PRNU-based Detection of Facial Retouching

C. Rathgeb[1], A. Botaljov[1], F. Stockhardt[1], S. Isadskiy[1], L. Debiasi[2], A.Uhl[2] and C. Busch[1]

[1] da/sec – Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany
[2] WaveLab – The Multimedia Signal Processing and Security Lab, University of Salzburg, Austria

christian.rathgeb@h-da.de

Abstract

Nowadays, many facial images are acquired using smart phones. To ensure the best outcome, users frequently retouch these images before sharing them, e.g. via social media. In particular retouching apps represent common tools which can be applied to improve one's facial appearance. Modifications of the facial geometry and texture resulting from such retouching algorithms might be a new challenge for face recognition technologies. Towards deploying robust face recognition as well as enforcing anti-photoshop legislations, a robust and reliable detection of retouched face images is needed.

In this work, the effects of facial retouching on face recognition are investigated. A qualitative assessment of 32 beautification apps available in different app stores is conducted. Based on this assessment five apps are chosen which are used to manually create a database of 800 beautified face images. Biometric performance is measured before and after retouching using a commercial face recognition system. Subsequently, a retouching detection system based on the analysis of Photo Response Non-Uniformity (PRNU) is presented. Specifically, scores obtained from analyzing spatial and spectral features extracted from PRNU patterns across image cells are fused. In a realistic scenario, in which unaltered bona fide images are compressed to the average target sizes of the retouched images using JPEG compression, the proposed PRNU-based retouching detection scheme is shown to robustly distinguish between bona fide and retouched face images achieving an average D-EER of 13.7% across all retouching algorithms.

1 Introduction

In the last several decades, face recognition has been a highly active research field [7, 8, 9]. In the recent past, the introduction of deep convolutional neural networks has shown impressive performance improvements in facial recognition technologies [10, 11, 12, 13, 14], which facilitated the use of facial recognition technologies in various application scenarios ranging from automated border control to access control for mobile devices. However, a number of covariates has been identified, which can degrade the recognition accuracy of face recognition, such as variations in pose, facial expression or image quality [15, 9]. Additionally, digital face beautification, i.e. *facial retouching*, was determined to be able to significantly alter the perceived shape and texture of a human face and therefore to potentially compromise the use of face recognition systems [1]. Facial retouching induces alterations similar to those achieved by plastic surgery [16] or facial cosmetics [17]. Beyond that, further changes in appearance can be made to face images in the digital domain, e.g. increase or repositioning of eyes. Besides professional image editing software, e.g. Photoshop, there exist plenty of mobile applications, i.e. apps, which provide numerous filters and special effects that can be easily applied even by unskilled users. An example of facial retouching using a popular beautification app is depicted in Fig. 1. It can be observed that the exemplary retouching app generates a more narrow chin and thinner nose appearance and enlarges the eyes. Thus, facial

(a) original (b) retouched (c) differences

Figure 1: Application of a beautification app: (a) original image, (b) retouched image, and (c) main differences between (a) and (b).

Table 1: Most relevant works on the impact and detection of facial retouching in face recognition (partially derived from [1]).

Authors	Database	Method(s)	Recognition performance		Retouching detection	Remarks
			Unaltered	Retouched		
Ferrara et al. [2]	AR face (118 subjects)	2× COTS, SIFT	∼0% EER (COTS)	∼ 2%,∼5%,∼17% EER for low/medium/high intensity (COTS)	–	3 intensities of retouching with LiftMagic, small amount of comparisons
Bharati et al. [3]	ND-IIITD Retouched Faces (325 subjects), Celebrity (165 subjects)	Recognition: COTS, OpenBR Detection: face patch-based deep supervised RBM with SVM	100% R-1 (COTS)	97.67% R-1 (average, COTS)	87.1% CCR on ND-IIITD Retouched Faces, 96.2% CCR on Celebrity	7 types of retouching with PortraitPro Studio Max
Bharati et al. [4]	Multi-Demographic Retouched Faces (600 subjects)	Sub-class supervised sparse Autoencoder	–	–	94.3% CCR (on average)	2 types of retouching with PortraitPro Studio Max and BeautyPlus
Jain et al. [5]	ND-IIITD Retouched Faces	CNN with SVM	–	–	99.65% CCR	–
Wang et al. [6]	Automatically generated based on OpenImage and Flickr (1.1M face images)	Dilated Residual Network	–	–	90% CCR	Detection of Photoshop image warping operation, manually created test set

retouching plays an important role in diverse scenarios in which face recognition is deployed:

1. **Social media:** If face recognition technologies are applied to images obtained from social media such as Facebook or Instagram, e.g. during a forensic investigation, the previous application of retouching is highly probable. Such a use-case might become of utmost relevance for face recognition in the future considering the increasing use of social media and the amount of available beautification apps.

2. **Document issuance:** Also, different kinds of image manipulation including retouching might be performed prior to the issuance of an electronic travel document. In many countries, the face image used for the ePassport issuance is provided by the applicant. Based on this security gap in the process the vulnerability of face recognition systems to so-called morphing attacks has recently been exposed [18]. Similarly, facial retouching could be applied which could significantly degrade the performance of a face recognition system, e.g. at an automated border control.

Besides the aforementioned scenarios the need for a reliable detection of digitally beautified face images is further motivated by the introduction of the so-called "photoshop law" [19]. People's behaviours are frequently influenced by advertising in which digitally manipulated image are displayed. Hence, people's preferences are often ill-formed and their choices might produce ill-advised effects. In response, in 2014 the state of Israel enacted a law in order to reduce growing eating disorders hazards resulting from beautified images used in advertisements. A similar law applies in France since 2017 while in many other countries, e.g. Belgium, Spain, Italy or Germany, suitable regulations and laws are under discussion. As a result, digitally retouched images must be labeled as "edited photograph". Exceptions are minor editing, such as smoothing skin, removing blemishes, airbrushing, changing hair colour [20].

In this context, the contribution of this work can be summarized as follows:

- Based on a subset of the publicly available FRGCv2 face database [21] a total number of 800 retouched face images are manually created with limited interaction to specify for instance the intensity of the beautification for each sample. For this purpose five different mobile apps are used to ensure a variety of retouching algorithms. The composed image sets can be used to directly evaluate the performance of face recognition systems before and after the application of facial retouching as well as retouching detection schemes.

- The impact of facial retouching on face recognition performance is estimated for the commercial Cognitec FaceVACS system v9.3 [22]. For this evaluation the most challenging scenario is considered, i.e. when facial retouching is applied either to the reference or probe face image. Obtained results show that facial retouching has negligible negative impact on the recognition accuracy of a state-of-the-art face recognition system. More specifically, at a practically relevant operation point which yields a FMR of 0.1% a FNMR of 0% is maintained for all considered beautification apps.

- A facial retouching detection system is proposed, which analyzes spatial and spectral features extracted from PRNU patterns across image regions. The presented scheme builds upon the works of Debiasi et al. [23, 24], Zhang et al. [25] and Scherhag et al. [26] in which an analysis of the PRNU pattern was successfully utilized to detect image manipulations resulting from face morphing [18]. These approaches are adapted and extended by a normalized score-level fusion of retouching of equally weighted detection scores obtained from the analysis of various spatial and spectral features of the PRNU. In the best configuration, the proposed fusion-based approach achieves

an average Detection-Equal-Error-Rate (D-EER) of 13.7% outperforming a state-of-the-art retouching detection system [6] and an image forgery detection scheme based on noise variance inconsistencies [27]. Compared to recently published schemes which make use of (deep) learning techniques the presented approach does not require extensive training. Further, in contrast to related works, the composed database consists of images created by a wider variety of retouching algorithms which is of utmost importance to test generalizability and avoid overfitting. Lastly, in the detection experiments it is ensured that image compression is applied at the same level for bona fide and retouched images which is an issue that has been ignored by recent works but significantly influences the detection accuracy as will be shown.

The remainder of this paper is organized as follows: related works are discussed in Sect. 2. Subsequently, the image databases used in this work are described in detail in Sect. 3. The impact of facial retouching on the face recognition performance of a commercial face recognition system is evaluated in Sect. 4. The proposed PRNU-based retouching detection approach is presented in Sect. 5. Detection results are summarized in Sect. 6 and conclusions are drawn in Sect. 7.

2 Related Work

Relevant works investigating the impact of facial retouching on face recognition along with used databases, applied methods and reported results are summarized in Table 1. Performance rates are mostly reported using standardized metrics for measuring biometric performance [60], e.g., Equal Error Rate (ERR) or Rank-1 Identification Rate (R-1). For detection schemes the Correct Classification Rate (CCR), which corresponds to the D-EER, is frequently used. Up until now, only a small amount of research regarding this topic has been conducted. Ferrara et al. [2, 61] were the first to analyse the impact of retouching on face recognition systems. After the application of heavy facial retouching a significant performance degradation was reported. These findings have been confirmed in further works, e.g. [3, 4]. Additionally, Bharati et al. [3, 4] proposed different facial retouching detection schemes based on deep learning. The development of deep learning-based retouching detection schemes is favoured by the possibility to automatically generate a large amount of training data. However, in contrast to conventional image forensic-based manipulation detection methods, e.g. [62, 63], in-depth analysis are required to investigate which types of features are learned by the aforementioned approaches to distinguish between unaltered and retouched facial images. The system proposed in [3] reported to achieve higher accuracy than a re-implementation of the scheme introduced by Kee et al. [62]. Moreover, the scheme introduced in [3] was shown to exhibit competitive detection performance for the task of makeup detection. However, tested databases, e.g. YMU, do not contain retouched face images but face images before and after the application of facial cosmetics. This suggests that this scheme detects exaggerated facial appearances, which might as well result from the use of facial cosmetics [1]. While the authors consider different types of beautification, only a single retouching software is

Table 2: App store ratings (out of five possible stars) and subjective assessment of various beautification apps w.r.t. usability (U), type of beautification (T) and quality of beautification (Q); "+", "○", and "−" refers to "good, "average", and "bad", respectively.

Nr.	App	Rating	U	T	Q
1.	Adobe Photoshop Lightroom CC [28]	4.4	○	○	+
2.	AirBrush [29]	4.9	+	+	+
3.	B612 [30]	4.2	+	+	−
4.	Beauty Camera [31]	4.0	+	−	+
5.	BeautyPlus [32]	4.6	+	+	−
6.	Camly [33]	4.2	+	○	−
7.	Camera 360 [34]	4.4	○	+	−
8.	Candy Camera [35]	4.4	○	+	−
9.	Cymera Camera [36]	4.4	○	+	−
10.	Face-App [37]	3.9	○	○	−
11.	Facelab [38]	4.1	+	−	+
12.	Facetune2 [39]	4.4	+	○	+
13.	Facey [40]	4.4	+	○	+
14.	FotoRus [41]	4.5	+	+	+
15.	Fotor Photo Editor [42]	4.5	+	−	+
16.	HDPhotoEditor [43]	4.0	○	−	+
17.	InstaBeauty Selfies [44]	3.3	+	+	+
18.	InstaBeauty [45]	3.9	+	+	+
19.	MakeupEditor [46]	4.0	+	−	−
20.	Manly [47]	4.2	+	−	+
21.	Moldiv [48]	4.5	○	○	−
22.	Photo Editor Pro [49]	4.7	+	−	+
23.	Photo Editor [50]	4.5	○	○	+
24.	Photo Lab Picture Editor FX [51]	3.8	−	○	+
25.	PicsArt Photo Studio [52]	4.0	○	○	−
26.	Polarr Foto Editor [53]	4.4	+	+	+
27.	Prequel [54]	4.5	−	○	−
28.	Selfie Editor [55]	4.1	○	○	−
29.	SNOW [56]	4.2	+	−	−
30.	Square Fit [57]	4.6	○	−	+
31.	YouCam Perfect [58]	4.6	+	+	+
32.	Z Camera [59]	4.4	−	○	−

employed. In [4] images belonging to two genders, male and female, and three ethnicities, Indian, Chinese, and Caucasian are retouched using two different software packages. Limitations of state-of-the-art algorithms, i.e. texture-based algorithms proposed for makeup and morphing detection [18] and the scheme of [3], for the task of retouching detection in cross ethnicity evaluations are shown. Further, in [4] it is demonstrated that the performance of these algorithms is negatively affected when trained on different ethnicities. Following a similar learning-based approach, Jain et al. [5] reported a significant decrease in the detection accuracy in case image compression is only applied to retouched images during training. Different retouching algorithms might employ image compression at various qualities as postprocessing. This means that, as opposed to bona fide images, retouched images might comprise compression artefacts which facilitate the detection of retouching and learning-based algorithms might even overfit to said artefacts. However, in a realistic scenario it is required that bona fide and retouched images have undergone the same image compression. This issue is largely ignored in the aforementioned works. Wang et al. [6] introduced a facial retouching detection scheme which is specifically designed to detect image warping operation performed using the Adobe Photoshop software.

Unfortunately, the majority of the summarized facial retouching detection systems are not publicly available, in particular pre-trained detection models. Since all of the aforementioned related works require an extensive training of classifiers, large datasets of retouched images would be required in order to train re-implementations. In addition, important optimizations might have been omitted in proposed retouching detection schemes. Due to these facts, a direct comparison of the presented detection scheme with published approaches in terms of detection performance is hampered.

3 Database generation

To the best of the authors' knowledge there exists only one publicly available database[1] of retouched face images which has been used in [3, 5]. However, the images included in said database are generated by using a single desktop retouching software, i.e. PortraitPro Studio Max. Further, the retouched facial images of this dataset appear to some extent rather unnatural or even dollish. The following steps are performed to create a new database of retouched face images targeted at reflecting real-world scenarios: selection criteria for beautification apps are defined (Sect. 3.1) which are then used to assess available apps (Sect. 3.2); subsequently, selected apps are manually applied to a subset of a public face database (Sect. 3.3).

3.1 Retouching app selection criteria

The criteria to select appropriate retouching apps are summarized as follows:

- **Costs:** only apps which provide a basic beautification functionality without any cost are considered[2].
- **Usability:** easy-to-use apps which allow for an (all-in-one) automatic beautification are favored.
- **Type of beautification:** only apps which modify the facial appearance are considered[3].
- **Quality of beautification:** the application of the app should result in a realistic and natural appearance.

Listed criteria should ensure a reasonably fast manual creation of the database which contains only beautifications that can be relevant for face recognition.

3.2 Assessment of retouching apps

Table 2 provides a qualitative assessment of free beautification apps available in app stores together with their app store rating[4]. As can be seen, users' experience may not coincide with the proposed assessment based on which the following five apps are chosen for the database creation:

1. **AirBrush** slightly enlarges the eyes, makes the face slightly slimmer, eliminates minor wrinkles and skin impurities, and reduces dark rings under the eyes;
2. **FotoRus** enlarges the eyes (and makes them more shiny), makes the face slimmer, performs a nose thinning/lifting, and reduces dark rings under the eyes (this app is used with medium and maximum intensity);
3. **InstaBeauty** enlarges the eyes, makes the face slightly slimmer, performs a slight nose thinning, and reduces small skin impurities by smoothing the entire image (this app is used with medium and maximum intensity);
4. **Polarr** slightly enlarges the eyes, makes the face slightly slimmer, eliminates minor wrinkles and skin impurities, and modifies the corners of the mouth to get a more smiley face;

[1] ND-IIITD Retouched Face Database: `https://cvrl.nd.edu/projects/data/`

[2] Note that free apps are more likely to be applied by users.

[3] Many retouching apps only allow for modifications which are expected to be irrelevant for face recognition, e.g. insertion of earrings.

[4] If apps are available in Google Play Store and Apple App Store the average rating is included.

Table 3: Recognition performance results for the Cognitec FaceVAC v9.3 face recognition systems.

Distribution	Retouching	Mean (μ)	Std. Dev. (σ)	d'	FNMR$_{0.1}$ (%)
Impostor	None (bona fide)	0.055	0.065	–	–
Genuine	None (bona fide)	0.978	0.012	19.85	0.0
	AirBrush	0.975	0.012	19.79	0.0
	FotoRus (medium)	0.976	0.015	19.47	0.0
	FotoRus (maximum)	0.949	0.024	18.36	0.0
	InstaBeauty (medium)	0.974	0.015	19.72	0.0
	InstaBeauty (maximum)	0.969	0.015	19.48	0.0
	Polarr	0.974	0.013	19.70	0.0
	YouCam Perfect (contour)	0.974	0.013	19.73	0.0
	YouCam Perfect (refresh)	0.971	0.014	19.54	0.0

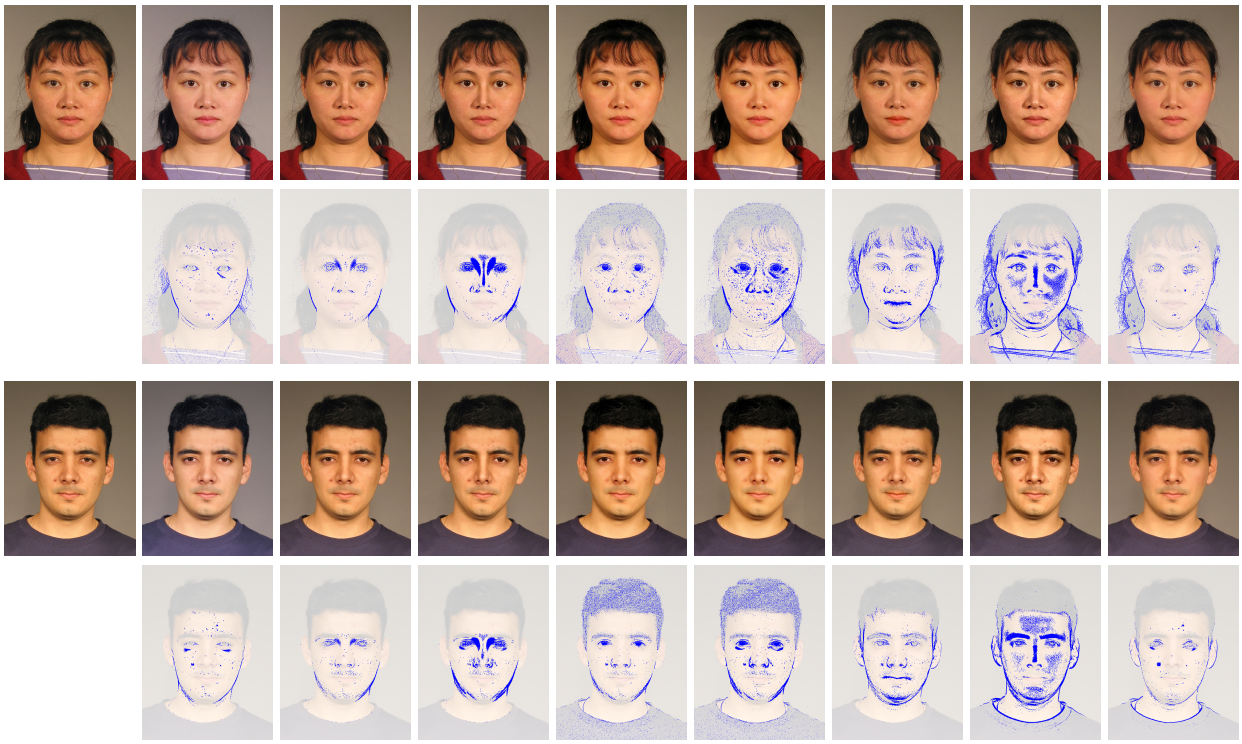


Figure 2: Example applications of selected beautification apps to face images of a female (top rows) and a male subject (bottom rows) depicted together with main differences. From left to right: original, AirBrush, FotoRus (medium), FotoRus (maximum), InstaBeauty (medium), InstaBeauty (maximum), Polarr, YouCam Perfect (contour) and YouCam Perfect (refresh).

5. **YouCam Perfect** enlarges the eyes, makes the cheeks more rosy, eliminates minor wrinkles and skin impurities, smooths the hair (this app is used in "contour" and "refresh" mode).

Fig. 2 depicts examples of applications of each selected app to a female and male face image.

3.3 Retouching database

The retouching database is created based on the FRGCv2 face database [21]. Face images of this database are manually filtered to meet ICAO requirements for electronic travel documents [64], e.g. frontal pose, neutral expression, homogeneous background and sufficient inter-ocular distance (at least 90 pixels between left and right eye). These specifications ensure that all facial images are of sufficient quality,

i.e. potential effects of beautification are isolated. Subsequently, images are cropped to a portrait format and aligned with respect to eye positions.

Out of this subset, the first 50 female and male subjects for which six ICAO-compliant images are available are chosen. The first face image of all of the 100 subjects is then interactively edited with each of the selected beautification apps resulting in 800 beautified images. Each app is applied only once per image[5].

4 Impact of Retouching on Face Recognition

In the following subsections the experimental protocol is described in detail (Sect. 4.1) and the obtained recognition performance results are reported (Sect. 4.2).

4.1 Experimental setup

The frequently deployed commercial Cognitec FaceVACS v9.3 [22] is used which returns a similarity score in the range $[0, 1]$ (i.e. high values indicate high similarity). Biometric performance is evaluated in terms of False Non-Match Rate (FNMR) and False Match Rate (FMR). More precisely, the FNMR at a FMR of 0.1%, referred to as $\text{FNMR}_{0.1}$, is reported which represents the operation point recommended in the guidelines of European Agency for the Management of Operational Cooperation at the External Borders (FRONTEX) [65]. In addition, Detection Error Trade-Off (DET) curves are presented. However, as the amount of facial images is limited, DET curves should be treated with caution. Therefore, rather than reporting Equal Error Rates (EERs) probability density distributions are shown and as a measure of decidability $d' = |\mu_g - \mu_i| / \sqrt{\frac{1}{2}(\sigma_g^2 + \sigma_i^2)}$ is reported, where μ_g and μ_i represent the means of the genuine (mated comparison trials) and the impostor (non-mated comparison trials) score distributions and σ_g and σ_i their standard deviations, respectively.

4.2 Recognition performance evaluation

Genuine comparisons are calculated by pairing the first image of each of the 100 chosen subjects with their remaining images. As there are six images per subject, i.e. one potentially beautified reference image and five unaltered probe images, 500 genuine comparisons are performed for the original images as well as for each of the five databases created by applying the chosen beautification apps. To obtain fixed thresholds for the $\text{FNMR}_{0.1}$ values impostor comparisons are obtained using original images of all subjects for which at least one ICAO-compliant image is available, resulting in 99,681 impostor scores. With respect to the $\text{FNMR}_{0.1}$ a fixed decision threshold of 0.47 for the normalized comparison score (in the range $[0, 1]$) was estimated.

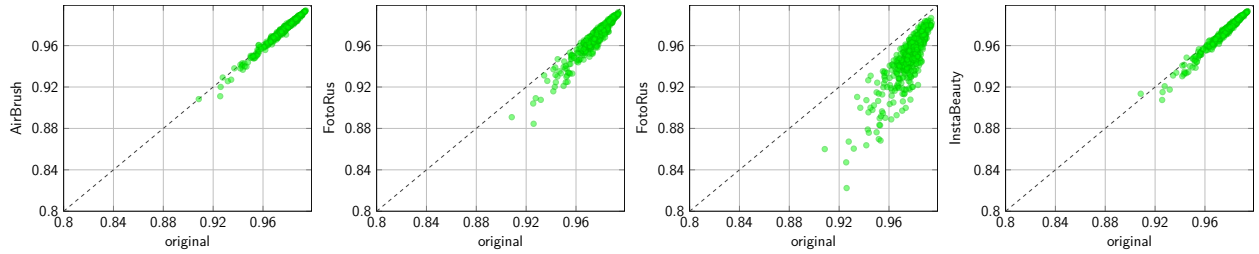
Obtained performance rates are summarized in Table 3. It can be observed that the commercial face recognition system obtains a zero $\text{FNMR}_{0.1}$ across all retouching apps. Also, from the lowest d' values it can be concluded that the FotoRus app has the most severe impact, followed by InstaBeauty and YouCam Perfect. These apps simulate anatomical alterations, i.e. enlargement of eyes or thinning of the nose, which negatively effect the recognition performance. The least impact is observed for Polarr and AirBrush which mainly apply cosmetic changes, e.g. removal of skin impurities or coloring of cheeks. In some cases such changes can even have a positive effect on recognition accuracy. Scatter plots of genuine comparison scores before and after beautification are shown in Fig. 3 and Fig. 4. Score distributions with and without the use of all selected apps are depicted in Fig. 5. Obtained results reveal that the use of beautification apps has negligible impact on the used commercial system. At a practically relevant threshold which yields a FMR of 0.1% the recognition performance is maintained. Focusing on open-source face recognition systems, the same experiments were conducted for a re-implementation of the well-known FaceNet algorithm [10] and the recently proposed ArcFace system [66]. The FaceNet system, which obtained significantly inferior recognition accuracy on bona fide images, was strongly affected by most facial retouching algorithms while the newer ArcFace system achieved robustness against all considered retouching apps. Note that in a more challenging scenario a decrease of comparison scores caused by facial retouching might have a stronger impact of recognition accuracy. Nevertheless, towards enforcing anti-photoshop legislations, a robust and reliable detection of retouched face image is required.

5 PRNU-based Retouching Detection

The photo response non-uniformity (PRNU), which is also known as sensor fingerprint, has been utilized as a reliable tool in different forensic tasks including device identification, device linking, recovery of processing history and the detection of digital forgeries. The PRNU describes the ratio between luminous flux on a pixel versus the electrical signal output. It is a weak noise-like signal which is inherently produced by every camera during the capturing process of an image. Hence, the PRNU represents an intrinsic property of digital imaging sensors.

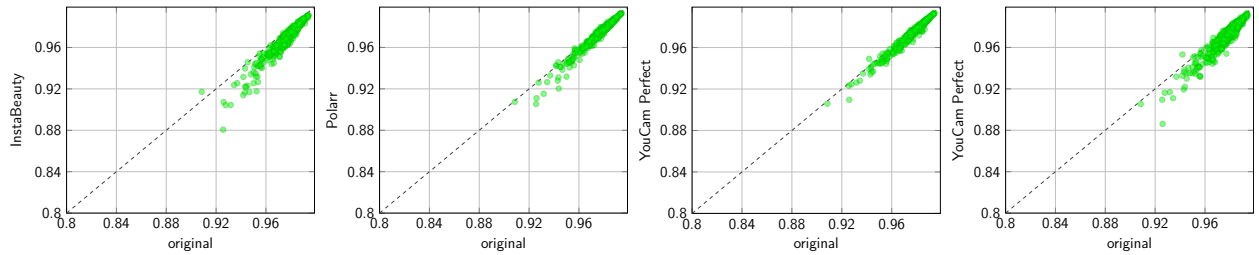
The extraction of the PRNU noise residual from an image can be performed by applying Fridrich's approach [67]. For each image I the noise residual W_I is estimated as de-

[5] Users might apply retouching apps multiple times on a single image to get a desired result.



(a) AirBrush (b) FotoRus (medium) (c) FotoRus (maximum) (d) InstaBeauty (medium)

Figure 3: Scatter plots of genuine comparison scores of the Cognitec FaceVACS v9.3 system before and after applying beautification apps AirBrush, FotoRus (medium), FotoRus (maximum) and InstaBeauty (medium).



(a) InstaBeauty (maximum) (b) Polarr (c) YouCam Perfect (contour) (d) YouCam Perfect (refresh)

Figure 4: Scatter plots of genuine comparison scores of the Cognitec FaceVACS v9.3 system before and after applying beautification apps InstaBeauty (maximum), Polarr, YouCam Perfect (contour) and YouCam Perfect (refresh).

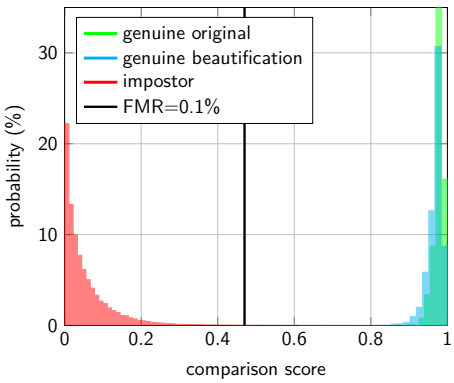


Figure 5: Score distributions before (original) and after (beautification) applying the selected apps.

scribed in Eq. (1),

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

where F denotes a denoising function which separates the noise from a an image. In this work, the denoising filter suggested by Mihcak et al. [68] is used. For further details on the denoising filter, the reader is referred refer to [68]. Fig. 7 depicts the PRNU signal estimated from an example face image.

Diverse signals present in an image might take an influence on the PRNU, e.g. high frequency image components and non-unique artefacts [69]. Therefore, different alternative PRNU extraction techniques, e.g. [70, 71], as well as PRNU enhancements, e.g. [72, 73], have been published in scientific literature in order to improve the quality of the extracted PRNU signal for the purpose of camera source identification. However, to the best of the authors' knowledge, no works have investigated their influence on the general properties of the PRNU signal. Therefore, the denoising filter introduced by Mihcak et al. [68] is used in the proposed scheme during the feature extraction step.

Different important properties of the PRNU which have been stated by Fridrich et al. in [74], make the PRNU highly suitable for the detection of facial retouching:

1. **Dimensionality**: the PRNU signal of an image carries a large amount of information which makes it possible to identify sensors.

2. **Unavoidability**: it is inherently embedded in all digital images during the capturing process.

3. **Universality**: the PRNU is present in every image regardless of the camera optics, camera settings, or scene content, completely dark images being an exception.

4. **Permanence**: it is permanent with respect to many factors including time, temperature or humidity.

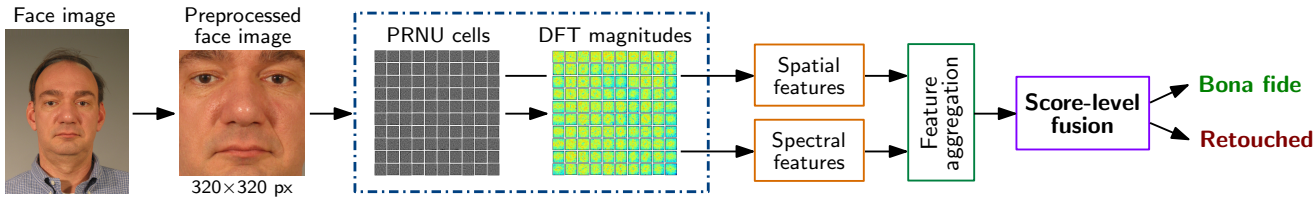


Figure 6: Overview of the proposed PRNU-based retouching detection system.

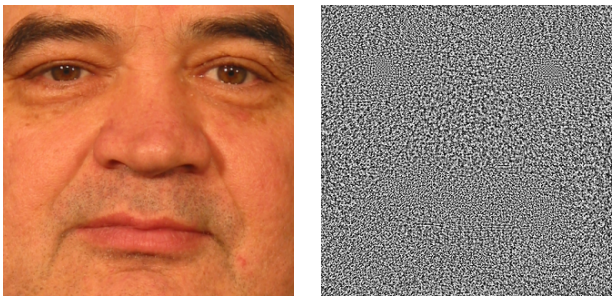
5. **Robustness**: the PRNU signal survives different types of image post-processing such as lossy image compression. Further, it was also reported to be extractable after high quality printing and scanning [75].

According to Fridrich [67], 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 retouching might induce significant alterations to a face image, e.g. smoothing, the distribution of the PRNU values is expected to change after these processing operations. Moreover, retouching produces inhomogeneous alterations across different image regions. Hence, an increased variance of the PRNU signal is expected across these regions if an image has been retouched, cf. Fig. 2. In previous works [23, 24, 25, 26], different statistics of spatial and spectral features extracted from the PRNU patterns of face images have been analysed for the task of morphing attack detection. The proposed detection system builds upon these works extending them by two major additions: on the one hand, a greater variety of spatial and spectral features is analysed in order to maximize the extracted information; on the other hand, to achieve high robustness and increased detection accuracy, a fusion of retouching detection scores obtained from each of the spatial and spectral features is performed.

The processing steps of the proposed retouching detection system are illustrated in Fig. 6. Specifically, the proposed system extracts the PRNU pattern from a preprocessed face image (Sect. 5.1), extracts a number of spatial and spectral features (Sect. 5.2), aggregates obtained feature values across image cells (Sect. 5.3) and performs a normalized score-level fusion (Sect. 5.4) of all detection scores.

5.1 Preprocessing and PRNU extraction

During preprocessing the facial region of a face image is extracted, normalized and then cropped to the facial area (320×320 or 640×640 pixels). Subsequently, the cropped image is converted to grayscale. Then, the PRNU signal is extracted and split into multiple equally sized image cells. In this work, divisions into 8×8, 10×10 and 16×16 cells



(a) Original image (b) Extracted PRNU

Figure 7: PRNU extraction for a pre-processed face image (320×320 pixels).

Table 4: Overview of extracted spatial and spectral features.

Feature type	Feature	Description
Spatial	P_{en}	Energy of PRNU values
	P_{ran}	Range of PRNU values
	P_{var}	Variance of PRNU values
	P_{var_H}	Variance of values in PRNU histogram
	P_{max_H}	Position of max. value in PRNU histogram
Spectral	D_{en}	Energy of DFT values
	D_{ran}	Range of DFT values
	D_{var}	Variance of DFT values
	D_{var_H}	Variance of values in DFT histogram
	D_{max_H}	Position of max. value in DFT histogram

are investigated. Generally, a larger number of cells retains local information and is expected to further expose variations in the PRNU signal. Finally, a total number of N equally sized cells $C_1, \ldots, C_N$ is obtained.

5.2 Feature extraction

At the time of feature extraction each image cell is processed individually. Two different types of features are analysed: spatial features based on the PRNU values and spectral features based on the PRNU's DFT magnitudes, representing the frequency domain of the PRNU. An

overview of extracted features is given in Table 4. Types of extracted features are partly inspired by previous works [23, 24, 25, 26]. In [26] it has been shown that these features exhibit high generalizability across cameras. Specifically, the usefulness of said types of features was confirmed on the Dresden database [76] containing images of 63 distinct digital cameras from 20 different camera models across many camera manufacturers. Further, in [26] it has been shown that these type of features are relatively stable across various camera types, i.e. adaptations are not expected to be required if images stem from different camera sources. All extracted features, which yield a simple scalar value for each PRNU cell, are described in more detail in the following.

5.2.1 Spatial Features

The spatial features aim at analysing the distribution of the PRNU values. As first spatial feature the energy of the PRNU values, P_{en}, is considered which is defined as,

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

where x is a value within all PRNU values V of a cell. Further, the range of PRNU values, P_{ran} is estimated as,

$$P_{ran} = \max_{x \in V}(x) - \min_{x \in V}(x) \tag{3}$$

Subsequently, the variance of PRNU values is determined as,

$$P_{var} = \frac{1}{|V|} \sum_{x=1}^{V} (V(x) - \bar{V})^2 \tag{4}$$

Additionally, the histogram of the PRNU values is estimated, which is constrained to a range of $[-5, 5]$ and divided into 100 bins. The variance of the histogram bin frequencies P_{var_H}, is calculated as,

$$P_{var_H} = \frac{1}{B} \sum_{n=1}^{B} (H(n) - \bar{H})^2 \tag{5}$$

where B is the amount of bins in the histogram H of a distinct PRNU cell. $\bar{H}$ represents the mean frequency of the histogram bins. Eventually, as last spatial feature the position of the peak in the histogram, P_{max_H}, is estimated as,

$$P_{max_H} = \arg\max_{n=1 \ldots B} H(n) \tag{6}$$

5.2.2 Spectral Features

For the spectral features the frequency spectrum of the PRNU is estimated in each cell by means of the discrete Fourier transform (DFT). Analogous to the spatial features the energy, D_{en}, the range, D_{ran}, and the variance, D_{var}, are estimated from the values of the DFT magnitude spectrum. Similarly, the DFT magnitude histograms which are constrained to the range of $[0, 8]$ and are calculated and divided into 100 bins. Again, The variance of the histogram bin frequencies, D_{var_H}, and the the position of the peak in the histogram, D_{max_H}, are determined.

5.3 Feature aggregation

In order to perform an analysis across all image cells, two measures of aggregation are considered. Firstly, the average feature value for all PRNU cells, S_{mean}, is estimated as,

$$S_{mean} = \bar{P} = \frac{1}{N} \sum_{n=1}^{N} P_n \tag{7}$$

where N is the number of total PRNU cells, P_n is the feature (scalar value) obtained for the PRNU cell C_n. Secondly, the variance, S_{var}, is given by,

$$S_{var} = Var(P) = \frac{1}{N} \sum_{n=1}^{N} (P_n - \bar{P})^2 \tag{8}$$

By analogy, the same aggregation methods are employed for spectral features. In both cases, a single scalar value S is obtained for each image.

Table 5: Number of images and average file sizes of the bona fide and
retouched face images.

Retouching	Images	Average size (in KB)	Image format
None (bona fide)	600	750	PNG
AirBrush	100	125	JPEG
FotoRus	200	580	JPEG
InstaBeauty	200	755	PNG
Polarr	100	140	JPEG
YouCam Perfect	200	110	JPEG

5.4 Score fusion

All possible combinations of feature extractors and cell aggregation methods result in in a total number of 20 score values. Hence, in the last processing step, the detection scores of all combinations are fused to obtain a single final score. For this purpose a score normalisation is performed using the z-score method. For this purpose means and standard deviations of detection scores of all combinations are

Table 6: Detection performance results for the proposed system (best performing system in terms of average D-EER is marked bold).

Cells	Retouching	**Cropped facial area** 320×320			**Cropped facial area** 640×640		
		D-EER (%)	**BPCER10 (%)**	**BPCER20 (%)**	**D-EER (%)**	**BPCER10 (%)**	**BPCER20 (%)**
8×8	AirBrush	14.0	16.66	24.5	22.0	38.83	42.33
	FotoRus	17.08	39.0	65.83	12.08	14.33	47.0
	InstaBeauty	2.5	0.33	1.66	3.0	0.83	1.0
	Polarr	13.16	25.0	38.0	30.0	57.49	67.0
	YouCam Perfect	24.0	72.5	88.33	27.08	59.16	83.16
	Average	*14.15*	*30.7*	*43.66*	*18.83*	*34.13*	*48.1*
10×10	AirBrush	15.0	19.16	21.66	20.41	32.83	41.5
	FotoRus	15.5	30.66	49.16	20.58	33.5	45.0
	InstaBeauty	1.0	0.0	0.5	3.16	0.66	1.0
	Polarr	13.0	15.83	25.83	30.0	55.5	64.0
	YouCam Perfect	24.0	73.5	93.0	30.0	69.0	85.0
	Average	***13.7***	***27.83***	***38.03***	*20.83*	*38.3*	*47.3*
16×16	AirBrush	11.0	11.0	23.33	19.0	28.33	34.5
	FotoRus	18.0	28.0	50.0	28.66	56.83	77.0
	InstaBeauty	0.5	0.0	0.0	1.5	0.33	0.5
	Polarr	20.0	41.5	59.5	28.99	61.83	69.83
	YouCam Perfect	24.5	75.5	91.5	28.0	67.33	79.66
	Average	*14.8*	*31.2*	*44.86*	*21.23*	*42.93*	*52.3*

obtained from a training set of bona fide images. That is, bona fide images exhibit average detection scores of zero and the absolute score denotes the normalized score. As previously mentioned, used types of features produce detection scores which have been found to be stable across numerous types of image sources [26]. Finally, the normalized scores are combined at score-level employing the sum-rule.

The proposed fusion targets two goals: on the one hand, a fusion of different feature extraction and feature aggregation methods is expected to lead to a more robust detection system; on the other hand, the proposed fusion is expected to maximize the information analyzed for the detection of facial retouching and hence is expected to yield increased detection accuracy. It is important to note that the proposed fusion has been neglected in the aforementioned previous works.

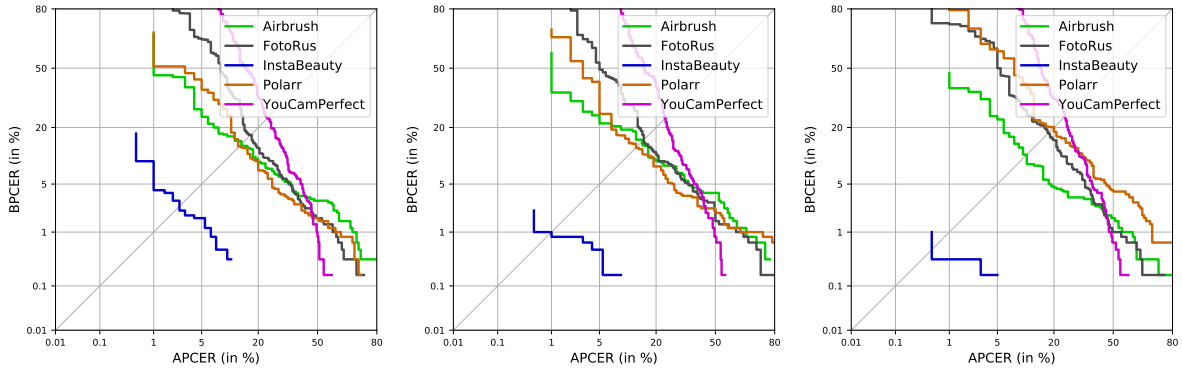
6 Detection Results

In the following subsections, the experimental setup (Sect. 6.1) and the detection performance evaluation (Sect. 6.2) are summarized in detail.

6.1 Experimental setup

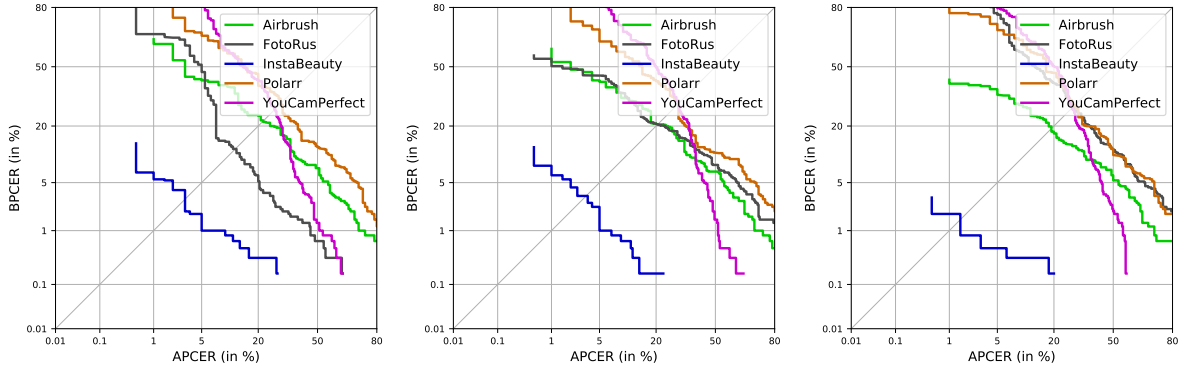
The proposed system is evaluated using the standardized metrics defined in ISO/IEC 30107-3 [77]. The Attack Presentation Classification Error Rate (APCER) is defined as the proportion of attack presentations using the same presentation attack instrument species incorrectly classified as bona fide presentations in a specific scenario [77]. 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 [77]. Further, the D-EER, which represents the operation point for which APCER = BPCER, is reported. In addition, the BPCER10 and BPCER20 are estimated, which are the operation points yielding an APCER of 10% and 5%, respectively.

Performance rates are estimated using all bona fide images including probe images which have been used before to investigate the impact of facial retouching on face recognition, see Sect. 4. Table 5 lists the number of images and average file sizes of bona fide and retouched face images. All algorithms preserve the resolution of the original face image. However, it can be observed that the majority of retouching algorithms applies JPEG compression as postprocessing. The most severe compression is applied in the YouCam Perfect algorithm, followed by AirBrush and Polarr.



(a) C =8×8 (b) C =10×10 (c) C =16×16

Figure 8: DET curves for different configurations of the proposed PRNU-based facial retouching detection system for a crop size of 320×320.



(a) C =8×8 (b) C =10×10 (c) C =16×16

Figure 9: DET curves for different configurations of the proposed PRNU-based facial retouching detection system for a crop size of 640×640.

Minor compression is employed in the FotoRus app while the InstaBeauty app does not apply any compression. In order to obtain a fair comparison of bonafide and retouched the bona fide face images are compressed with JPEG to exhibit corresponding target file sizes using the ImageMagick convert tool [78] before separately evaluating the detection performance for each retouching algorithm.

6.2 Performance evaluation

Table 6 lists obtained detection performance rates for different configurations of the proposed system. Corresponding DET curves are depicted in Fig. 8 and Fig. 9. The score-level fusion of all combinations of feature extraction and feature aggregation was found to outperform each single combination as well as score-level fusions of subsets of them in terms of average D-EER across all retouching algorithms. The average D-EER is estimated as the mean of all separately evaluated D-EERs per retouching algorithm.

Table 7: Comparison with other retouching detection algorithms in terms of D-EER (%).

Retouching	**Detection algorithm**		
	Noise Variance [27]	Wang et al. [6]	Proposed
AirBrush	44.0	28.0	15.0
FotoRus	50.0	22.0	15.5
InstaBeauty	38.0	26.0	1.0
Polarr	50.0	6.0	13.0
YouCam Perfect	48.0	12.0	24.0
Average	*46.0*	*18.8*	*13.7*

The best average D-EER of 13.7% is achieved for a cropped facial area of 320×320 pixels and a division of images into 10×10 cells which corresponds to a CCR of 86.3%. In general, superior detection performance is obtained for smaller cropped facial areas. It can be observed that the amount

of retouching as well as image compression highly influences the detection performance. In case of minor beautification, e.g. Airbrush, a detection of retouching generally becomes more difficult. In contrast, if stronger alterations are induced by the retouching method, e.g. InstaBeauty, high detection accuracy can be achieved. Detection performance is expected to further improve if severe alterations are caused by retouching. If strong compression is applied after retouching, e.g. YouCam Perfect, detection accuracy significantly drops since the PRNU signal is attenuated. It is important to note that for the best system configuration the average D-EER drops to 5.45% if bona fide images are not compressed to the estimated target file sizes yielded by the considered retouching algorithms. This is an important finding which was also partially observed by Jain et al. [5].

Table 7 compares the best configuration of the proposed system against two publicly available detection systems: a generic image forgery detection tool which aims at detecting inconsistencies in noise variances [27] and the recently proposed approach by Wang et al. [6]. Note that the latter approach is mainly designed to detect image warping operations. It can be observed that the proposed detection systems outperforms both other methods in terms of average D-EER. In summary, the proposed PRNU-based retouching detection approach could be used as a tool to enforce anti-photoshop legislations if to be analysed image data exhibits sufficient quality in terms of image compression.

7 Conclusion

In this work, the impact of moderate facial retouching on the recognition performance of state-of-the-art face recognition has been investigated. For this purpose a database has been manually created using five different beautification apps. It has been shown that facial retouching causes negligible drops in comparison scores which do not impact the overall accuracy if face images exhibit sufficient quality. This is of particular interest in scenarios where face recognition is employed in social media or at automated border control. Nevertheless, towards enforcing anti-photoshop legislations, a robust and reliable detection of retouched face image is required.

Further, a retouching detection system has been proposed which analyses different features extracted from the PRNU pattern across image regions and estimates detection scores using different aggregation methods. A multi-algorithm score-level fusion of numerous detection scores is utilized to obtain a final detection score. In contrast to many related works, the proposed retouching detection system does not require exhaustive training. In experimental evaluations, bona fide face images are compressed to exhibit target file sizes of used retouching algorithms yielding a realistic but challenging detection scenario which has commonly been ignored in previous works. The proposed system has been shown to reveal promising accuracy which is negatively affected by severe image compression. Further improvements with respect to detection performance might be obtained through a weighted score-level fusion or the use of machine learning techniques, e.g. support vector machines, instead of the proposed score-level fusion. Note that the latter extension of the system would require extensive classifier training. The presented system could also be applied to detect other types of face image manipulation, e.g. deep-fakes [79]. Eventually, the presented detection system might be circumvented by a manipulation of the PRNU pattern after retouching an image, as discussed in [26].

Acknowledgments

This research work has been partly funded by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE. This work was furthermore supported in part by the European Union's Horizon 2020 Research and Innovation Program under Grant 690907 (IDENTITY). The authors thank Cognitec Systems GmbH for providing a research license of Cognitec FaceVACS face recognition system SDK v9.3.

References

[1] C. Rathgeb, A. Dantcheva, and C. Busch, "Impact and detection of facial beautification in face recognition: An overview," *IEEE Access*, vol. 7, 2019.

[2] M. Ferrara, A. Franco, D. Maltoni, and Y. Sun, "On the impact of alterations on face photo recognition accuracy," in *Image Analysis and Processing – ICIAP 2013*. Springer Berlin Heidelberg, 2013, pp. 743–751.

[3] A. Bharati, R. Singh, M. Vatsa, and K. W. Bowyer, "Detecting facial retouching using supervised deep learning," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1903–1913, 2016.

[4] A. Bharati, M. Vatsa, R. Singh, K. W. Bowyer, and X. Tong, "Demography-based facial retouching detection using subclass supervised sparse autoencoder," in *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 2017, pp. 474–482.

[5] A. Jain, R. Singh, and M. Vatsa, "On detecting gans and retouching based synthetic alterations," in *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, 2018, pp. 1–7.

[6] S. Wang, O. Wang, A. Owens, R. Zhang, and A. A. Efros, "Detecting photoshopped faces by scripting photoshop," in *International Conference on Computer Vision (ICCV)*, 2019.

[7] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition," *ACM Computing Surveys*, vol. 35, no. 4, pp. 399–458, dec 2003.

[8] A. F. Abate, M. Nappi, D. Riccio, and G. Sabatino, "2D and 3D face recognition: A survey," *Pattern Recognition Letters*, vol. 28, no. 14, pp. 1885 – 1906, 2007.

[9] S. Z. Li and A. K. Jain, Eds., *Handbook of Face Recognition*. Springer London, 2011.

[10] 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.

[11] 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.

[12] R. Ranjan, S. Sankaranarayanan, A. Bansal, N. Bodla, J. Chen, V. M. Patel, C. D. Castillo, and R. Chellappa, "Deep learning for understanding faces: Machines may be just as good, or better, than humans," *IEEE Signal Processing Magazine*, vol. 35, no. 1, pp. 66–83, 2018.

[13] M. Kawulok, M. E. Celebi, and B. Smolka, *Advances in Face Detection and Facial Image Analysis*, 1st ed. Springer, 2016.

[14] S. Pouyanfar, S. Sadiq, Y. Yan, H. Tian, Y. Tao, M. P. Reyes, M.-L. Shyu, S.-C. Chen, and S. S. Iyengar, "A survey on deep learning: Algorithms, techniques, and applications," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 92:1–92:36, Sep. 2018.

[15] W. Funk, M. Arnold, C. Busch, and A. Munde, "Evaluation of image compression algorithms for fingerprint and face recognition systems," in *Proc. Sixth Annual IEEE SMC Information Assurance Workshop*, 2005, pp. 72–78.

[16] R. Singh, M. Vatsa, H. S. Bhatt, S. Bharadwaj, A. Noore, and S. S. Nooreyezdan, "Plastic surgery: A new dimension to face recognition," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 441–448, 2010.

[17] A. Dantcheva, C. Chen, and A. Ross, "Can facial cosmetics affect the matching accuracy of face recognition systems?" in *Int'l Conf. on Biometrics: Theory, Applications and Systems (BTAS'12)*, 2012, pp. 391–398.

[18] U. Scherhag, C. Rathgeb, J. Merkle, R. Breithaupt, and C. Busch, "Face recognition systems under morphing attacks: A survey," *IEEE Access*, vol. 7, pp. 23 012–23 026, 2019.

[19] J. Szewczyk, "Photoshop law: Legislating beauty in the media and fashion industry," *SSRN Electronic Journal*, 01 2014.

[20] N. Eggert. BBC News: Is she Photoshopped? In France, they now have to tell you. https://www.bbc.com/news/world-europe-41443027. 30th September, 2017.

[21] 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.

[22] Cognitec: the face recognition company, "FaceVACS Engine 9.3," http://www.cognitec.com/technology.html, 2018.

[23] 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.

[24] 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.

[25] 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.

[26] U. Scherhag, L. Debiasi, C. Rathgeb, C. Busch, and A. Uhl, "Detection of face morphing attacks based on prnu analysis," *IEEE Transactions on Biometrics, Behavior, and Identity Science (TBIOM)*, 2019, accepted.

[27] A. Levandoski and J. Lobo. Image forgery detection: Developing a holistic detection tool. https://github.com/andrewlevandoski/Image-Forgery-Detection. Accessed Feb. 2020.

[28] Adobe Systems, Inc. Adobe Lightroom CC.

[29] Meitu Technology, Inc. AirBrush: Easy Photo Editor for the best moments. http://www.appairbrush.com/en/. Meitu Technology, Inc. Accessed Jun. 2019.

[30] SNOW Inc. B612 - Beauty & Filter Camera. https://play.google.com/store/apps/details?id=com.linecorp.b612.android. SNOW Inc. Accessed Jun. 2019.

[31] InShot Inc. Beauty Camera - Selfie Camera. https://play.google.com/store/apps/details?id=com.northpark.beautycamera. InShot Inc. Accessed Jun. 2019.

[32] Meitu Technology Inc. BeautyPlus - Easy Photo Editor & Selfie Camera. http://global.meitu.com/. Meitu Technology, Inc. Accessed Jun. 2019.

[33] A. Kobozev. Camly photo editor & collages. http://camlyapp.com/. Camly. Accessed Jun. 2019.

[34] PinGuo Inc. Camera360. http://www.camera360.com/. PinGuo Inc. Accessed Jun. 2019.

[35] JP Brothers Inc. Candy Camera. https://www.jpbrothers.com/. JP Brothers Inc. Accessed Jun. 2019.

[36] SK Communications. Cymera Camera - Collage, Selfie Camera, Pic Editor. www.cymera.com. SK Communications. Accessed Jun. 2019.

[37] FaceApp Inc. Face-App. www.faceapp.com/app. FaceApp Inc. Accessed Jun. 2019.

[38] Onix Business Llp. Facelab - Face & Body Editor. https://facelab.mobi/. Onix Business Llp. Accessed Jun. 2019.

[39] Lightricks Ltd. facetune2 - Wow your friends with every selfie. http://www.facetuneapp.com/. Lightricks Ltd. Accessed Jun. 2019.

[40] Alpha Mobile Limited. Facey: Face Editor & Makeup Cam. https://itunes.apple.com/us/app/facey-face-editor-makeup-cam/id1387741890. Alpha Mobile Limited. Accessed Jun. 2019.

[41] Fotoable, Inc. FotoRus - Camera & Photo Editor. https://play.google.com/store/apps/details?id=com.wantu.activity&hl=en. Fotoable, Inc. Accessed Jun. 2019.

[42] Chengdu Everimaging Science and Technology Co. Ltd. Fotor Photo Editor - Photo Collage & Photo Effects. https://www.fotor.com/. Chengdu Everimaging Science and Technology Co., Ltd. Accessed Jun. 2019.

[43] H. Parikh. HD Photo Editor. https://itunes.apple.com/app/hd-photo-editor/id1019624855. Accessed Jun. 2019.

[44] Cidade. InstaBeauty Selfies. https://www.microsoft.com/de-de/p/instabeauty-selfies/9nblggh6jk60. Cidade. Accessed Jun. 2019.

[45] Fotoable Inc. InstaBeauty -Makeup Selfie Cam. https://play.google.com/store/apps/details?id=com.fotoable.fotobeauty. Fotoable, Inc. Accessed Jun. 2019.

[46] J. Zhou. Photo Editor.

[47] Alpha Mobile Limited. Manly - Body Muscle Editor Pro. https://itunes.apple.com/app/manly-muskel-fotobearbeitung/id1263326810. Alpha Mobile (Hong Kong) Limited. Accessed Jun. 2019.

[48] JellyBus Inc. MOLDIV - Photo Editor, Collage. http://www.jellybus.com/moldiv. JellyBus Inc. Accessed Jun. 2019.

[49] InShot Inc. Photo Editor Pro. https://play.google.com/store/apps/details?id=photo.editor.photoeditor.photoeditorpro. InShot Inc. Accessed Jun. 2019.

[50] Axiem Systems. Photo Editor. http://axiemsystems.com/editor/. Axiem Systems. Accessed Jun. 2019.

[51] VicMan LLC. Photo Lab Picture Editor FX: filters & art montage. https://pho.to/de/#visage-lab. VicMan LLC. Accessed Jun. 2019.

[52] PicsArt, Inc. PicsArt Photo Studio & Collage. https://picsart.com/apps/picsart-photo-studio/. PicsArt, Inc. Accessed Jun. 2019.

[53] Polarr Inc. Photo Editor. https://www.polarr.co. Polarr Inc. Accessed Jun. 2019.

[54] AIAR Labs Inc. Prequel: Video & Photo Editor. https://itunes.apple.com/us/app/prequel-story-photo-editor/id1325756279. AIAR Labs Inc. Accessed Jun. 2019.

[55] Editr Apps Inc. Selfie Editor: face cam filter. http://www.tapstarapps.com/. Editr Apps Inc. Accessed Jun. 2019.

[56] SNOW Inc. SNOW - Beauty & makeup camera. https://snow.me/. SNOW Inc. Accessed Jun. 2019.

[57] A. Cushway. Square Fit Photo Video Editor. https://itunes.apple.com/us/app/square-fit-photo-video-editor/id692998669. Alan Cushway. Accessed Jun. 2019.

[58] Perfect Corp. YouCam Perfect - Foto Editor & Selfie Camera App. https://www.perfectcorp.com/app/ycp. Perfect Corp. Accessed Jun. 2019.

[59] GOMO, "Z Camera - Photo Editor, Beauty Selfie, Collage," https://play.google.com/store/apps/details?id=com.jb.zcamera, accessed Jun. 2019.

[60] ISO/IEC TC JTC1 SC37 Biometrics, *ISO/IEC 19795-1:2006. Information Technology – Biometric Performance Testing and Reporting – Part 1: Principles and Framework*, International Organization for Standardization and International Electrotechnical Committee, 2006.

[61] 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.

[62] E. Kee and H. Farid, "A perceptual metric for photo retouching," *Proceedings of the National Academy of Sciences*, vol. 108, no. 50, pp. 19 907–19 912, 2011.

[63] E. Kee, J. F. O'Brien, and H. Farid, "Exposing photo manipulation from shading and shadows," *ACM Transactions on Graphics*, vol. 33, no. 5, pp. 165:1–165:21, 2014, presented at SIGGRAPH 2014.

[64] 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.

[65] Frontex, "Best Practice Technical Guidelines for Automated Border Control (ABC) Systems," 2016.

[66] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2019.

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

[68] 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.

[69] 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.

[70] 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.

[71] 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.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

[76] 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.

[77] 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.

[78] ImageMagick. ImageMagick - Convert, Edit, or Compose Bitmap Images. https://imagemagick.org/. ImageMagick Studio LLC. Accessed Jun. 2019.

[79] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: A survey of face manipulation and fake detection," 2020.