Analysis of face embeddings to facilitate image pre-selection for face morphing

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

Roman Kessler (rkesslerx@gmail.com), Kiran Raja, Juan Tapia Farias, & Christoph Busch

NTNU

Motivation

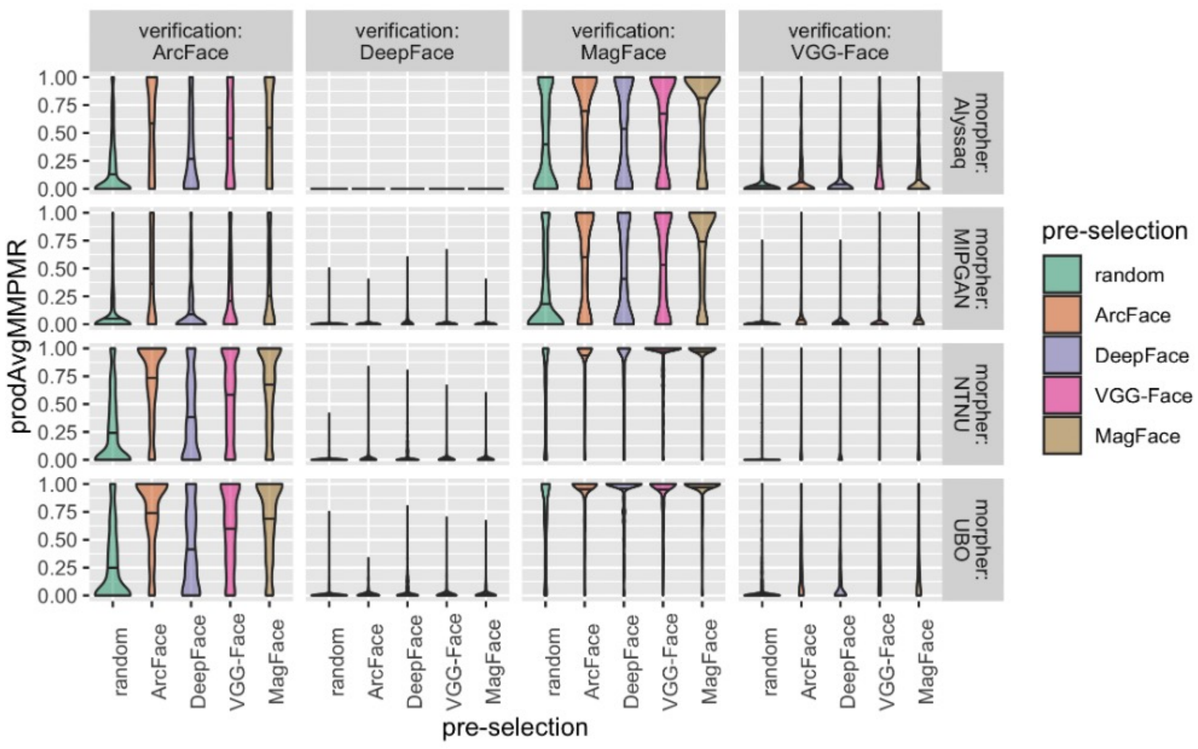
- Face Morphing Attacks jeopardize biometric systems and passport security
- Research needs large datasets of morphed face images e.g. to develop Morph Attack Detection (MAD)
- Finding appropriate image pairs for morphing must be conducted in an automated fashion to be scalable

Methods

- Face embeddings of different Face Recognition Systems (FRSs) have been evaluated for similarity-based image pre-selection
- Vulnerabilities to morphs were evaluated using different verification FRSs
- Different morphing algorithms were applied
- Face embeddings have been evaluated to also facilitate MAD

Results: Morph vulnerability assessment

- pre-selection based on embeddings improved the ability of resulting morphs to fool FRSs, as indicated by high prodAvgMMPMR (MagFace > ArcFace > VGG-Face > DeepFace)
- good FRSs were particularly vulnerable to attacks
- UBO morpher and NTNU morpher were most suited to jeopardise FRSs



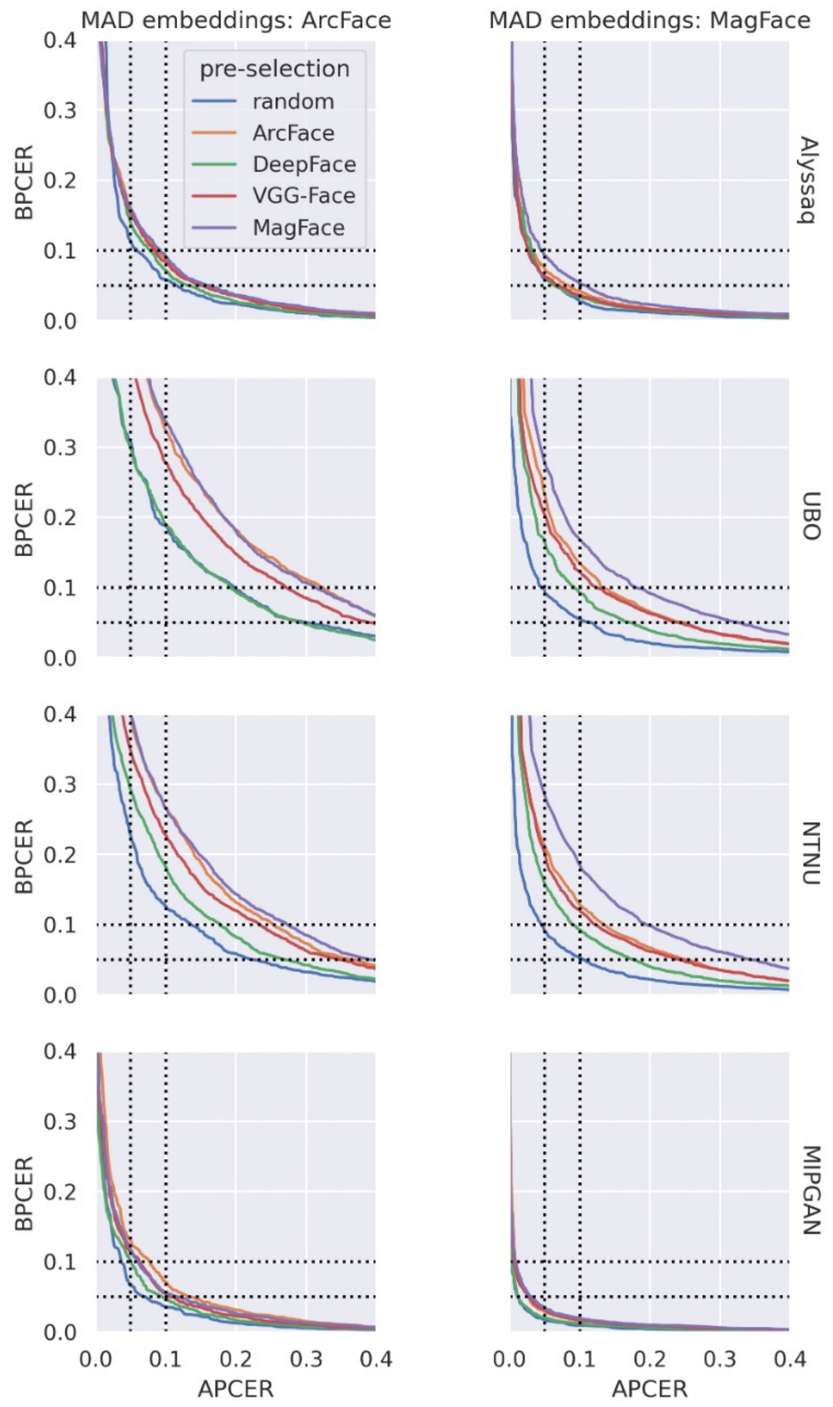
- Relative Mated Morph Rate (RMMR) reinforced the performance of different FRSs for image pre-selection, with MagFace performing best amongst the tested FRSs

pre-selection	average rank
random	1.1250
ArcFace	3.6250
DeepFace	2.6250
VGG-Face	3.5625
MagFace	4.0625

Metrics

- APCER: Attack Presentation Classification Error Rate
- BPCER: Bona fide Presentation Classification Error Rate
- prodAvgMMPMR: product Average Mated Morph Presentation Match Rate
- RMMR: Relative Morph Match Rate

Results: Morph Attack Detection



- pre-selection based on embeddings improved the ability to fool MAD algorithms
- MAD based on MagFace embeddings was more successfull to detect morphed faces than MAD based on ArcFace embeddings

Further Results

- Cosine and Euclidean distances were suitable metrics for pre-selection
- Commercial FRSs were similarly vulnerable to face morphs, and vulnerability increased with pre-selection via embeddings
- Deploying embeddings of soft-biometrics models was weak in improving morph vulnerability

ATHENE National Research Center for Applied Cybersecurity

University of Applied Sciences Darmstadt – Biometrics and Internet Security Research Group
Norwegian University of Science and Technology – Norwegian Biometrics Lab