PRNU-based Detection of Morphed Face Images

Luca Debiasi*, Ulrich Scherhag†, Christian Rathgeb†, Andreas Uhl* and Christoph Busch†
*WaveLab – The Multimedia Signal Processing and Security Lab, Universität Salzburg, Austria
†da/sec – Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany
{ldebiasi,uhl}@cosy.sbg.ac.at
{ulrich.scherhag,christian.rathgeb,christoph.busch}@h-da.de

***Abstract*—In the recent past, face recognition systems have been found to be highly vulnerable to attacks based on morphed biometric samples. Such attacks pose a severe security threat to biometric recognition systems across various applications. Apart from some algorithms, which have been reported to reveal practical detection performance on small in-house datasets, approaches to effectively detect morphed face images of high quality have remained elusive. In this paper, we propose a morph detection algorithm based on an analysis of photo response non-uniformity (PRNU). It is based on a spectral analysis of the variations within the PRNU caused by the morphing process. On a comprehensive database of 961 bona fide and 2,414 morphed face images practical performance in terms of detection equal error rate (D-EER) is achieved. Additionally, the robustness of the proposed morph detection algorithm towards different post-processing procedures, e.g. histogram equalization or sharpening, is assessed.**

I. Introduction

Automated face recognition represents a longstanding field of research and a variety of methods have been proposed over the past three decades [1], [2]. Generic face recognition systems comprise four major modules: face detection, face alignment, feature extraction, and comparison, where the latter two are generally conceded as key modules. The potentially high intra-class variability within human faces across time represents a main challenge in face recognition systems. Hence, in order to achieve acceptable False Non-Match Rates (FNMRs) deployments of face recognition systems are operated at rather high False Match Rates (FMRs) [3].

In past years, researchers have pointed out diverse potential vulnerabilities of biometric recognition systems [4]. In particular, face recognition systems have been found to be vulnerable to presentation attacks [5]. Presentation attacks refer to a presentation of an attack instrument (e.g. print outs or electronic displays) to the biometric capture device with the goal of interfering with the operation of the biometric recognition system [6]. More recently, attacks on face recognition systems based on morphed biometric images have been presented [7], [8], which represent a presentation attack at the time of enrolment. Morphing techniques can be used to create artificial biometric samples, which resemble the biometric information of two (or more) individuals in image and feature domain. If morphed biometric images are infiltrated to a biometric recognition system during enrolment the subjects contributing to the morphed image will both (or all) be successfully verified against that single enrolled template. Hence, the unique link between individuals and their biometric reference data is not warranted. Fig. 1 shows an example of morphing two facial images.

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

Fig. 1: Examples for bona fide and morphed face images

Attacks based on morphed biometric samples were first introduced by Ferrara *et al.* [7]. Motivated by security gaps in the issuance process of electronic travel documents, the authors showed that commercial face recognition software tools are highly vulnerable to such attacks, i.e. different images of either subject are successfully matched against the morphed image. In their experiments, decision thresholds yielding a FMR of 0.1% have been used, according to the guidelines provided by the European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX) [3]. In a further study, the authors show that morphed face images are realistic enough to fool human examiners [9]. Scherhag *et al.* [8] reported moderate detection performance for benchmarking several general purpose texture descriptors used in conjunction with machine learning techniques to detect morphed face images. With respect to the above attack scenario, it is stressed that a detection of morphed face images becomes even more challenging if images are printed and scanned. Hildebrandt *et al.* [10] suggest to employ generic image forgery detection techniques, in particular multi-compression anomaly detection, to reliably detect morphed facial images. Kraetzer *et al.* [11] evaluate the feasibility of detecting facial morphs with keypoint descriptors and edge operators. The benefits of deep neural networks for detecting morphed images has been recently investigated by Ramachandra *et al.* [12].

Gomez-Barrero *et al.* [13] proposed the first theoretical framework for measuring the vulnerability of biometric systems to attacks based on morphed biometric samples. Further, key factors which take a major influence on a system's

vulnerability to such attacks have been identified, e.g. the shape of genuine and impostor score distributions or the FMR the system is operated at. To evaluate the vulnerability of biometric systems to attacks based on morphed images or templates, Scherhag *et al.* [14] introduced new metrics for vulnerability reporting, which strongly relate to the metrics defined in [15]. In addition, the authors provide recommendations on the assessment of morphing techniques. It is emphasized that unrealistic assumptions with respect to the quality of morphed biometric samples might cloud the picture regarding the performance of detection algorithms. It is important to note that so far there is no publicly available database of morphed face images and no publicly available morph detection algorithms.

In this work, the photo response non-uniformity (PRNU) is used to detect morphed face images. The PRNU [16] of an imaging sensor has emerged as an important tool for diverse forensic tasks including the detection of digital forgeries. It is shown that the proposed region-based analysis of PRNU behaviour reliably detects morphed face images. On a comprehensive database of bona fide and morphed face images practical detection performance is achieved. Moreover, we estimated the impact of different image post-processing steps applied to morphed face images on the detection performance of the proposed approach.

This paper is organized as follows: details on the employed extraction of PRNU signals are summarized in Sect. II. The proposed morph detection system is described in detail in Sect. III. Experimental results are presented in Sect. IV. Finally, conclusions are given in Sect. V.

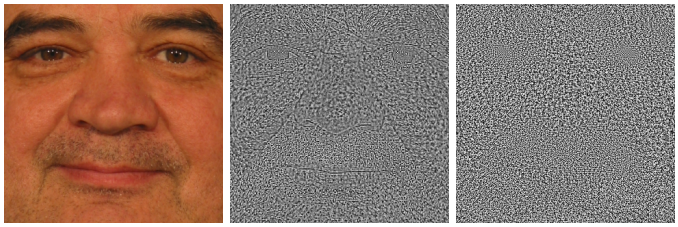
II. PRNU EXTRACTION

The PRNU is a noise-like pattern, originating from slight variations among individual pixels during the conversion of photons to electrons in digital image sensors. It forms an inherent part of those sensors, whereas this weak signal is embedded into each and every image they capture.

This systemic and individual pattern is essentially an unintentional stochastic spread-spectrum watermark that survives processing, such as lossy compression or filtering. The extraction of the PRNU noise residual from an image is performed by applying Fridrich's approach [17]. For each image I the noise residual W_I is estimated as described in Eq. (1),

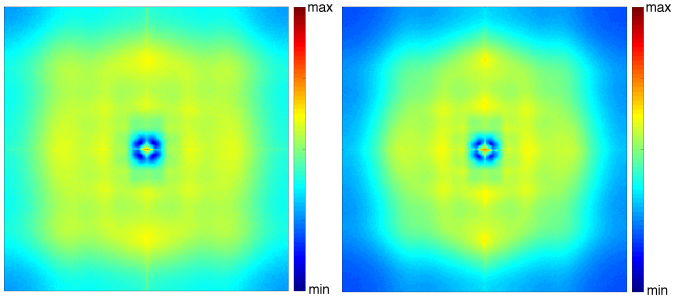
$$W_I = I - F(I) \tag{1}$$

where F is a denoising function which filters out the sensor pattern noise. In this work, the denoising filter proposed by Mihcak *et al.* [18] is used in conjunction with a filtering distortion removal (FDR) PRNU enhancement proposed by Lin *et al.* [19]. Said enhancement aims at improving the SNR of the extracted PRNU noise residual W_I in a two step process by abandoning certain components that are severely contamined by filtering errors introduced during the denoising of images. For further details on the denoising filter and FDR PRNU enhancement we refer to [18], [19]. Fig. 2 presents



(a) Original (b) PRNU (c) FDR enh.

Fig. 2: Example of PRNU extraction and FDR enhancement for a pre-processed face image.



(a) Bona fide (b) Morphs

Fig. 3: DFT magnitude spectra of the PRNUs extracted from bona fide and morphed face images, averaged over the whole dataset.

the extracted PRNU and FDR enhancement result for an exemplary image.

The following essential criteria, which have been described by Fridrich *et al.* [20], make the PRNU well suited for the face morph detection scenario dealt with in this work:

1) *Universality*: all imaging sensors exhibit PRNU.
2) *Generality*: the PRNU is present in every picture independently of the scene content, with the exception of completely dark or overexposed images.
3) *Robustness*: it survives lossy compression, filtering, gamma correction, and many other typical processing procedures. It is even reported to survive high quality printing and scanning [21].

We decided to use the PRNU for the morphing detection, because it is unrelated to the image content and is present in every image acquired with a digital camera, as described above. Thus, it offers significant advantages over analysing other high-frequency image components.

By investigating the spectral 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 strength of the PRNU [17]. By taking into consideration the processing steps applied during the face morphing, which consist of non-linear warping and averaging operations introducing interpolation artefacts, the distribution of the PRNU values is expected to change after such processing operations. Fig. 3 shows the discrete Fourier transform (DFT) magnitude spectra obtained by averaging the PRNU of all bona fide and morphed face images contained in the

investigated dataset, which is described in Sect. IV. It clearly reveals a reduction of the high-frequency components within the DFT magnitude spectrum for the morphed images, as compared to the bona fide images. Furthermore, the spectrum is compressed, causing the area of the larger magnitudes to shrink. These effects are likely caused by the averaging and non-linear warping operations that occur during the morphing process and change the distribution of the DFT magnitudes.

Our approach aims at exploiting these effects in order to perform a blind no-reference face morph detection, which is presented in the following section.

III. Detection of morphed face images

As stated in the previous section, the goal of the proposed PRNU-based morph detection system is to exploit the spectral alterations introduced by the non-linear warping during the face morphing process within the PRNU to be able to discriminate between bona fide and morphed images. Furthermore, the discrimination is performed in a blind manner, i.e. without the need for any trusted bona fide reference image of one of the morphed subjects.

The proposed system follows the divide and conquer principle and consists of four major components: (A) *PRNU extraction*, (B) *PRNU splitting*, (C) *cell-wise feature extraction*, and (D) *cell aggregation*. The remainder of this section will discuss the different processing steps in more detail.

A. PRNU Extraction

The PRNU for each individual image is extracted, as described in Sect. II, by using the wavelet-based denoising filter by Mihcak *et al.* [18]. The extracted PRNU is then further enhanced using the FDR (frequency distortion removal) PRNU enhancement proposed by Lin *et al.* [19]. The PRNU is always extracted for the whole image, whereat every colour image is converted to grey-scale first according to [17]. The outcome of the PRNU extraction and PRNU enhancement process is illustrated in Fig. 2.

B. PRNU Splitting

The proposed system is able to work with the PRNU from the whole image, as well as arbitrary splits of the PRNU into multiple equisized cells. In this work, we investigate different cells configurations, from the whole image as a single cell up to $N = 10 \times 10$ cells. A larger number of cells is expected to further expose the non-linear transformations of the PRNU during the morphing process by putting stronger emphasis on local variations within an image. Eventually, we obtain N different cells $C_1, \ldots, C_N$. Fig. 4 shows an example of how the PRNU is split into $N = 2 \times 2$ equisized cells.

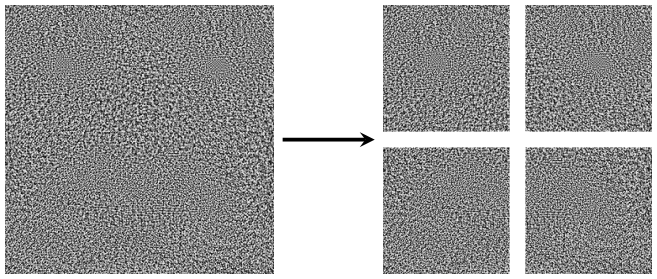


Fig. 4: Example for splitting the PRNU into $N = 4$ equisized cells (2×2).

C. Cell-wise Feature Extraction

The feature extraction is performed for every cell individually. The first step consists in obtaining the frequency spectrum of the PRNU in each cell, which is done by means of the discrete Fourier transform (DFT). The resulting magnitude spectrum, as already shown in Sect. II, reveals the alterations of the PRNU signal caused by the morphing process. To quantify these effects, we calculate the histogram of the DFT magnitudes in order to represent the magnitude distribution within the spectrum. Fig. 5 shows the DTF magnitude spectra of a bona fide and morphed sample image with the corresponding histograms, where a shift of the magnitude distribution can be observed. All DFT magnitude histograms have been constrained to the same universal range of $[0, 8]$ and are divided into 100 bins. The range has been established with the values obtained from the DFT of all extracted PRNUs.

Based on the observations from Sect. II, this magnitude histogram forms the basis for the different morph detection approaches in this work. We select the position of the peak P_{pos} in the histogram and its height or value P_{val} as being suited for the discrimination between bona fide and morphed images. We obtain P_{val} and P_{pos} as follows:

$$P_{val} = \max_{n=1\ldots b} H(n) \tag{2}$$

$$P_{pos} = \arg\max_{n=1\ldots b} H(n) \tag{3}$$

where b is the number of bins and H is the histogram of a cell. P_{pos} describes the position (bin) of the peak in the DFT magnitude histogram, while P_{val} represents the value (relative frequency) of the corresponding bin.

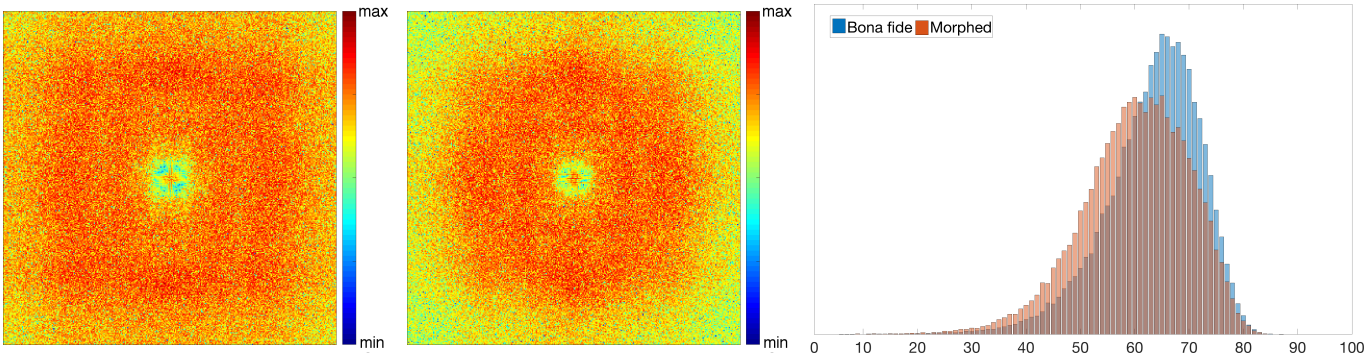
Furthermore, we consider the product of the peak position and value P_{pv} within the DFT magnitude histograms as a third combined feature:

$$P_{pv} = \max_{n=1\ldots b} H(n) * \arg\max_{n=1\ldots b} H(n) \tag{4}$$

Finally, we obtain a scalar value P for each PRNU cell, which is calculated using one of the the three approaches defined in Eqs. 2 to 4.

D. Cell Aggregation

As final step, the extracted features P for each cell C_n, in form of scalar values, are aggregated to obtain a global score S for the image. We investigated various strategies, whereas



(a) Bona fide image (b) Morphed image (c) DFT magnitude histograms

Fig. 5: Comparison of DFT magnitude spectra and histograms of a bona fide and a morphed sample image.

TABLE I: Database used for experimental evaluations

Gender	No. of subjects	No. of images	Bona fide images	Morphed images
Male	58	2,210	499	1,711
Female	39	1,165	462	703
All	97	3,375	961	2,414

we will present the two best performing ones. The aggregation strategies used in this work are:

$$S_{mean} = \frac{1}{N}\sum_{n=1}^{N} P_n \tag{5}$$

$$S_{rms} = \sqrt{\frac{1}{N}\sum_{n=1}^{N} P_n^2} \tag{6}$$

where N is the number of total PRNU cells and P_n is the feature (scalar value) obtained for the PRNU cell C_n, as described in the previous processing step.

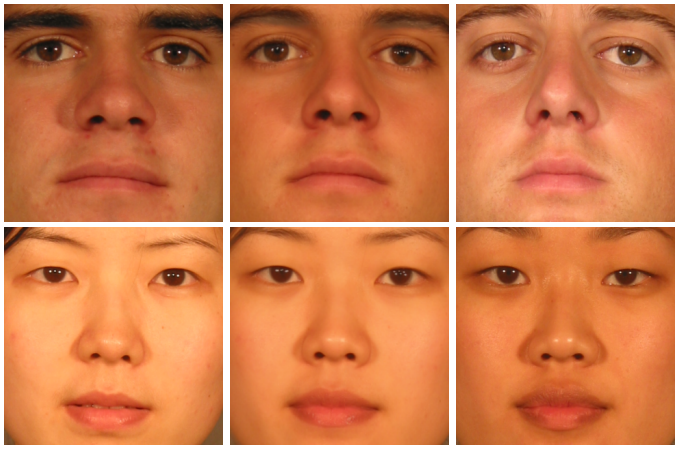
S_{mean} simply averages the scores of the individual cells, while S_{rms} characterizes the root mean square of the scores of all PRNU cells within an image. Eventually, we obtain a single scalar value S per image using one of the Eqs. 5 or 6. The value of S then indicates whether a face image has been created by morphing other face images or not. The final decision for a face image can be taken by a simple threshold.

IV. Experiments

In the following subsection, the generation of morphed face images and applied post-processing steps are described. In subsequent subsections, experimental results are reported which comprise a face recognition vulnerability assessment and a morph detection performance estimation.

A. Morph Generation and Post-processing

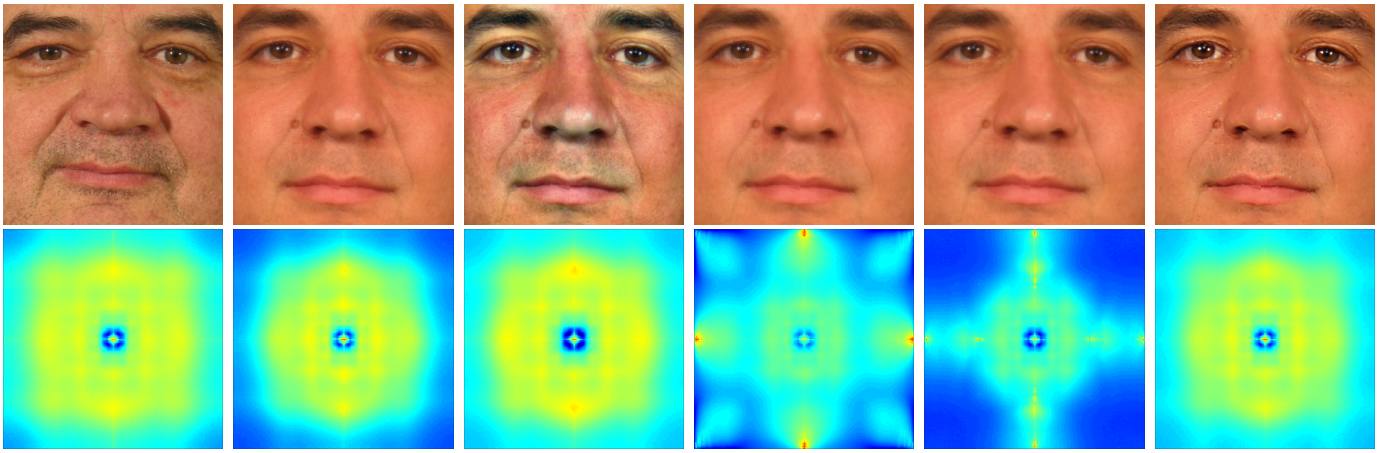
Experiments are performed on a subset of the FRGCv2 face database. A total number of 961 frontal faces with neutral expression have been manually selected and ICAO compliance has been verified, i.e. the distance between the eyes of a face has to be at least 90 pixels [22]. Details about the employed database are listed in Table I. In order to morph two face images the *dlib* facial landmark detector [23] is applied to both images. Subsequently, a Delaunay triangulation is performed to the average of corresponding points. An affine transform is then applied to the sets of triangles in both face images resulting in two warped images which are alpha blended using a alpha value of 0.5. In the pre-processing stage an image is segmented and normalized according to eye coordinates detected by the landmark detector. Subsequently, the normalized region is cropped to 320×320 pixels using predefined offsets to ensure that the morph detection algorithm is only applied to the facial region. Based on this subset 2,414 morphed faces have been automatically generated for pairs of subjects of same gender using the *OpenCV* library. Example images of bona fide and morphed face images are shown in Fig. 6, which illustrates the high quality of morphed face images being well in the quality limits set forth by ICAO and ISO/IEC standards.



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

Fig. 6: Examples of bona fide and morphed face images of subjects of same gender, ethnicity and age group

In addition, we also investigate the robustness of the proposed morphing detection system against different post-processing techniques. For this work we investigate four dif-



(a) Bona fide (b) Morph (c) EQU (d) SCL_{50} (e) SCL_{75} (f) SHRP

Fig. 7: Bonafide image (a) and results of applying the different post-processings to a morphed image (b to f). Below, the corresponding DFT magnitude spectra are shown (averaged over the whole dataset).

ferent techniques, which aim at further modifying the quality of the morphed face images:

- *EQU*: Contrast limited adaptive histogram equalization (CLAHE)
- SCL_{50}: Downscaling the image to 50% of its original size and subsequent upscaling
- SCL_{75}: Downscaling the image to 75% of its original size and subsequent upscaling
- *SHRP*: Sharpening the image using unsharp masking

The results of applying these post-processings to a morphed image and how they affect its DFT magnitude spectrum are demonstrated in Fig. 7.

B. Face Recognition Vulnerability Assessment

The attack success of the generated morphing attacks on a commercial-of-the-shelf face recognition system is evaluated using the metrics defined in [14]. In particular, the Relative Morph Match Rate (RMMR) and the ProdAvg Mated Morph Presentation Match Rate (ProdAvg-MMPMR).

When employing the default decision threshold of the COTS face recognition system a near-perfect MMPMR and RMMR (> 0.99) is obtained for using original morphed face images as well as post-processed. This means almost all face images of subjects contributing to a morphed face image are successfully matched against it which emphasizes the necessity of a robust morph detection subsystem. While the post-processings have a negligible impact on the vulnerability of the face recognition systems to morphing attacks, they should hamper the automatic detection of morphs.

C. Morph Detection Performance Evaluation

The performance of the detection algorithms is reported according to metrics defined in ISO/IEC 30107-3 [15]. The Attack Presentation Classification Error Rate (APCER) is defined as the proportion of attack presentations using the same presentation attack instrument species incorrectly classified as bona fide presentations in a specific scenario. The Bona Fide Presentation Classification Error Rate (BPCER) is defined as the proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario. The D-EER, i.e. the operation point where APCER $=$ BPCER, is used as general operation point and reported for images with and without post-processing. In addition, the BPCER10, i.e. the operation point where APCER $= 10\%$, and BPCER20, i.e. the operation point where APCER $= 5\%$, are estimated.

The performance of the proposed morph detectors is listed in Table II. The *Feature* column contains different combinations of extracted features P and aggregation strategies S, which are defined in Sect. III. The basic attempt using the whole image as a single cell, denoted as 1×1 in the table, is suitable to detect morphed face images with an D-EER as low as 2.1%. It is possible to improve the performance by splitting the image into cells, however, if the fragmentation is smaller than 8×8 cells, where a D-EER as low as 1.4% is achieved, the detection performance decreases again. Due to the lack of robustness to histogram shifts some post-processing techniques, e.g. equalization (*EQU*) and sharpening (*SHRP*), are severely influencing the performance of the algorithm. Note that depending on the direction of the histogram shift the results might even improve, as for *SCL*. This lack of robustness can be partially compensated for *SHRP* by employing a higher fragmentation of 8×8 cells, which is able to lower the D-EER to 11.9%. However, the *EQU* post-processing cannot be compensated at all. Clearly, further improvement of the detection algorithms is needed to counter this type of post-processing. The performance of the detectors highly depends on the type of aggregation (only the two best performing ones are presented in this work), as well as on the number of cells. On the given dataset the best overall performance was achieved with $P_{pos}|S_{mean}$ and $P_{pos}|S_{rms}$ with 8×8 cells (marked bold in Table II), yielding a D-EER as low as 2.2% on

TABLE II: Performance of proposed PRNU-based morph detectors

		D-EER					BPCER10					BPCER20				
Feature	**Cells**	**Morph**	**EQU**	**SCL$_{50}$**	**SCL$_{75}$**	**SHRP**	**Morph**	**EQU**	**SCL$_{50}$**	**SCL$_{75}$**	**SHRP**	**Morph**	**EQU**	**SCL$_{50}$**	**SCL$_{75}$**	**SHRP**
$P_{val}\|S_{mean}$	1	2.1%	34.8%	0.7%	2.2%	46.4%	0.6%	52.2%	0.2%	0.7%	78.4%	1.1%	58.5%	0.3%	1.3%	85.9%
$P_{val}\|S_{rms}$		2.1%	34.8%	0.7%	2.2%	46.4%	0.6%	52.2%	0.2%	0.7%	78.4%	1.1%	58.5%	0.3%	1.3%	85.9%
$P_{pos}\|S_{mean}$		5.1%	36.4%	4.5%	0.3%	20.1%	1.5%	68.2%	1.4%	0.0%	39.4%	5.3%	77.4%	3.8%	0.0%	57.0%
$P_{pos}\|S_{rms}$		5.1%	36.4%	4.5%	0.3%	20.1%	1.5%	68.2%	1.4%	0.0%	39.4%	5.3%	77.4%	3.8%	0.0%	57.0%
$P_{pv}\|S_{mean}$		2.2%	32.9%	0.9%	0.2%	36.9%	0.2%	50.5%	0.1%	0.0%	64.3%	0.6%	59.1%	0.2%	0.0%	77.3%
$P_{pv}\|S_{rms}$		2.2%	32.9%	0.9%	0.2%	36.9%	0.2%	50.5%	0.1%	0.0%	64.3%	0.6%	59.1%	0.2%	0.0%	77.3%
$P_{val}\|S_{mean}$	2	2.0%	36.3%	0.7%	2.0%	45.8%	0.5%	53.2%	0.1%	0.7%	77.4%	1.0%	59.9%	0.3%	1.1%	84.3%
$P_{val}\|S_{rms}$		2.0%	36.3%	0.6%	2.0%	45.9%	0.5%	53.0%	0.1%	0.7%	77.7%	1.0%	59.8%	0.3%	1.1%	84.6%
$P_{pos}\|S_{mean}$		3.3%	33.4%	2.5%	0.2%	17.1%	0.9%	63.2%	0.8%	0.0%	31.3%	2.1%	74.3%	1.4%	0.0%	49.6%
$P_{pos}\|S_{rms}$		3.2%	33.1%	2.4%	0.2%	17.0%	0.8%	62.8%	0.7%	0.0%	31.1%	1.9%	73.5%	1.3%	0.0%	47.4%
$P_{pv}\|S_{mean}$		1.7%	32.8%	1.0%	0.1%	32.6%	0.4%	50.7%	0.1%	0.1%	60.7%	0.8%	60.3%	0.3%	0.1%	74.0%
$P_{pv}\|S_{rms}$		1.6%	32.6%	1.0%	0.1%	33.1%	0.4%	50.4%	0.1%	0.1%	61.0%	0.8%	60.0%	0.3%	0.1%	74.4%
$P_{val}\|S_{mean}$	4	1.9%	35.3%	0.5%	3.6%	40.5%	0.7%	51.4%	0.1%	1.7%	64.5%	1.1%	58.2%	0.2%	3.0%	72.8%
$P_{val}\|S_{rms}$		1.9%	35.1%	0.5%	3.6%	41.3%	0.7%	51.3%	0.1%	1.8%	66.0%	1.1%	58.3%	0.2%	2.9%	73.6%
$P_{pos}\|S_{mean}$		2.9%	33.0%	1.5%	0.1%	12.3%	0.2%	59.9%	0.1%	0.0%	16.5%	1.1%	71.8%	0.4%	0.0%	39.5%
$P_{pos}\|S_{rms}$		2.8%	32.8%	1.4%	0.1%	12.3%	0.2%	59.5%	0.1%	0.0%	16.6%	1.0%	71.4%	0.4%	0.0%	40.0%
$P_{pv}\|S_{mean}$		1.5%	32.3%	0.5%	0.1%	22.0%	0.2%	48.9%	0.0%	0.0%	41.0%	0.4%	57.8%	0.1%	0.0%	58.3%
$P_{pv}\|S_{rms}$		1.5%	32.0%	0.5%	0.1%	23.7%	0.2%	48.5%	0.0%	0.0%	43.7%	0.4%	57.6%	0.1%	0.0%	60.7%
$P_{val}\|S_{mean}$	8	3.2%	35.5%	0.4%	7.4%	34.5%	1.2%	53.5%	0.0%	6.2%	54.5%	2.1%	61.1%	0.1%	9.3%	64.1%
$P_{val}\|S_{rms}$		3.3%	35.6%	0.4%	7.6%	35.8%	1.3%	53.5%	0.0%	6.5%	56.7%	2.3%	61.0%	0.1%	10.1%	65.9%
$P_{pos}\|S_{mean}$		**2.2%**	**33.8%**	**0.7%**	**0.0%**	**10.8%**	**0.1%**	**60.2%**	**0.0%**	**0.0%**	**11.7%**	**0.6%**	**71.5%**	**0.1%**	**0.0%**	**30.8%**
$P_{pos}\|S_{rms}$		**2.3%**	**33.6%**	**0.8%**	**0.0%**	**11.0%**	**0.1%**	**59.8%**	**0.0%**	**0.0%**	**13.2%**	**0.6%**	**71.4%**	**0.1%**	**0.0%**	**32.8%**
$P_{pv}\|S_{mean}$		1.4%	31.8%	0.3%	0.1%	15.9%	0.2%	51.9%	0.0%	0.0%	24.0%	0.4%	60.5%	0.0%	0.0%	44.2%
$P_{pv}\|S_{rms}$		1.5%	31.3%	0.3%	0.0%	17.3%	0.2%	51.2%	0.0%	0.0%	26.9%	0.4%	60.2%	0.0%	0.0%	48.8%
$P_{val}\|S_{mean}$	10	3.8%	36.7%	0.3%	9.0%	33.1%	1.5%	54.5%	0.0%	8.3%	51.2%	3.0%	60.4%	0.1%	13.2%	61.3%
$P_{val}\|S_{rms}$		3.9%	36.7%	0.3%	9.3%	34.1%	1.6%	54.8%	0.1%	8.6%	53.2%	3.3%	60.7%	0.1%	14.3%	63.0%
$P_{pos}\|S_{mean}$		2.4%	34.9%	0.6%	0.0%	10.5%	0.0%	61.7%	0.0%	0.0%	11.2%	0.7%	71.6%	0.0%	0.0%	28.4%
$P_{pos}\|S_{rms}$		2.6%	34.6%	0.6%	0.0%	10.9%	0.0%	61.3%	0.0%	0.0%	12.3%	0.8%	71.6%	0.0%	0.0%	30.3%
$P_{pv}\|S_{mean}$		1.8%	32.8%	0.2%	0.1%	13.9%	0.1%	53.3%	0.0%	0.0%	20.8%	0.3%	62.7%	0.0%	0.0%	41.7%
$P_{pv}\|S_{rms}$		1.8%	32.4%	0.2%	0.0%	15.0%	0.1%	52.7%	0.0%	0.0%	25.0%	0.3%	62.3%	0.0%	0.0%	46.1%

the original morphed images, 0.0% to 0.8% on scaled images and as low as 10.8% on sharpened images. An appropriate choice for the amount of used cells obviously relates on the resolution of the processed image. Overall, it can be observed that both aggregation strategies S_{mean} and S_{rms} obtain similar results across all extracted features. Furthermore, a higher fragmentation of up to 8×8 cells, and therefore analysis of the local alterations within the image, is observed to be beneficial to the detection performance. The position of the peak P_{pos} in the DFT magnitude spectrum emerged as the most stable among the extracted features across all applied post-processings.

V. Conclusion and Future Work

In this work, we proposed an automated morph detection for face images based on the PRNU. The procedure of creating morphed face images takes influence on the property of PRNU values, in particular across different image regions. It is shown that a cell-based PRNU analysis allows for a reliable detection of morphed face images. Furthermore, we analysed the impact of different image post-processing techniques on the detection performance, where the proposed detection system was robust against scaling and sharpening of the images, and only failed for the applied histogram equalisation. Deeper investigation and an improvement of the detection approaches is clearly needed to counter the failed detection of morphed images in this case.

Future studies might also include a vulnerability analysis of proposed detection algorithms to attacks based on PRNU insertion/substitution. Additionally, an investigation of the proposed morph detection systems for images from different cameras as well as for printed and scanned images could be subject to future work.

Acknowledgements

This work was supported by the German Federal Ministry of Education and Research (BMBF) as well as by the Hessen State Ministry for Higher Education, Research and the Arts (HMWK) within the Center for Research in Security and Privacy (CRISP). Furthermore, this work was also supported by the Austrian Science Fund (FWF) under Project No. P26630.

References

[1] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM Comput. Surveys*, vol. 35, no. 4, pp. 399–458, 2003.

[2] S. Z. Li and A. K. Jain, *Handbook of Face Recognition (2nd edition)*. Springer, 2011.

[3] "FRONTEX – Research and Development Unit: Best practice technical guidelines for automated border control (ABC) systems," 2012, version 2.0.

[4] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.

[5] S. Marcel, M. Nixon, and S. Z. Li, *Handbook of Biometric Anti-Spoofing*. Springer-Verlag New York, Inc., 2014.

[6] ISO/IEC TC JTC1 SC37 Biometrics, *ISO/IEC IS 30107-1. Information Technology – Biometrics presentation attack detection – Part 1: Framework*, International Organization for Standardization, Mar. 2016.

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

[8] 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.

[9] M. Ferrara, A. Franco, and D. Maltoni, "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.

[10] M. Hildebrandt, T. Neubert, A. Makrushin, and J. Dittmann, "Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps," in *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, 2017, pp. 1–6.

[11] C. Kraetzer, A. Makrushin, T. Neubert, M. Hildebrandt, and J. Dittmann, "Modeling attacks on photo-ID documents and applying media forensics for the detection of facial morphing," in *Proc. Workshop on Information Hiding and Multimedia Security (IH& MMSec)*, 2017, pp. 21–32.

[12] R. Ramachandra, K. Raja, S. Venkatesh, and C. Busch, "Transferable deep-cnn features for detecting digital and print-scanned morphed face images," in *2017 IEEE Conf. on Computer Vision and Pattern Recognition Workshop (CVPRW)*, July 2017.

[13] M. Gomez-Barrero, C. Rathgeb, U. Scherhag, and C. Busch, "Is your biometric system robust to morphing attacks?" in *Proc. Int. Workshop on Biometrics and Forensics (IWBF)*, 2017, pp. 1–6.

[14] 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.

[15] ISO/IEC JTC1 SC37 Biometrics, *ISO/IEC IS 30107-3:2017, IT – Biometric presentation attack detection – Part 3: Testing and Reporting*.

[16] M. Chen, J. Fridrich, M. Goljan, and J. Lukas, "Determining image origin and integrity using sensor noise," *Trans. Info. For. Sec.*, vol. 3, no. 1, pp. 74–90, Mar. 2008.

[17] J. Fridrich, "Digital image forensic using sensor noise," *IEEE Signal Processing Magazine*, vol. 26, no. 2, March 2009.

[18] 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.

[19] 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.

[20] J. Fridrich, "Sensor defects in digital image forensics," in *Digital Image Forensics: There is more to a picture than meets the eye*, H. Sencar and N. Memon, Eds. Springer Verlag, 2012, ch. 6, pp. 179–218.

[21] 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.

[22] International Organization for Standardization, "Information technology – Biometric data interchange formats – Part 5: Face image data," JTC 1/SC 37, ISO/IEC 19794-5:2005 consolidated, 2005.

[23] D. E. King, "Dlib-ml: A machine learning toolkit," *Journal of Machine Learning Research*, vol. 10, 2009.