PRNU-based Detection of Morphed Face Images

6th International Workshop on Biometrics and Forensics
Sassari, IT

Luca Debiasi[1], Ulrich Scherhag[2], Christian Rathgeb[2], Andreas Uhl[1], Christoph Busch[2]

[1]Multimedia Signal Processing and Security Lab, University of Salzburg, Austria

[2]Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany

June 7th, 2018

Outline

Outline

What is Face Morphing?

Morphing - Creating an in-between image by blending two images

(a) Subject 1 (b) Morph (c) Subject 2

Figure: High Quality face morph of two subjects.

Steps for morphing face images:

1. Find location of facial feature points (landmarks) in both images
2. Compute Delaunay Triangulation for both images
3. Calculate affine transformations and warp triangles
4. Alpha blending of warped images

The Magic Passport

- Face selected as primary biometric trait for electronic Machine Readable Travel Documents (eMRTD) in 2002
- “The Magic Passport”[1]: Use morphed face images of multiple subjects for passport application

Figure: Passport application with morphed image.

The Magic Passport (cont.)

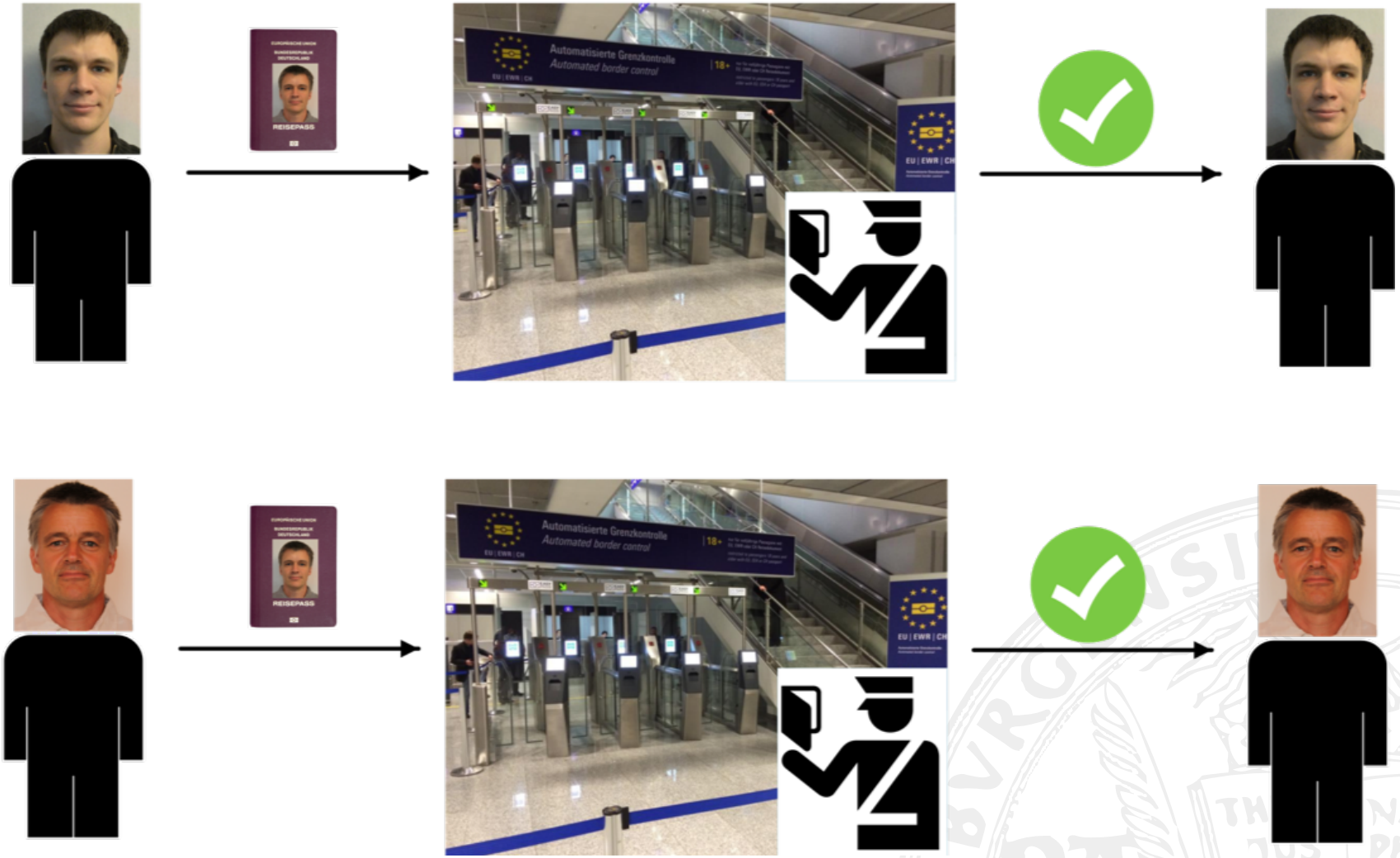


Figure: Both subjects are able to pass automated border control with the same passport.

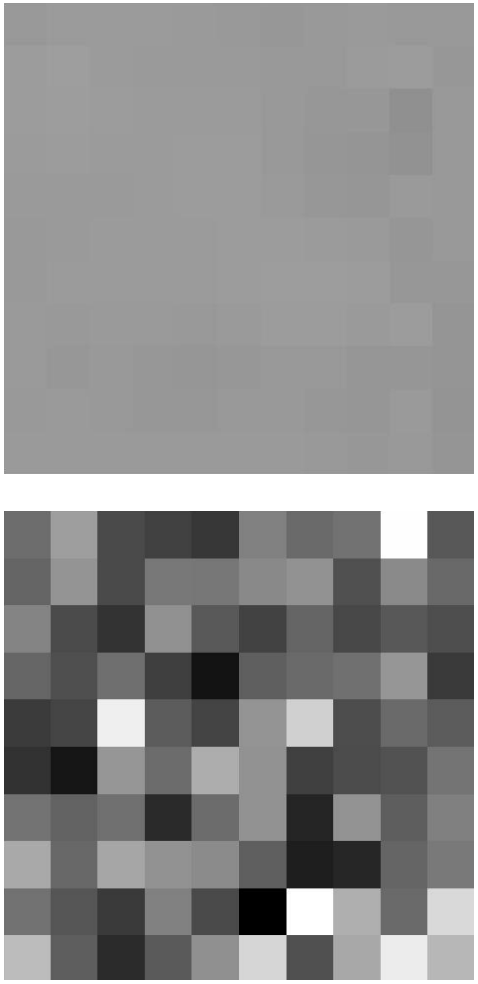
Related Work

- Ferrara *et al.* [1]: Morphed face images are successfully verified against both subjects using 2 commercial face recognition tools in verification mode at False Accept Rate (FAR) of 0.1%
- Ferrara *et al.* [2]: High quality morphed face images are realistic enough to fool human examiners
- Scherhag *et al.* [3]: Presentation attack detection using general purpose texture descriptors and machine learning techniques fail at reliably detecting morphed face images
- Detection of morphed face images becomes even more challenging if images are printed and scanned

$\rightarrow$ **SERIOUS RISK** for automated border control

Outline

PRNU



- PRNU: Photo-response non-uniformity
- Intrinsic property of CCD/CMOS sensors
- Noise-like pattern
- Variations in quantum efficiency among pixels
- PRNU noise residual W_I:

$$W_I = I - F(I)$$

Why PRNU?

1. **Universality**: All imaging sensors exhibit PRNU.
2. **Generality**: The PRNU is present in every picture independently of the camera optics, camera settings, or scene content.
3. **Robustness**: It survives lossy compression, filtering, gamma correction, and many other typical processing procedures. It even survives high quality printing and scanning [4].

By investigating the spectral and spatial characteristics of the PRNU it is possible to detect whether the images have been subject to further processing, e.g. non-geometrical operations have an influence on the PRNU's signal strength [5].

PRNU-based Morphing Detection Approach

- Goal: Blind detection of morphed images without the need of reference image
- Exploit the effects caused by morphing in spectral domain through non-linear warping

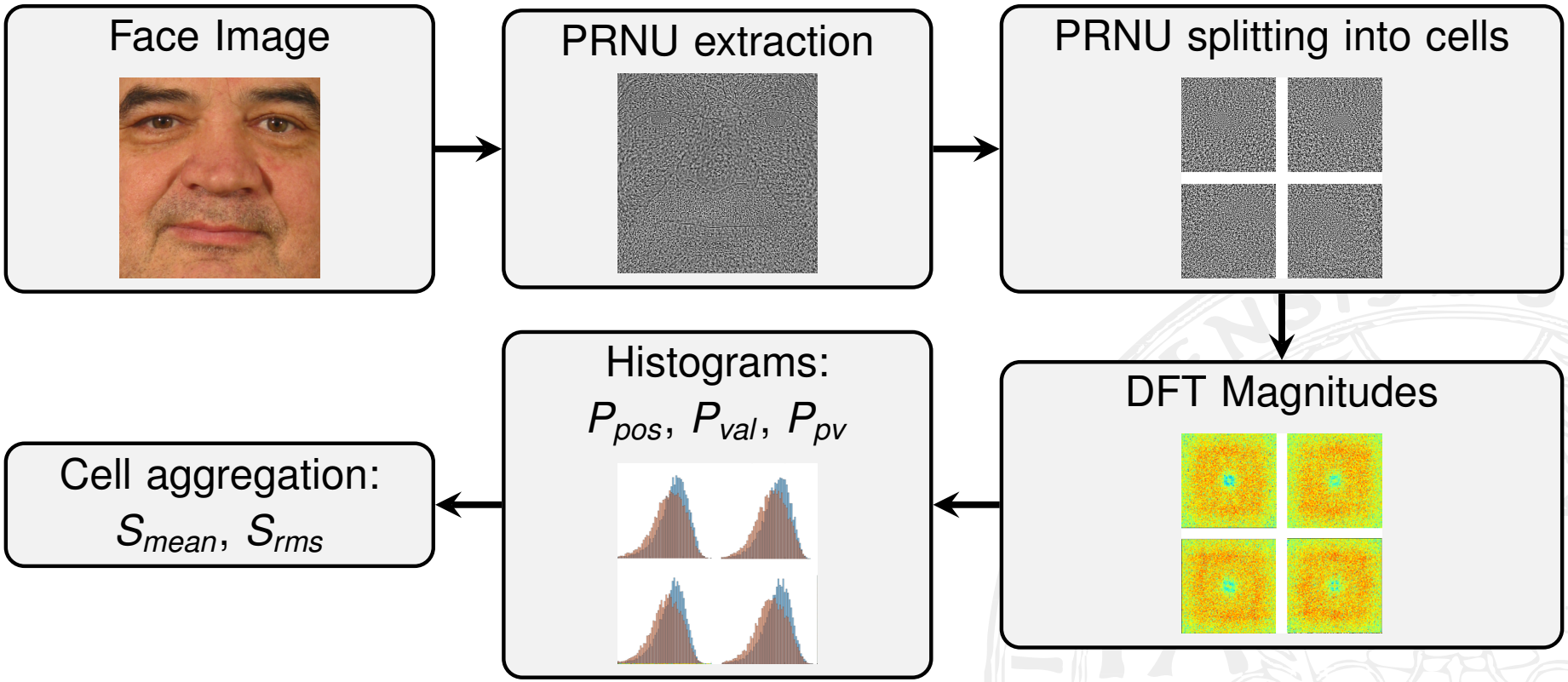


Figure: Processing steps.

Outline

Experimental Setup

- Dataset: Subset of FRGCv2
  - Face images with resolution of 320x320 pixels (ICAO compliant)
  - 961 bona fide images (male and female), 2414 morphed images
- PRNU extraction: Mihcak denoising filter [6] + FDR enhancement [7]
- Different block configurations: 1x1 . . . 10x10
- Experiments:
  - Experiment A: Detection of morphed face images
  - Experiment B: Face recognition vulnerability assessment
  - Experiment C: Detection of post-processed morphs
- Post-processings of morphs used in Experiment B and C:
  - SHRP: Sharpening (unsharp masking)
  - SCL: Downscaling (75% and 50%) with subsequent upscaling
  - EQU: Histogram equalization (CLAHE)

Evaluation Metrics

- Face recognition vulnerability assesment (according to [8])
  - How well do both subjects match against the mated morphed image?
  - Evaluation using a commercial face recognition system
  - **MMPMR**: Mated Morph Presentation Match Rate
  - **RMMR**: Relative Morph Match Rate (considering match rate of subjects)

- Detection of morphed face images (according to ISO/IEC 30107-3 [9])
  - How well are morphed images correctly classified?
  - **APCER**: Attack Presentation Classification Error Rate - attacks incorrectly classified as bona fides
  - **BPCER**: Bona Fide Presentation Classification Error Rate - bona fides incorrectly classified as attacks
  - **D-EER**: Detection Equal Error Rate, APCER = BPCER

Experiment A: Morphing Detection

Feature	Cells				
	1×1	2×2	4×4	8×8	10×10
$P_{val} \vert S_{mean}$	2.1	2.0	1.9	3.2	3.8
$P_{val} \vert S_{rms}$	2.1	2.0	1.9	3.3	3.9
$P_{pos} \vert S_{mean}$	5.1	3.3	2.9	2.2	2.4
$P_{pos} \vert S_{rms}$	5.1	3.2	2.8	2.3	2.6
$P_{pv} \vert S_{mean}$	2.2	1.7	**1.5**	**1.4**	1.8
$P_{pv} \vert S_{rms}$	2.2	1.6	**1.5**	**1.5**	1.8

Table: D-EERs in % for detection of morphed images.

Experiment B: Face Recognition Vulnerability Assessment

- **MMPMR** $>$ **99.99%** for morphed and post-processed images
- **RMMR** $>$ **99.99%** for morphed and post-processed images

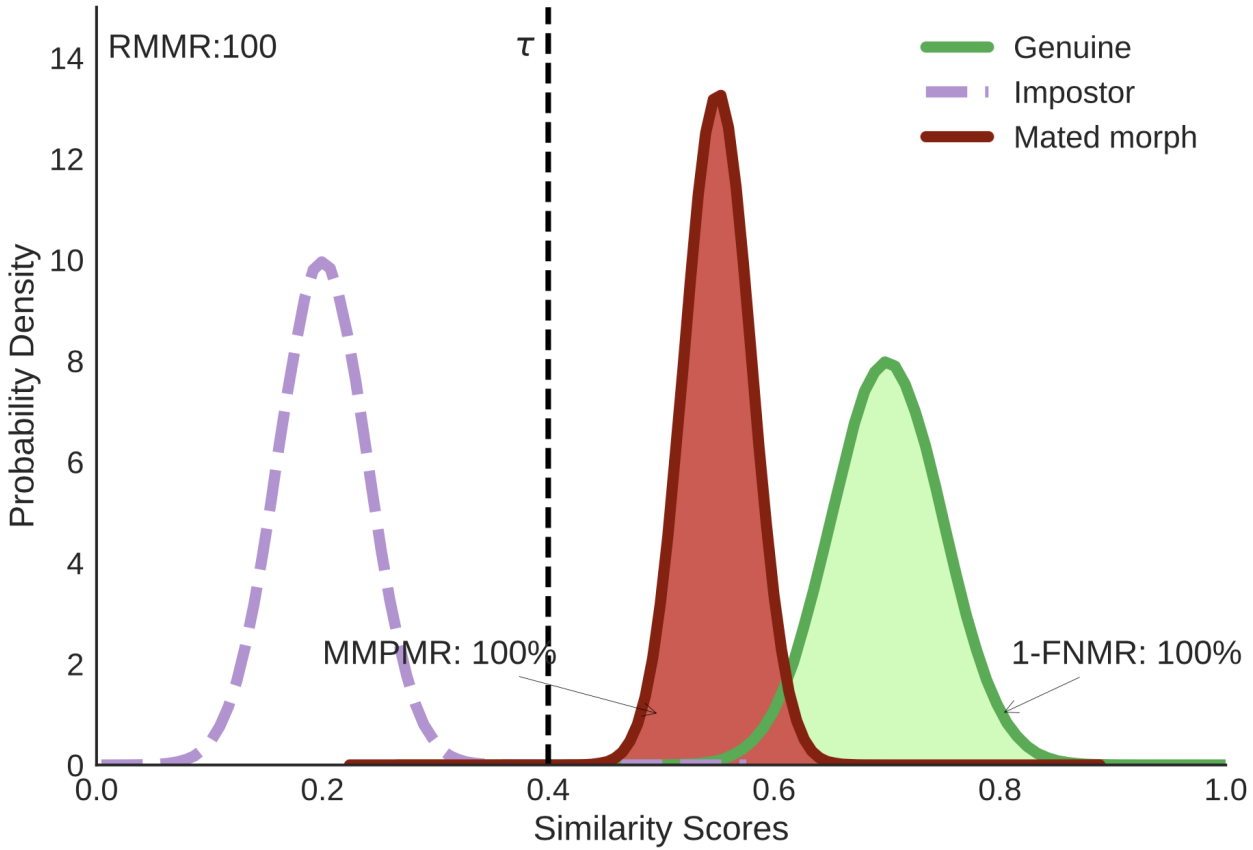


Figure: Illustration of score distributions for RMMR = MMPMR = 100%.

$\rightarrow$ **Nearly all face images are matched against their morphs**

Experiment C: Post-processing Examples

(a) Original

(b) Morphed

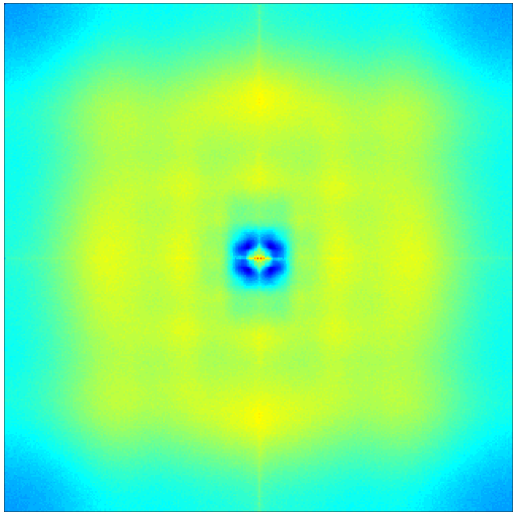
(c) SCL 50%

(d) SCL 75%

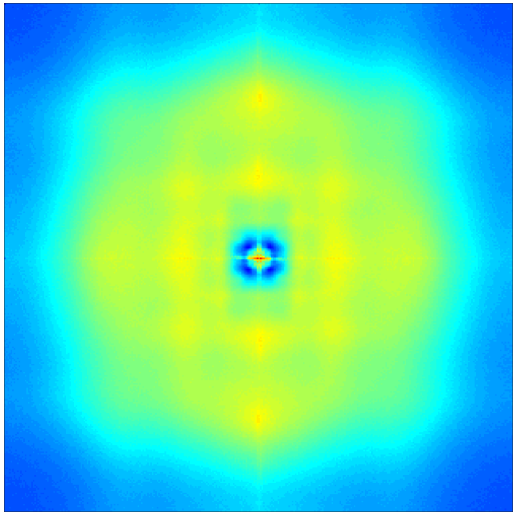
(e) SHRP

(f) EQU

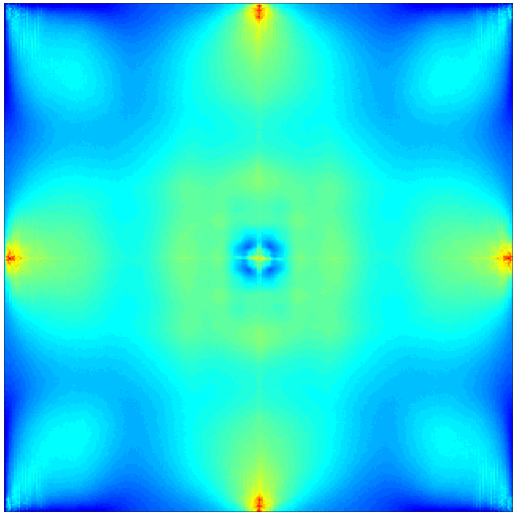
Experiment C: Averaged DFT Magnitude Spectra



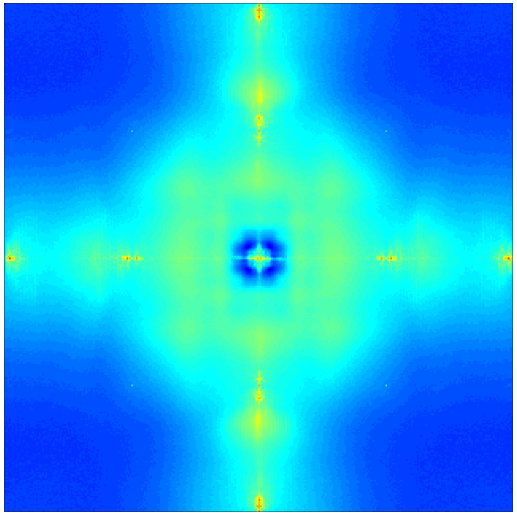
(g) Original



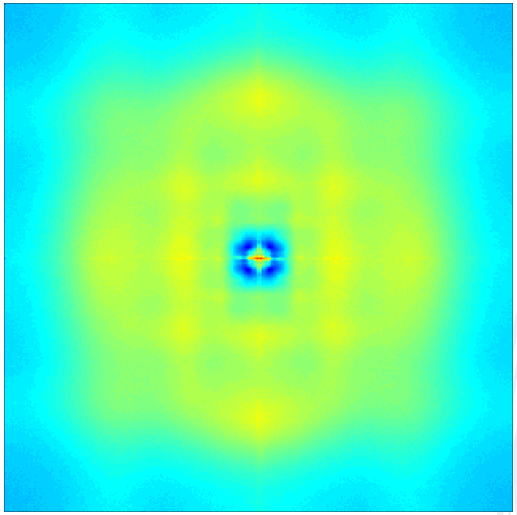
(h) Morphed



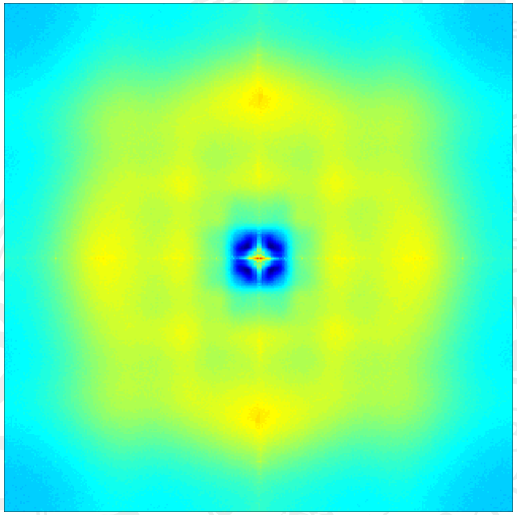
(i) SCL 50%



(j) SCL 75%



(k) SHRP



(l) EQU

Experiment C: Detection of Post-processed Morphs

Feature	Cells	Morph	EQU	SCL_{50}	SCL_{75}	SHRP
$P_{val}\|S_{mean}$	1×1	2.1	34.8	0.7	2.2	46.4
$P_{val}\|S_{rms}$		2.1	34.8	0.7	2.2	46.4
$P_{pos}\|S_{mean}$		5.1	36.4	4.5	0.3	20.1
$P_{pos}\|S_{rms}$		5.1	36.4	4.5	0.3	20.1
$P_{pv}\|S_{mean}$		2.2	32.9	0.9	0.2	36.9
$P_{pv}\|S_{rms}$		2.2	32.9	0.9	0.2	36.9
$P_{val}\|S_{mean}$	2×2	2.0	36.3	0.7	2.0	45.8
$P_{val}\|S_{rms}$		2.0	36.3	0.6	2.0	45.9
$P_{pos}\|S_{mean}$		3.3	33.4	2.5	0.2	17.1
$P_{pos}\|S_{rms}$		3.2	33.1	2.4	0.2	17.0
$P_{pv}\|S_{mean}$		1.7	32.8	1.0	0.1	32.6
$P_{pv}\|S_{rms}$		1.6	32.6	1.0	0.1	33.1
$P_{val}\|S_{mean}$	8×8	3.2	35.5	0.4	7.4	34.5
$P_{val}\|S_{rms}$		3.3	35.6	0.4	7.6	35.8
$P_{pos}\|S_{mean}$		**2.2**	**33.8**	**0.7**	**0.0**	**10.8**
$P_{pos}\|S_{rms}$		**2.3**	**33.6**	**0.8**	**0.0**	**11.0**
$P_{pv}\|S_{mean}$		1.4	31.8	0.3	0.1	15.9
$P_{pv}\|S_{rms}$		1.5	31.3	0.3	0.0	17.3

Table: D-EERs in % for detection of morphed images.

Outline

Conclusion and Future Work

Conclusion

- Creating morphed face images affects the PRNU.
- Reliable detection of morphed face images possible with the proposed cell-based PRNU approach.
- Robust against some post-processings (SHRP, SCL).
- Detection can be attacked with EQU post-processing.

Future work

- Improve robustness against post-processing of morphed images.
- Is the approach robust against PRNU insertion/substitution?
- How well does it work for images from different cameras?
- Does it also work as well for printed and scanned images?

References

[1] M. Ferrara, A. Franco, and D. Maltoni, “The magic passport”, in *Proc. Int. Joint Conf. on Biometrics (IJCB)*, 2014, pp. 1–7.

[2] ——,“On the effects of image alterations on face recognition accuracy”, in *Face Recognition Across the Imaging Spectrum*, T. Bourlai, Ed., Springer International Publishing, 2016, pp. 195–222.

[3] U. Scherhag, R. Raghavendra, K. B. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch, “On the vulnerability of face recognition systems towards morphed face attacks”, in *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, 2017, pp. 1–6.

[4] M. Goljan, J. Fridrich, and J. Lukas, “Camera identification from printed images”, in *Proceedings of SPIE, Electronic Imaging, Forensics, Security, Steganography, and Watermarking of Multimedia Contents X*, San Jose, CA, USA: SPIE, Jan. 2008.

[5] J. Fridrich, “Digital image forensic using sensor noise”, *IEEE Signal Processing Magazine*, vol. 26, no. 2, Mar. 2009.

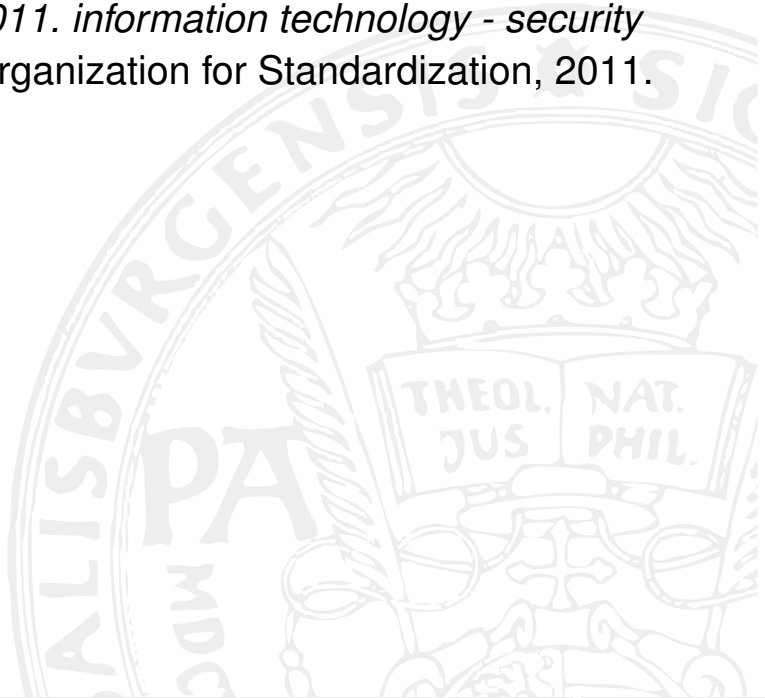
[6] M. Mihcak, I. Kozintsev, and K. Ramchandran, “Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising”, in *Proceedings of the 1999 IEEE International Conference on Acoustics, Speech, and Signal Processing, ICASSP ’99*, Phoenix, AZ, USA: IEEE, Mar. 2009, pp. 3253–3256.

[7] X. Lin and C.-T. Li, “Enhancing sensor pattern noise via filtering distortion removal”, *IEEE Signal Processing Letters*, vol. 23, no. 3, pp. 381–385, 2016.

References (cont.)

[8] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, and C. Busch, “Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting”, in *Int. Conf. of the Biometrics Special Interest Group (BIOSIG)*, 2017, pp. 1–12.

[9] ISO/IEC JTC1 SC27 Security Techniques, *ISO/IEC 24745:2011. information technology - security techniques - biometric information protection*, International Organization for Standardization, 2011.



Thank you for your attention!
Any questions?