Detection and Generation of Morphing Attacks

NTNU

Motivation

- Morphing attacks have shown the vulnerability of face recognition systems.
- Existing algorithms for generating morphing attacks also generate artefacts and usually need manual work for refinement.
- Robust methods for detection of morphing attacks can reduce the vulnerability of face recognition applications.

Approach

✓Explanatory approaches with hand-crafted features

✓Deep learning based classification approaches

✓GAN-based image manipulation approaches

Objectives

- Improve the performance of morph generation algorithms based on identity information and feedback of detection algorithms
- Develop and study on explicit and implicit morphing attack detection algorithms
- Evaluate the applicability of using augmented large-scale morphs for training and tuning the detection models.
- Develop solutions for presentation attacks at not only enrolment with high-quality capture devices but also at border gates with mixed-quality.

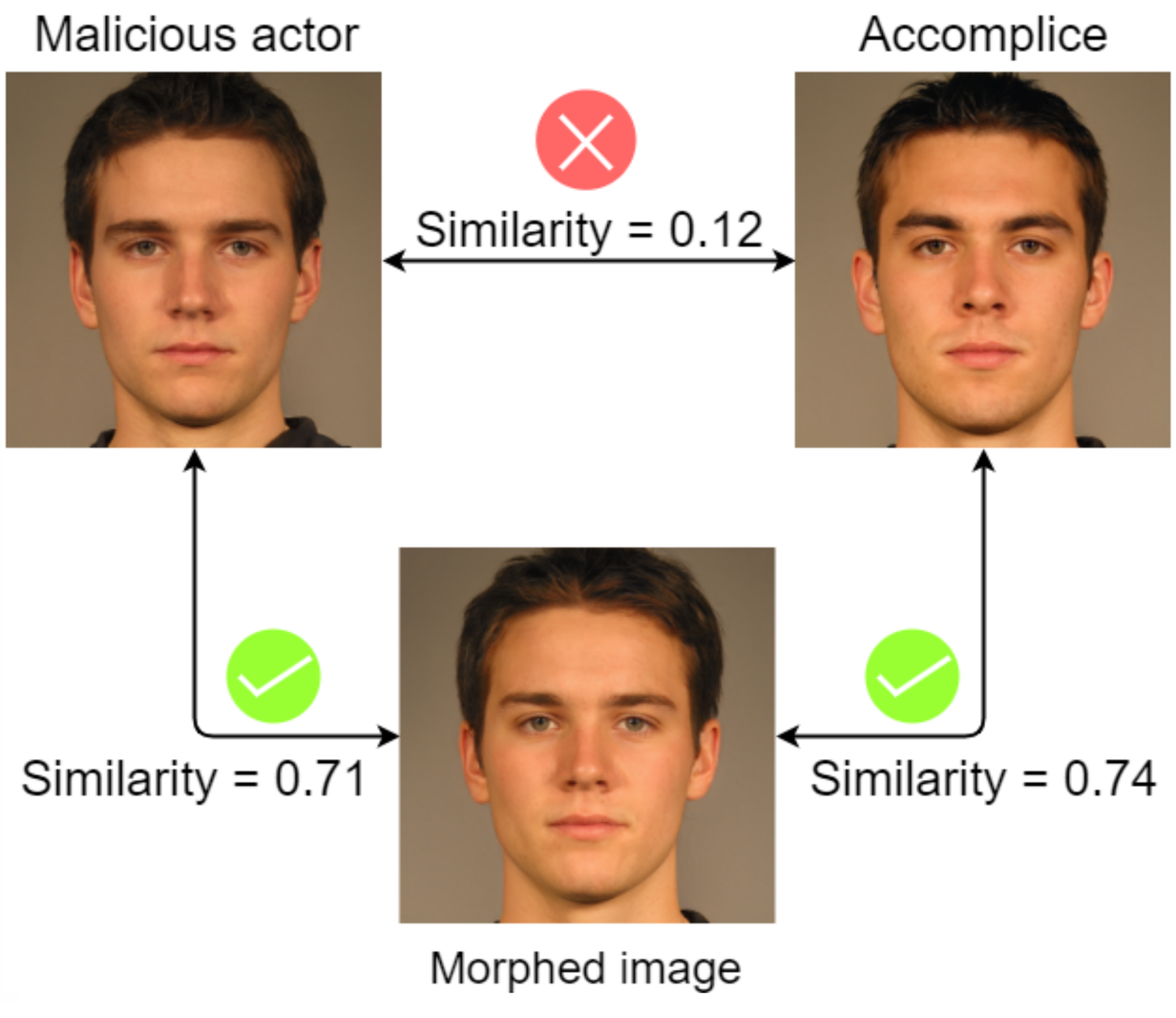
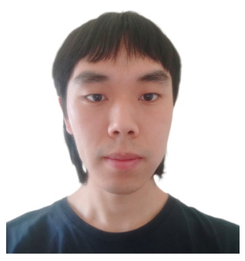


Fig 1: An example of morphing attack

MARS

image manipulation attack
resolving solutions



Haoyu Zhang
haoyu.zhang@ntnu.no

Dr. R. Raghavendra
raghavandra.ramachandra@ntnu.no

Prof. Dr. Christoph Busch
christoph.busch@ntnu.no

Norwegian University of Science and Technology – Norwegian Biometrics Lab