

MorDeepy: Face Morphing Detection Via Fused Classification

Iurii Medvedev*

*University of Coimbra
Institute of Systems
and Robotics
3030-194, Coimbra, Portugal

iurii.medvedev@isr.uc.pt

Farhad Shadmand*

farhad.shadmand@isr.uc.pt

Nuno Gonçalves*,†

†Portuguese Mint and Official
Printing Office (INCM)
1000-042, Lisbon, Portugal

nunogon@deec.uc.pt

Abstract

Face morphing attack detection (MAD) is one of the most challenging tasks in the field of face recognition nowadays. In this work, we introduce a novel deep learning strategy for a single image face morphing detection, which implies the discrimination of morphed face images along with a sophisticated face recognition task in a complex classification scheme. It is directed onto learning the deep facial features, which carry information about the authenticity of these features. Our work also introduces several additional contributions: the public and easy-to-use face morphing detection benchmark and the results of our wild datasets filtering strategy. Our method, which we call MorDeepy, achieved the state of the art performance and demonstrated a prominent ability for generalising the task of morphing detection to unseen scenarios.

1. Introduction

Last decades with the development of deep learning techniques the evident advances have been reached in the area of face recognition. However, evolved and sophisticated techniques for performing the presentation attacks continue to appear, which require the development of new protection solutions.

Face morphing is one such image manipulating technique. It is usually performed by blending several (usually two) digital face images and allows to match different persons with this synthetic image that contains characteristics from both faces. While being simple to implement, face morphing poses the security risks of issuing an identification document that may be validated for two or more persons. Presentation attacks with face morphing usually can be hardly detected by humans which usually perform poorly in matching unfamiliar faces on photos of ID and travel documents [31] and by face recognition software in

ABC (automatic border control) systems [17].

In the last years, face morphing has become a matter of research interest in academia [36] and industry [42]. Morphing detection methods in facial biometric systems may be distinguished into two pipelines depending on the processing scenario. In *no-reference* morphing attack detection algorithm receives a single image, where morphing is detected. In practice, these methods are directed to mitigate risks related to the false acceptance of manipulated images in the *enrollment* process. The authentic document, which is generated with a successfully accepted forged image, may further help to deceive the face recognition system.

The *differential* morphing detection implies additional live data acquisition from an authentication system which gives the reference information for the detection algorithm. This scenario usually takes place while passing an Automated Border Control (ABC) system, when the recently enrolled image (which is already accepted and printed on the ID Document) is tested against morphing detection.

First morphing detection solutions relied on the behaviour of local image characteristics (like texture, noise). Recent approaches usually employ deep learning computer vision tools. However, many of these methods utilize a straightforward learning strategy that is limited by binary classification or contrast learning, which in our opinion is not optimal for a task of face morphing detection and may lead to various convergence problems.

In this work, we introduce a novel deep learning method for single image face morphing detection, which incorporates sophisticated face recognition tasks and implies utilising a combined classification scheme (discussed in Section 3). Also, we develop the public face morphing detection benchmark, which is designed to be adaptive to the developer needs and at the same time to be simple for comparison of algorithms of different developers. As an additional contribution, we introduce the results of our datasets filtering strategy (image name lists), which is described in Section 4.1.

Regarding the limitations of the work, it is important to note that at the current stage we focus on single image morphing detection. Also, we do not take into account redigitized face images (by printing/scanning). At the same time, we are limited to utilising landmark-based methods for performing face morphing. GAN (Generative adversarial Network) based methods require large computational resources (namely for projecting images to latent space) and at the same time, face recognition systems are less vulnerable to presentation attacks with GAN morphs, rather than to landmark-based morphs [61]. However, we intend to cover those limitations in further research.

2. Related Work

To introduce our methodology, we need to discuss recent advances in face morphing, face morphing detection (focusing on the no-reference scenario) and face recognition.

2.1. Face Morphing

The generic pipeline of creating face morph from original images includes the following steps: face features extraction → features averaging → generating morphed image from averaged features → optional restoring image context (namely background).

Landmark based approaches, first introduced by Ferrara *et al.* [17], follow this pipeline straightforwardly in the image spatial domain by the face landmark alignment, image warping and blending. Different reported morphing algorithms employ variations of this strategy [26, 28, 46].

With recent advances in generative deep learning approaches, several face morphing methods, which utilise deep latent feature domain, were proposed.

The above face morphing pipeline may adapt various deep learning tools like variational autoencoders (VAE) [9] or generative adversarial networks (GANs) [61, 67].

2.2. Face Morphing Detection

Single image (no-reference) face morphing detection algorithms usually utilize local image information and image statistics.

Various morphing detection approaches employ Binary Statistical Image Features (BSIF) [38], Photo Response Non-Uniformity (PRNU), known as sensor noise [12, 47], texture features [41], local features in frequency and spatial image domain [33] or complex combination of these features [29, 48].

Several deep learning approaches for no-reference case were proposed. For face morphing detection these approaches usually follow binary classification of pretrained face recognition features [39], which may be finetuned [19, 53] or utilized in a combination with local texture characteristics [62]. Damer *et al.* [11] introduced a better regularized strategy for morphing detection by replacing

the trivial binary classification with pixel-wise supervision. Aghdaie *et al.* [1] adopted the attention mechanism which is controlled by wavelet decomposition.

Differential face morphing detection is a less challenging task and security risks in this scenario indeed may be combated by increasing the discriminability of face deep representation, which is utilized for recognition.

Several approaches for differential detection was recently proposed. Scherhag *et al.* [50] followed the classification of pretrained deep features in differential scenario. Borghi *et al.* [6] performed differential morphing detection by finetuning the pretrained networks in a complex setup with identity verification and artifacts detection blocks. Rather different approach to the differential scenario was introduced by Ferrara *et al.* [18] who proposed an approach to revert morphing by retouching the testing face image with a trusted live capture to reveal the identity of the legitimate document owner.

In comparison to the considered approaches, we propose to focus our method on learning the authenticity of deep face features, regularizing the morphing detection with a delicate face recognition task.

2.3. Face Recognition

Modern face recognition approaches rely on deep learning tools, which give the ability to learn highly discriminative features themselves from unconstrained images. Among several techniques to perform the tasks of extracting features, the convolutional neural network (CNN) is one of the most efficient for the pattern recognition problems [44].

There are several strategies for approaching face recognition via deep learning. However, all of them are focused on extracting low-dimensional face representation (deep face features) and increasing the discriminative power of that representation.

Metric learning methods are directed on optimising the face representation itself through the contrast of match/non-match pairs [8, 52]. However, for reliable convergence, these methods require enormously large datasets and sophisticated sample mining techniques.

Another concept (which we indeed follow in our work) is learning face representation implicitly via a closed-set identity classification task. Deep networks in these methods encapsulate face representation in the last hidden layer and usually adopt softmax loss and its modifications for classification [57–59].

Improvement of the performance in this technique was achieved by various techniques for increasing intra-class compactness and maximizing inter-class discrepancy. For example, by applying additional regularisation for pushing intra-class features to their centre [64], or by introducing several kinds of marginal restrictions for inter-class variance [14, 27, 56, 63].

Several recent works were directed onto investigating sample specific learning strategies, which are controlled by sample quality [60], hardness [23, 66], data augmentation [55] or even by treating facial representation in distributional manner (by specifying sample *uncertainty*) [54].

In our work, we consider face morphing detection from the perspective of face recognition. In the case of following the approach via identity classification, face morphing introduces a problem, since a face morph image indeed belongs to several identities, which leads to the ambiguity of proper class labelling. In this work, we address this issue (Section 4.2) in search of the method for single image morphing detection.

3. Methodology

In this section, we describe our technique for single image morphing detection via deep learning.

In our research, we intuitively tried to invent a setup that will allow learning high-level deep features, that also carry some information about their authenticity. This resulted in the schematic that includes two backbone CNN based networks that are trained in a similar manner but biased in a way to discriminate morphed and bona fide images. Namely, our idea implies training two parallel networks which consider bona fide samples similarly and morphed samples differently (see Fig. 1).

Both networks learn high-level features via classification tasks, which are different in terms of identity labelling of face morphs. *First Network* labels them by the original identity from the first source image, the *Second Network* - by the second original label.

The extracted features are also explicitly compared by similarity metric (which is the dot product due to the softmax properties) and the result is classified according to the ground truth authenticity label of the image (bona fide/morph).

The identity classification parts of the training scheme act as a regularisation that retains the facial discriminability of feature layers. That is why for identity classification we utilize a standard softmax, which allows easier convergence in comparison with its modifications (like ArcFace [14]).

Following the common formulation of softmax, our training process is regularized by the losses:

$$L_1 = -\frac{1}{N} \sum_i^N \log\left(\frac{e^{\tilde{W}_{\hat{y}_i}^T \tilde{f}_i + \tilde{b}_{\hat{y}_i}}}{\sum_j^C e^{\tilde{W}_{\hat{y}_j}^T \tilde{f}_i + \tilde{b}_{\hat{y}_j}}}\right) \quad (1)$$

$$L_2 = -\frac{1}{N} \sum_i^N \log\left(\frac{e^{\tilde{W}_{\check{y}_i}^T \check{f}_i + \check{b}_{\check{y}_i}}}{\sum_j^C e^{\tilde{W}_{\check{y}_j}^T \check{f}_i + \check{b}_{\check{y}_j}}}\right) \quad (2)$$

where $\{\tilde{f}_i, \check{f}_i\}$ denote the deep features of the i -th sample, $\{\hat{y}_i, \check{y}_i\}$ are the indexes of the class of the i -th sample,

$\{\tilde{W}, \check{W}\}$ and $\{\tilde{b}, \check{b}\}$ are weights and biases of last fully connected layer (respectively for the *{First, Second}* networks). N is the number of samples in a batch and C is the total number of classes.

The target driver of the training process tries to explicitly discriminate morph/non-morph images. The dot product of backbones outputs indicates the morphing detection score. It is activated by sigmoid function, and the corresponding loss is defined as binary cross-entropy:

$$\begin{aligned} L_3 = & -\frac{1}{N} \sum_i^N t \log \frac{1}{1 + e^{-D}} + \\ & +(1-t) \log \left(1 - \frac{1}{1 + e^{-D}}\right), \end{aligned} \quad (3)$$

where class-label t is computed by a comparison of input class labels:

$$t = \text{abs}(\text{sgn}(\hat{y}_i - \check{y}_i)), \quad (4)$$

and D is a dot product of high level features extracted by *First* and *Second* backbones:

$$D = \tilde{f} \cdot \check{f} \quad (5)$$

The result loss for optimisation is combined as a weighted sum:

$$L = \alpha_1 L_1 + \alpha_2 L_2 + \beta L_3 \quad (6)$$

By minimizing this loss in the fused classification setup, we learn the discriminative facial features that are explicitly regularized for morphing detection.

At the testing stage, the identity classification parts of the network are redundant and may be removed from the setup. The morphing detection decision is made by thresholding the scalar product of the backbones outputs.

Although our strategy is adapted for single image morphing detection indeed it is naturally also suitable for differential verification scenario. In this case, *First* and *Second* networks shall receive respectively two images (enrolled and life capture) instead of the same single image.

4. Datasets

The proposed methodology requires the large labelled face dataset with an accompaniment of morphed images of identities from this dataset.

The academic community still doesn't have public ID document compliant datasets which are large enough for efficient training of modern deep networks (as an example, one of the largest FRGC_V2 [37] contains only $\sim 50k$ images and ~ 500 identities). That is why our strategy for this work is to utilize the wild dataset which is filtered by the criteria of *suitability for face morphing*. Conceptually this

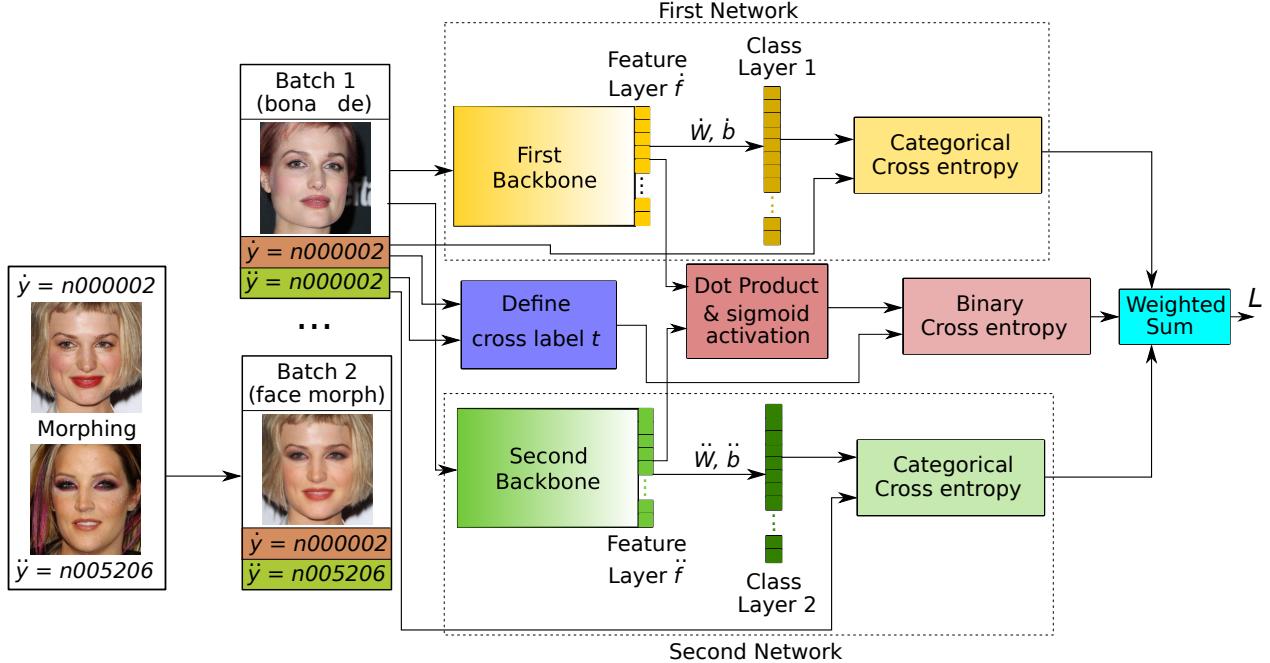


Figure 1. Schematic of the proposed method. For simplicity of visualisation batch contains a single image. Labels \hat{y} and \ddot{y} are indicated by names, when the real setup utilizes their numerical index value, which is encoded to one-hot vector.

approach indeed is not novel and was recently utilized in face morphing research [10, 11]. In this work, we introduce a technique for semi-automatic wild dataset filtering for our method.

As a source wild dataset we use VGGFace2 [7] ($\sim 3M$ images, $\sim 9k$ classes, ~ 360 samples per class, Licence - CC BY-SA 4.0) due to large average number of samples per identity (in comparison to other popular wild face datasets like CASIA-WebFace [65], MS-Celeb-1M [20, 25], Glint360K [2], WebFace260M [69]) in order to have enough samples per identity after filtering.

4.1. Wild Dataset Filtering

Our dataset filtering strategy is based on a thresholding by quality metrics. Following Tremoço *et al.* [60] we used a set of quality scores for labeling the face images in the dataset: Blur [4], FaceQNet [22], BRISQUE [32], Face Illumination [68] and Pose [43]. This set of scores allow to discriminate and select samples by their natural quality (Blur, BRISQUE), ID documents suitability (FaceQNet), face image acquisition parameters (Illumination, Pose).

Next, we randomly select samples and manually label them with a binary value (accept/reject). This acceptance is defined by the criteria of suitability for application in face morphing (namely by user's choice). In our setup, we assure that samples are selected distributively across the quality scores values. Namely, we split the total quality score range into a set of sub-ranges and define the minimum number of

samples to be selected from each sub-range. By proceeding around 4k images in our setup, we harvest the dependency of FAR (False Acceptance Rate) and FRR (False Rejection Rate) from quality scores values (see Fig. 2).

The dataset filtering is then performed with joint thresholding by those quality metrics. For each score, we select the threshold at a point of EER (Equal Error Rate). As a result we get the *VGGFace2-selected* dataset with the same identity list as original source and around 500k images (see Fig. 3).

4.2. Morph Dataset Harvesting Strategy

For application in our method, the filtered wild dataset is needed to be accompanied by a large collection of face morphs. We automatically generate these images with our customized landmark-based morphing approach (with blending coefficient $\alpha = 0.5$) (see Fig. 4).

A key requirement for effective learning is to provide unambiguity of proper class labelling in our training method. Namely after generating face morph from two arbitrary samples of the original dataset, the resulting image indeed belongs to both source identities. That is why fully random image pairing (for generating morphs) will result in classification confusion.

To avoid that we utilize the following strategy. First, we separate the total list of identities into two disjoint parts, which are attributed to the *First* and the *Second* networks respectively. Next, to generate a face morph, we randomly

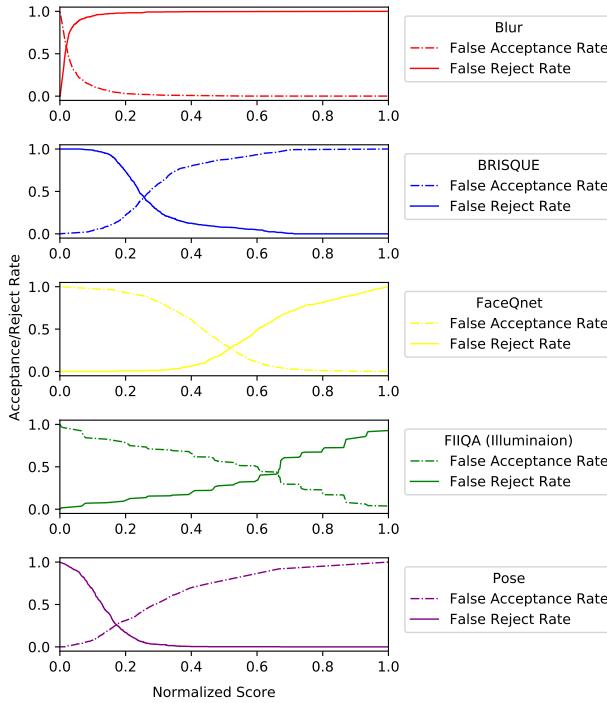


Figure 2. FAR and FRR for result manual quality labeling of random samples from VGGFace2.



Figure 3. Example of VGGFace2 filtering result. Accepted images (green box) and Rejected images (red box).

pair images from identities of these list halves. Each generated image is then labelled according to the attributed sub-list for classification by the *First* and the *Second* networks. Let us note that this labelling is made differently for each morphed image and similarly for bona fide images in both networks (see Fig. 1). That is why this technique, which primarily acts as a regularisation, also amplifies the morphing detection performance.

Following the above procedure, we generate *VGGFace2-selected-morph* dataset, which contains around 1M morphed images.

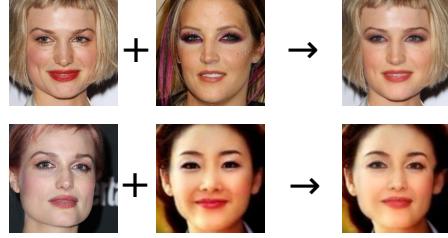


Figure 4. Examples of generated morphs with landmark based approach. Background is restored by one of the source images (chosen randomly).

4.3. Selfmorphing

The fully automatic landmark morphing methods may introduce a number of visible artefacts to the generated images (like blending artefacts). That is why without additional regularisation our method will be biased to learning those artefacts, which is not a realistic scenario. Real fraudulent morphs are retouched with the intention to remove any perceptual artefacts.

To address this problem, we utilize *selfmorphs*, which are generated by applying face morphing to images of the same identity. This concept was indeed recently introduced by Borghi *et al.* [5] and was used for generating images with visible artefacts. Then for removing these artefacts the authors trained the Conditional GAN using original images as a ground truth reference.

In this work, we utilize selfmorph images to focus morphing detection onto the deep face features behaviour, rather than to detecting artefacts. We assume that deep discriminative face features remain after performing selfmorphing. In the proposed method schematic (Fig. 1) we consider selfmorphs as bona fide samples.

We perform a random pairing of samples within each identity from the *VGGFace2-selected* and generate *VGGFace2-selected-selfmorph* dataset, which contains around 500k images (see Fig. 5).



Figure 5. Examples of generated selfmorphs. Images contain blending artefacts but the identity is perceptually retained.

5. Benchmarking

There are few public benchmarks for evaluating the performance of morphing detection or morphing resistant algorithms: the NIST FRVT MORPH [35] and FVC-onGoing MAD [15, 40]. Both of these benchmarks accept no-reference and differential morphing algorithms, however,

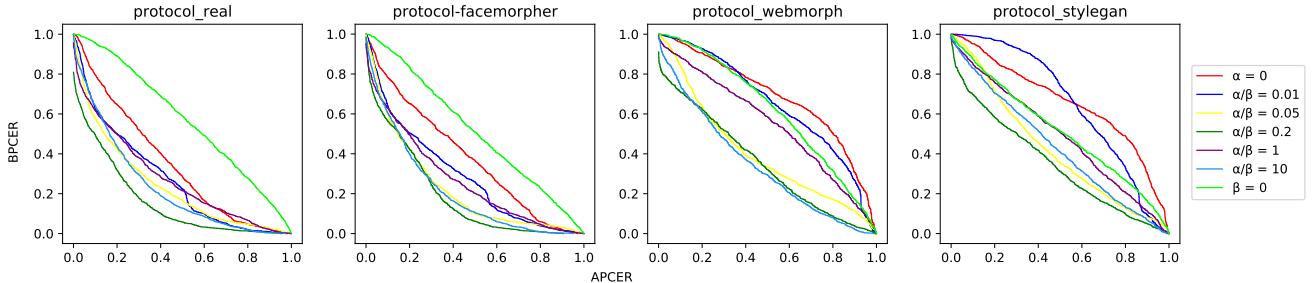


Figure 6. Detection Error Trade-off curves for various α/β proportions in different protocols.

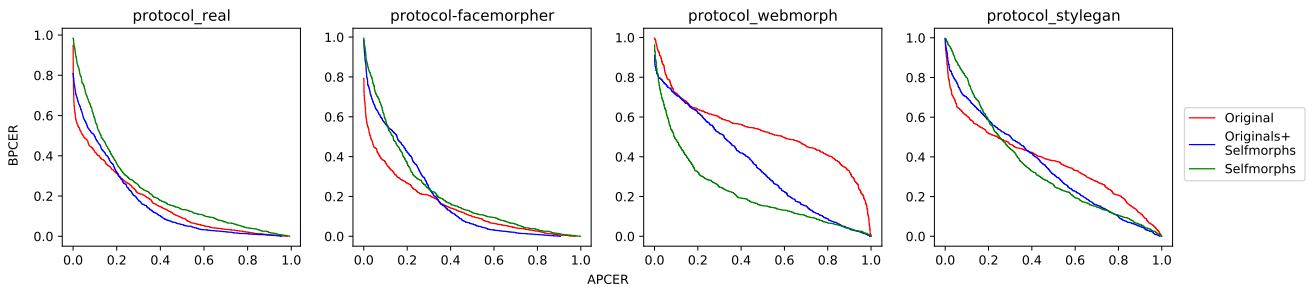


Figure 7. Detection Error Trade-off curves for various bona fide images selection in different protocols.

they are proprietary and are executed on the maintainer side. Thus they have a number of submission restrictions.

The straightforward metric for evaluating single image morphing detection is the dependency of Bona fide Presentation Classification Error Rate (BPCER) from Attack Presentation Classification Error Rate (APCER) (according to ISO/IEC 30107-3 [24]), which may be plotted as a Detection Error Trade-off (DET) curve.

5.1. Face Morphing Detection Benchmark

For this work, we develop an custom benchmark, which is to be executed on the developer side. *We are not making it public at this stage*. The existing public benchmarks provide useful data but usually specify the protocols for the certain software frameworks [45].

Our benchmark intends to provide the functionality for estimating the morphing detection performance, for generating custom protocols and also for further comparison of the results from different developers with existing protocols. At this stage of our work, we focus on the single image morphing detection with only the usage of public data (however, we assume the possibility of further adapting private datasets).

We generate several protocols for single image morphing detection. Our benchmark is based on the FRGC-Morphs, FRLL-Morphs [45], AMSL [34] and Dustone datasets [16]. Using this data we combine several benchmark protocols with various types of face morphs:

- *protocol-real* ($\sim 3k$ morphs(Dustone+AMSL)), which includes morphs with low level of visible blending ar-

tifacts, and imitates realistic presentation attacks.

- *protocol-facemorpher* ($\sim 2k$ morphs), which includes simple morphs with foreground and background artifacts
- *protocol-webmorph* ($\sim 1k$ morphs), which includes images with background artifacts but the low level of artifacts inside the face contour
- *protocol-stylegan* ($\sim 2k$ morphs), which includes StyleGAN morphs

As bona fide images all our protocols use frontal faces from the following public datasets: FRLL Set [13], FEI [3], AR [30], Aberdeen and Utrecht [51] ($\sim 1.5k$ images in total).

6. Experiments and Results

To analyze the performance of our approach we perform several experiments with our method. As backbone networks we use ResNet-50 [21], which are initialized with weights, pretrained on the ImageNet dataset. Followed by pooling and dropout layers each backbone returns 512 deep features. Input images (RGB 3-channel) are aligned and resized to 224×224 . We report the performance by $APCER@BPCER = (0.1, 0.01)$ and $BPCER@APCER = (0.1, 0.01)$.

Our default training dataset is a joined and shuffled concatenation of *VGGFace2-selected*, *VGGFace2-selected-selfmorph*, and *VGGFace2-selected-morph*. It is important to note that in all experiments we assured the equal balance between the numbers of morphed and non-morphed (which are bona fide + selfmorphed) images in the training dataset.

Method	$APCER@BPCER = \delta$							
	protocol-real		protocol-facemorpher		protocol-webmorph		protocol-stylegan	
	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$
$\alpha = 0$	0.697	0.947	0.756	0.939	0.976	0.995	0.980	0.998
$\alpha/\beta = 0.01$	0.601	0.895	0.651	0.957	0.945	0.992	0.895	0.991
$\alpha/\beta = 0.05$	0.607	0.965	0.502	0.968	0.915	0.999	0.842	0.996
$\alpha/\beta = 0.2$	0.401	0.835	0.431	0.786	0.778	0.979	0.799	0.969
$\alpha/\beta = 1$	0.711	0.935	0.670	0.928	0.942	0.995	0.913	0.982
$\alpha/\beta = 10$	0.556	0.839	0.513	0.791	0.749	0.923	0.852	0.969
$\beta = 0.0$	0.945	0.996	0.922	0.993	0.954	0.997	0.949	0.997
$\alpha/\beta = 0.2$ Original	0.481	0.875	0.498	0.876	0.987	0.997	0.915	0.993
$\alpha/\beta = 0.2$ Selfmorphs	0.608	0.938	0.568	0.911	0.704	0.986	0.816	0.983

Table 1. $APCER@BPCER = (0.1, 0.01)$ of our method for various α/β proportions and bona fide images selection in different protocols.

Method	$BPCER@APCER = \delta$							
	protocol-real		protocol-facemorpher		protocol-webmorph		protocol-stylegan	
	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$
$\alpha = 0$	0.795	0.993	0.781	0.971	0.961	0.998	0.952	0.998
$\alpha/\beta = 0.01$	0.625	0.968	0.638	0.979	0.969	0.997	0.991	1.0
$\alpha/\beta = 0.05$	0.577	0.950	0.598	0.951	0.841	0.989	0.895	0.991
$\alpha/\beta = 0.2$	0.494	0.726	0.562	0.848	0.710	0.822	0.697	0.904
$\alpha/\beta = 1$	0.616	0.871	0.628	0.843	0.882	0.963	0.851	0.960
$\alpha/\beta = 10$	0.642	0.892	0.604	0.913	0.742	0.931	0.829	0.967
$\beta = 0.0$	0.956	0.998	0.932	0.998	0.971	0.998	0.874	0.986
$\alpha/\beta = 0.2$ Original	0.417	0.601	0.370	0.595	0.718	0.963	0.605	0.862
$\alpha/\beta = 0.2$ Selfmorphs	0.580	0.912	0.587	0.905	0.484	0.842	0.798	0.976

Table 2. $BPCER@APCER = (0.1, 0.01)$ of our method for various α/β proportions and bona fide images selection in different protocols.

6.1. Fused Classification Balance

For effective convergence and further morphing detection, our method requires choosing the proper balance between the elements of the loss function. Namely the balance between $\alpha (= \alpha_1 = \alpha_2)$ and β (disbalance of α_1 and α_2 didn't demonstrate any interesting behaviour in our tests). We perform training of our method with different proportional settings also including the ablation of particular parts from the overall loss. Our experiments demonstrate (see Fig. 6 and Tab. 1, 2) that by varying α/β proportion it is possible to achieve some optimal performance of morphing detection in different protocols. Our strategy allows generalizing the detection of morphing even to the images, which are generated with GANs even accounting that this type of morphing is totally unseen in the training.

On the edge case with excluded main loss function driver (namely binary morph/bona fide classification), our method demonstrates the almost random detection decision. At the same time, ablation of the regularisation ($\beta = 0$) also leads to bad performance, which we relate with the overfitting on the trivial binary classification learning task.

Summing up, we can conclude that our strategy allows

learning such face features which are discriminative by the criteria of authenticity.

6.2. Data combination experiments

Further experiments are performed with the selected proportion $\alpha/\beta = 0.2$ in order to understand the impact of selfmorphing for our method.

In comparison to the dataset selection in Section 6.1 where the collection of bona fide samples is split evenly to original and selfmorphs, we test two more options where these particular parts are ablated from the total dataset.

Our results (see Fig. 7 and Tab. 1,2) proves the significant importance of selfmorphs in our strategy. Utilizing selfmorphs at the training stage allows to reduce the emphasis of the detection of facial blending artefacts and shift it to the behaviour of the deep feature for generalizing to unseen types of attacks.

6.3. NIST FRVT MORPH Results

We have performed the comparison of the results of our method and the state of the art face morphing detection approaches with NIST FRVT MORPH Benchmark (Report of October 28, 2021) [35].

Method	APCER@BPCER = δ							
	P1		P2		P3		P4	
	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$
Aghdaie <i>et al.</i> [1]	0.965	0.998	0.923	0.991	0.015	0.200	0.271	0.721
Debiasi <i>et al.</i> [12]	0.049	0.823	0.994	1.000	1.000	1.000	0.985	0.994
Ramachandra <i>et al.</i> [41]	0.375	0.990	0.938	0.985	0.159	0.998	0.936	0.996
Scherhag <i>et al.</i> [49]	1.000	1.000	0.997	1.000	0.996	1.000	0.993	1.000
Lorenz <i>et al.</i> [29]	0.380	1.000	0.966	1.000	0.819	1.000	0.971	0.995
Ferrara <i>et al.</i> [19]	0.477	0.999	0.978	1.000	0.037	0.810	0.420	0.777
Ours	0.434	0.686	0.842	0.954	0.323	0.639	0.499	0.805

Table 3. Comparison with the state of the art single image morphing detection methods by APCER@BPCER = (0.1, 0.01).

Method	APCER@BPCER = δ							
	P1		P2		P3		P4	
	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$	$\delta = 0.1$	$\delta = 0.01$
Scherhag <i>et al.</i> [50]	0.109	1.000	0.094	1.000	0.031	1.000	0.093	1.000
Lorenz <i>et al.</i> [29]	0.432	1.000	0.634	1.000	0.168	1.000	0.732	1.000
Scherhag <i>et al.</i> [49]	0.208	1.000	0.927	1.000	0.451	1.000	0.934	1.000
Ours	0.865	0.967	0.948	0.981	0.815	0.929	0.861	0.987

Table 4. Comparison with the state of the art differential morphing detection methods by APCER@BPCER = (0.1, 0.01).

We select the model with $\alpha/\beta = 0.2$ from Section 6.1 as our best model and present results of comparison in several protocols:

- *P1* - Visa-Border (25727 Morphs)
- *P2* - Manual (323 Morphs)
- *P3* - MIPGAN-II (2464 Morphs)
- *P4* - Print + Scanned (3604 Morphs)

As bona fide samples all protocols utilize a large collection of 1047389 Bona Fide images. The comparison is performed by the metrics APCER@BPCER = (0.1, 0.01).

6.4. Single Image MAD

First, we perform the comparison in the target single image morphing detection scenario (see Table 3).

MorDeepy outperforms other techniques in detecting landmark-based morphs and challenging manual morphs and achieves comparable results in other protocols.

Also, our method does not demonstrate bias to a particular morphing generative strategy and has the most stable performance across all protocols in comparison to other approaches.

It is important to note that these results are achieved by utilizing a rather straightforward and simple morphing technique during training (without any adaptation to realistic scenario or modifications for removing artefacts), which proves that our method allows generalizing morphing detection to various unseen generative approaches by focusing on deep face features behaviour.

6.5. Differential MAD

The suitability of the approach for the differential scenario was previously mentioned. We perform the straightforward application of our method to the differential detection and compare with several SOTA methods (see Table 4). In order to do it the *Second network* (see Fig. 1) receives the life capture image (instead of the same image as the *First network*) on the testing stage.

The comparison demonstrates that our method has more regular characteristics and outperforms other ones by APCER on low demanding BPCER. These results are achieved with zero effort of training our method in a differential manner, which proves that the extracted deep authentically discriminative features are not only characteristic for a particular sample but are generalised to the identity.

7. Conclusion

We introduce a novel deep learning strategy for single image face morphing detection, which implies utilising a complex classification task. It is directed onto learning the deep facial features, which carry information about the authenticity of these features. Our method achieved the state of the art performance and demonstrated a prominent ability for generalising the task of morphing detection to unseen scenarios (like GAN morphs and print/scan morphs).

Our work also introduces several additional contributions, which are the public and easy-to-use face morphing detection benchmark and the results of our wild datasets filtering strategy.

In our further work, we will focus on improving the performance by applying more sophisticated morphing techniques during training and on explicit adapting our method to the differential scenario, which will require sophisticated sampling strategies.

References

- [1] Poorya Aghdaie, Baaria Chaudhary, Sobhan Soleymani, Jeremy M. Dawson, and Nasser M. Nasrabadi. Attention Aware Wavelet-based Detection of Morphed Face Images. *2021 IEEE International Joint Conference on Biometrics (IICB)*, pages 1–8, 2021. [2](#), [8](#)
- [2] Xiang An, Xuhan Zhu, Yuan Gao, Yang Xiao, Yongle Zhao, Ziyong Feng, Lan Wu, Bin Qin, Ming Zhang, Debing Zhang, and Ying Fu. Partial FC: Training 10 Million Identities on a Single Machine. In *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV) Workshops*, pages 1445–1449, October 2021. [4](#)
- [3] Artificial Intelligence Laboratory of FEI in São Bernardo do Campo, São Paulo, Brazil. FEI face database, 2006. <https://fei.edu.br/~cet/facedatabase.html>. (accessed: November 1, 2021). [6](#)
- [4] Raghav Bansal, Gaurav Raj, and Tanupriya Choudhury. Blur image detection using laplacian operator and open-cv. In *2016 International Conference System Modeling Advancement in Research Trends (SMART)*, pages 63–67, 2016. [4](#)
- [5] Guido Borghi, Annalisa Franco, Gabriele Graffetti, and Davide Maltoni. Automated artifact retouching in morphed images with attention maps. *IEEE Access*, 9:136561–136579, 2021. [5](#)
- [6] Guido Borghi, Emanuele Pancisi, Matteo Ferrara, and Davide Maltoni. A double siamese framework for differential morphing attack detection. *Sensors*, 21:3466, 05 2021. [2](#)
- [7] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman. Vggface2: A dataset for recognising faces across pose and age. In *International Conference on Automatic Face and Gesture Recognition*, 2018. [4](#)
- [8] Sumit Chopra, Raia Hadsell, and Yann LeCun. Learning a similarity metric discriminatively, with application to face verification. *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05)*, 1:539–546 vol. 1, 2005. [2](#)
- [9] N. Damer, A. M. Saladié, A. Braun, and A. Kuijper. MoR-GAN: Recognition Vulnerability and Attack Detectability of Face Morphing Attacks Created by Generative Adversarial Network. In *2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–10, 2018. [2](#)
- [10] N. Damer, A. M. Saladié, S. Zienert, Y. Wainakh, P. Terhörst, F. Kirchbuchner, and A. Kuijper. To Detect or not to Detect: The Right Faces to Morph. In *2019 International Conference on Biometrics (ICB)*, pages 1–8, 2019. [4](#)
- [11] Naser Damer, Noémie Spiller, Meiling Fang, Fadi Boutros, Florian Kirchbuchner, and Arjan Kuijper. PW-MAD: Pixel-wise Supervision for Generalized Face Morphing Attack Detection. *ArXiv*, abs/2108.10291, 2021. [2](#), [4](#)
- [12] Luca Debiasi, Ulrich Scherhag, Christian Rathgeb, Andreas Uhl, and Christoph Busch. PRNU-based detection of morphed face images. *2018 International Workshop on Biometrics and Forensics (IWBF)*, pages 1–7, 2018. [2](#), [8](#)
- [13] Lisa DeBruine and Benedict Jones. Face research lab london set, May 2017. https://figshare.com/articles/dataset_Face_Research_Lab_London_Set/5047666/3. (accessed: November 1, 2021). [6](#)
- [14] J. Deng, J. Guo, N. Xue, and S. Zafeiriou. ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 4685–4694, 2019. [2](#), [3](#)
- [15] Bernadette Dorizzi, Raffaele Cappelli, Matteo Ferrara, Dario Maio, Davide Maltoni, Nesma Houmani, Sonia Garcia-Salicetti, and Aurélien Mayoue. Fingerprint and On-Line Signature Verification Competitions at ICB 2009. In *Advances in Biometrics : Third International Conference, ICB 2009, Alghero, Italy*, volume 5558, 06 2009. [5](#)
- [16] Ted Dustone. New face morphing database for vulnerability research, 2017. <https://www.linkedin.com/pulse/new-face-morphing-dataset-vulnerability-research-ted-dunstone>. (accessed: November 1, 2021). [6](#)
- [17] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. The magic passport. *IJCB 2014 - 2014 IEEE/IAPR International Joint Conference on Biometrics*, 12 2014. [1](#), [2](#)
- [18] M. Ferrara, A. Franco, and D. Maltoni. Face demorphing. *IEEE Transactions on Information Forensics and Security*, 13(4):1008–1017, 2018. [2](#)
- [19] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. Face morphing detection in the presence of printing/scanning and heterogeneous image sources. *IET Biometrics*, 10, 02 2021. [2](#), [8](#)
- [20] Yandong Guo, Lei Zhang, Yuxiao Hu, Xiaodong He, and Jianfeng Gao. MS-Celeb-1M: A Dataset and Benchmark for Large-Scale Face Recognition. In *Proceedings of ECCV*, volume 9907, pages 87–102, 10 2016. [4](#)
- [21] K. He, X. Zhang, S. Ren, and J. Sun. Deep residual learning for image recognition. In *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 770–778, Las Vegas, NV, USA, June 2016. IEEE. [6](#)
- [22] J. Hernandez-Ortega, J. Galbally, J. Fierrez, R. Haraksim, and L. Beslay. FaceQnet: Quality Assessment for Face Recognition based on Deep Learning. In *2019 International Conference on Biometrics (ICB)*, pages 1–8, 2019. [4](#)
- [23] Yuge Huang, Yuhan Wang, Ying Tai, Xiaoming Liu, Pengcheng Shen, Shaoxin Li, Jilin Li, and Feiyue Huang. CurricularFace: Adaptive Curriculum Learning Loss for Deep Face Recognition. In *The IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, June 2020. [3](#)
- [24] International Organization for Standardization. ISO/IEC 30107-3:2017. Information Technology—Biometric Presentation Attack Detection — Part 3: Testing and Reporting. ISO/IEC JTC 1/SC 37 Biometrics, 09 2017. [6](#)
- [25] Chi Jin, Ruochun Jin, Kai Chen, and Yong Dou. A community detection approach to cleaning extremely large face

- database. *Computational intelligence and neuroscience*, 2018, 2018. 4
- [26] Biometric System Laboratory. UBO-Morpher, 2018. <http://biolab.csr.unibo.it/Research.asp>. (accessed: November 1, 2021). 2
- [27] W. Liu, Y. Wen, Z. Yu, M. Li, B. Raj, and L. Song. SphereFace: Deep Hypersphere Embedding for Face Recognition. In *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 6738–6746, 2017. 2
- [28] Moment Media LLC. FaceFusion application, 2010. www.wearemoment.com/FaceFusion/. (accessed: November 1, 2021). 2
- [29] S. Lorenz, U. Scherhag, C. Rathgeb, and C. Busch. Morphing attack detection: A fusion approach. In *IEEE Fusion*, 2021. 2, 8
- [30] A. Martinez and Robert Benavente. The AR face database. *Tech. Rep. 24 CVC Technical Report*, 01 1998. 6
- [31] I. Medvedev, N. Gonçalves, and L. Cruz. Biometric System for Mobile Validation of ID And Travel Documents. In *2020 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–5, 2020. 1
- [32] A. Mittal, A. K. Moorthy, and A. C. Bovik. No-reference image quality assessment in the spatial domain. *IEEE Transactions on Image Processing*, 21(12):4695–4708, 2012. 4
- [33] Tom Neubert, Christian Kraetzer, and Jana Dittmann. A Face Morphing Detection Concept with a Frequency and a Spatial Domain Feature Space for Images on eMRTD. In *Proceedings of the ACM Workshop*, pages 95–100, 07 2019. 2
- [34] Tom Neubert, Andrey Makrushin, Mario Hildebrandt, Christian Kraetzer, and Jana Dittmann. Extended stirtrace benchmarking of biometric and forensic qualities of morphed face images. *IET Biometrics*, 7(4):325–332, 2018. 6
- [35] NIST. NIST FRVT MORPH. https://pages.nist.gov/frvt/html/frvt_morph.html. (accessed: November 1, 2021). 5, 7
- [36] NIST. International Face Performance Conference, 2020. <https://www.nist.gov/news-events/events/2020/10/international-face-performance-conference-ifpc-2020>. (accessed: November 1, 2021). 1
- [37] P. Jonathon Phillips, P.J. Flynn, T. Scruggs, Kevin Bowyer, Jin (Kyong) Chang, K. Hoffman, J. Marques, Jaesik Min, and W. Worek. Overview of the Face Recognition Grand Challenge. In *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, volume 1, pages 947–954, 07 2005. 3
- [38] R. Raghavendra, K. B. Raja, and C. Busch. Detecting morphed face images. In *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–7, 2016. 2
- [39] Ramachandra Raghavendra, Kiran B. Raja, Sushma Venkatesh, and Christoph Busch. Transferable Deep-CNN Features for Detecting Digital and Print-Scanned Morphed Face Images. *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 1822–1830, 2017. 2
- [40] Kiran Raja, Matteo Ferrara, Annalisa Franco, Luuk Spreeuwiers, Ilias Batskos, Florens Wit, Marta Gomez-Barrero, Ulrich Scherhag, Daniel Fischer, Sushma Venkatesh, Jag Mohan Singh, Guoqiang Li, Loïc Bergéron, Sergey Isadskiy, R. Raghavendra, Christian Rathgeb, Dinusha Frings, Uwe Seidel, Fons Knopjes, and Christoph Busch. Morphing Attack Detection - Database, Evaluation Platform and Benchmarking. *IEEE Transactions on Information Forensics and Security*, PP:1–1, 11 2020. 5
- [41] Raghavendra Ramachandra, Sushma Venkatesh, Kiran Raja, and Christoph Busch. Towards making morphing attack detection robust using hybrid scale-space colour texture features. In *2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA)*, pages 1–8, 2019. 2, 8
- [42] The Community Research and Development Information Service. Image Manipulation Attack Resolving Solutions, 2020. <https://cordis.europa.eu/project/id/883356>. (accessed: November 1, 2021). 1
- [43] N. Ruiz, E. Chong, and J. Rehg. Fine-grained head pose estimation without keypoints. In *The IEEE Conference on Conference on Computer Vision and Pattern Recognition (CVPR) Workshops*, 06 2018. 4
- [44] Olga Russakovsky, Jia Deng, Hao Su, Jonathan Krause, Sanjeev Satheesh, Sean Ma, Zhiheng Huang, Andrej Karpathy, Aditya Khosla, Michael Bernstein, Alexander C. Berg, and Li Fei-Fei. ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision (IJCV)*, 115(3):211–252, 2015. 2
- [45] Eklavya Sarkar, Pavel Korshunov, Laurent Colbois, and Sébastien Marcel. Vulnerability analysis of face morphing attacks from landmarks and generative adversarial networks. *arXiv preprint*, Oct. 2020. 6
- [46] Mallick Satya. Face Morph Using OpenCV, 2016. www.learnopencv.com/face-morph-using-opencv-cpp-python/. (accessed: November 1, 2021). 2
- [47] 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*, 1(4):302–317, 2019. 2
- [48] U. Scherhag, R. Raghavendra, K. B. Raja, M. Gomez-Barrero, C. Rathgeb, and C. Busch. On the vulnerability of face recognition systems towards morphed face attacks. In *2017 5th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2017. 2
- [49] Ulrich Scherhag, Christian Rathgeb, and Christoph Busch. Morph Detection from Single Face Image: a Multi-Algorithm Fusion Approach. In *Proceedings of the 2018 2nd International Conference on Biometric Engineering and Applications*, pages 6–12, 05 2018. 8
- [50] U. Scherhag, C. Rathgeb, J. Merkle, and C. Busch. Deep Face Representations for Differential Morphing Attack Detection. *IEEE Transactions on Information Forensics and Security*, 15:3625–3639, 2020. 2, 8
- [51] School of Natural Sciences University of Stirling. Psychological Image Collection of Stirling, 1998. <http://pics.stir.ac.uk>. (accessed: November 1, 2021). 6

- [52] F. Schroff, D. Kalenichenko, and J. Philbin. FaceNet: A unified embedding for face recognition and clustering. In *2015 IEEE Conference CVPR*, pages 815–823, 2015. [2](#)
- [53] Clemens Seibold, Wojciech Samek, Anna Hilsmann, and Peter Eisert. Detection of Face Morphing Attacks by Deep Learning. In *Proceedings of Digital Forensics and Watermarking: 16th International Workshop, IWDW 2017*, pages 107–120, 07 2017. [2](#)
- [54] Y. Shi and A. Jain. Probabilistic Face Embeddings. In *2019 IEEE/CVF International Conference on Computer Vision (ICCV)*, pages 6901–6910, 2019. [3](#)
- [55] Yichun Shi, Xiang Yu, Kihyuk Sohn, Manmohan Chandraker, and Anil Jain. Towards Universal Representation Learning for Deep Face Recognition. In *Proceedings of 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 6816–6825, 06 2020. [3](#)
- [56] J. Sun, W. Yang, J. Xue, and Q. Liao. An Equalized Margin Loss for Face Recognition. *IEEE Transactions on Multimedia*, pages 1–1, 2020. [2](#)
- [57] Y. Sun, Y. Chen, X. Wang, and X. Tang. Deep Learning Face Representation by Joint Identification-Verification. In *NIPS*, 2014. [2](#)
- [58] Y. Sun, X. Wang, and X. Tang. Deep Learning Face Representation from Predicting 10,000 Classes. In *2014 IEEE Conference on Computer Vision and Pattern Recognition*, pages 1891–1898, 2014. [2](#)
- [59] Y. Sun, X. Wang, and X. Tang. Deeply learned face representations are sparse, selective, and robust. *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 2892–2900, 2015. [2](#)
- [60] João Tremoço, Iurii Medvedev, and Nuno Gonçalves. QualFace: Adapting Deep Learning Face Recognition for ID and Travel Documents with Quality Assessment. In *2021 International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–6, 2021. [3, 4](#)
- [61] Sushma Krupa Venkatesh, Haoyu Zhang, Raghavendra Ramachandra, K. Bommanna Raja, Naser Damer, and Christoph Busch. Can GAN Generated Morphs Threaten Face Recognition Systems Equally as Landmark Based Morphs? - Vulnerability and Detection. *2020 8th International Workshop on Biometrics and Forensics (IWBF)*, pages 1–6, 2020. [2](#)
- [62] L. Wandzik, G. Kaeding, and R. V. Garcia. Morphing Detection Using a General- Purpose Face Recognition System. In *2018 26th European Signal Processing Conference (EUSIPCO)*, pages 1012–1016, 2018. [2](#)
- [63] H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, and W. Liu. CosFace: Large Margin Cosine Loss for Deep Face Recognition. In *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 5265–5274, 2018. [2](#)
- [64] Yandong Wen, Kaipeng Zhang, Zhifeng Li, and Yu Qiao. A Discriminative Feature Learning Approach for Deep Face Recognition. In Bastian Leibe, Jiri Matas, Nicu Sebe, and Max Welling, editors, *Computer Vision – ECCV 2016*, pages 499–515, Cham, 2016. Springer International Publishing. [2](#)
- [65] Dong Yi, Zhen Lei, Shengcai Liao, and S. Li. Learning face representation from scratch. *ArXiv*, abs/1411.7923, 2014. [4](#)
- [66] D. Zeng, H. Shi, H. Du, J. Wang, Z. Lei, and T. Mei. NPCFace: A Negative-Positive Cooperation Supervision for Training Large-scale Face Recognition. *CoRR*, abs/2007.10172, 2020. [3](#)
- [67] Haoyu Zhang, S. Venkatesh, R. Ramachandra, K. Raja, Naser Damer, and C. Busch. MIPGAN - Generating Robust and High Quality Morph Attacks Using Identity Prior Driven GAN. *ArXiv*, abs/2009.01729, 2020. [2](#)
- [68] L. Zhang, L. Zhang, and L. Li. Illumination Quality Assessment for Face Images: A Benchmark and a Convolutional Neural Networks Based Model. *Lecture Notes in Computer Science*, 10636 LNCS:583–593, 2017. [4](#)
- [69] Zheng Zhu, Guan Huang, Jiankang Deng, Yun Ye, Junjie Huang, Xinze Chen, Jiagang Zhu, Tian Yang, Jiwen Lu, Dalong Du, and Jie Zhou. WebFace260M: A Benchmark Unveiling the Power of Million-Scale Deep Face Recognition. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 10492–10502, June 2021. [4](#)