h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

INNOVECTIS

Technology offer

Detecting artificial facial images

Benefits

- Promising and highly robust detection performance
- Significant reductions in morph miss rates (APCER) & false detection rates (BPCER)
- Algorithms outperform other methods by orders of magnitude

Project Status

- Proof of concept very sucessfully conducted
- Best in class algorithms according to performance test: NIST FRVT MORPH
- Several studies published e.g. - DeepFace-TIFS-2020 - LandmarkMAD-ICISP

Intellectual Property

- EP3642756A1 pending, priority 2017-06-20
- US20200218885A1, Notice of Allowance
- Additional licenses on extended algorithms available

Offer

- The technology can be licensed or assigned
- Several algorithms can be provided

Kontakt:

INNOVECTIS

Innovectis
Altenhöferallee 3
D – 60438 Frankfurt am Main
Phone: +49 69 25 61 632-0
E-Mail: matthias.goetz@innovectis.de

Scientists of the Darmstadt University of Applied Sciences (Hochschule Darmstadt, h_da) are world leading experts in the area of automated face recognition and morphed face image detection. Morphs are synthetic images created by fusion of the face images of at least two different subjects. The underlying technology for Morphing Attack Detection (MAD) and several corresponding algorithms have been developed & tested sucessfully, patent protected and are offered to interested companies.

In many countries, the facial image submitted for an electronic travel document is provided by the applicant in analogue or digital form. Therefore, an attacker – e.g., a wanted criminal – can morph his face image with the face image of an accomplice who applies for a passport with the morphed image. Since almost all morphed images are similar enough to deceive face recognition systems, the attacker can then use the electronic travel document to pass through border controls. The vulnerability of automated and manual face recognition systems against such a Morphing Attack is a well known issue.

So, the ability to detect morphed face images is of high interest to photo-credential issuance agencies, companies & organizations to verify the identity especially with the widespread deployment of automatic biometric recognition systems.

Figure: Example for a morphed face image of two subjects that is classified by the invention

The Darmstadt scientists focus on differential MAD methods that compare the image in question with a trusted probe image. Well aware that impressive detection rates are challenging to be applied to real-world scenarios, the inventors propose a novel framework for the detection of morphed face images based on facial landmarks. Another approach proposes a differential MAD system based on deep face representations.

The Darmstadt methods proof great performance in studies and independent tests e.g. conducted by the US National Institute of Standards and Technology. The algorithms outstandingly combine a low morph miss rate (low Attack Presentation Classification Error Rate - APCER), the proportion of morphs that are incorrectly classified as bona fides (nonmorphs), with a low false detection rate (low Bona fide Presentation Classification Error Rate - BPCER), the proportion of bona fides falsely classified as morphs.

The scientific team and the Darmstadt University of Applied Sciences would look forward to cooperate with commercial partners to foster further developments in the field of Morphing Attack Detection.