



ORIGINAL RESEARCH PAPER

Face morphing detection in the presence of printing/scanning and heterogeneous image sources

Matteo Ferrara  | Annalisa Franco  | Davide MaltoniDepartment of Computer Science and Engineering,
University of Bologna, Cesena, Italy**Correspondence**Matteo Ferrara, Department of Computer Science
and Engineering, University of Bologna, Cesena,
Italy.Email: matteo.ferrara@unibo.it**Abstract**

Nowadays, face morphing represents a big security threat in the context of electronic identity documents as well as an interesting challenge for researchers in the field of face recognition. Despite the good performance obtained by state-of-the-art approaches on digital images, no satisfactory solutions have been identified so far to deal with cross-database testing and printed-scanned images (typically used in many countries for document issuing). To solve this problem, the authors propose new approaches to train Deep Neural Networks for morphing attack detection: in particular the generation of simulated printed-scanned images together with other data augmentation strategies and pre-training on large face recognition datasets, allowed reaching state-of-the-art accuracy on challenging datasets from heterogeneous image sources.

1 | INTRODUCTION

The widespread adoption of biometric identification techniques in the context of identity documents poses some concerns for the possibility of fraudulent misuses. Recent studies [1–4] revealed that ePassports are particularly sensitive to the so called morphing attack, in which the face photo printed on paper and provided by the citizen can be altered. Such attack was first described in [2] in the context of face verification at automated border control (ABC) gates where two subjects cooperate to produce a morphed face image (mixing their identities) in order to obtain a regular travel document that could be exploited by both subjects. Of course, in order to succeed in the attack, the morphed face image must be very similar to one of the two subjects (the one applying for the document) to fool the officer during the issuing process, but at the same time must contain enough features of the hidden subject to enable positive verification at the gate for both individuals.

The feasibility of this attack has been analysed and confirmed by several researchers and some police agencies, thus making the development of proper countermeasures very urgent.

One of the main challenges for the development of effective solutions for morphing attack detection is that typically the id photo, natively digital, is printed by the photographer and then scanned by the officer to be stored into the document chip. This printing/scanning (P&S) process alters

the image information, removing most of the fine details (i.e., digital processing artefacts) that could help to detect morphing. Some preliminary studies, more widely discussed in the next section, show that morphing detection from digital images can be addressed to some extent, but P&S images are still difficult to manage [5]. Promising solutions have been recently obtained by using Deep Neural Networks (DNN), which proved to effectively detect and recognise faces in uncontrolled scenarios [6]. However, to reach a good accuracy, DNN typically require a large training dataset. Unfortunately, in the context of morphing attack detection, it is difficult to collect large databases of samples: manually producing high quality morphed images is in general a boring and time-consuming activity. Moreover, due to the need of detecting morphing from P&S images, the costs/efforts for printing the images and scanning them again must be also considered. For this reason, most of the approaches in the literature exploit pre-trained deep networks as feature extractors and build on the top of them traditional classifiers (e.g., Support-Vector Machine (SVM)) that can be trained with relatively small datasets. The aim of this study is to investigate the possibility of artificially generating large sets of morphed images to train DNNs. In particular, the authors focus on the simulation of the P&S process which, coupled with the automatic generation of morphs, can produce large datasets for (i) training new networks from scratch or (ii) fine-tuning pre-trained DNNs such as AlexNet [7]

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.

© 2021 The Authors. *IET Biometrics* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

or VGG [8]. Moreover, an extensive analysis of the network behaviour with respect to bona fide/morphed and digital/printed-scanned images enables a deeper understanding of the most relevant image features exploited for classification.

The rest of the paper is organised as follows: Section 2 discusses the state of the art; in Sections 3 and 4, the procedure for automatic printed/scanned image generation and the databases used for train and test are described, respectively. The DNNs used for the experiments are briefly introduced in Section 5 and the experimental results are reported and commented in Section 6. Finally, Section 7 draws some conclusions and discusses possible future research directions.

2 | RELATED WORKS AND CONTRIBUTION

Although face morphing detection is a recently emerged research area, an increasing number of researchers are working on this topic and the related literature is constantly growing [9–11]. Existing techniques can be mainly framed under two categories:

- *Single-image based*, where the presence of morphing alterations is detected on a single image, such as the id photo presented to the officer at enrolment time or the face image read from an e-document during verification at the gate; *image-pair based* (a.k.a. *differential morphing attack detection*), where the comparison between a live image (e.g., acquired at the gate) and that stored on the e-document is exploited for morphing attack detection.

Several literature approaches belong to the first category. The works based on handcrafted features mainly try to analyse the small image degradations produced by the morphing process. In [12], the authors propose a technique for morphing attack detection based on the analysis of micro-texture variations using Binarized Statistical Image Features (BSIF): an SVM classifier is trained to discriminate bona fide/morphed faces. The authors of [13] argue that the morphed images are characterised by a different texture with respect to the unaltered ones and that a progressive JPG compression can further highlight this aspect; the image content is finally represented by different corner features exploited for classification. In [14–16], morphing detection is based on Benford features extracted from quantized DCT coefficients and in [17] key-points features (such as SURF, ORB, FAST, etc.) are used, while in [18–21] texture features such as LBP or BSIF are analysed. An interesting outcome of [18] is that low-level features are not robust when used in cross-database testing or in the presence of simple image manipulations (e.g., rescaling). The authors of [22–24] exploit the principle of image source identification for morphing attack detection, observing that a morphing is a computer-generated image and its sensor-pattern noise is different from that of a real image. Other works make use of topological analysis of facial landmarks to detect alterations introduced by morphing [25, 26]; the idea is interesting in

principle, but overall the results obtained are unsatisfactory for real application. Most of the referred approaches, when tested on digital images only, provide good classification performance, but the use of different databases and different evaluation metrics make a comparison more difficult.

Deep learning techniques based on convolutional neural network (CNN) have been proposed for face morphing detection [19, 27–29]. The authors of [19] evaluate some networks, pre-trained for face recognition, as feature extractor for digital images, without performing any fine-tuning on the specific morphing detection task, while in [27] two pre-trained networks, AlexNet [7] and VGG19 [8], are used for feature extraction after a fine-tuning step. The authors perform tests on both digital and P&S images and the experimental results clearly confirm that the second type of images provide the main challenge for morphing detection. In [28], some CNNs are used for morphing attack detection from digital images; the accuracy of pre-trained networks is compared to that of networks learned from scratch, finally leading to the conclusion that pre-trained networks are more robust for this task. The authors of [29] analyse the accuracy of pre-trained networks against semantic (partial morphing on some specific face regions) and black box attacks (partial occlusions), and highlight, for the two kind of images, the most relevant regions analysed by the networks for classification. Finally the authors of [30] combine features of different nature, hand-crafted and extracted by CNNs, demonstrating that a substantial improvement in detection performance can be achieved by their integration.

A limited number of approaches perform morphing detection by image-pair comparison. The first approach has been introduced in [31, 32] where the inverse process of morphing (called demorphing) is adopted to revert the effects produced by morphing. The demorphing technique proved to be effective both on digital and P&S images. The same detection scheme has been considered in [33] where different features are evaluated both for single-image and differential morphing detection. Deep features extracted from different networks are used in [34] for image comparison, while the authors of [35] exploit features from 3D shape and the diffuse reflectance component estimated from the image. Finally, a landmark-based morphing detection approach is proposed in [36] to compare bona fide and suspected morphed images.

Overall, an analysis of the literature allows identifying two major challenges for morphing detection techniques: (i) robustness to the P&S process and (ii) ability to generalise across different databases [37]. The work of authors mainly focuses on these two aspects. In particular, this paper provides the following contributions:

- Adoption of a simple P&S simulation model [38] for data augmentation, enabling the possibility of producing training images without the cost/effort of the real P&S process. The state-of-the-art about simulating the P&S process in the context of face recognition is very limited. We think that the most relevant paper [39] has been proposed very recently to the best of our knowledge. The approach exploits generative

networks to simulate the real process, providing interesting results from the visual point of view. This technique requires a training stage based on real P&S images; on the contrary, an advantage of the model used in our work is that no real P&S images are needed for training and a variety of devices or acquisition conditions can easily be simulated just varying the main algorithm parameters. The experimental results will show that such simulation produces a significant performance improvement on morphing detection from P&S images.

- Extensive experiments using four different well-known DNN architectures on several test datasets and public benchmarks.
- Thorough performance evaluation on several public benchmarks and comparison with state-of-the-art techniques.
- Experimental results confirming the feasibility of the print/scan simulation model proposed here to deal with real P&S images.

3 | AUTOMATIC IMAGE GENERATION

In order to exploit the great potential of CNNs for classification, a very large set of images is typically needed and data augmentation techniques are applied usually [40] to increase the number of samples available for training; geometric and photometric transformations are the most frequently adopted modifications. In the context of morphing attack detection, the network training requires both real and morphed image samples, possibly in the two formats (digital and P&S). So, we proposed new techniques for automatically generating high quality morphed face images (Section 3.1) and simulating the P&S process (Section 3.2), which would avoid the effort/cost of collecting a large dataset.

3.1 | Face morphing

Morphed images can be obtained quite easily using one of the many existing tools and plugins (e.g., Squirrelz Morph [41]). However, the systematic generation of morphed images with specific characteristics can be better realised by ad hoc techniques. Here we adopt the approach described in [31] which includes an automatic image retouching phase to minimise visible artefacts. Given two images I_0 and I_1 , the process generates a set of frames $\mathbb{M} = \{I_\alpha, \alpha \in \mathbb{R}, 0 < \alpha < 1\}$ representing the transformation of the first image (I_0) into the second one (I_1) (see Figure 1). In general, each frame is a weighted linear combination of I_0 and I_1 , obtained by geometric warping of the two images based on corresponding landmarks and pixel-by-pixel blending.

$$I_\alpha(\mathbf{p}) = (1 - \alpha) \cdot I_0(w_{p_a \rightarrow p_0}(\mathbf{p})) + \alpha \cdot I_1(w_{p_a \rightarrow p_1}(\mathbf{p})) \quad (1)$$

where

- \mathbf{p} is a generic pixel position;
- α is the frame weight factor (representing the presence of the two contributing subjects);
- P_0 and P_1 are the two sets of landmarks in I_0 and I_1 , respectively;
- P_α is the set of landmarks aligned according to the frame weight factor α ; and
- $w_{B \rightarrow A}(\mathbf{p})$ is a warping function.

A number of different morphed images can be obtained according to the value of the weighting factor α (i.e., the weight of the two subjects in the combination) as shown in Figure 1.

3.2 | Modelling the printing and scanning process

The P&S process is quite complex: digital images are first conveyed to the physical, continuous domain and then reported in a digital format and discretized by the scanning process. The image alterations introduced involve both pixel value distortions (i.e., luminance, contrast and gamma corrections, chrominance variations, and blurring of adjacent pixels) as well as minor geometric alterations due to the positioning on the scanner surface.

Focusing on the pixel value distortion, according to the model proposed in [38] the P&S process of a generic digital image I produces a modified, discrete version of the image \tilde{I} as:

$$\tilde{I}(\mathbf{p}) = K[I(\mathbf{p}) * \tau_1(\mathbf{p}) + (x(\mathbf{p}) * \tau_2(\mathbf{p})) \cdot N_1] \cdot s(\mathbf{p}) \quad (2)$$

where

- Function K represents the responsivity of the acquisition device;
- $s(\mathbf{p})$ is the sampling function which characterises the digitalisation process of the continuous printed image;
- τ_1 models the system point spread function $\tau_1(\mathbf{p}) = \tau_P(\mathbf{p}) * \tau_S(\mathbf{p})$ where $\tau_P(\mathbf{p})$ and $\tau_S(\mathbf{p})$ represent the point spread function of printer and scanner, respectively;
- τ_2 is a high-pass filter used to represent higher noise variance near the edges; and
- N_1 is a white Gaussian random noise.

The following responsivity function K is adopted:

$$K(x) = \omega \cdot (x - \beta_x)^\gamma + \beta_K + N_2(x) \quad (3)$$

The equation includes colour adjustments coefficients (β_x and β_K), gamma correction (γ) and a noise component $N_2(x)$ whose power is related to pixel intensity (usually higher noise

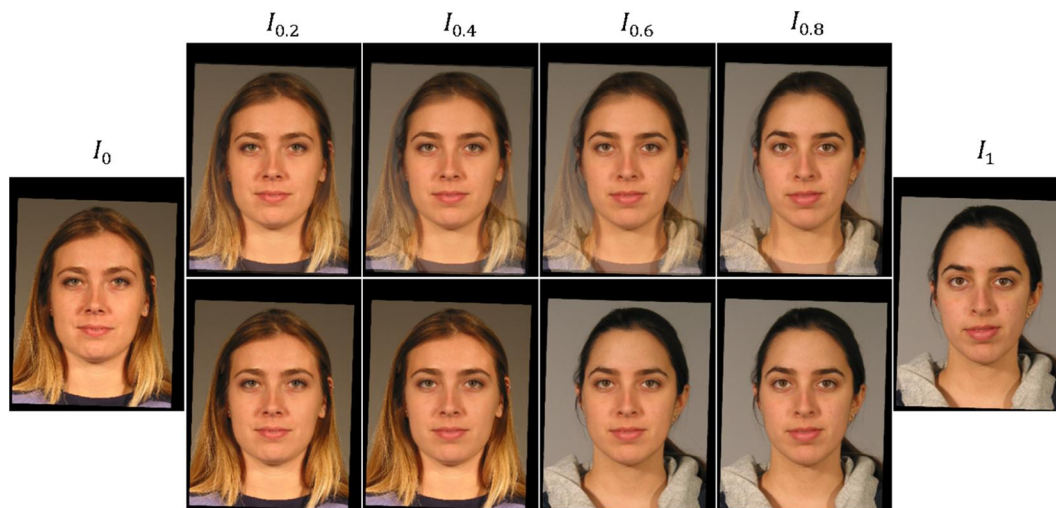


FIGURE 1 Example of morphed frames obtained by the morphing procedure, gradually moving from I_0 to I_1 (first row). In the second row the result of the automatic retouching process used to remove visible artefacts is shown

FIGURE 2 Variation of ω parameter in the P&S simulation model applied to Figure 6a: this parameter mainly affects image contrast and brightness

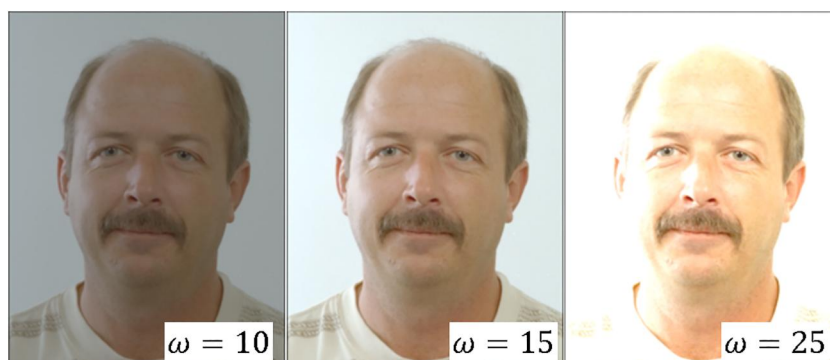
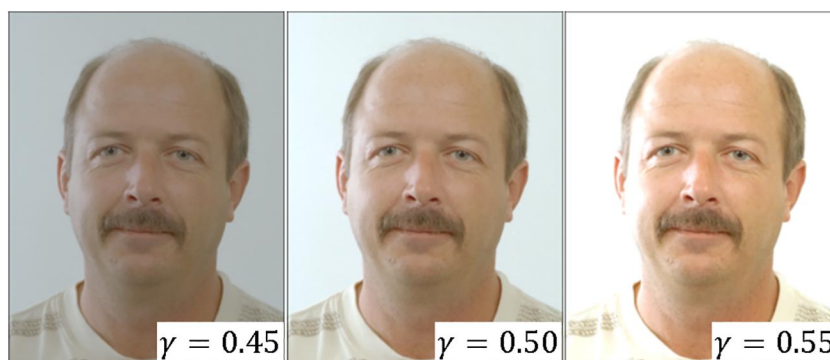


FIGURE 3 Variation of γ in the P&S simulation model applied to Figure 6a: this parameter regulates the gamma corrections produced by the printing and scanning devices



on dark pixels is observed due to the different sensors' sensitivity to the image reflectivity).

Due to some device-dependent unknown parameters, the adaption of this model to real cases is not straightforward. In particular, the point spread functions of the devices (τ_P and τ_S in Equation (2)) are not available, and they are approximated by two Gaussian blurring filters of size k_1 , k_2 and standard deviation σ_1 , σ_2 .

The model is quite flexible and allows modifying different image characteristics, related to both visual quality and low-

level signal content. Figures 2–5 show the impact of the different model parameters on the result. In particular, ω mainly controls the image contrast and brightness. Formally (see Figure 2), while the overall system gamma, that is, the combined effect of all gamma values applied to the imaged by the P and S devices can be adjusted by properly tuning γ (see Figure 3).

Further variations to image colour and saturation can be obtained through β_K and β_X parameters (see Figure 4). Finally the parameters of the Gaussian smoothing filter (k and σ) produce

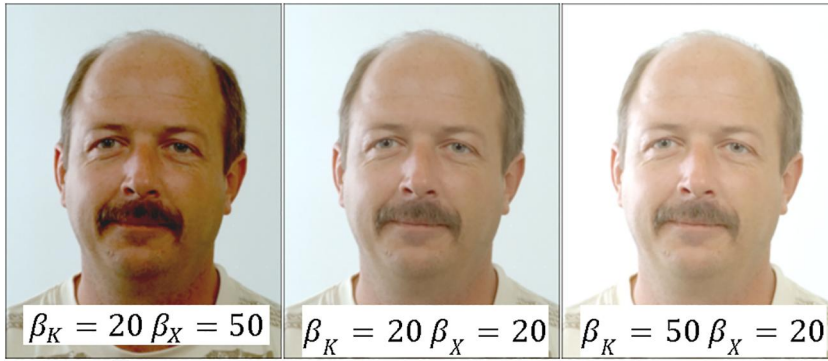


FIGURE 4 Variation of β_K and β_X in the P&S simulation model applied to Figure 6a: these parameters control the image colour and saturation

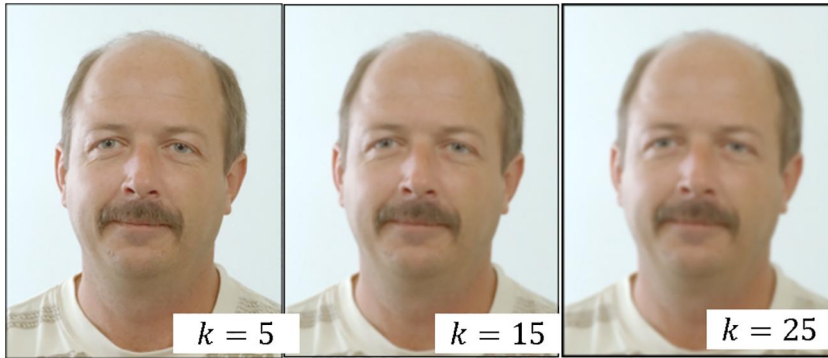


FIGURE 5 Variation of k in the P&S simulation model applied to Figure 6a: this parameter controls the amount of image blurring

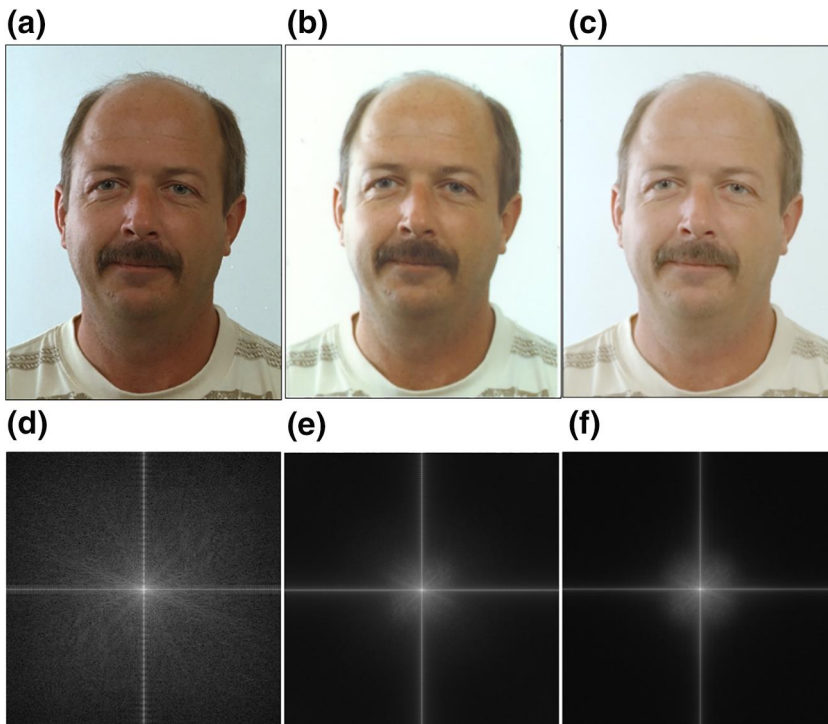


FIGURE 6 For the digital image (a), the result of the real (b) and simulated (c) P&S processes is provided. The corresponding image spectrum is also given for the digital image (d), the real (e) and the simulated P&S (f)

the most evident modification introduced by the P&S process, that is, the blurring effect represented in Figure 5.

In Figure 6, a real P&S image is compared with a simulated P&S image of the same digital image. The image spectrum is also reported to appreciate the low-level signal modifications

produced by the P&S process. As clearly visible in the example, the digital image is much richer with fine details (high frequencies), which are noticeably attenuated after P&S. The spectrum of the simulated P&S image (Figure 6f) is quite similar to that of the real one (Figure 6e). We can quantify the

similarity between the image spectra adopting commonly used metrics such as the spectral angle [42] (a measure of distance between two spectra) or the correlation value. If we compare the digital image and the real P&S of Figure 6, the spectral angle is quite high (0.69) with a correlation value of 0.77. The similarity between the real P&S and the simulated one is much higher, as confirmed by the smaller spectral angle (0.38) and a higher correlation value (0.93).

The parameters used for image generation (see Table 1) have been chosen in order to produce images visually similar to the real P&S ones (*MorphDB_{PES}* database described in Section 4.2), but no specific optimisations have been carried out (see Figure 6).

4 | DATABASES

4.1 | Training sets

The Progressive Morphing Database (PMDB) described in [31] is used for network training. It contains 6000 morphed images automatically generated starting from 280 different

subjects selected from the AR [43], FRGC [44] and Color Feret [45, 46] databases using different morphing factors ($\alpha \in \{0.1, 0.15, 0.2, 0.25, 0.3, 0.35, 0.4, 0.45\}$ in Equation (1)).

Since PMDB contains a different number of bona fide and morphed images, a new balanced database (called *Digital*) has been derived as follows:

1. two images of each subject are chosen resulting in 560 bona fide images;
2. 560 morphed images are randomly selected from the PMDB morphed images.

The P&S process has been simulated by applying the procedure described in Section 3.2 on all *Digital* images; we will refer to this dataset as *P&S*.

4.2 | Test sets

The models trained on the datasets introduced in Section 4.1 are then tested on the following databases:

- *MorphDB_D* [31]: it consists of 130 bona fide images (not morphed) and 100 morphed images (50 males and 50 females) produced with a significant manual intervention in order to minimise visible artefacts (see Figure 7).

TABLE 1 Parameter values used in for P&S simulation

Parameter	ω	β_X	β_K	γ	k_1, k_2	σ_1, σ_2
Value	15.5	20	20	0.5	3	1.2

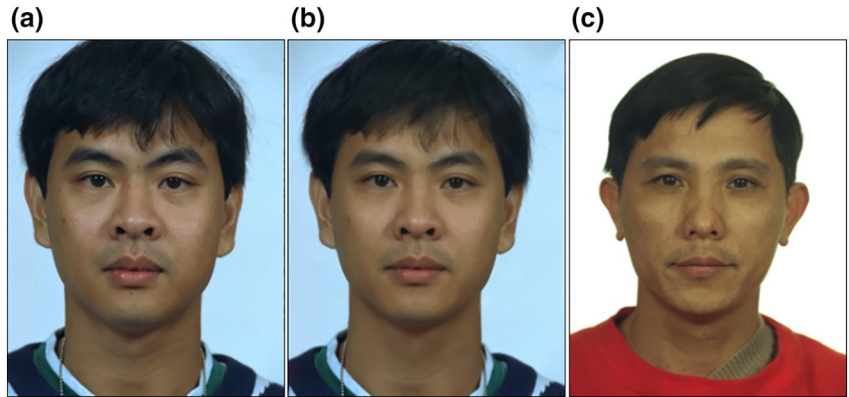


FIGURE 7 Images from *MorphDB_D* database: digital version of bona fide images of two subjects (a) and (c) and the resulting morphed image (b)



FIGURE 8 Images from *MorphDB_{PES}* database: P&S version of the images reported in Figure 7



FIGURE 9 Normalised images from Figures 7 (first row) and 8 (second row)

TABLE 2 Characteristics of the different training datasets

Name	P&S simulation	Data augmentation				# Images		
		Horizontal mirroring	Rotation	Horizontal and vertical translation	Multi-crop	Bona fide	Morphed	Total
<i>Digital</i>						560	560	1120
$\widetilde{P \& S}$	✓							
<i>Digital_{Au}</i>		✓	✓	✓		30,240	30,240	60,480
$\widetilde{P \& S_{Au}}$	✓	✓	✓	✓				
<i>Digital_{Mc}</i>		✓	✓		✓	16,800	16,800	33,600
$\widetilde{P \& S_{Mc}}$	✓	✓	✓		✓			

- *MorphDB_{P&S}* [31]: P&S version of *MorphDB_D*. The images have been printed on high quality photographic paper by a professional photographer and then scanned (see Figure 8).
- NIST FRVT-MORPH benchmark [47], including several image subsets of variable quality. The morphed images in this dataset have been generated with a plurality of morphing algorithms, thus representing a very hard challenge.
- SOTAMD benchmark [10], including high quality morphed images (both digital and printed/scanned).

The *MorphDB_D*, *MorphDB_{P&S}* and SOTAMD datasets are publicly available for testing in the FVC-onGoing platform [48, 49], a web-based automated evaluation system for biometric recognition algorithms.

4.3 | Data normalisation

Since face images come from various sources presenting different size and resolution, it is important to normalise them

(see Figure 9) before they are passed to the network for morphing attack detection. For this reason, each image is normalized as follows:

1. the eye centres and the nose tip are detected using Neurotechnology VeriLook SDK 10.0 [50];
2. the image is resized to obtain an eye centre distance of 150 pixels;
3. a sub-image of size 350×400 pixels is cropped centred on the nose tip.

4.4 | Data augmentation

Both training databases (*Digital* and $\widetilde{P \& S}$) contain 1120 images, not many for an effective network training. To increase the number of samples, data augmentation is applied obtaining different augmented databases (see Table 2). In particular, the following transformations are applied:

TABLE 3 Neural networks used in the experimentation

Name	Architecture	Pre-trained on			
		Image Type	Database name	Database size	Input image size
AlexNet [7] [52]	AlexNet-BVLC version	Natural	ImageNet [51], specific ILSVRC subsets [53]	1.2M	227×227
VGG19 [8]	VGG – 19 weight layers				224×224
VGG-Face16 [54]	VGG – 16 weight layers [8]	Face	VGG-Face dataset [54]	2.6M	224×224
VGG-Face2 [55]	ResNet-50 [56]		VGG-Face 2 dataset [55]	More than 3M	

- horizontal mirroring;
- rotation centred on the nose tip ($\{-5^\circ, 0^\circ, +5^\circ\}$);
- horizontal and vertical translation ($\{-1, 0, +1\}$);
- multi-crop, that is, extracting from each image (size 350×400) five sub-images corresponding to the four corners and the central region [7]. The crop size is fixed according to the image input size of the specific network (see Section 5). In the tests where multi-crop is not enabled, only the central region is used.

5 | DEEP NEURAL NETWORKS FOR MORPHING DETECTION

The authors considered different well-known pre-trained DNNs (see Table 3). The first two networks, already used for morphing attack detection in previous works [27, 28], have been trained on natural images (i.e., ImageNet [51]) and therefore the learned filters are not specific for face representation. The last two networks are state-of-the-art models trained on very large face datasets: we can expect that the filters in the low and intermediate levels of these networks are capable of extracting very powerful face features that can be exploited for morphing detection.

The last layer of all the considered architectures has been changed to deal with a two class problem (morphed vs. bona fide): as a consequence, the corresponding weights need to be learned from scratch.

5.1 | Fine-tuning

Starting from the pre-trained networks, a first fine-tuning step has been performed on *Digital_{Au}* and *Digital_{Mc}* datasets, separately, for 5 epochs each. Therefore, for each network architecture, two differently tuned networks are obtained that will be able to detect digital morphed images but presenting poor results on P & S ones (see Section 6.2). To overcome this limit, a second fine-tuning step has been performed on *PE_{S_{Au}}* and *PE_{S_{Mc}}* datasets, for a single epoch each. For both fine-tuning stages, SGD optimisation is used with a fixed learning rate of 0.0001 and a momentum of 0.9.

At test time, if multi-crop augmentation were used during training, the prediction probabilities are calculated as the average

probabilities across five sub-images (i.e., the four corners and the central region) cropped from the normalised 350×400 image. Otherwise only the central region is used for classification.

6 | EXPERIMENTS

Several experiments have been carried out to evaluate the robustness of DNNs for morphing attack detection with respect to: (i) cross-database testing and (ii) P&S images.

6.1 | Testing protocol and performance indicators

For each experiment bona fide and morphed face images are used to compute Bona fide Classification Error Rates (BPCER) and Attack Presentation Classification Error Rate (APCER), as defined in [57].

The following performance indicators are calculated:

- Accuracy: the percentage of face images correctly classified as bona fide or morphed; Equal-Error Rate (EER): the error rate for which both BPCER and APCER are identical;
- $BPCER@APCER=p\%$: the lowest BPCER for $APCER \leq p\%$;

Detection Error Tradeoff (DET) curve: the plot of APCER against BPCER.

6.2 | Results on *MorphDB_D* and *MorphDB_{P&S}*

Table 4 reports the results obtained in terms of accuracy, EER and BPCER (at different levels of APCER) as a function of (i) the testing database, (ii) the network and (iii) the training set used. The corresponding DET curves are available in [58].

The results show a variable behaviour over different test databases. The performance measured over the *MorphDB_D* dataset is good for all the evaluated networks, even if here the ImageNet pre-trained models (AlexNet and VGG-19) often achieve the best results. It can be argued that in detection of artefacts and traces of digital manipulations that characterise digital morphed images, the general filters learned from natural

TABLE 4 Performance indicators of the evaluated networks on the testing databases using different training sets. The best result on each test database is highlighted in bold

Test	Net	Training	Accuracy (%)	EER (%)	BPCER (%) at		
					APCER = 10%	APCER = 5%	APCER = 1%
<i>MorphDB_D</i>	AlexNet	<i>Digital_{Au}</i>	98.3	1.8	0.8	0.8	3.8
		<i>Digital_{Mc}</i>	96.1	1.3	0.8	1.5	1.5
	VGG19	<i>Digital_{Au}</i>	92.2	3.9	0.8	3.8	10.8
		<i>Digital_{Mc}</i>	94.3	4.3	0.8	3.1	5.4
	VGG-Face16	<i>Digital_{Au}</i>	93.9	3.9	0.8	1.5	10.0
		<i>Digital_{Mc}</i>	97.4	0.9	0.0	0.0	0.0
	VGG-Face2	<i>Digital_{Au}</i>	95.2	1.8	0.0	1.5	3.1
		<i>Digital_{Mc}</i>	93.0	0.9	0.0	0.8	0.8
<i>MorphDB_{P&S}</i>	AlexNet	<i>Digital_{Au}</i>	43.5	28.7	50.8	53.8	66.2
		<i>Digital_{Mc}</i>	43.5	32.7	64.6	74.6	83.1
		<i>Digital_{Au}</i> + $P \widetilde{E} S_{Au}$	67.4	20.9	43.1	52.3	70.0
		<i>Digital_{Mc}</i> + $P \widetilde{E} S_{Mc}$	83.5	13.9	25.4	41.5	77.7
	VGG19	<i>Digital_{Au}</i>	47.0	32.7	57.7	71.5	89.2
		<i>Digital_{Mc}</i>	44.3	30.4	52.3	66.9	84.6
		<i>Digital_{Au}</i> + $P \widetilde{E} S_{Au}$	60.4	18.2	36.9	45.4	70.0
		<i>Digital_{Mc}</i> + $P \widetilde{E} S_{Mc}$	56.5	24.8	49.2	54.6	55.4
	VGG-Face16	<i>Digital_{Au}</i>	60.4	12.7	13.8	20.8	69.2
		<i>Digital_{Mc}</i>	56.5	11.3	12.3	22.3	63.1
		<i>Digital_{Au}</i> + $P \widetilde{E} S_{Au}$	89.6	7.3	7.7	15.4	39.2
		<i>Digital_{Mc}</i> + $P \widetilde{E} S_{Mc}$	93.5	6.1	2.3	6.9	43.8
	VGG-Face2	<i>Digital_{Au}</i>	51.7	16.5	20.0	23.8	40.0
		<i>Digital_{Mc}</i>	45.7	15.7	18.5	33.1	80.0
		<i>Digital_{Au}</i> + $P \widetilde{E} S_{Au}$	74.3	8.2	6.2	9.2	25.4
		<i>Digital_{Mc}</i> + $P \widetilde{E} S_{Mc}$	86.5	6.1	4.6	7.7	17.7

images can be even more powerful than specific filters optimised for invariant face recognition. This observation is aligned with the outcomes of [28].

The test on *MorphDB_{P&S}*, allows evaluating the performance when the P&S process comes into play. In general, the results show that networks trained only on digital images are not able to deal with P&S images; all the architectures suffer from this issue and provide quite bad results. Exploiting simulated P&S images for network training allows in some cases to obtain a significant improvement (e.g., the accuracy of VGG-Face16 network trained with multi-crops grows from about 56% to 93%); these results are quite encouraging if we consider that no real P&S images have been used during training. Overall an accuracy of 85%–90% can be reached with reasonable values of EER and BPCER at APCER=10% and 5%.

In general, the multi-crop approach provides better results among the different data augmentation techniques. Looking at the performance of the different networks, an opposite behaviour is observed here with respect to the experiments on digital images: in fact, the best performing nets are the VGG-Face models pre-trained on large face datasets with AlexNet and VGG19 struggling to reach decent performance. Since P&S remove most of the digital artefacts, we argue that more powerful and problem specific feature detectors are needed to solve such a complex problem.

To better analyse the effects of extending the digital training set with simulated P&S images, the bona fide and morphed score distributions of AlexNet and VGG-Face16 networks trained with the *Digital_{Au}* and the

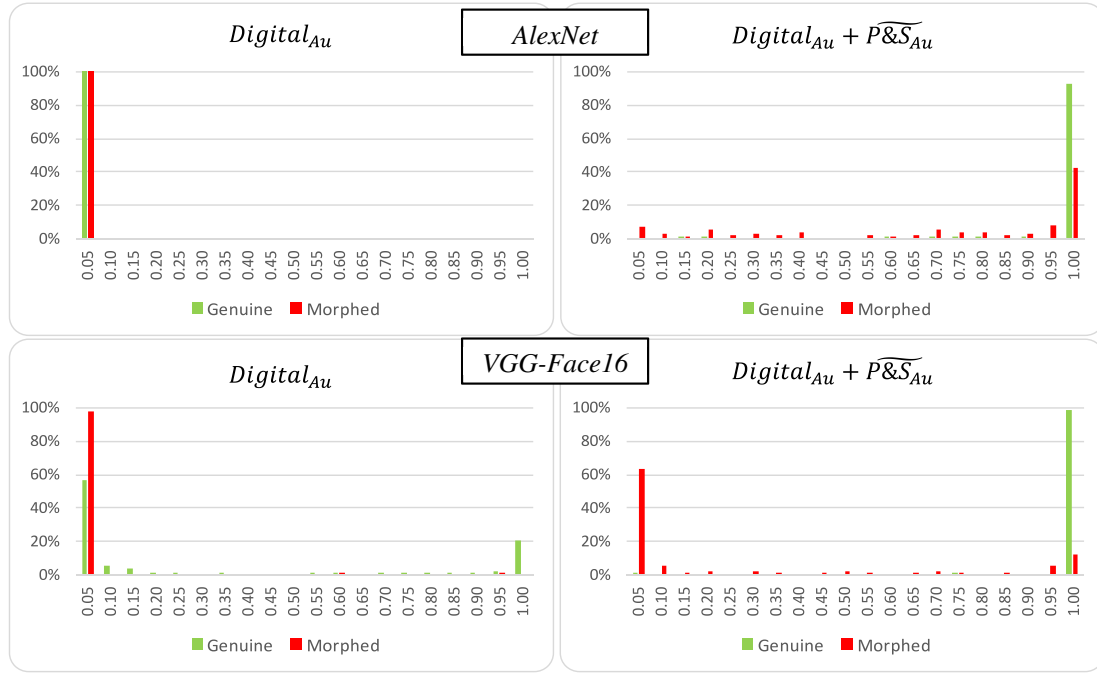


FIGURE 10 Bona fide and morphed score distribution on *MorphDB_{P&S}* for AlexNet and VGG-Face16 networks obtained using the *Digital_{Au}* training set (first column) and the *Digital_{Au} + P&S_{Au}* training set (second column)

Digital_{Au} + P&S_{Au} training sets are reported in Figure 10. The graphs clearly show that the networks trained on digital images only (*Digital_{Au}*) return a score close to 0 for both bona fide and morphed images. This means that the modifications introduced by P&S remove the textural details that makes bona fide and morphed images distinguishable. When training is extended with simulated P&S images (*Digital_{Au} + P&S_{Au}*), the network pre-trained on face images (VGG-Face16) is able to learn P&S specific features making it able to discriminate bona fide from morphed images. Therefore, the bona fide scores become higher, while the morphed scores are generally kept quite low, as clearly visible from the score distributions for VGG-Face16. On the contrary AlexNet does not benefit of this further training step and its introduction determines an increment of all the scores (bona fide and morphed).

6.3 | Results on NIST FRVT MORPH

Two of the most promising solutions identified in our internal tests (AlexNet trained on *Digital_{Au}* for the digital images and VGG-Face16 trained on *Digital_{Au} + P&S_{Au}* for the P&S images) have been submitted for evaluation at NIST FRVT MORPH which provides a huge and thorough comparative evaluation of face morphing detection algorithms; most of the tests are related to the digital context, but a small set of printed and scanned images is also considered for performance evaluation. Please refer to the report [47] and the evaluation website [59] for the full set of results; for lack of space, Figure 11 is used to report a subset of the NIST DET plots

comparing single-image based detection algorithms on several image subsets (5 digital and 1 printed and scanned). Overall the results show that morphing attack detection from single images is a very hard task, in particular, when heterogeneous datasets are considered. The proposed approach compares favourably with most of the evaluated approaches, and presents overall comparable performance with the *ntnussl_002* algorithm. In the *Lincoln* subset (Figure 11e) the proposed approach is outperformed by other techniques, even if the best reference value ($\text{APCER@BPCER} = 0.01\%$) is reached by the proposed algorithm. In the *Print and Scan* dataset the proposed approach ranks second among the tested algorithms and this is very encouraging if we consider that no real printed/scanned images have been used to train our system; this confirms the efficacy of the simulation procedure proposed here.

The results in Figure 11d are worth of attention; in this case the morphed images were generated using the morphing algorithm described in Section 3.1 so the level of performance achieved is of course very good, which is significantly better than all the other results. This behaviour confirms the importance of training the system with representative data and suggests that a higher robustness can be achieved by extending the training data to a variety of morphing algorithms. This would probably also allow to improve the results on the subsets of Figures 11e and 11(f)

6.4 | Results on SOTAMD benchmark

The same solutions tested at NIST have also been tested on the SOTAMD benchmark, which revealed to be a very hard

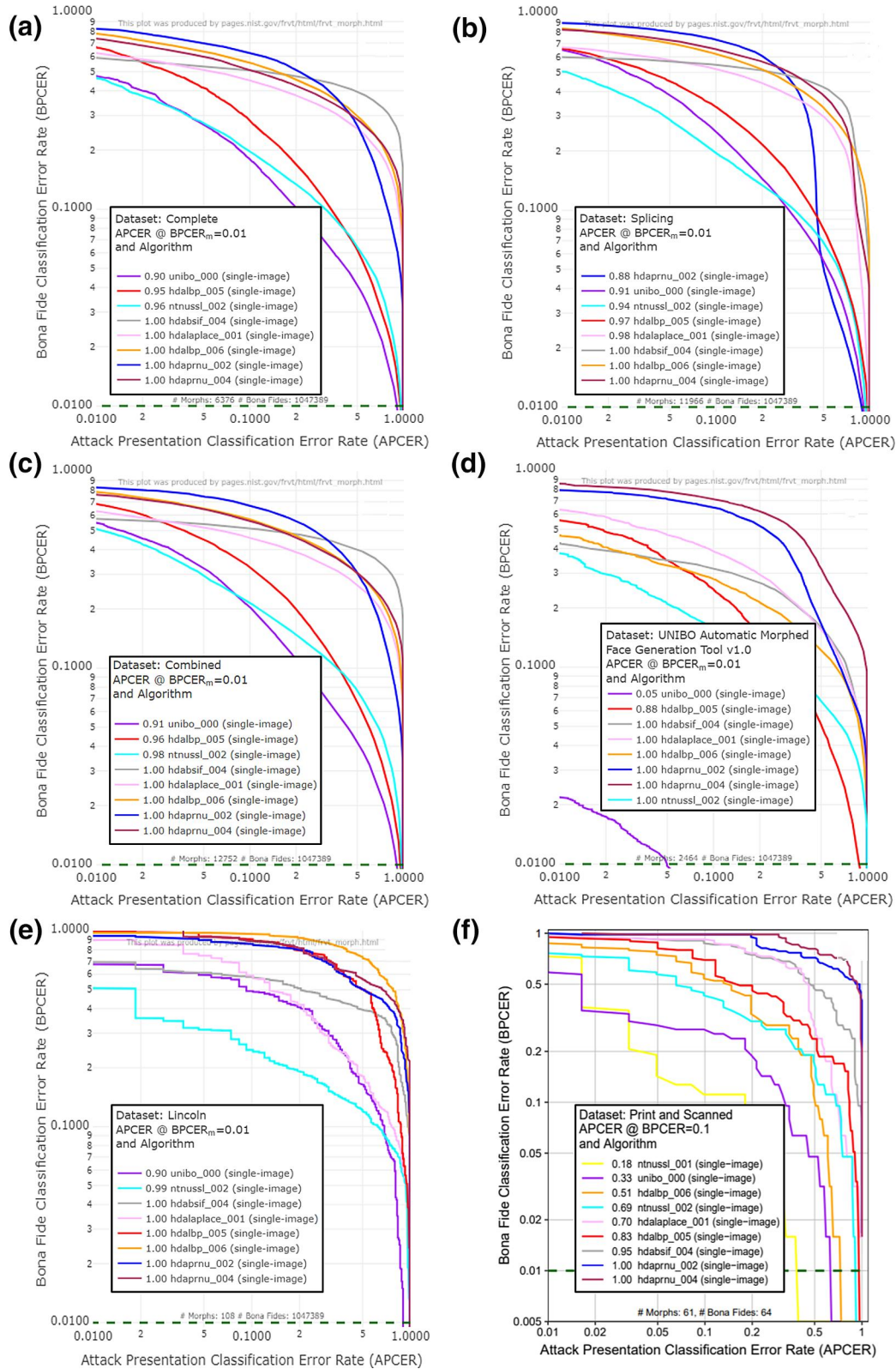


FIGURE 11 DET plots reporting BPCER as a function of APCER for different testing subsets. The horizontal dotted dark green line represents BPCER=0.01. The proposed algorithm corresponds to the violet curve (unibo_000)

challenge, as confirmed by the very modest results reached by the tested algorithms (see Table 5). The proposed approach achieves an EER value better than the other approaches in the

P&S testing set and this is a positive indicator since the SOTAMD P&S images have been produced by multiple processing pipelines reproducing the real workflow used by

TABLE 5 Results on the SOTAMD benchmark

Test	Algorithm	EER (%)	BPCER (%) at	
			APCER = 10%	APCER = 5%
P&S	Proposed approach	37.10	100.00	100.00
	[24]	48.04	85.86	97.35
	[27]	54.37	94.89	98.27
	[33]	43.34	100.00%	100.00
Digital	Proposed approach	38.99	100.00%	100.00
	[24]	44.81	100.00%	100.00
	[27]	31.80	65.00%	79.33
	[33]	41.38	100.00%	100.00

different countries for passport issuing. However, in general, the BPCER values measured in this benchmark are very bad, confirming that morphing attack detection from single images is still an open problem.

7 | CONCLUSIONS

In this work, different network architectures have been used for single image face morphing detection in both digital and P&S scenarios. In particular, P&S images are focused, which still represent a big challenge today. Our initial experiments on the *MorphDB_D* dataset proved that good performance can be achieved on digital images (BPCER=0% at APCER=10%), confirming the effectiveness of different networks already discussed in [19, 27, 28]. Unfortunately such low error rates cannot be extended to P&S images (BPCER about 12% at APCER=10% on *MorphDB_{P&S}*) if only digital images are used for training. To overcome this problem, an automatic generation procedure has been proposed to simulate the typical P&S image degradation. When combined with automatic morphing generation it allows to produce a vast amount of training data for network training/tuning without the costs/efforts needed to manually print and scan face images. The use of simulated P&S images allowed to significantly improve morphing attack detection performance, achieving a BPCER=2.3% at APCER=10% on the *MorphDB_{P&S}* dataset. As to the different network architectures analysed, the limited size of our training databases does not allow to train large models from scratch, so all the CNN used in this work were pre-trained.

The experiments highlighted that CNN pre-trained on natural images (ImageNet) can perform well on digital images, while CNN specifically pre-trained on face images (VGG Face datasets) perform better on P&S images. We argue that to detect textural differences between bona fide and morphed (digital) images, the filters learned from natural images are quite good, while in presence of P&S images

more sophisticated and face-specific filters are necessary to detect the fine artefacts that survive the printing and scanning process.

The tests on the NIST and SOTAMD benchmarks confirm the superiority of the proposed approach over other existing solutions for several data subsets, but generally the results obtained are quite modest. The complexity of those two benchmarks is high and single-image based morphing attack detection approaches struggle to reach decent performance. Therefore morphing attack detection from single images has to be considered as a still open challenge and the unsatisfactory results suggests the importance of a very robust training, which can only be realised by increasing the variability and representativeness of training data. Because of this reason a direct extension of our work will be to further increase the training set, using for instance different morphing algorithms or different sets of parameters for the P&S process.

The other important point to investigate in the future works is to gain some insight about the factors influencing the network decision. Some preliminary works [29] analysed the importance of different face regions for morphing detection on digital images. Further studies are necessary to better understand and explain these phenomena especially on P&S images: we believe that existing visualisation techniques (see [60]) can be profitably used for this purpose.

Finally, recently Generative Adversarial Networks (GAN) [61] have been successfully used for various image generation applications (e.g., [39, 62]); their adoption for morphed image generation and P&S simulation will be investigated in our future researches.

ORCID

Matteo Ferrara  <https://orcid.org/0000-0002-4020-1419>

Annalisa Franco  <https://orcid.org/0000-0002-6625-6442>

REFERENCES

1. Ferrara, M., Franco, A., Maltoni, D.: On the effects of image alterations on face recognition accuracy. In: Face Recognition Across the Electromagnetic Spectrum, pp. 195–222. Springer International Publishing (2016)
2. Ferrara, M., Franco, A., Maltoni, D.: The magic passport. In: IEEE International Joint Conference On Biometrics (IJCB). Clearwater, FL (2014)
3. Gomez-Barrero, M., et al.: Is your biometric system robust to morphing attacks? 5th International Workshop on Biometrics and Forensics (IWBF), Coventry, UK (2017)
4. Gomez-Barrero, M., et al.: Predicting the vulnerability of biometric systems to attacks based on morphed biometric information. IET Biometr. 7(4), 333–341 (June 2018)
5. Scherhag, U., et al.: On the vulnerability of face recognition systems towards morphed face attacks. 5th International Workshop on Biometrics And Forensics (IWBF). Coventry, UK (2017)
6. University of Massachusetts: Labeled Faces in the Wild. <http://vis-www.cs.umass.edu/lfw/>
7. Krizhevsky, A., Sutskever, I., Hinton, G.E.: ImageNet classification with deep convolutional neural networks. 25th International Conference on Neural Information Processing Systems (NIPS), Nevada, Lake Tahoe (2012)

8. Simonyan, K., Zisserman, A.: Very Deep Convolutional Networks for Large-Scale Image Recognition. [arXiv:1409.1556](https://arxiv.org/abs/1409.1556) (2015)
9. Makrushin, A., Wolf, A.: An overview of recent advances in assessing and mitigating the face morphing attack. 26th European signal processing conference (EUSIPCO). Italy, Rome (2018)
10. Raja, K., et al.: Morphing attack detection - database, evaluation platform and benchmarking. IEEE Transactions on Information Forensics and Security (TIFS) (2020). <https://doi.org/10.1109/TIFS.2020.3035252>
11. Scherhag, U., et al.: Face recognition systems under morphing attacks: a survey. IEEE Access. 7, 23012–23026 (2019)
12. Raghavendra, R., Raja, K. B., Busch, C.: Detecting morphed face images. IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS). Niagara Falls, NY (2016)
13. Neubert, T.: Face morphing detection: an approach based on image degradation analysis. International Workshop on Digital Watermarking (IWDW), Magdeburg, Germany (2017)
14. Makrushin, A., et al.: Generalized Benford's law for blind detection of morphed face images. 6th ACM Workshop on Information Hiding and Multimedia Security, Innsbruck, Austria (2018)
15. Makrushin, A., Neubert, T., Dittmann, J.: Automatic Generation and Detection of Visually Faultless Facial Morphs. 12th International Joint Conference on Computer Vision, Imaging and computer Graphics Theory and Applications, Porto, Portugal (2017)
16. Hildebrandt, M., et al.: Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps. 5th International Workshop on Biometrics and Forensics (IWBF), Coventry, UK (2017)
17. Kraetzer, C., et al.: Modeling Attacks on Photo-ID Documents and Applying Media Forensics for the Detection of Facial Morphing. 5th ACM workshop on information hiding and multimedia security, Philadelphia, PA (2017)
18. Spreuwers, L., Schils, M., Veldhuis, R.: Towards robust evaluation of face morphing detection. 26th European signal processing conference. EUSIPCO, Rome, Italy (2018)
19. Wandzik L., Kaeding G., Garcia R.V.: Morphing detection using a general-purpose face recognition system. 26th European Signal Processing Conference (EUSIPCO), Rome, Italy (2018)
20. Raghavendra, R., et al.: Face morphing versus face averaging: vulnerability and detection. IEEE International Joint Conference on Biometrics (IJCB 2017). Denver, CO (2017)
21. Raghavendra, R., et al.: Detecting face morphing attacks with collaborative representation of steerable features. In: 2018 International Conference on Computer Vision and Image Processing, Singapore (2018)
22. Zhang, L.B., Peng, F., Long, M.: Face morphing detection using Fourier spectrum of sensor pattern noise. IEEE International Conference on Multimedia and Expo, (ICME), San Diego, CA (2018)
23. Debiasi, L., et al.: PRNU-based detection of morphed face images. International Workshop on Biometrics and Forensics (IWBF), Sassari, Italy (2018)
24. Scherhag, U., et al.: Detection of face morphing attacks based on prnu analysis. IEEE Trans. Biometr. Behav. Identity Sci. 1(4), 302–317 (2019)
25. Scherhag, U., et al.: Detecting morphed face images using facial landmarks. International Conference on Image and Signal Processing (ICISP), Cherbourg, France (2018)
26. Jassim, S., Asaad, A.: Automatic detection of image morphing by topology-based analysis. 26th European Signal Processing Conference (EUSIPCO), Rome, Italy (2018)
27. Raghavendra, R., et al.: Transferable Deep-CNN features for detecting digital and print-scanned morphed face images. IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI (2017)
28. Seibold, C., et al.: Detection of face morphing attacks by deep learning. International Workshop on Digital Watermarking (IWDW), Magdeburg, Germany (2017)
29. Seibold, C., et al.: Accurate and Robust Neural Networks for Security Related Applications Exemplified by Face Morphing Attacks (2018). [arXiv:1806.04265](https://arxiv.org/abs/1806.04265)
30. Scherhag, U., Rathgeb, C., Busch, C.: Morph detection from single face image: a multi-algorithm fusion approach. 2nd International Conference on Biometric Engineering and Applications (ICBEA), Amsterdam, The Netherlands (2018)
31. Ferrara, M., Franco, A., Maltoni, D.: Face demorphing. IEEE Trans. Infor. Forens. Secur. 13(4), 1008–1017 (April 2018)
32. Ferrara, M., Franco, A., Maltoni, D.: Face demorphing in the presence of facial appearance variations. European Signal Processing Conference (EUSIPCO), Rome, Italy (2018)
33. Scherhag, U., Rathgeb, C., Busch, C.: Towards detection of morphed face images in electronic travel documents. 13th IAPR international Workshop on Document Analysis Systems (DAS), Vienna, Austria (2018)
34. Scherhag, U., et al.: Deep face representations for differential morphing attack detection. IEEE Trans. Inform. Forens. Secur. 15, 3625–3639 (2020)
35. Singh, J.M., et al.: Robust morph-detection at automated border control gate using deep decomposed 3D shape & diffuse reflectance. In: 2019 International Conference on signal-Image Technology & Internet-Based, Sorrento (2019)
36. Damer, N., et al.: Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts. In: 2018 German Conference on Pattern Recognition, Stuttgart (2018)
37. Scherhag, U., Rathgeb, C., Busch, C.: Performance variation of morphed face image detection algorithms across different datasets. International Workshop on Biometrics and Forensics (IWBF). Sassari, Italy (2018)
38. Lin, C., Chang, S.: Distortion modeling and invariant extraction for digital image print-and-scan process. International Symposium on Multimedia Information Processing (ISMIP), Taipei, Taiwan (1999)
39. Mitkovski, A., et al.: Simulation of print-scan transformations for face images. In: 2020 International Conference of the Biometrics Special Interest Group (BIOSIG 2020), Darmstadt (2020)
40. Taylor, L., Nitschke, G.: Improving Deep Learning using Generic Data Augmentation. [arXiv:1708.06020](https://arxiv.org/abs/1708.06020) (2017)
41. Xiberpix. <http://www.xiberpix.net/SqrlzMorph.html> (September 2020)
42. Robila, S.A.: Using spectral distances for speedup in hyperspectral image processing. Int. J. Remote Sens. 26(24), 5629–5650 (2005)
43. Martinez, A.M., Benavente, R.: The AR Face Database, CVC Technical Report #24 (1998)
44. Phillips, P.J., et al.: Overview of the face recognition grand challenge. Proceedings IEEE Computer Vision and Pattern Recognition (2005)
45. Phillips, P.J., et al.: The FERET database and evaluation procedure for face-recognition algorithms. Image Vision Comput. 16(5), 295–306 (April 1998)
46. Phillips, P.J., et al.: The FERET evaluation methodology for face-recognition algorithms. IEEE Trans. Pattern Anal. Mach. Intell. 22(10), 1090–1104 (October 2000)
47. Ngan, M., et al.: Face Recognition Vendor Test (FRVT) Part 4: MORPH–Performance of Automated Face Morph Detection. NIST Report #8292, 2020
48. Dorizzi, B., et al.: Fingerprint and on-line signature verification competitions at ICB 2009. In: Proceedings of 3rd IAPR/IEEE International Conference on Biometrics (ICB09), Alghero (2009)
49. BioLab. [Online]. <http://biolab.csr.unibo.it/fvcongoing> (September 2020)
50. Neurotechnology Inc.: <http://www.neurotechnology.com/> (September 2020)
51. Deng, J., et al.: ImageNet: a large-scale hierarchical image database. IEEE Conference on Computer Vision and Pattern Recognition. Miami, FL (2009)
52. BVLIC AlexNet Caffe Model, https://github.com/BVLIC/caffe/tree/master/models/bvlc_alexnet (September 2020)
53. Russakovsky, O., et al.: ImageNet large scale visual recognition challenge. Intl. J. Comput. Vis. 115(3), 211–252 (December 2015)
54. Parkhi, O.M., Vedaldi, A., Zisserman, A.: Deep Face Recognition. British Machine Vision Conference (BMVC), pp. 41.1–41.12. BMVA Press (2015)
55. Cao, Q., et al.: VGGFace2: a dataset for recognising faces across pose and age. 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, China (2018)

56. He, K., et al.: Deep residual learning for image recognition. IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Las Vegas, NV (2016)
57. International Organization for Standardization (ISO): ISO/IEC 30107-3:2017 - Information Technology – Biometric Presentation Attack Detection – Part 3: Testing and Reporting. ISO, Geneva, Switzerland (2017)
58. Ferrara, M., Franco, A., Maltoni, D.: Face morphing detection in the presence of printing/scanning and heterogeneous image sources. <https://arxiv.org/abs/1901.08811>. Accessed 7 December 2020
59. NIST: https://pages.nist.gov/frvt/html/frvt_morph.html (September 2020)
60. Olah, C., Mordvintsev, A., Schubert, L.: Feature Visualization. Distill (2017)
61. Goodfellow, I., et al.: Generative adversarial nets. Conference on neural information processing systems (NIPS), Montreal, Quebec, Canada (2014)
62. Peng, F., Zhang, L.B., Long, M.: FD-GAN: Face-Demorphing Generative Adversarial Network for Restoring Accomplice's Facial Image. [arXiv:1811.07665](https://arxiv.org/abs/1811.07665) (2018)

How to cite this article: Ferrara M, Franco A, Maltoni D. Face morphing detection in the presence of printing/scanning and heterogeneous image sources. *IET Biome.* 2021;10:290–303. <https://doi.org/10.1049/bme2.12021>