This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

Detection of Face Morphing Attacks based on PRNU Analysis

Ulrich Scherhag, Luca Debiasi, Christian Rathgeb, Christoph Busch and Andreas Uhl

Abstract—Recent research found that attacks based on morphed face images, i.e. morphing attacks, pose a severe security risk to face recognition systems. A reliable morphing attack detection from a single face image remains a research challenge since cameras and morphing techniques used by an attacker are unknown at the time of classification. These issues are commonly overseen while many researchers report encouraging detection performance for training and testing morphing attack detection schemes on images obtained from a single face database employing a single morphing algorithm.

In this work, a morphing attack detection system based on the analysis of Photo Response Non-Uniformity (PRNU) is presented. More specifically, spatial and spectral features extracted from PRNU patterns across image cells are analyzed. Differences of these features for bona fide and morphed images are estimated during a threshold-selection stage using the Dresden image database which is specifically built for PRNU analysis in digital image forensics. Cross-database evaluations are then conducted employing an ICAO compliant subset of the FRGCv2 database and a Print-Scan database which is a printed and scanned verison of said FRGCv2 subset. Bona fide and morphed face images are automatically generated employing four different morphing algorithms. The proposed PRNU-based morphing attack detector is shown to robustly distinguish bona fide and morphed face images achieving an average D-EER of 11.2% in the best configuration. In scenerios where image sources and morphing techniques are unknown, it is shown to significantly outperform other previously established morphing attack detectors. Finally, the limitations and potential of the approach are demonstrated on a dataset of printed and scanned bona fide and morphed face images.

Index Terms—Biometrics, face recognition, face morphing, face morphing attack, morphing attack detection, photo response non-uniformity.

1 Introduction

Face recognition systems have recently been exposed to be vulnerable against attacks based on morphed face images [1], [2]. Image morphing has been an active field of image processing research since the 1980s [3], [4] with a variety of application scenarios, especially in the film industry. Morphing techniques can be used to create artificial biometric samples that resemble the biometric information of two (or more) individuals in the image and feature domain. An example of a morphed face image is shown in Fig. 1. The morphed face image is successfully verified against probe samples of both subjects involved using state-of-the-art face recognition systems. This means that if a morphed face image is somehow stored as a reference in the database of a face recognition system, both individuals involved are successfully verified against this manipulated reference. Morphed face images thus pose a serious threat to face recognition systems, as the basic principle of biometrics, the unique link between the biometric reference data and the subject, is violated.

In many countries, the face image used for the ePassport application process is provided by the applicant either in analogue or digital form. In the scenario of a face morphing attack, a wanted *criminal* could morph his facial image with one of a lookalike *accomplice*. If the accomplice applies for an ePassport with the morphed face image, he will receive a valid ePassport equipped with corresponding document security features. It is important to note that morphed face images can be realistic enough to fool human examiners [6], [7] as well as commercial face recognition systems. Both the criminal and the accomplice could then be successfully verified against the morphed image stored in the ePassport. This means that the criminal can use the ePassport issued to the accomplice to pass through Automated Border Control (ABC) gates (or even human inspections at border crossings). The risk of this attack, called *face morphing attack*, is amplified by the fact that realistic face morphs can be generated by non-experts using user-friendly face morphing software that is either freely available or can be purchased at a reasonable price.

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

Fig. 1. Example for a morphed face image (b) of subject 1 (a) and subject 2 (c) (images taken from [5]).

In 2014 Ferrara et al. [1] were the first to thoroughly investigate the vulnerability of commercial face recognition systems to attacks based on morphed face images. So far, a considerable amount of morphing attack detection approaches has been published, see Sect. 2. For a comprehensive survey the reader is referred to [2]. Proposed ap-

- *U. Scherhag, C. Rathgeb and C. Busch are with the da/sec - Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany.*
- *L. Debiasi and A. Uhl are with the WaveLab - The Multimedia Signal Processing and Security Lab, Universität Salzburg, Austria.*

proaches can be categorized with respect to the considered morphing attack detection scenario:

- *No-reference morphing attack detection*: the detector processes a single image, e.g. the analysis of a printed image that is presented and scanned in a passport application procedure and subsequently stored in an electronic travel document or at any later point in time an off-line authenticity check of said document by police investigators (this scenario is also referred to as single image morphing attack detection or forensic morphing attack detection);
- *Differential morphing attack detection*: a trusted live capture from an authentication attempt serves as additional source of information for the morph detector, e.g. during authentication at an ABC gate (this scenario is also referred to as image pair-based morphing attack detection). Note that all information extracted by no-reference morph detectors might as well be leveraged within this scenario [8].

Obviously, the no-reference scenario turns out to be more challenging compared to the differential one. While the majority of no-reference approaches reports practical detection error rates, these are commonly evaluated on a dataset of bona fide and morphed face images which are extracted from a single (in-house) face database. In such an experimental setup the use of machine learning-based feature extractors or/and classifier increases the risk of overfitting, i.e. the robustness of morph detection algorithms may not be retained with regard to images stemming from other sources as shown in [9].

This work represents a significant extension of the preliminary studies towards PRNU-based morphing attack detection previously published in [5], [10]. The proposed system has been complemented by a more thorough investigation of different features and aggregation strategies, more specifically spatial features have been investigated in addition to spectral ones from previous work. Complementary to those efforts cross-database experiments on morphed face images generated by four different morphing algorithms have been conducted. The generalizability of the PRNU-based morphing attack detection across a wide range of distinct cameras of various makers is further investigated on a database specifically built for PRNU analysis in digital image forensics and it is shown that said database is suitable to determine the decision threshold for the proposed system. In addition, a database of printed and scanned face images is employed in evaluations. Moreover, in experiments the proposed system is benchmarked against state-of-the-art morphing attack detectors. Also, vulnerability analysis of the proposed concept with respect to potential attacks to circumvent the detection system is given.

The remainder of this work is organized as follows: related works are discussed in Sect. 2. Fundamentals of PRNU extraction are explained in Sect. 3. The proposed morph detection method is described in detail in Sect. 4. Experimental results are reported in Sect. 5. Finally, conclusions are summarized in Sect. 6.

2 Related Work

In recent years, numerous no-reference face morphing attack detection schemes have been proposed. Published methods and their properties are summarized in Table 1 which has been derived from [2]. In some papers more than one system was presented, in such cases approaches that showed the best performance in detecting morphing attacks are listed. It is important to note that the generalizability/robustness of the published approaches could not be demonstrated. So far, there are no publicly accessible large databases of bona fide and morphed facial images and hardly any publicly available morph recognition algorithms which allow comprehensive experimental evaluations. The vast majority of published methods were trained and tested on various sequestered databases, which hampers reproducibility of results[1]. In addition, morph detection methods are usually trained and tested on a single database with a single morph generation algorithm. Based on these facts, a comparison of published approaches with respect to reported detection performance would be potentially misleading and is deliberately avoided in this work. However, it is expected that planned benchmark tests, e.g. by the National Institute of Standards and Technology (NIST) [40], will enable a meaningful quantitative comparison of published approaches in the near future.

Several researchers have suggested the use of general-purpose image descriptors, such as Local Binary Patterns (LBP) [41] or Binarized Statistical Image Features (BSIF) [42], which are widely used for biometric recognition. Ramachandra et al. [11] proposed a system based on a Support Vector Machine (SVM) trained on extracted BSIF features. For the training and evaluation of the SVMs, an internal database with morphed facial images was created. In a derivative version of the same database, Scherhag et al. [12] examined the accuracy of morphing detection on printed and scanned images using the proposed algorithm. Furthermore, Ramachandra et al. [13] proposed a Probabilistic Collaborative Representation Classifier (Pro-CRC) [43] trained on LBP features extracted from the color channels. The database used was an internal database derived from FRGCv2 [14]. The authors concentrate on the differences between morphed and averaged images in the evaluation.

A more complex method for morphing attack detection is proposed in [16], [17], where a Vietoris-Rips complex is formed from the reactions of uniform LBP extractors on the image. In [38] a high detection performance was shown by Wandzik et al. for a linear SVM trained on high-dimensional LBP features [44] extracted from the FEI database [45]. In [46] Ramachandra et al. proposed an LBP extraction of Laplacian pyramids build on different color channels. Agarwal et al. [15] suggest training an SVM with Weighted Local Magnitude Pattern. Similar to LBP, the proposed descriptor encodes the differences between a central pixel and its neighbors. However, instead of binarizing them, it assigns weights inversely proportional to the difference to

1. Also the morphed images used in this work can not be published due to licensing conditions as these are generated based on subsets of available image database collected by different institutions. However, efforts are currently made by different research laboratories to acquire new datasets of bona fide and morphed face images that shall serve future open benchmarks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

TABLE 1
Overview of most relevant no-reference face morphing attack detection algorithms.

Ref.	Approach	Morphing method	Source face database	Post-processing	Remarks
[11]	BSIF + SVM	GIMP/GAP	in-house	-	-
[12]	BSIF + SVM	GIMP/GAP	in-house	print and scan	fixed database of [11]
[13]	Multi-channel-LBP + Pro-CRC	OpenCV	FRGCv2 [14]	print and scan	-
[15]	WLMP + SVM	Snapchat	in-house	-	-
[16], [17]	ULBP + RIPS + KNN	[18]	Utrecht [19]	-	-
[20]	Image degradation	triangulation + blending (+ swapping)	in-house, Utrecht [19]	-	-
[8]	BSIF + SVM	triangulation + blending	FRGCv2 [14]	-	-
[21]	Score-level fusion of general purpose image descriptors	triangulation + blending	FRGCv2 [14]	-	-
[9]	HOG + SVM	triangulation + blending	FRGCv2 [14], FERET [22], ARface [23]	-	cross database performance evaluation
[24]	LBP + SVM	triangulation + blending	FRGCv2 [14], FERET [22]	-	cross database performance evaluation
[25]	LBP + SVM	MorGan [25]	CelebA [26]	-	-
[5], [10]	PRNU analysis	triangulation + blending	FRGCv2 [14]	hist. equalization scaling, sharpening	-
[27]	SPN analysis	triangulation + blending (+ swapping)	Utrecht [19], FEI [28]	-	-
[18]	Double-compression artefacts analysis	triangulation + blending (+ swapping)	Utrecht [19], FEI [28]	-	-
[29]	Double-compression artefacts analysis	[18]	Utrecht [19], FEI [28]	-	-
[30]	Reflection analysis	triangulation + blending (+ swapping)	in-house	-	-
[31]	Luminance component + steerable pyramid + ProCRC	unclear	[13] extended	print and scan	-
[32]	VGG19 + AlexNet + ProCRC	[12]	in-house	print and scan	-
[33]	VGG19	triangulation + blending (+ swapping)	BU-4DFE [34], CFD [35], FEI [28], FERET [22], PUT [36], scFace [37], Utrecht [19], in-house	motion blur, Gaussian blur, salt-and-pepper noise, Gaussian noise	trained on all combinations (no unseen attack classes)
[38]	High-Dim. LBP + SVM	triangulation + blending + swapping	Multi-PIE [39]	-	-

the middle pixel. Depending on the feature representation of texture descriptors, the input of classifiers has to be adjusted. E.g. for Scale-Invariant Feature Transform (SIFT) [47] it has been shown that the number of extracted key points is suitable for the task of morph recognition [8], [20]. A score level fusion of several image descriptors could further improve the recognition rate [21]. Therefore, LBP, BSIF, SIFT, Speeded Up Robust Features (SURF) [48], Histogram of Oriented Gradients (HOG) [49] and the deep features of Openface [50] were merged and evaluated by Scherhag et al. [21]. Damer et al. [25] tested the suitability of LBP features for the detection of morphs generated by Generative Adversarial Networks (GANs). In the no-reference scenario, classifiers may rely on different microtexture properties. These can be dataset-specific features that are changed or can be introduced by the morphing process. Especially the combination of features that reflect different information, e.g. LBP and SIFT, leads to improvements. It has been shown that the performance of morph detectors based on general-purpose image descriptors may decrease significantly if training and test images are taken from another image source [9], [24].

During the morphing process, not only the texture but the entire signal of the image is manipulated. A further recognition approach is therefore the analysis of the changes in the sensor noise pattern, e.g. PRNU [5]. Therefore, the PRNU pattern, which originates from imperfections within the camera's sensor, not only differing for each model, but also for each individual camera, is extracted from a facial image and the discrete Fourier variables are calculated. The mean value and variance are then derived from the resulting histogram. Recently, Debiasi et al. [10] proposed an improved version of this scheme based on PRNU variance analysis across image blocks. A similar approach has been proposed by Zhang et al. [27] confirming the usefulness of morph detection based on sensor noise pattern analysis.

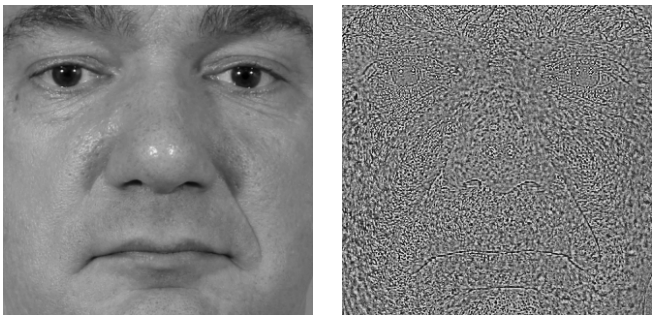
Both PRNU-based morph detection approaches analyse the Fourier Spectrum of the PRNU and quantify spectral differences between bona fide and morphed images using statistical measures. The main difference between both approaches lies within the processing pipeline, block-based analysis in the spatial [5], [10] vs. spectral domain [27], and final classification. The morph detector proposed in [5] and [10] does not need any training data, since it solely relies on a simple thresholding for the final decision, while the one in [27] utilises a linear SVM, which needs to be trained with bona fide and morphed images and makes the latter approach potentially more vulnerable against unknown morphing attacks. Furthermore, different PRNU extraction and enhancement techniques are used for both approaches. In contrast to [5], [10], the authors of [27] did not consider image post-processings. Also, no cross-database performance evaluations were performed.

Morphing attack detection methods based on continuous image degradation were proposed in [20], [51], [52]. The basic idea behind these methods is to continuously deteriorate the image quality, e.g. by JPEG compression, in order to generate several artificial self-references of a facial image. The distances between these references and the original image are then analyzed for morph detection. Ramachandra et al. [31] suggests the analysis of high

frequencies. In their approach images are converted to grayscale and a controllable pyramid is built and a Collaborative Representation Classifier (CRC) is trained on the high frequencies. The database used was printed and scanned. An alternative to handcrafted feature extractors is the use of statistical machine learning on the unprocessed image to distinguish between morphed and bona fide images. Ramachandra et al. [32] suggested adapting two convolutional neural networks (CNNs) (VGG19 [53] and AlexNet [54]) by transfer learning and combining the intermediate features to train a CRC. In [55] three CNNs, namely VGG19, AlexNet and GoogLeNet [56], are assessed as pre-trained and non-pre-trained models with respect to their morph detection abilities. Also with these methods there is a potential problem of over-fitting. In particular, the resulting classifiers may prefer image sites where artefacts, such as shadows around the iris region, may occur due to an imperfect automated morphing process. In order to avoid over-fitting, Seibold et al. [33] trained a VGG19 network on a series of different images with two different databases, morphing algorithms and postprocessings (motion blur, Gaussian blur, salt and pepper noise, Gaussian noise). Since the CNN has been trained on all types of databases, morphing algorithms, and postprocessing, it is difficult to assess the resulting robustness of the classifier. Wandzik et al. [38] suggested to use pre-trained facial recognition networks, e.g. VGG-Face [57] or FaceNet [58], to detect morphing attacks. The high-level features generated by the networks are classified with a linear SVM.

Different approaches based on media forensics were presented, too. In several papers the detection of JPEG double compression artefacts for the purpose of morph detection was proposed [18], [29]. However, the presence of such artefacts implies a strong assumption of the image format of facial images used for morphing and the resulting morphed facial image. ICAO proposes to store facial image data in accordance with the specifications of the International Standard ISO/IEC 19794-5 [59]. More specifically, ICAO requires facial images to be stored in electronic travel documents with an average compressed size of 15kB to 20kB in JPEG or JPEG 2000 format [60], [61]. However, JPEG 2000 is the de-facto standard for electronic travel documents as it maintains a higher quality when compressing facial images to 15kB. Therefore, depending on the image size and the compression algorithm used, JPEG double compression artefacts may not be detected. A morph detection method based on reflection analysis in facial images is introduced by Seibold et al. [30]. The flash direction is estimated based on reflections detected in the eyes of a potentially morphed image. Reflections from the nose of the face are then analyzed. However, the ISO/IEC standard requires the absence of hot spots and reflections in facial images used in electronic travel documents. In particular, diffuse lighting, multiple symmetrical sources or other lighting methods should be used, i.e. a single bright "point" light source such as a camera-internal flash is not acceptable for imaging [59].

Apart from no-reference approaches differential morphing attack detection schemes have been presented, too. Most notably, face de-morphing [62], [63] and facial landmark-based approaches have been introduced [64], [65]. Additionally, some no-reference approaches, e.g. general-purpose image descriptors, can be extended to a differential scenario by estimating differences between feature vectors extracted from trusted live captures and potential morphs [8].



(a) Original image (b) Extracted PRNU

Fig. 2. PRNU extraction example for a pre-processed face image.

3 PRNU-based Image Forensics

The photo response non-uniformity (PRNU), also known as sensor noise, has previously been utilised as a reliable tool to perform various forensic tasks such as device identification, device linking, recovery of processing history and the detection of digital forgeries. The PRNU origins from slight variations among individual pixels during the photoelectric conversion in digital image sensors. All digital image sensors cast this weak noise-like signal into all acquired images. Thus, the PRNU can be considered as an intrinsic property of all digital imaging sensors and an inherent part of their output.

3.1 PRNU extraction and analysis

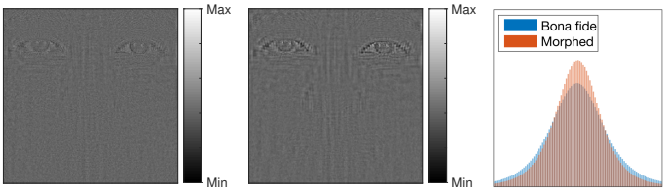
In this work, we make use of the PRNU to detect morphed face images. This systemic and individual pattern can be seen as an unintentional stochastic spread-spectrum watermark that survives processing, such as lossy compression or filtering. The extraction of the PRNU noise residual from an image can be performed by applying Fridrich's approach [66]. 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. The extraction is performed using the denoising filter proposed by Mihcak et al. [67]. For further details on the denoising filter, we refer to [67]. Fig. 2 presents the extracted PRNU for an exemplary image. Further visualizations of PRNU signals extracted from face images can be found in [5], [10].

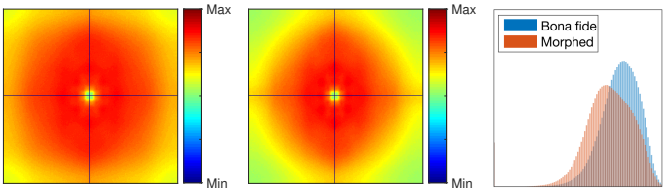
Since the PRNU extraction is relying on a denoising of the image, the resulting pattern might be contaminated with different signals, such as other high frequency image components, e.g. edges, or different types of non-unique artefacts (NUAs) [**?**]. Many alternative PRNU extraction schemes [69], [70], [71], [72], [73], [74], [75] and PRNU enhancements [76], [77], [78], [79], [80] have been proposed in literature to attenuate different types of PRNU contaminations and improve the quality of the extracted PRNU in source camera identification scenarios. However, to the best

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science



(a) Bona fide (b) Morphed (c) Histograms

Fig. 3. PRNU values and histograms of the PRNU extracted from a single bona fide image (a) and morphed face images (b). The PRNU values have been averaged over 500 randomly selected images of the FRGCv2 dataset.



(a) Bona fide (b) Morphed (c) Histograms

Fig. 4. DFT magnitude spectra and histograms of the PRNU extracted from bona fide and morphed face images. The DFT spectra have been averaged over 500 randomly selected images of the FRGCv2 dataset.

of our knowledge, their impact on the general properties of the PRNU signal has not yet been extensively investigated. Therefore, we decided to rely on Mihcak et al.'s [67] denoising filter for the PRNU extraction.

The following essential properties, based on the characteristics of the PRNU described by Fridrich et al. in [81], make the PRNU well suited for a face morph detection scenario:

1) **Dimensionality**: The sensor fingerprint is stochastic in nature and has a large information content, which makes it unique to each sensor.
2) **Unavoidability**: All imaging sensors exhibit PRNU.
3) **Universality**: The sensor fingerprint is present in every picture independently of the camera optics, camera settings, or scene content, with the exception of completely dark images.
4) **Permanence**: It is stable in time and under a wide range of environmental conditions (temperature, humidity, etc.).
5) **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 [82].

Due to the criteria described above, the PRNU offers significant advantages over analysing other high-frequency image components to detect morphed face images.

According to Fridrich [66], the spectral characteristics of the PRNU reveal whether an image has been subject to further processing, e.g. non-geometrical operations have an influence on the strength of the embedded PRNU signal. Since the face morphing process involves non-linear warping and averaging operations, the distribution of the PRNU values is expected to change after these processing operations. Fig. 3 illustrates the PRNU and Fig. 4 the Discrete Fourier Transform (DFT) magnitude spectra obtained by averaging the extracted PRNU of 500 bona fide and 500 morphed face images from the FRGCv2 dataset, which is described in more detail in Sect. 5.

These effects on the distribution of the PRNU values in the spatial domain can be observed in Fig. 3(c), where the distribution of morphed images is squashed compared to bona fide ones, i.e. the values around the mean of the distribution become more frequent and the values around the tails of the distribution become less frequent which leads to a steeper slope. Furthermore, some undesired components of the PRNU, e.g. edges in the image content, are emphasised in the morphed images, as it can be observed in Fig. 3(b). These effects are caused by the averaging operations applied during the morphing process.

The magnitude spectra of bona fide and morphed face images in Fig 4, representing the frequency domain of the PRNU, show a clearly visible discrepancy among each other, where the most obvious differences can be observed in the reduction of high-frequency components within the morphed images' DFT magnitude spectrum as compared to the bona fide ones. Furthermore, the DFT spectrum of the morphed face images appears more compressed, i.e. the area covered by the large magnitudes is smaller compared to bona fide images.

These effects are caused by the previously mentioned operations involved in the face morphing process, which lead to changes in the distribution of the PRNU values. The approach presented in this work aims at exploiting these effects in order to perform a blind *no-reference* face morph detection.

3.2 Potential attacks and PRNU robustness

PRNU-based forensics and counter forensics can be considered as a cat-and-mouse game, since attacks and counter attacks are presented on a regular basis in the related literature. While attackers try to bypass various forensic approaches and conceal their counter-forensic approaches, techniques are developed to reveal such attacks.

The counter-forensic techniques proposed to overcome PRNU-based forensics can be divided into the following categories:

- **Destroying the image identity:** This class of counter forensic techniques tries to conceal the identity of an image and therefore prevents an identification of the image source or camera, respectively. Some examples are: removing the PRNU [83], [84], [85], [86], seam carving [87], [88], adaptive PRNU denoising [89]. Applying these techniques to morphed face images poses a lower threat to a PRNU-based morph detection system, since the aim is not to detect the image source, but to analyse the general properties of the PRNU signal. When the PRNU is destroyed, it can be assumed that its general properties are also not preserved.
- **Forging the image identity:** The goal of this class of counter forensic techniques is to fake the identity of an image, i.e. changing the identity of the image or concealing traces of its modification. Some examples for this are: Insertion of a differing PRNU signal [84], [86], fingerprint copy attacks [90], [91], [92], hiding of post-processing operations [84]. When applied to

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

morphed face images, these type of counter forensic techniques can most likely be considered as a threat for a PRNU-based morph detection system, because their aim is to spoof an authentic image source, which usually contains similar characteristics to the PRNU of unaltered images. A potential attack on the PRNU-based morph detection system could involve extracting the PRNU from an authentic image and inserting it into a morphed image. This would restore the original properties of the PRNU when it is extracted again for the detection and therefore conceal the morphing operations.

Different approaches are proposed in literature to detect such intentional counter forensic attacks, e.g. the "Triangle Test" [93] and more recently Sameer et al. [94] proposed a deep learning based CNN model for the detection of counter forensic images. In biometrics, forging of the image identity has only been investigated for iris sensor data by Banerjee, Mirjalili and Ross in [95] and Uhl and Höller in [96], where the detection of such attacks is furthermore evaluated in the latter.

Another type of attacks on the PRNU are unintentional ones, such as recompression, geometric transformations (cropping, scaling, rotation), photometric transformations and post-processing of the images. These attacks might occur unintentionally, i.e. when images are simply processed to enhance the appearance of a subject within the image, like it is often done for portrait photos. The PRNU has been shown to be resilient to photometric transformations [97] to a certain degree. While geometric transformations heavily affect the image source identification because they destroy the alignment of the PRNU signal, they are expected to not affect the general properties of the PRNU. However, post-processing of images, such as sharpening, blurring or contrast enhancement, can severely affect the PRNU. In previous work we showed that different post-processing techniques might even completely prevent a PRNU-based detection of morphed face images [5], [10]. Furthermore, recompression [98] is reported to alter the PRNU pattern after several passes in a way that source identification performance is affected. However, its influence on the general properties of the PRNU has not been investigated.

We consider intentional attacks on the PRNU to be less likely compared to unintentional ones, because the former require profound knowledge about the PRNU and its properties as well as an attacker with experience in the field. As the robustness of PRNU-based morph detection against simple post-processings has been already investigated in previous works [5], [10], an evaluation of four morphing algorithms has been included in order to provide a more comprehensive performance analysis in Sect. 5.2. The four morphing algorithms picture a more realistic attack scenario, since they use different combinations of the simple post-processings. To address the question whether a PRNU-based approach can be applied for a wide range of distinct cameras, in Sect. 5.3 we evaluated the generalizability of the proposed morph detection approach on the Dresden Image Database [99] containing images from 63 different cameras from multiple manufacturers.

4 Proposed System

Based on the observed effects of the face warping procedure on the spatial and spectral characteristics of the PRNU, in this work we propose a PRNU-based morph detection system which is able to discriminate between bona fide and morphed images. Therefore, we analyse the spatial and spectral characteristics of the PRNU in a *no-reference* manner, thus there is no need for a trusted bona fide reference image of one of the morphed subjects.

The proposed system relies on a divide and conquer principle and its processing steps are illustrated in Fig. 5. In the remainder of this section, we will discuss the various processing steps in more detail.

4.1 Preprocessing and PRNU extraction

The first step of the system consists in extracting the facial region from a face image, which is normalised and then cropped to the facial area (320×320 pixels) before being converted to grayscale. This process is described in more detail in Sec. 5.1.

Following, the PRNU is extracted from the preprocessed image, as described in Sect. 3, using the wavelet-based denoising filter by Mihcak et al. [67] in conjunction with the filtering distortion removal (FDR) enhancement proposed in [80]. The extracted PRNU is then split into multiple equally sized cells. The proposed system is able to work with arbitrary splits from 1 cell (whole image) to N cells. In this work, only a cell size of 10×10 cells is investigated, because it yields the best performance according to previous work [5], [10]. In general, 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. 5 shows an example of how the face image is preprocessed and the PRNU is extracted and split into 10×10 equisized cells.

4.2 Feature extraction

The feature extraction is performed individually for each cell. In previous work [5], [10], only spectral features based on the DFT magnitude histogram and magnitude energy have been investigated. In this work, two different feature types are investigated: spectral features based on the PRNU's DFT magnitudes and new spatial features based on the PRNU values, since the PRNU values are affected by the morphing procedures and post-processings in the spatial domain as well the spectral one.

Both feature types are described in more detail in the following.

4.2.1 Spatial Features

The newly proposed spatial features aim at analysing the distribution of the PRNU values, which is observed to differ between bona fide and morphed images according to Fig. 3(a) and Fig. 3(b).

For the first spatial feature, P_{var}, the histogram of the PRNU values is computed, which is constrained to a range of $[-5, 5]$ and divided into 100 bins. These values have been selected by analysing the DFT spectra of extracted PRNUs of

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

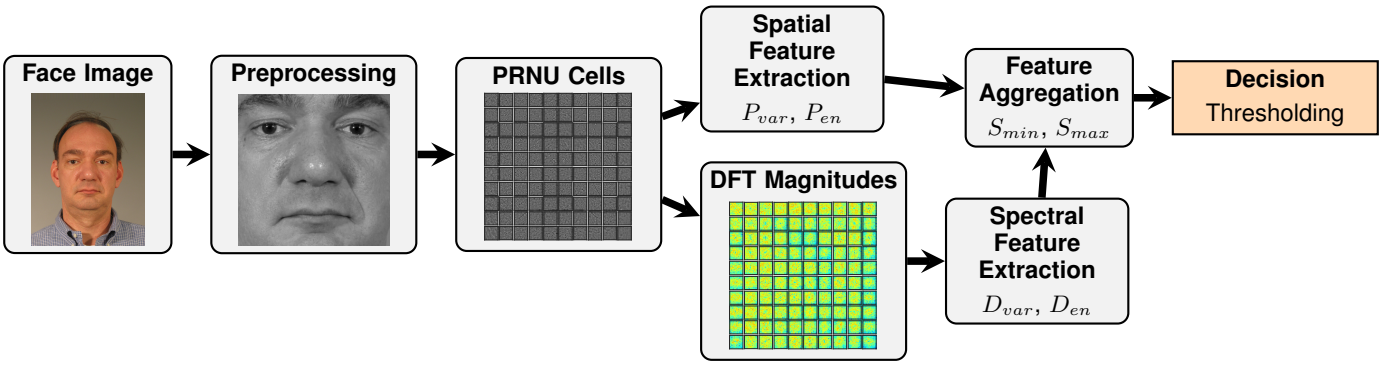


Fig. 5. Processing steps of the proposed PRNU-based morph detection system and different feature types: spatial features (upper path) and spectral features (lower path).

bona fide and morphed images. Due to the different slope of bona fide and morphed image's PRNU value distributions that can be observed in Fig. 3(c), we decided to compute the variance of the histogram bin frequencies P_{var}, which we defined as

$$P_{var} = \frac{1}{B}\sum_{n=1}^{B}(H_P(n) - \bar{H_P})^2 \tag{2}$$

where B is the number of bins in the PRNU cell's histogram H_P. $\bar{H_P}$ represents the mean frequency of the histogram bins.

As second spatial feature, we consider the energy of the PRNU values, P_{en}, which is defined as

$$P_{en} = \sum_{x \in V} |x|^2 \tag{3}$$

where x is a value within all PRNU values V of a cell.

As the Eqs. 2 and 3 show, both spatial features yield a simple scalar value SV for each PRNU cell.

4.2.2 Spectral Features

In order to compute the spectral features, the first step consists in obtaining the frequency spectrum of the PRNU in each cell, which is done by means of the DFT. The resulting magnitude spectrum, which is illustrated in Fig. 4(a) and 4(b) respectively, reveals the alterations of the PRNU signal caused by the morphing process.

These effects are quantified, on one hand, by calculating the DFT magnitude histogram to represent the magnitude distribution within the spectrum. As described in Sect. 3, a shift of the magnitude distribution can be observed for morphed images. The DFT magnitude histograms are constrained to the same universal range of $[0, 8]$ and are divided into 100 bins. These values have again been estimated by analysing the DFT spectra of extracted PRNUs of bona fide and morphed images. Based on the observations in Sect. 3, we select the variance of the histogram D_{var} as being suited for the discrimination between bona fide and morphed images. We obtain D_{var} in a similar manner as the previously described P_{var}:

$$D_{var} = \frac{1}{B}\sum_{n=1}^{B}(H_M(n) - \bar{H_M})^2 \tag{4}$$

where B is the number of bins in a cell's DFT magnitude histogram H_M, with $\bar{H_M}$ being the mean frequency of the histogram bins.

On the other hand, we propose to compute the energy of the PRNU's DFT magnitudes D_{en}, as defined in Eq. 5, where M are the DFT magnitudes within a cell and x their respective values.

$$D_{en} = \sum_{x \in M} |x|^2 \tag{5}$$

As for the spatial features, both spectral features yield a simple scalar value SV for each PRNU cell when considering Eqs. 4 and 5.

4.3 Feature aggregation

After obtaining the scalar values SV for all cells C_n, the values are aggregated to obtain a global aggregation score A for the image. We investigated various strategies, where we present the two best performing ones. The aggregation strategies used in this work are:

$$A_{min} = \min_{\forall n \in 1 \ldots N} SV_n \tag{6}$$

$$A_{max} = \max_{\forall n \in 1 \ldots N} SV_n \tag{7}$$

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

A_{min} yields the minimum score among the individual cells, while A_{max} characterizes maximum score among all cells. As already mentioned, we obtain a single scalar value A for each image using one of the Eqs. 6 or 7.

4.4 Decision

The final decision, whether a face image has been created through morphing of multiple images or not, is taken by a simple thresholding.

Previous work [5] showed that a one dimensional decision was not able to reliably detect some of the post-processed morphed images for some spectral features. Hence, we introduce an additional decision step and derive a mean value $\bar{B}$ from bona fide images, where the characteristics of the PRNU are well known. With this property,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

we can calculate the distance D of an investigated image to bona fide images as

$$D = |A - \bar{B}| \tag{8}$$

$$\bar{B} = \frac{1}{N_B} \sum_{n=1}^{N_B} A \tag{9}$$

where A is the cell aggregation result, $\bar{B}$ is the mean variation of the N_B bona fide images.

It has to be noted, that this distance calculation is only applied for the two spatial and spectral energy-based features P_{en} and D_{en}, while it is not calculated for the histogram-based features P_{var} and D_{var}, due to the histogram-based features yielding more consistent scores among different post-processings which can be classified with a one dimensional threshold.

If the distance calculation is applied, the final decision for a presented face image is taken by thresholding the calculated distance D. Otherwise, the final decision simply relies on thresholding of the value A, which is obtained directly from the cell aggregation.

5 Experiments

In the following subsection the experimental setup, i.e. used databases, morphing algorithms, baseline systems and performance metrics, are described. Subsequently, the detection performance of the proposed systems and the baseline systems is reported and discussed. Further, the generalizability of the proposed PRNU-based morph detection approach with respect to utilized cameras and printed and scanned face images is investigated.

5.1 Experimental setup

Performance evaluations are conducted based on a subset of 1,948 images selected from the FRGCv2 [14] face image database. Face images have been manually filtered to meet ICAO requirements for electronic travel documents [60], e.g. frontal pose, neutral expression, homogeneous background and sufficient resolution (at least 90 pixels between left and right eye center). Images of this database have been developed using a Fujifilm Frontier 5700R Minlab and scanned using a Epson DS-50000 Scanner at 300dpi to obtain the Print-Scan database of equal size. In addition, a subset of 1,058 images from the FERET [22] face image database which exhibit the same properties are used for training purposes of baseline morph detection algorithms. Note that the latter database is not used for evaluation of the proposed PRNU-based morph detection scheme since it has been acquired using an analog camera. PRNU is primary caused by Pixel Uniformity Noise related to the sensor which are non-existent if images are acquired with a film camera, i.e. only the PRNU signal of the sensor inside the scanner used to digitize the images might be present in this case. Instead, the Dresden Image Database [99] is used for training the PRNU-based morph detection schemes to underline the claim that the proposed PRNU-based morph detector is not dependent of a specific camera unit, since it contains images from 63 distinct cameras from various models and manufacturers. More details on how the bona fide and morphed images have been generated using the Dresden Image Database are given in Sect. 5.3.

In a pre-processing step the face of a subject is segmented and normalized according to eye coordinates detected by the *dlib* landmark detector [100]. Subsequently, the normalized region is cropped to 320×320 pixels to ensure that the morph detection algorithm is only applied to the facial region. Finally, the cropped face part is converted to a grayscale image. Examples of original face images (cropped to portrait format) and pre-processed face images of the FRGCv2 and Print-Scan database are depicted in Fig. 6.

The subsets are split into images used for morph creation and images used as bona fide references. The resulting database constellation is listed in Table 2. In order to generate a great variation of morphs, four morphing algorithms were employed:

1) **OpenCV/dlib**, a self-scripted morphing algorithm based on th "Face Morph Using OpenCV" tutorial[2] using the dlib landmark detector [100].
2) **FaceMorpher**[3], an open-source implementation using python.
3) **FaceFusion**[4], a proprietary morphing algorithm.
4) **UBO**, the morphing tool developed by the University of Bologna, as used e.g. in [62].

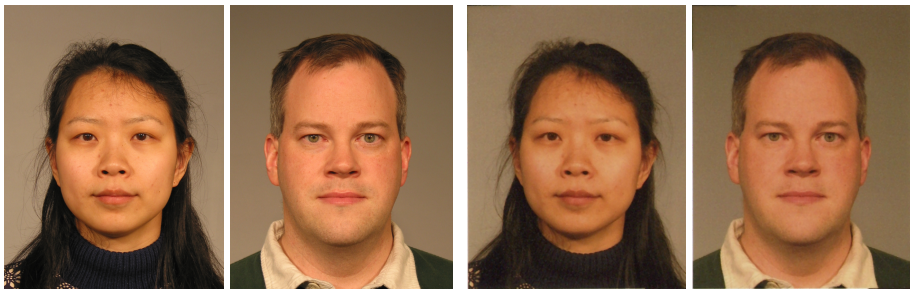
In order to be able to conduct comparable experiments, the same combination of morphed face images was created for each of the listed algorithms. All algorithms detect corresponding landmarks in two face images to be morphed which are averaged. Subsequently, both face images are warped accordingly. Finally, alpha-blending is performed to create the morphed face image. All morphs were created in a way such that both used images tend to contribute equally to the inner facial region. Note that FaceFusion and UBO morphing algorithms are closed-source and might apply certain image post-processing methods to enhance the quality of resulting morphs. Examples of cropped facial regions of morphed face images generated all four morphing algorithms are shown in Fig. 7.

The vulnerability of a COTS facial recognition system to attacks based on the generated morphed face images is assessed by using the metrics specified in [101], in particular the Mated Morph Presentation Match Rate (MMPMR). This measure is an adaptation of the general Impostor Attack Presentation Match Rate (IAPMR) introduced in ISO/IEC 30107-3 [102] and is defined as the proportion of attack presentations using the same type of presentation attack instruments in which the target reference matches. In the adaptation, however, the MMPMR covers the fact that not one target subject (contained in the morphed reference) is matched - but for a successful face morphing attack, both data subjects that previously contributed to the morphed image are expected to match.

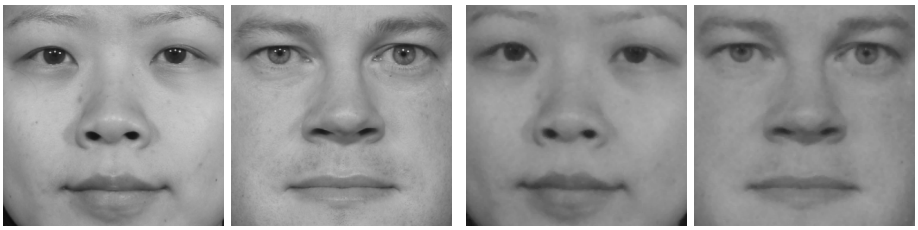
Using the default decision threshold of the COTS facial recognition system, an MMPMR of 1 is obtained across all used face image databases and morphing techniques. This means that all facial images of individuals contributing to

2. http://www.learnopencv.com/face-morph-using-opencv-cpp-python/
3. https://github.com/alyssaq/face_morpher
4. http://www.wearemoment.com/FaceFusion/

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science



(a) Portrait face images: FRGCv2 (left) and Print-Scan (right)



(b) Pre-processed face images: FRGCv2 (left) and Print-Scan (right)

Fig. 6. Examples of bona fide portrait and pre-processed face images of the used datasets. Due to the printing and scanning face images from the Print-Scan dataset exhibit slightly lower resolution.

(a) Subject 1 (b) OpenCV/dlib (c) FaceMorpher (d) FaceFusion (e) UBO (f) Subject 2

Fig. 7. Used morphing algorithms applied to a female (top) and a male (bottom) image pair. Note that the FaceFusion algorithm uses the inner eye regions and nostrils of subject 1 in order to avoid artefacts in these regions.

TABLE 2
Number of subjects, bona fide and morphed face images of used datasets. "F" and "M" indicate female and male subjects, respectively.

Database	Subjects	Face images	
		bona fide	morphed
FRGCv2	533 (231 F, 302 M)	984	964*
Print-Scan	533 (231 F, 302 M)	984	964*
FERET	529 (200 F, 329 M)	529	529*

*per morphing algorithm

a morphed facial image are successfully compared to it, so that the attacks have a 100% chance of success.

As baseline face morphing attack detection systems Local Binary Patterns (LBP) [103], Binarized Statistical Image Features (BSIF) [42], FaceNet features [58] and the FS-SPN analysis of [27] are applied. At feature extraction for LBP and BSIF the pre-processed face image is optionally divided into 4×4 cells to retain local information. That is, feature extractors are applied pixel-wise storing feature value in histograms for each texture cell. The final feature vector is formed as a concatenation of histograms extracted from each cell. While LBP simply processes neighboring pixel values of each pixel, BSIF utilizes specific filters learned from a set of images. For details on these texture descriptors the reader is referred to [42], [103]. The use of these well-established general purpose texture descriptors has shown to be successful in diverse texture classification problems. As the process of image morphing is expected to cause changes in textual properties between bona fide and morphed face images said texture descriptors have been shown to reveal competitive morphing attack detection performance [8], [11], [12], [21]. Minimum filter sizes of 3×3 pixels which have been reported to reveal best detection performance in [8] are used for both texture descriptors. In the training stage feature vectors are extracted for each baseline system and SVMs with Radial Basis Function (RBF) kernels are trained to distinguish between bona fide and morphed face images. Similarly, an SVM is trained with deep facial features extracted from cropped face image using

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

TABLE 3
Performance results in terms of D-EER (in %) for different configurations of the baseline morphing attack detection systems. Best performing systems are marked bold. μ is the mean error and σ^2 the variance over all morphing methods.

System	Morphing method				μ	σ^2
	OpenCV/dlib	FaceMorpher	FaceFusion	UBO		
$LBP_{1\times1}$ [8]	35.5%	15.3%	28.1%	26.1%	26.5%	±5.82
$LBP_{4\times4}$ [8]	20.5%	**4.2%**	14.7%	**12.7%**	**13.0%**	±4.66
$BSIF_{1\times1}$ [8]	27.6%	26.0%	16.7%	17.6%	22.0%	±4.87
$BSIF_{4\times4}$ [8]	27.4%	29.0%	**7.9%**	16.6%	20.2%	±8.57
FaceNet [58]	30.1%	29.8%	32.0%	33.2%	31.3%	±1.33
FS-SPN [27]	**17.5%**	4.9%	30.8%	19.5%	18.2%	±7.0

the FaceNet recognition system. This approach resembles the schemes proposed in [31], [33]. The SVM-based classifiers of these morph detection schemes are trained on the subset of the FERET image database. Eventually, the pre-trained open-source implementation[5] of [27] is directly applied for morph detection. The major advantage of the proposed PRNU-based morph detection over the baseline algorithms is that it does not need any training. Only for some of the proposed features, a pre-computed decision threshold has to be computed. In such cases, the threshold has been estimated on the Dresden image database [99].

The performance of the detection algorithms is reported according to metrics defined in ISO/IEC 30107-3 [102]. 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 the different morphing methods.

5.2 Performance evaluation

Table 3 lists the D-EERs for different configurations of the baseline systems. It can be observed that morphs created using OpenCV with dlib are generally harder to detect, in contrast to the images created by other morphing algorithms. However, FS-SPN performs best detecting morphs created with OpenCV and dlib, but the detection rate drops when detecting morphs created by FaceFusion or the UBO algorithm. In contrast, $BSIF_{4\times4}$ shows improved performance for detecting FaceFusion morphs, but lacks detecting morphs created by OpenCV. The DET curves for the baseline systems in presence of all morphing attacks are shown in Fig. 8. In summary, it appears that a heterogeneous training and test database as well as the utilization of different morphing algorithms significantly deteriorate the detection performance of the baseline systems leading to significantly worse results to what has been reported in previous works.

Performance results for the proposed PRNU-based morphing attack detection scheme for best performing feature extractors and cell aggregation techniques are summarized in Table 4. DET plots for the best performing proposed approaches across all post-processings are shown in Fig. 9.

5. https://github.com/Le-BingZhang/FS-SPN

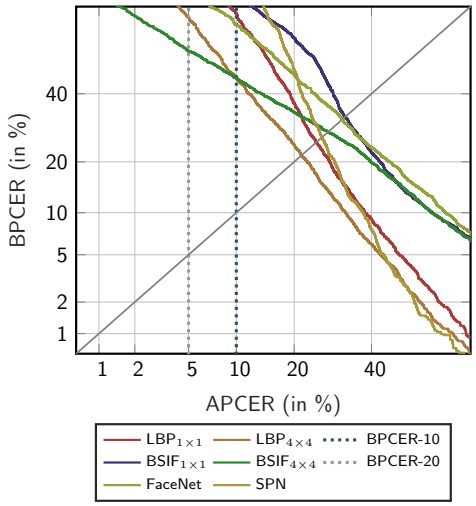


Fig. 8. DET curves for different configurations of the baseline morphing attack detection systems in the presence of all morphing attacks on FRGCv2.

In addition, Fig. 10 compares the average D-EERs and their variances of all proposed morphing attack detection schemes to the baseline systems. In contrast to the baseline systems, the PRNU-based approaches yield low error rates detecting morphs created using OpenCV and dlib, but struggle detecting FaceFusion morphs. However, compared to the baseline systems average D-EER are observably lower and exhibit smaller standard deviations. Additionally, smaller variance in detection performance across different datasets and morphing algorithms are obtained, which is vital for an application of any morphing attack detection algorithm in real world scenarios where said parameters are unknown.

Compared to the baseline systems, significantly improved results are achieved for the newly proposed spatial features, i.e. P_{var} followed by P_{en}, which significantly outperform the baseline systems. The spectral D_{en} feature, proposed in previous work, also obtains very competitive results on this new dataset. Another aspect to note is that the energy-based features D_{en} and P_{en}, whose mean bona fide threshold $\bar{B}$ has been determined on the Dresden image database, underlines the generalisability of the approach in regard to cameras from different models and manufacturers.

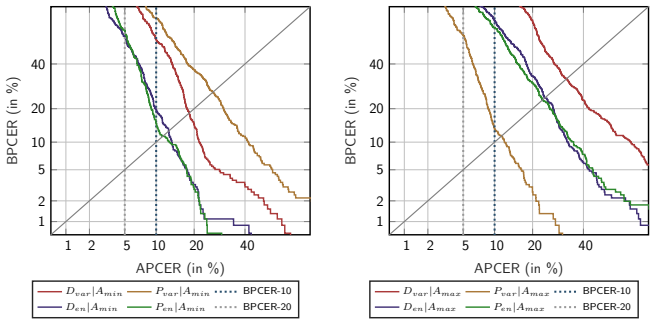
At this point, it is important to note that morphing attack detection algorithms analyze cropped faces only. Thereby higher generalizability is achieved since outer facial parts can be created in different ways during morph creation. Many morph generators copy the outer facial image part of one subject contributing to the morph, e.g. in [29], [62]. In such cases, the PRNU signal of the outer part of the morph is expected to remain almost unaltered. That is, if the proposed PRNU-based morphing attack detection schemes are extended to analyze the entire face image, a variance-based cell aggregation is expected to reveal improved results for detecting morphs created in the aforementioned way.

Overall, some of the proposed PRNU-based morphing attack detection configurations reveal promising results considering the challenging experimental setup. In contrast to trained morphing attack detection schemes, e.g. [32], [55],

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

TABLE 4
Performance results in terms of D-EER (in %) for different configurations of the proposed PRNU-based morphing attack detection systems. Best performing systems are marked bold. μ is the mean error and σ^2 the variance over all morphing methods.

Feature Extraction	Cell aggregation	Morphing method				μ	σ^2
		OpenCV/dlib	FaceMorpher	FaceFusion	UBO		
D_{var}	A_{min}	1.7%	7.9%	40.3%	15.8%	18.3%	$\pm$ 2.86
	A_{max}	13.1%	20.2%	50.0%	29.6%	32.3%	$\pm$ 2.56
P_{var}	A_{min}	15.8%	7.5%	45.9%	26.2%	26.3%	$\pm$ 2.76
	A_{max}	**0.2%**	**0.5%**	**28.2%**	**8.9%**	**11.2%**	$\pm$ **1.73**
D_{en}	A_{min}	0.6%	1.0%	29.5%	11.0%	12.4%	$\pm$ 1.84
	A_{max}	7.5%	5.3%	47.9%	21.7%	24.1%	$\pm$ 3.84
P_{en}	A_{min}	0.2%	0.6%	28.7%	9.6%	11.3%	$\pm$ 1.79
	A_{max}	11.8%	4.8%	44.0%	22.6%	23.3%	$\pm$ 2.92



(a) A_{min} (b) A_{max}

Fig. 9. DET curves for different configurations of the baseline morphing attack detection system in the presence of all morphing attacks.

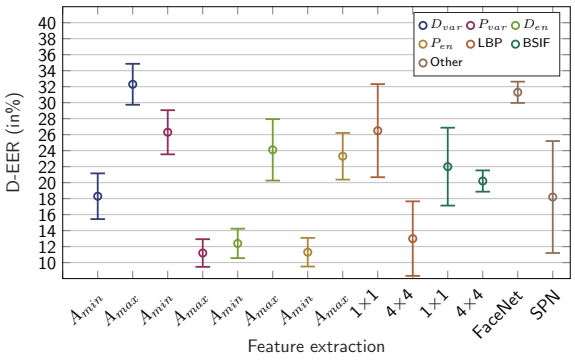


Fig. 10. Error bars of D-EERs for different configuration of the proposed PRNU-based morphing attack detection system and the baseline morphing attack detection systems in presence of all morphing attacks.

the proposed schemes do not rely on the presence of distinct artefacts, e.g. ghost artefacts, which might occur due to imperfect morph creation. Hence, similar results are to be expected if advanced morphing algorithms are developed which allow for an automated creation of morphs comprising less or no artefacts.

5.3 Generalizability across cameras

As mentioned in Sect. 3, the proposed PRNU-based morph detection system relies on changes in the distribution of the PRNU values. Since the PRNU differs for each camera, it might contain camera (model) specific contaminations (non-unique artefacts) that might affect the PRNU values' distribution.

In order to investigate the generalizability of the proposed morph detection approach and due to a lack of suitable face image datasets acquired with different cameras, we decided to fall back to the Dresden image database [99], which offers images from multiple cameras and even multiple instances of the same camera model. More specifically, we selected the *flatfield* dataset, since it contains images beneficial for PRNU extraction, i.e. bright images of an evenly illuminated surface, which do not contain any contaminations from the image content like edges or other high-frequency patterns. The flatfield dataset contains images from 63 distinct digital cameras from 20 different camera models across many camera manufacturers. For some camera models, images from up to 5 instances are available in the dataset.

To generate the bona fide and morphed images, we first selected 315 images from the Dresden image database [99], consisting of 5 random images for every one of the 63 cameras. For the generation of the morphed image samples, we used the same morphing parameters as they would occur in a face morphing attack. In this experiment, they were obtained from applying the OpenCV with dlib approach on the FRGCv2 database, as described in Sect 5.1. With these parameters, we generated a total of 53,362 morphed images from bona fide image pairs of different cameras. Finally, a patch of 320×320 pixels is cropped from the center of all bona fide and morphed images.

The results of applying the proposed PRNU-based face morphing system on these bona fide and morphed images are presented in Table 5. Looking at the overall results for all cameras at the bottom of the table, we obtain a D-EER of 13.65% with $P_{var}|A_{min}$ aggregation. For most cameras the detection error rate is very low. However, some cameras exhibit higher error rates of around 15-20% and cameras of a specific model (Practica DCZ59) even of up to 41.56%. We assume that this degradation might be caused by camera-specific non-unique artefacts, since the degradation mostly occurs for all cameras of the same model, as the mentioned Practica DCZ59 or FujiFilm FinePixJ50 and Panasonic DMC-FZ50. Though, it has to be noted that the degradation does not persist among all investigated features, where a fusion of multiple features might yield improved performance and more consistent results. The other proposed features D_{en}, P_{var} and P_{en} also achieve respectable overall results between 14.5 and 28.6% D-EER. The histogram-based feature P_{var}, which is independent of any training data, show a better generalizability over the various cameras compared to the energy-based features D_{en} and P_{en}.

These results demonstrate that PRNU-based features in general are able to generalize well over a large number of different cameras and show promising results for a face morph detection scenario.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

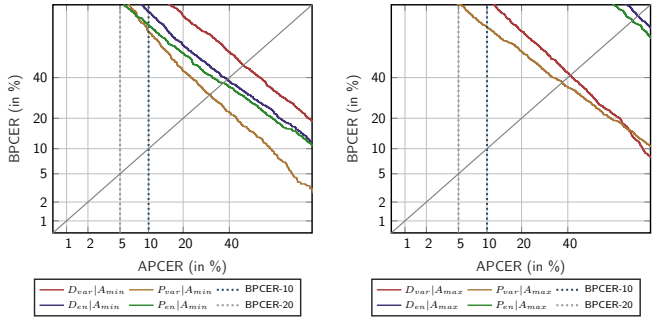
TABLE 5
Performance results in terms of D-EER (in %) for different configurations of the proposed PRNU-based morphing attack detection systems (cell size of 10×10) and 63 different cameras from the Dresden image database. "All" indicates the result for all camera instances.

Camera ID	D_{var}		P_{var}		D_{en}		P_{en}	
	A_{min}	A_{max}	A_{min}	A_{max}	A_{min}	A_{max}	A_{min}	A_{max}
Canon Ixus55 0	48.04	42.69	0.00	0.00	1.12	0.56	0.00	0.00
Canon Ixus70 0	30.00	15.61	0.00	0.00	6.94	14.82	0.00	0.00
Canon Ixus70 1	23.94	18.19	0.00	0.00	5.15	10.59	0.00	0.00
Canon Ixus70 2	20.32	13.58	0.00	0.00	11.28	13.97	0.00	0.00
Casio EXZ150 0	9.49	6.54	0.02	0.01	2.12	1.43	0.00	0.00
Casio EXZ150 1	16.33	10.58	0.05	0.01	1.27	2.35	0.00	0.00
Casio EXZ150 2	17.61	12.67	0.00	0.00	5.70	4.49	0.00	0.00
Casio EXZ150 3	14.96	9.04	0.02	0.00	2.55	2.35	0.00	0.00
Casio EXZ150 4	18.43	8.43	0.00	0.00	4.46	2.84	0.00	0.00
FujiFilm FinePixJ50 0	33.53	27.97	20.97	40.24	37.86	22.84	38.68	21.54
FujiFilm FinePixJ50 1	30.31	34.57	17.98	31.86	29.07	20.06	31.21	17.11
FujiFilm FinePixJ50 2	31.86	30.86	19.03	30.93	25.59	15.85	26.67	17.16
Nikon CoolPixS710 0	6.92	10.99	0.01	16.67	17.01	1.34	16.67	0.00
Nikon CoolPixS710 1	8.54	4.32	0.02	0.00	1.27	1.33	0.00	0.00
Nikon CoolPixS710 2	8.91	9.86	0.04	0.00	0.42	0.39	0.00	0.00
Nikon CoolPixS710 3	15.97	18.17	0.07	0.00	0.31	1.06	0.00	0.00
Nikon CoolPixS710 4	18.40	9.54	0.05	0.00	16.78	16.83	16.67	16.67
Nikon D200 0	22.62	25.77	1.91	0.21	0.41	3.53	1.06	7.03
Nikon D200 1	16.31	11.35	11.69	7.09	1.18	5.88	3.67	14.24
Nikon D70 0	43.25	44.70	0.66	1.35	0.96	2.04	1.57	1.92
Nikon D70 1	47.11	45.54	0.07	0.16	0.20	1.61	0.77	0.96
Nikon D70s 0	45.68	43.98	0.44	1.84	1.39	1.88	1.80	2.60
Nikon D70s 1	45.73	46.01	0.03	0.01	0.12	0.45	0.21	0.23
Olympus mju 1050SW 0	33.07	34.13	0.00	0.00	1.38	0.01	0.00	0.01
Olympus mju 1050SW 1	24.48	21.08	0.00	0.00	0.59	0.02	0.00	0.01
Olympus mju 1050SW 2	31.95	29.91	0.00	0.00	0.74	0.02	0.00	0.01
Olympus mju 1050SW 3	32.56	22.17	0.00	0.00	1.09	0.03	0.00	0.01
Olympus mju 1050SW 4	27.07	32.65	0.00	0.00	0.89	0.02	0.00	0.01
Panasonic DMCFZ50 0	23.07	16.60	19.24	37.37	29.59	20.76	34.51	19.29
Panasonic DMCFZ50 1	22.35	16.81	15.43	34.88	24.46	15.09	31.91	17.26
Panasonic DMCFZ50 2	18.50	17.86	19.06	34.75	32.00	19.37	33.98	19.26
Pentax OptioA40 0	38.86	38.45	0.87	12.58	17.15	1.53	14.19	2.80
Pentax OptioA40 1	44.65	41.29	2.36	11.13	8.40	8.60	8.28	6.74
Pentax OptioA40 2	47.85	41.52	0.20	2.91	4.73	0.81	2.78	0.70
Pentax OptioA40 3	47.75	44.23	0.00	0.01	0.04	1.05	0.00	0.01
Pentax OptioW60 0	38.69	27.98	0.00	0.00	34.42	20.41	0.00	0.00
Praktica DCZ59 0	1.02	0.24	40.17	48.61	13.32	19.56	33.23	34.97
Praktica DCZ59 1	0.27	0.56	40.27	49.07	16.38	19.07	34.91	34.34
Praktica DCZ59 2	0.89	0.57	41.56	49.43	15.49	16.54	36.56	32.43
Praktica DCZ59 3	0.64	0.30	41.19	48.01	12.17	19.87	31.85	35.41
Praktica DCZ59 4	1.19	0.67	40.87	48.01	14.85	18.78	35.05	34.87
Ricoh GX100 0	12.09	11.54	0.00	0.00	15.74	5.12	0.00	0.00
Ricoh GX100 1	16.12	13.53	0.00	0.00	9.28	1.96	0.00	0.00
Ricoh GX100 2	16.12	13.27	0.00	0.00	16.82	5.64	0.00	0.00
Ricoh GX100 3	13.34	12.14	0.00	0.00	14.83	5.62	0.00	0.00
Ricoh GX100 4	9.93	8.95	0.00	0.00	17.61	10.04	0.00	0.00
Rollei RCP7325XS 0	33.14	29.70	8.50	12.68	14.42	21.98	14.41	14.98
Rollei RCP7325XS 1	43.21	35.58	6.71	8.02	13.14	16.86	11.91	10.83
Rollei RCP7325XS 2	30.54	32.78	9.30	15.85	17.40	19.60	18.81	15.16
Samsung L74wide 0	4.71	3.58	3.53	2.83	0.00	0.05	0.48	1.03
Samsung L74wide 1	2.53	1.50	3.97	2.06	0.00	0.01	0.32	1.63
Samsung L74wide 2	4.35	2.00	3.55	3.05	0.00	0.02	0.62	1.40
Samsung NV15 0	26.59	13.21	0.35	0.67	0.00	0.58	0.13	0.01
Samsung NV15 1	15.59	14.08	0.23	0.11	0.97	0.82	0.07	0.00
Samsung NV15 2	21.48	11.80	0.29	0.40	0.08	0.37	0.00	0.01
Sony DSCH50 0	11.51	14.21	0.00	0.00	9.54	13.00	0.00	0.00
Sony DSCH50 1	8.30	5.31	0.00	0.01	1.09	4.57	0.00	0.00
Sony DSCT77 0	15.89	8.83	0.00	0.00	19.45	15.80	0.00	0.00
Sony DSCT77 1	9.79	11.90	0.00	0.00	26.03	17.94	0.00	0.00
Sony DSCT77 2	12.25	5.37	0.00	0.00	25.01	23.85	0.00	0.00
Sony DSCT77 3	32.13	24.66	0.00	2.01	1.56	6.83	0.00	0.00
Sony DSCW170 0	1.82	1.48	0.10	1.97	1.09	5.10	0.15	0.00
Sony DSCW170 1	3.17	1.49	0.07	4.19	0.12	3.05	0.06	0.00
All	**28.60**	**25.80**	**13.65**	**16.65**	**17.17**	**16.42**	**17.28**	**14.50**

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TBIOM.2019.2942395, IEEE Transactions on Biometrics, Behavior, and Identity Science

TABLE 6
Performance results in terms of D-EER (in %) for different configurations of the proposed PRNU-based morphing attack detection systems (cell size of 10×10) for the Print-Scan dataset.

Feature Extraction	Cell aggregation	D-EER
D_{var}	A_{min}	46.87
	A_{max}	41.07
P_{var}	A_{min}	**30.52**
	A_{max}	36.81
D_{en}	A_{min}	38.63
	A_{max}	49.97
P_{en}	A_{min}	36.51
	A_{max}	49.92



(a) A_{min} (b) A_{max}

Fig. 11. DET curves for different configurations of the proposed morphing attack detection on the printed and scanned images for all morphing algorithms (OpenCV/dlib, FaceMorpher, FaceFusion, UBO).

5.4 Printed and scanned images

In this last experiment, we look at the performance of the PRNU-based morph detection approach when applied to the Print-Scan dataset described in Sect. 5.1. This scenario is very challenging for a PRNU-based approach, since the scanning process of the images embeds the scanner's PRNU within all scanned images, which might prevent the detection of the morphed images. The D-EER results are presented in Table 6.

We can observe, that the detection performance significantly drops for all proposed feature-aggregation combinations, where the best result is obtained with $P_{var}|A_{min}$ with a D-EER of 30.52%. Fig. 11 illustrates the DET plots for all proposed morph detection algorithms on the printed and scanned images, where all morphing algorithms, i.e. OpenCV/dlib, FaceMorpher, FaceFusion and UBO, have been included. These results show that the scanners PRNU leads to a detection performance degradation for the proposed PRNU-based approach, however $P_{var}|A_{min}$ is still able to discriminate bona fide and morphed images to some degree in this print and scan scenario.

6 Conclusions

Face morphing attacks pose a serious security risk to face recognition systems. In this work, the potential PRNU analysis has been thoroughly analyzed for the challenging task of *no-reference* face morph detection. In comprehensive cross-database experiments for which different face morphing and image post-processing techniques have been applied, the proposed PRNU-based morphing attack detection system has been shown to outperform other state-of-the-art methods. Moreover, the feasibility of detecting morphed face images from printed and scanned image data has been investigated. Since the proposed system is based on a simple and minimal approach, further detection performance improvements can be expected by fusing multiple PRNU features and by a more sophisticated classification approach based on machine learning techniques.

In contrast to *differential* morphing attack detection schemes, e.g. [62], which additionally process a trusted live capture of a subject's face the proposed approach is particularly useful in cases where only a single potentially morphed face image is presented, e.g. digital transmission of a face image for issuance of an electronic travel document which turns out to be relevant in some countries. In other scenarios, e.g. facial recognition at ABC gates, the presented PRNU-based morphing attack detection scheme could be fused with other (differential) approaches to further improve the detection performance.

7 Acknowledgments

This work was partially 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 CRISP (www.crisp-da.de) and by the European Union's Internal Security Fund – Borders and Visa under grant agreement n° 842250 - SOTAMD. This work was furthermore supported in part by the European Union's Horizon 2020 Research and Innovation Program under Grant 690907 (IDENTITY).

References

[1] M. Ferrara, A. Franco, and D. Maltoni, "The magic passport," in *Proceedings of the 2014 International Joint Conference on Biometrics (IJCB)*. IEEE, sep 2014.

[2] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, "Face recognition systems under morphing attacks: A survey," *IEEE Access*, 2019.

[3] G. Wolberg, "Image morphing: a survey," *The Visual Computer*, vol. 14, no. 8-9, pp. 360–372, dec 1998.

[4] A. Patel and P. Lapsiwala, "Image morphing algorithm: A survey," *International Journal of Computer Applications (IJCA)*, vol. 5, no. 3, pp. 156–160, 2015.

[5] L. Debiasi, U. Scherhag, C. Rathgeb, A. Uhl, and C. Busch, "PRNU-based detection of morphed face images," in *Proceedings of the 6th International Workshop on Biometrics and Forensics (IWBF)*. IEEE, 2018.

[6] M. Ferrara, A. Franco, and D. Maltoni, "On the effects of image alterations on face recognition accuracy," in *Face Recognition Across the Imaging Spectrum*. Springer International Publishing, 2016, pp. 195–222.

[7] D. J. Robertson, A. Mungall, D. G. Watson, K. A. Wade, S. J. Nightingale, and S. Butler, "Detecting morphed passport photos: a training and individual differences approach," *Cognitive Research: Principles and Implications*, vol. 3, no. 1, jun 2018.

[8] U. Scherhag, C. Rathgeb, and C. Busch, "Towards detection of morphed face images in electronic travel documents," in *Proceedings of the 13th IAPR Workshop on Document Analysis Systems (DAS)*, 2018.

[9] ——, "Performance variation of morphed face image detection algorithms across different datasets," in *Proceedings of the 6th International Workshop on Biometrics and Forensics (IWBF)*. IEEE, Jun. 2018.

[10] L. Debiasi, C. Rathgeb, U. Scherhag, A. Uhl, and C. Busch, "PRNU variance analysis for morphed face image detection," in *Proceedings of the 9th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*. IEEE, 2018.

[11] R. Ramachandra, K. B. Raja, and C. Busch, "Detecting morphed face images," in *Proceedings of the 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*. IEEE, sep 2016.

[12] U. Scherhag, R. Ramachandra, K. B. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch, "On the vulnerability of face recognition systems towards morphed face attacks," in *Proceedings of the 5th International Workshop on Biometrics and Forensics (IWBF)*. IEEE, Apr. 2017.

[13] R. Ramachandra, K. Raja, S. Venkatesh, and C. Busch, "Face morphing versus face averaging: Vulnerability and detection," in *Proceedings of the 2017 International Joint Conference on Biometrics (IJCB)*. IEEE, oct 2017.

[14] P. Phillips, P. Flynn, T. Scruggs, K. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek, "Overview of the face recognition grand challenge," in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*. IEEE, 2005.

[15] A. Agarwal, R. Singh, M. Vatsa, and A. Noore, "SWAPPED! digital face presentation attack detection via weighted local magnitude pattern," in *Proceedings of the 2017 International Joint Conference on Biometrics (IJCB)*. IEEE, oct 2017.

[16] A. Asaad and S. Jassim, "Topological data analysis for image tampering detection," in *Digital Forensics and Watermarking*. Springer International Publishing, 2017, pp. 136–146.

[17] S. Jassim and A. Asaad, "Automatic detection of image morphing by topology-based analysis," in *Proceedings of the 26th European Signal Processing Conference (EUSIPCO)*, 2018.

[18] A. Makrushin, T. Neubert, and J. Dittmann, "Automatic generation and detection of visually faultless facial morphs," in *Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*. SCITEPRESS - Science and Technology Publications, 2017.

[19] "Utrecht ECVP," European Conference on Visual Perception, 2008.

[20] 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 *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security - IHMMSec '17*. ACM Press, 2017.

[21] U. Scherhag, C. Rathgeb, and C. Busch, "Morph detection from single face images: a multi-algorithm fusion approach," in *Proceedings of the 2018 International Conference on Biometrics Engineering and Application (ICBEA)*. ACM, 2018.

[22] P. Phillips, H. Wechsler, J. Huang, and P. J. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image and Vision Computing*, vol. 16, no. 5, pp. 295–306, apr 1998.

[23] A. Martinez and R. Benavente, "The AR face database," Computer Vision Center (CVC), Tech. Rep. 24, Jun. 1998.

[24] L. Spreeuwers, M. Schils, and R. Veldhuis, "Towards robust evaluation of face morphing detection," in *Proceedings of the 26th European Signal Processing Conference (EUSIPCO)*, 2018.

[25] N. Damer, Y. Wainakh, V. Boller, S. von den Berken, P. Terhörst, A. Braun, and A. Kuijper, "MorGAN: Recognition vulnerability and attack detectability of face morphing attacks created by generative adversarial network," in *Proceedings of the 9th IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*. IEEE, 2018.

[26] Z. Liu, P. Luo, X. Wang, and X. Tang, "Deep learning face attributes in the wild," in *2015 IEEE International Conference on Computer Vision (ICCV)*. IEEE, dec 2015, celebA.

[27] L.-B. Zhang, F. Peng, and M. Long, "Face morphing detection using fourier spectrum of sensor pattern noise," in *2018 IEEE International Conference on Multimedia and Expo (ICME)*. IEEE, jul 2018.

[28] C. E. Thomaz and G. A. Giraldi, "A new ranking method for principal components analysis and its application to face image analysis," *Image and Vision Computing*, vol. 28, no. 6, pp. 902–913, jun 2010.

[29] 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 *Proceedings of the 5th International Workshop on Biometrics and Forensics (IWBF)*. IEEE, apr 2017.

[30] C. Seibold, A. Hilsmann, and P. Eisert, "Reflection analysis for face morphing attack detection," in *Proceedings of the 26th European Signal Processing Conference (EUSIPCO)*, 2018.

[31] R. Ramachandra, S. Venkatesh, K. Raja, and C. Busch, "Detecting face morphing attacks with collaborative representation of steerable features," in *Proceedings of the 3rd Computer Vision and Image Processing (CVIP)*, 2018.

[32] R. Ramachandra, K. B. Raja, S. Venkatesh, and C. Busch, "Transferable deep-CNN features for detecting digital and print-scanned morphed face images," in *Proceedings of the 2017 Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. IEEE, jul 2017.

[33] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Accurate and robust neural networks for security related applications exampled by face morphing attacks," *Computer Vision and Pattern Recognition (CVPR)*, 2018.

[34] L. Yin, X. Wei, Y. Sun, J. Wang, and M. Rosato, "A 3d facial expression database for facial behavior research," in *7th International Conference on Automatic Face and Gesture Recognition (FGR06)*. IEEE, 2006.

[35] D. S. Ma, J. Correll, and B. Wittenbrink, "The chicago face database: A free stimulus set of faces and norming data," *Behavior Research Methods*, vol. 47, no. 4, pp. 1122–1135, jan 2015.

[36] A. Kasinski, A. Florek, and A. Schmidt, "The PUT face database," *Image Processing & Communications*, Jan. 2008.

[37] M. Grgic, K. Delac, and S. Grgic, "SCface surveillance cameras face database," *Multimedia Tools and Applications*, vol. 51, no. 3, pp. 863–879, oct 2009.

[38] L. Wandzik, G. Kaeding, and R. V. Garcia, "Morphing detection using a general-purpose face recognition system," in *Proceedings of the 26th European Signal Processing Conference (EUSIPCO)*, 2018.

[39] R. Gross, I. Matthews, J. Cohn, T. Kanade, and S. Baker, "Multi-PIE," in *2008 8th IEEE International Conference on Automatic Face & Gesture Recognition*. IEEE, sep 2008.

[40] M. Ngan, P. Grother, and K. Hanaoka, "Performance of automated facial morph detection and morph resistant face recognition algorithms," National Institue of Standards and Technology (NIST), Tech. Rep., 2018.

[41] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on featured distributions," *Pattern Recognition*, vol. 29, no. 1, pp. 51–59, jan 1996.

[42] J. Kannala and E. Rahtu, "BSIF: Binarized statistical image features," in *Proceedings of the 21st International Conference on Pattern Recognition (ICPR2012)*, Nov 2012, pp. 1363–1366.

[43] S. Cai, L. Zhang, W. Zuo, and X. Feng, "A probabilistic collaborative representation based approach for pattern classification," in *Proceedings of the 2016 Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, jun 2016.

[44] D. Chen, X. Cao, F. Wen, and J. Sun, "Blessing of dimensionality: High-dimensional feature and its efficient compression for face verification," in *Proceedings of the 2013 Conference on Computer Vision and Pattern Recognition*. IEEE, jun 2013.

[45] C. E. Thomaz and G. A. Giraldi, "A new ranking method for principal components analysis and its application to face image analysis," *Image and Vision Computing*, vol. 28, no. 6, pp. 902–913, Jun. 2010.

[46] R. Ramachandra, S. Venkatesh, K. Raja, and C. Busch, "Towards making morphing attack detection robust using hybrid scale-space colour texture features," in *Proceedings of 5th International Conference on Identity, Security and Behaviour Analysis (ISBA)*, 2019, pp. 22–24.

[47] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110, nov 2004.

[48] H. Bay, A. Ess, T. Tuytelaars, and L. V. Gool, "Speeded-up robust features (SURF)," *Computer Vision and Image Understanding*, vol. 110, no. 3, pp. 346–359, jun 2008.

[49] C. Shu, X. Ding, and C. Fang, "Histogram of the oriented gradient for face recognition," *Tsinghua Science and Technology*, vol. 16, no. 2, pp. 216–224, apr 2011.

[50] B. Amos, B. Ludwiczuk, and M. Satyanarayanan, "OpenFace: A general-purpose face recognition library with mobile applications," School of Computer Science Carnegie Mellon University, Tech. Rep., 2016.

[51] T. Neubert, "Face morphing detection: An approach based on image degradation analysis," in *Digital Forensics and Watermarking*. Springer International Publishing, 2017, pp. 93–106.

[52] A. Makrushin, C. Kraetzer, T. Neubert, and J. Dittmann, "Generalized benfords law for blind detection of morphed face images," in *Proceedings of the 6th ACM Workshop on Information Hiding and Multimedia Security - IH&MMSec '18*. ACM Press, 2018.

[53] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *Computer Vision and Pattern Recognition*, 2014.

[54] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Communications of the ACM*, vol. 60, no. 6, pp. 84–90, may 2017.

[55] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Detection of face morphing attacks by deep learning," in *Digital Forensics and Watermarking*. Springer International Publishing, 2017, pp. 107–120.

[56] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," in *Proceedings of the 2015 Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, jun 2015.

[57] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep face recognition," in *Procedings of the British Machine Vision Conference 2015*. British Machine Vision Association, 2015.

[58] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proceedings of the 2015 Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, jun 2015.

[59] ISO/IEC JTC1 SC37 Biometrics, *Information technology – Biometric data interchange formats – Part 5: Face image data*, 2005.

[60] International Civil Aviation Organization, "ICAO doc 9303, machine readable travel documents – part 9: Deployment of biometric identification and electronic storage of data in mrtds (7th edition)," ICAO, Tech. Rep., 2015.

[61] W. Funk, M. Arnold, C. Busch, and A. Munde, "Evaluation of image compression algorithms for fingerprint and face recognition systems," in *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005.* IEEE, 2005.

[62] M. Ferrara, A. Franco, and D. Maltoni, "Face demorphing," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 4, pp. 1008–1017, apr 2018.

[63] ——, "Face demorphing in the presence of facial appearance variations," in *Proceedings of the 26th European Signal Processing Conference (EUSIPCO)*, 2018.

[64] U. Scherhag, D. Budhrani, M. Gomez-Barrero, and C. Busch, "Detecting morphed face images using facial landmarks," in *Lecture Notes in Computer Science*. Springer International Publishing, 2018, pp. 444–452.

[65] N. Damer, V. Boller, Y. Wainakh, F. Boutros, P. Terhörst, A. Braun, and A. Kuijper, "Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts," in *Proceedings of the 40th German Conference of Pattern Recognition (GCPR)*, 2018.

[66] J. Fridrich, "Digital image forensic using sensor noise," *IEEE Signal Processing Magazine*, vol. 26, no. 2, 3 2009.

[67] M. Mihcak, I. Kozintsev, and K. Ramchandran, "Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising," in *Proc. of the 1999 IEEE Intl. Conf. on Acoustics, Speech, and Signal Processing, ICASSP '99*. IEEE, 2009.

[68] T. Gloe, S. Pfennig, and M. Kirchner, "Unexpected artefacts in PRNU-based camera identification: a'dresden image database'case-study," in *Proceedings of the on Multimedia and security*. ACM, 2012, pp. 109–114.

[69] A. Cortiana, V. Conotter, G. Boato, and F. De Natale, "Performance comparison of denoising filters for source camera identification," in *Media Watermarking, Security, and Forensics III*, vol. 7880. International Society for Optics and Photonics, 2011, p. 788007.

[70] W. van Houten and Z. Geradts, "Using anisotropic diffusion for efficient extraction of sensor noise in camera identification," *Journal of forensic sciences*, vol. 57, no. 2, pp. 521–527, 2012.

[71] F. Gisolf, A. Malgoezar, T. Baar, and Z. Geradts, "Improving source camera identification using a simplified total variation based noise removal algorithm," *Digital Investigation*, vol. 10, no. 3, pp. 207–214, 2013.

[72] A. J. Cooper, "Improved photo response non-uniformity (PRNU) based source camera identification," *Forensic science international*, vol. 226, no. 1-3, pp. 132–141, 2013.

[73] X. Kang, J. Chen, K. Lin, and P. Anjie, "A context-adaptive spn predictor for trustworthy source camera identification," *EURASIP Journal on Image and Video Processing*, vol. 2014, no. 1, p. 19, 2014.

[74] M. Al-Ani, F. Khelifi, A. Lawgaly, and A. Bouridane, "A novel image filtering approach for sensor fingerprint estimation in source camera identification," in *2015 12th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE, 2015, pp. 1–5.

[75] H. Zeng and X. Kang, "Fast source camera identification using content adaptive guided image filter," *Journal of forensic sciences*, vol. 61, no. 2, pp. 520–526, 2016.

[76] C.-T. Li, "Source camera identification using enhanced sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 280–287, 2010.

[77] C.-T. Li and Y. Li, "Color-decoupled photo response non-uniformity for digital image forensics," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 22, no. 2, p. 260, 2012.

[78] X. Kang, Y. Li, Z. Qu, J. Huang *et al.*, "Enhancing source camera identification performance with a camera reference phase sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 393–402, 2012.

[79] X. Lin and C.-T. Li, "Preprocessing reference sensor pattern noise via spectrum equalization," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 1, pp. 126–140, 2016.

[80] ——, "Enhancing sensor pattern noise via filtering distortion removal," *IEEE Signal Processing Letters*, vol. 23, no. 3, 2016.

[81] 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.

[82] M. Goljan, J. Fridrich, and J. Lukas, "Camera identification from printed images," in *Proc. of SPIE, Electronic Imaging, Forensics, Security, Steganography, and Watermarking of Multimedia Contents X*. SPIE, 2008.

[83] J. Lukáš, J. Fridrich, and M. Goljan, "Digital camera identification from sensor pattern noise," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 205–214, 2006.

[84] T. Gloe, M. Kirchner, A. Winkler, and R. Böhme, "Can we trust digital image forensics?" in *Proceedings of the 15th ACM international conference on Multimedia*. ACM, 2007, pp. 78–86.

[85] A. Karaküçük and A. E. Dirik, "Adaptive photo-response non-uniformity noise removal against image source attribution," *Digital Investigation*, vol. 12, pp. 66–76, 2015.

[86] L. J. G. Villalba, A. L. S. Orozco, J. R. Corripio, and J. Hernandez-Castro, "A PRNU-based counter-forensic method to manipulate smartphone image source identification techniques," *Future Generation Computer Systems*, vol. 76, pp. 418–427, 2017.

[87] S. Bayram, H. T. Sencar, and N. D. Memon, "Seam-carving based anonymization against image & video source attribution," in *2013 IEEE 15th International Workshop on Multimedia Signal Processing (MMSP)*. IEEE, 2013, pp. 272–277.

[88] A. E. Dirik and A. Karaküçük, "Forensic use of photo response non-uniformity of imaging sensors and a counter method," *Optics express*, vol. 22, no. 1, pp. 470–482, 2014.

[89] A. Elliethy and G. Sharma, "Image anonymization for PRNU forensics: A set theoretic framework addressing compression resilience," in *2016 IEEE International Conference on Image Processing (ICIP)*. IEEE, 2016, pp. 3907–3911.

[90] R. Caldelli, I. Amerini, and A. Novi, "An analysis on attacker actions in fingerprint-copy attack in source camera identification," in *2011 IEEE International Workshop on Information Forensics and Security*. IEEE, 2011, pp. 1–6.

[91] F. Marra, F. Roli, D. Cozzolino, C. Sansone, and L. Verdoliva, "Attacking the triangle test in sensor-based camera identification," in *2014 IEEE International Conference on Image Processing (ICIP)*. IEEE, 2014, pp. 5307–5311.

[92] M. Barni, M. Nakano-Miyatake, H. Santoyo-Garcìa, and B. Tondi, "Countering the pooled triangle test for PRNU-based camera identification," in *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE, 2018, pp. 1–8.

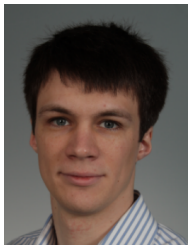
[93] M. Goljan, J. Fridrich, and M. Chen, "Defending against fingerprint-copy attack in sensor-based camera identification," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 1, pp. 227–236, 2011.

[94] V. U. Sameer, R. Naskar, N. Musthyala, and K. Kokkalla, "Deep learning based counter–forensic image classification for camera model identification," in *International Workshop on Digital Watermarking*. Springer, 2017, pp. 52–64.

[95] S. Banerjee, V. Mirjalili, and A. Ross, "Spoofing PRNU patterns of iris sensors while preserving iris recognition," in *Proceedings of the 5th IEEE International Conference on Identity, Security and Behavior Analysis (ISBA)*. ACM, 2019.

[96] A. Uhl and Y. Höller, "Iris-sensor authentication using camera PRNU fingerprints," in *2012 5th IAPR International Conference on Biometrics (ICB)*. IEEE, 2012, pp. 230–237.

[97] S. Banerjee and A. Ross, "Impact of photometric transformations on PRNU estimation schemes: A case study using near infrared ocular images," in *2018 International Workshop on Biometrics and Forensics (IWBF)*. IEEE, 2018, pp. 1–8.
[98] K. Rosenfeld and H. T. Sencar, "A study of the robustness of prnu-based camera identification," in *Media Forensics and Security*, vol. 7254. International Society for Optics and Photonics, 2009, p. 72540M.
[99] T. Gloe and R. Böhme, "The 'Dresden Image Database' for benchmarking digital image forensics," in *Proceedings of the 25th Symposium On Applied Computing (ACM SAC 2010)*, vol. 2, 2010, pp. 1585–1591.
[100] D. E. King, "Dlib-ml: A machine learning toolkit," *J. Mach. Learn. Res.*, vol. 10, pp. 1755–1758, Dec. 2009.
[101] U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. N. J. Veldhuis, L. Spreeuwers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Ramachandra, and C. Busch, "Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting," in *Proceedings of the 2017 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, sep 2017.
[102] ISO/IEC JTC1 SC37 Biometrics, "Information technology – biometric presentation attack detection – part 3: Testing and reporting," International Organization for Standardization, Geneva, Switzerland, ISO ISO/IEC IS 30107-3:2017, 2017.
[103] S. Liao, X. Zhu, Z. Lei, L. Zhang, and S. Z. Li, "Learning multi-scale block local binary patterns for face recognition," in *Advances in Biometrics*. Springer Berlin Heidelberg, 2007, pp. 828–837.



Ulrich Scherhag received his B.Eng degree (Electrical Engineering) in 2012 from the Duale Hochschule Baden-Württemberg, Mannheim. He stated studying computer science in 2014 at Hochschule Darmstadt and received the M.Sc degree (Computer Science, IT-Security) in 2016, for which he was granted the CAST Award IT-Security 2016. Since 2016 he is a Ph.D. Student Member of da/sec at the Center for Research in Security and Privacy (CRISP). He is a member of the European Association for Biometrics (EAB) and a Reviewer for the International Conference of the Biometrics Special Interest Group (BIOSIG) and IEEE Access. His current research focuses on presentation attack detection and morphed face detection.

Luca Debiasi received his B.Eng degree (Computer Science) in 2011 from the University of Salzburg. He continued the computer science masters program in at the University of Salzburg and received his Dipl.-Ing. degree in Computer Science in 2015. Since 2015, he is a Ph.D. Student and member of the Multimedia Signal Processing and Security Lab (WaveLab) at the Department of Computer Sciences at the University of Salzburg. His main research interests include digital image forensics, biometrics (hand- and finger-veins, iris, face), presentation attack detection, privacy enhancing technologies and texture classification.

Dr. Christian Rathgeb is a Senior Researcher with the Faculty of Computer Science, Hochschule Darmstadt (HDA), Germany. He is a Principal Investigator in the Center for Research in Security and Privacy (CRISP). His research includes pattern recognition, iris and face recognition, security aspects of biometric systems, secure process design and privacy enhancing technologies for biometric systems. He co-authored over 100 technical papers in the field of biometrics. He is a winner of the EAB - European Biometrics Research Award 2012, the Austrian Award of Excellence 2012, Best Poster Paper Awards (IJCB'11, IJCB'14, ICB'15) and the Best Paper Award Bronze (ICB'18). He is a member of the European Association for Biometrics (EAB), a Program Chair of the International Conference of the Biometrics Special Interest Group (BIOSIG) and a editorial board member of IET Biometrics (IET BMT). He has served for various program committees and conferences (e.g. ICB, IJCB, BIOSIG, IWBF) and journals as a reviewer (e.g. IEEE TIFS, IEEE TBIOM, IET BMT).

Prof. Dr. Christoph Busch is member of the Department of Information Security and Communication Technology (IIK) at the Norwegian University of Science and Technology (NTNU), Norway. He holds a joint appointment with the computer science faculty at Hochschule Darmstadt (HDA), Germany. Further he lectures Biometric Systems at Technical University of Denmark (DTU) since 2007. Christoph Busch co-authored more than 400 technical papers and has been a speaker at international conferences. He served for various program committees (NIST IBPC, ICB, ICHB, BSI-Congress, GI-Congress, DACH, WEDELMUSIC, EUROGRAPHICS) and served for several conferences, journals and magazines as reviewer (e.g. ACM-SIGGRAPH, ACM-TISSEC, IEEE CG&A, IEEE Transactions on Signal Processing, on Information Forensics and Security, on Pattern Analysis and Machine Intelligence and the Elsevier Journal Computers & Security). He is also an appointed member of the editorial board of the IET journal on Biometrics and of IEEE TIFS journal. Furthermore, on behalf of Fraunhofer, he chairs the biometrics working group of the TeleTrusT association as well as the German standardization body on Biometrics (DIN-NIA37). He is convenor of WG3 in ISO/IEC JTC1 SC37 on Biometrics and active member of CEN TC 224 WG18.

Prof. Dr. Andreas Uhl received the Ph.D. degree from the University of Salzburg. He is currently a Professor with the Department of Computer Sciences, University of Salzburg. He has co-authored over 400 scientific publications. His research interests are in processing and analysis of visual data in general, and in biometric systems, multimedia security and forensics, and medical data analysis in particular. He acts as an Associate Editor for ACM TOMM, Signal Processing: Image Communication, the Journal of Visual Communication and Image Representation, and the ETRI Journal.