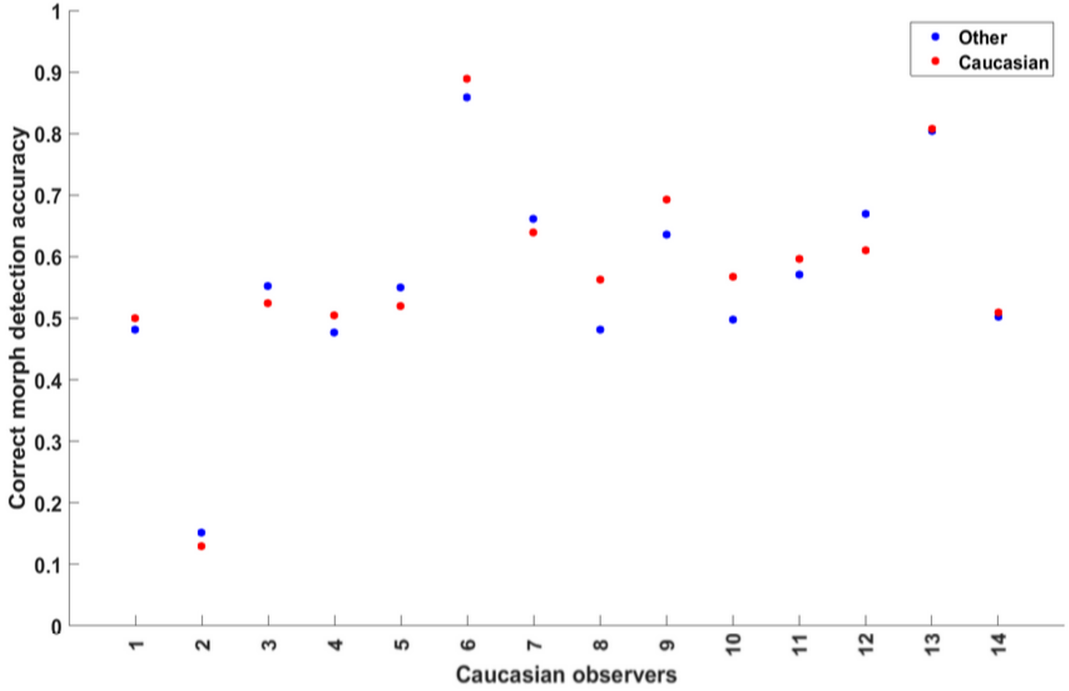
Human Observer Accuracy - Benchmark



RANCHA GODAGE Sankini, Investigating and Analyzing Human Observer Ability in Detecting Face Morph Attacks, Master Thesis NTNU, 2020

Human Observer Accuracy - Benchmark



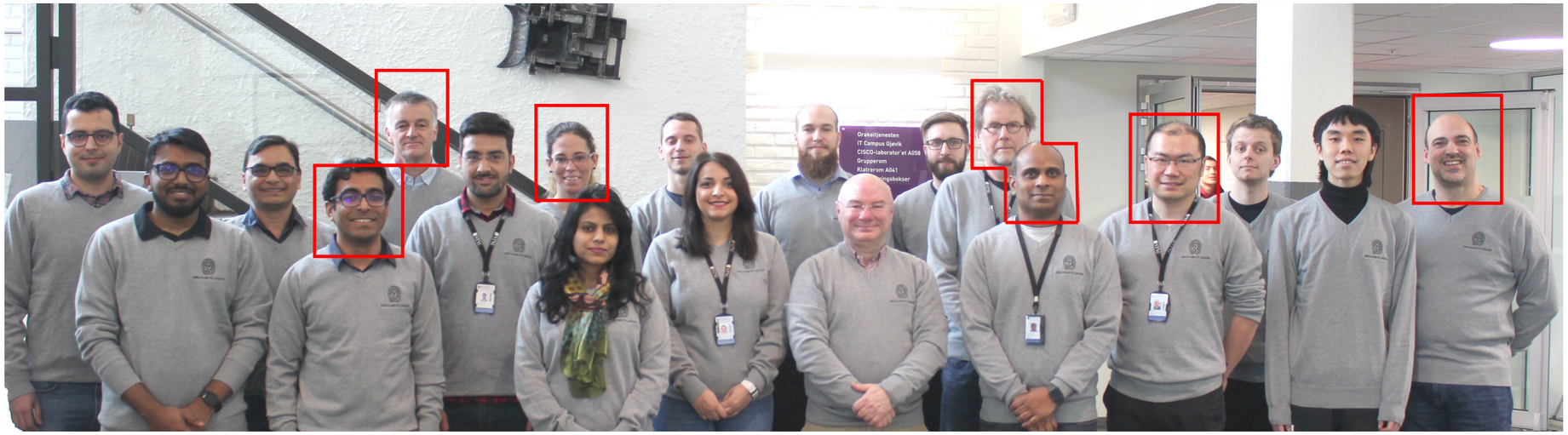


RANCHA GODAGE Sankini, Investigating and Analyzing Human Observer Ability in Detecting Face Morph Attacks, Master Thesis NTNU, 2020

Unsolved Challenges in MAD

- Given the number of covariates impacting the MAD performance such as age, gender and ethnicity, accurate and better algorithms need to be developed.
- Print and scan process reduces the MAD accuracy to a larger extent – need further research for developing **generalizable algorithms**.
- **Human detection performance** should be studied in a **standardized manner** to understand the key factors in spotting the morphing attacks on FRS – helpful in **border control**.

Contact



Fons Knopjes
Email: Fons.Knopjes@rvig.nl

Dinusha Frings
Email: Dinusha.Frings@rvig.nl

Uwe Seidel
UWE.SEIDEL04@bka.bund.de

Luuk Spreeuwers
Email: l.j.spreeuwers@utwente.nl

Raymond veldhuis
Email: r.n.j.veldhuis@utwente.nl

Christian Rathgeb
Email: christian.rathgeb@h-da.de

Marta Gomez-Barrero
Email: marta.gomez-barrero@hs-ansbach.de

Davide Maltoni
Email: davide.maltoni@unibo.it

Matteo Ferrara
Email: matteo.ferrara@unibo.it

Annalisa Franco
Email: annalisa.franco@unibo.it

Christoph Busch
Email: christoph.busch@ntnu.no

Ragahvendra Ramachandra
Email: ragahvendra.ramachandra@ntnu.no

Kiran Raja
Email: kiran.raja@ntnu.no

National Office for Identity Data
Ministry of the Interior and Kingdom Relations

Bundeskriminalamt

UNIVERSITY OF TWENTE.

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

NTNU

NTNU