FACE MORPHING DETECTION: ISSUES AND CHALLENGES

[redacted] [redacted]

Hochschule Darmstadt, CRISP, da/sec Research Group

Warsaw, 10.10.2019

MAD schemes

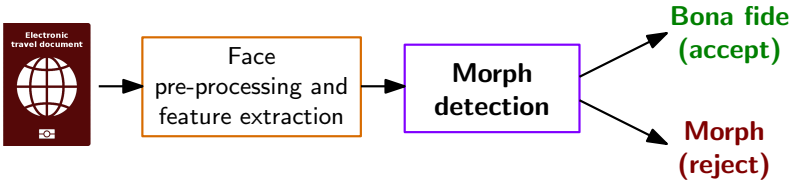
MAD approaches

MAD based on deep face representations

Questions and Challenges

MAD schemes

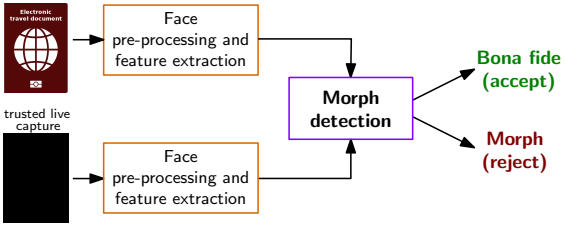
No-Reference Detection (single image MAD)



- single image, e.g. at application desk
- detection of certain artefacts (e.g. ghost artefacts)
- carefully created morphs contain only a few recognizable artefacts
- sensitive to post processing, e.g. print-scan transformation

MAD schemes

Reference Based Detection Scheme (differential MAD)



- compares the potentially morphed reference image with a trusted probe image, e.g. at eGates
- differences between potential morph and trusted live capture are analyzed
- less sensitive to post-processing

MAD approaches

Categories of MAD approaches

Single image MAD:

- Texture descriptors
- Forensic image analysis
- Deep-Learning approaches

Differential MAD:

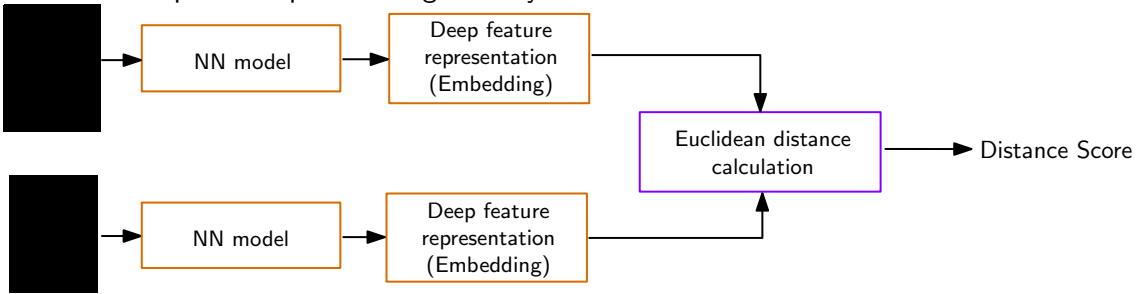
- comparison of two facial images (e.g. differences in deep face representations)
- reversing of the morphing process (De-Morphing)

MAD based on deep face representations

MAD based on deep face representations

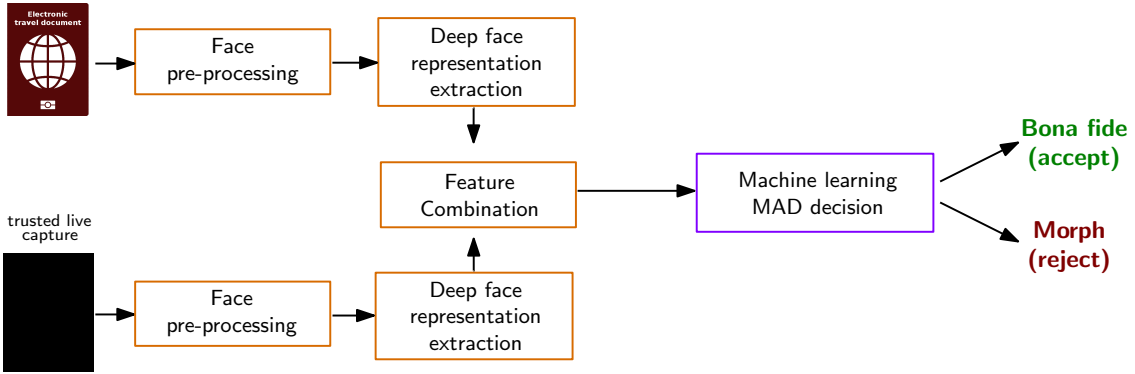
Deep face representation

General concept of Deep face recognition systems



MAD based on deep face representations

System Scheme



Advantages of MAD based on deep face representations

- CNNs are trained to extract relevant features from face images
- no expensive training of new CNNs required
- CNNs are not trained on morphed face images (no over-fitting)
- the feature extractors are highly robust to various changes in the image

MAD based on deep face representations

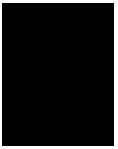
Database

Requirements for realistic databases:

- Passport images:
  - ICAO compliant
  - may be printed and scanned
  - JPEG 2000 compression
- Probe images (Gate images):
  - semi-controlled environment
  - may be grayscale
  - pose variations
  - different expressions
  - lack of sharpness

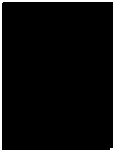
m r

Reference



Printed & Scanned

Probe 1



Probe 2

MAD based on deep face representations

Database

Database parameters:

- two databases
- selection of potential probe and reference images
- four different morphing algorithms (Open Source and Commercial)
- carefully created image pairs (e.g. glasses)
- resized to passport format
- print and scan (300dpi and 600dpi)
- JPEG-2000 compression (digital and print-scan) (15kB)

MAD based on deep face representations

Database Examples

Bona Fide

original | resized | jp2 | print-scan | ps + jp2

MAD based on deep face representations

Database Examples

Morph Algorithms

Algorithm 1 Algorithm 2 Algorithm 3 Algorithm 4

Conclusions regarding performance/generalizability

- *Performance:* Promising performance and robustness to post-processing (image compression, print-scan transformation, ...)
- *High quality morphs:* Morphs generated by morphing algorithms avoiding obvious artefacts are generally harder to detect than morphs comprising these artefacts
- *Morphing algorithms:* The morphing algorithms used for creating train data are less relevant
- *Realistic databases:* Probe images with higher variations in pose and illumination are more challanging for MAD algorithms

MAD based on deep face representations

Further Conclusions

- *Machine learning algorithms:* Support Vector Machines (SVMs) reveal the most competitive performance among the tested classifiers (AdaBoost, Gradient Boosting, Random Forest)
- *Open-Source vs. Commercial:* in contrast to the face recognition task, MAD algorithms based on open-source feature vectors might outperform those of commercial systems.

Questions and Challenges

MAD schemes

MAD approaches

MAD based on deep face representations

Questions and Challenges

Questions and Challenges

Open questions and challenges

- Evaluation metrics
- Evaluation protocols
- Generalizability of MAD approaches
- Databases
- Transparency of results

Questions and Challenges

Thank you!