Detecting Morphed Face Images Using Facial Landmarks

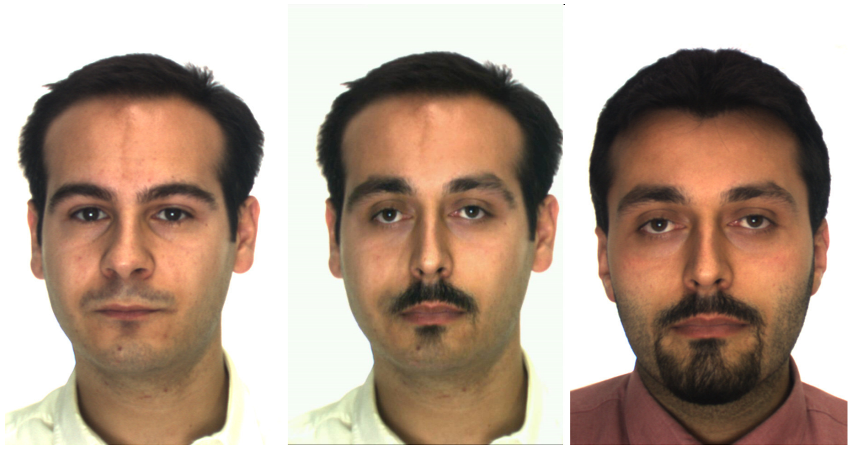
Ulrich Scherhag[1], Dhanesh Budhrani[2], Marta Gomez-Barrero[1], and Christoph Busch[1]

[1] Hochschule Darmstadt, da/sec – Security Research Group, Darmstadt, Germany,
{ulrich.scherhag, marta.gomez-barrero, christoph.busch} @h-da.de
[2] Danmarks Tekniske Universitet, DTU Compute, Kongens Lyngby, Denmark,
dhanesh.budhrani@gmail.com

Abstract. With the widespread deployment of automatic biometric recognition systems, some security issues have been unveiled. In particular, face recognition systems have been recently shown to be vulnerable to attacks carried out with morphed face images. Such synthetic images can be defined as the fusion of the face images of two (or more) different subjects. The associated risk lies on the ability of multiple subjects to be positively verified with a single enrolled morphed face image. As common texture based features have limited capabilities to tackle this problem, we propose a novel method for morphed face image detection, based on the computation of the differences between the landmarks of a probe bona fide (i.e., captured under supervision) image of the attacker, and the landmarks of the enrolled image (i.e., the suspected morphed image). In this work, a new database is created for the experiments, comprising both bona fide and morphed images created with two different morphing methods. The experiments show that for the detection task, the proposed algorithm achieves Equal Error Rates at 32.7%.

1 Introduction

Biometrics refers to the automated recognition of individuals based on their biological and behavioural characteristics [1]. Due to their convenience, Face Recognition Systems (FRSs) are widely-used for user authentication, e.g. for Automated Border Control (ABC) based on the biometric passport (ePass) as defined in [2]. The main advantage of biometric systems over common authentication systems is the unique link, which is established between the Machine Readable Travel Document (MRTD), containing the biometric reference, and the data subject (i.e. the owner of the electronic passport). However, current research [3] [4] has revealed a weakness of the passport issuance process, which allows to inject manipulated images into the biometric database, e.g. the ePass. The key deficiency in the passport issuance process lies in the way the facial picture of an applicant is processed. In many countries, the applicant provides a printed facial image, which is scanned and then digitally transferred to the passport production site. Thus, an artificial facial image, resembling two or more subjects in their visual and feature representation (see Figure 1b), can be submitted to the passport issuance authority. If the artificial image is used for verification, both constituting subjects can be verified successfully. This type of attack is referred to as morphed face image attack.



(a) Subject 1 (b) Morph Subj. 1 + 2 (c) Subject 2

Fig. 1: Example of face morphing

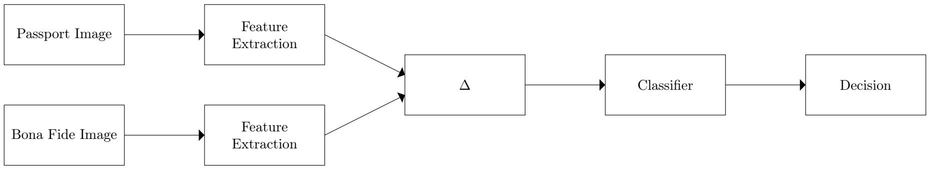


Fig. 2: Scheme for differential morphing detection

The feasibility of this attack was first analyzed in [3] [4] on a dataset of 12 morphed face images on two Commercial-Of-The-Shelf (COTS) Face Recognition Systems (FRSs), and verified recently in [5] [6] on a larger dataset of 450 morphed images. The datasets used in [3] [4] [5] [6] were generated utilizing GIMP and GAP. In addition, a theoretical framework for the estimation of the success of morphing attacks on a specific system was presented in [7].

In [5], a first detection system for morphed face images was proposed, based on well-established multi-purpose image descriptors. The method aims at detecting morphed face images without a bona fide reference, hence referred to as *no-reference* morphed face image detection in the remainder of this article. A bona fide presentation is defined in ISO/IEC 30107-3 as a "interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system" [8]. Among the analyzed feature extractors, Binarized Statistical Image Features (BSIF) [9] with a filter of 11×11 pixels and 12-bit performed best on the given dataset.

The morphed face image attack detection algorithm proposed in [5] focuses on digital samples, as used for ePass renewal in New-Zealand, where face images are uploaded electronically. However, the application process of the ePass in many countries (e.g.

most of the European Schengen states) still requires a printed face image that will be handed over to the public authority office during the application process.

Taking this real-world scenario of printed and scanned face images into account, [6] focuses on the effect of the print-scan process of a digitally morphed face image on FRSs and morphing detection. The print and scan process adds some noise and granularity to the face image, which affects the performance of both FRSs and morphed face image detection algorithms. Despite such noise, it was shown in [6] that morphed face images pose a severe threat to face recognition systems even after printing and scanning, and many well-established multi-purpose image descriptors are not suitable for detecting ether digital nor printed and scanned morphed face images.

Ferrara *et al.* [10] proposed face demorphing for morph detection employing a trusted live capture in addition to the questioned sample. Scherhag *et al.* [11] analyzed multiple general purpose image feature extractors in this differential scenario. Further, Hildebrandt *et al.* [12] suggest to employ generic image forgery detection techniques, in particular multi-compression anomaly detection, to reliably detect morphed facial images. Kraetzer *et al.* [13] evaluate the feasibility of detecting facial morphs with key-point descriptors and edge operators. However for the current state of the art detection accuracy is very limited and generalisation capabilities of detectors are yet unexplored.

In this paper we propose a novel framework for the detection of morphed face images based on facial landmarks. In contrast to previously proposed *no-reference* methods, we compare a bona fide face image with the passport image we want to classify (see Figure 2). This approach will be referred to as differential morphing detection. The required bona fide face image could be either captured at the ABC-Gate or during the application process at the public authority office. In either scenario the assumption holds that the capture process is semi-supervised (i.e. via video surveillance) or supervised (i.e. in the passport application office).

The paper is organized as follows: The differential morphed face image detection framework is introduced in Section 2. In Section 3 we present the new morphed face image database, and the experiments conducted with the framework are described in Section 4. Final conclusions are drawn in Section 5.

2 Proposed Algorithm

The algorithm is motivated by the observations made in [14], that meaningful landmarks are suitable for face recognition. In addition, landmark based face recognition systems are robust to ageing, which is an important property for passport scenarios [14]. The position of each landmark of the morphed face image, $l_m(x_m, y_m)$, is situated between the corresponding landmarks, $l_i(x_i, y_i)$ and $l_j(x_j, y_j)$, of both constituting subjects, i and j:

$$\begin{aligned} x_m &= (1-\alpha)x_i + \alpha x_j \\ y_m &= (1-\alpha)y_i + \alpha y_j, \end{aligned} \tag{1}$$

where α defines the ratio of the contribution of Subject j to the morph, and consequently $1-\alpha$ describes the contribution of Subject i. It can be assumed that the intra-subject

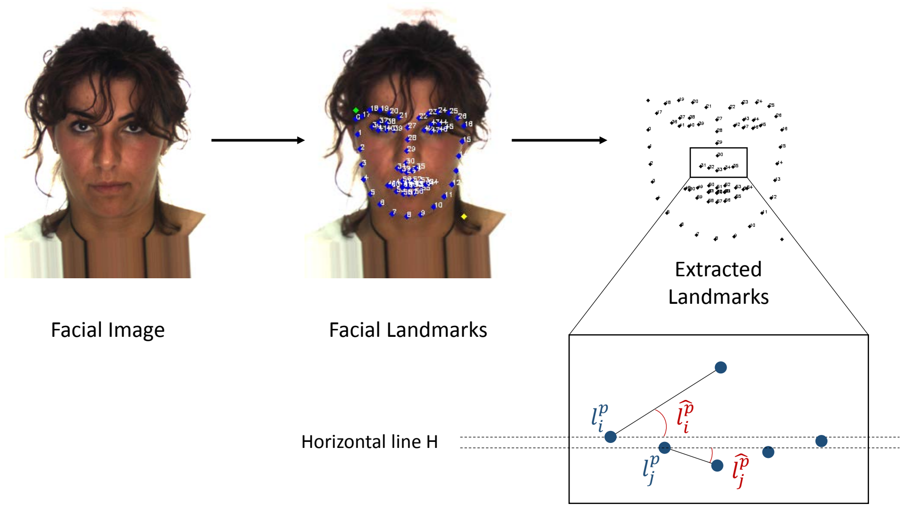


Fig. 3: Facial landmarks and angle calculation

variance of landmarks extracted from bona fide images is smaller than the variance between the landmarks of the morphed image and its contributing subjects. Based on this assumption, two feature extraction methods are designed: (1) distance based, and (2) angle based.

(1) **Distance based:** The landmarks of both images (bona fide image, I_b, and passport image, I_p) are determined utilizing the facial landmark predictor of dlib [15], which returns the absolute position of 68 facial landmarks ($l_0 \dots l_{67}$), as depicted in Figure 3. In order to achieve a scaling-robust system, the landmarks are normalized to a range between 0 and 1. To that end, the green and yellow dots depict the upper-left $(0.0, 0.0)$ and lower-right $(1.0, 1.0)$ boundaries for the normalization. In the next step, the Euclidean distance of the relative position of each landmark l_i between both images I_p and I_b is calculated (depicted in red in Figure 4), resulting in a feature vector of length 2278, which referred to as distance features.

(2) **Angle based:** Depending on the face region, pose and expression, the position of the landmarks varies. Even if the images utilized in this work are normalized according to ICAO recommendations [2], minor pose variations and expressions can not be completely avoided. Those minor changes in the positioning of the landmarks affect the calculation of the distance, thereby decreasing the morphing detection accuracy. Therefore, in order to achieve a more robust feature extractor, the angles of each landmark, l_i, to a predefined neighbor (in order to obtain the most discriminative dependencies) are calculated as $\hat{l}_i$ (depicted in Figure 3). The corresponding angles of I_p and I_b are compared as shown in Figure 4. In order to avoid unrealistic high differences when the angles cross the horizontal line, the difference is calculated as:

$$d(\hat{l}_i^p, \hat{l}_i^b) = min(|\hat{l}_i^p - \hat{l}_i^b|, 360 - |\hat{l}_i^p - \hat{l}_i^b|), i = 0 \dots 67, \quad (2)$$

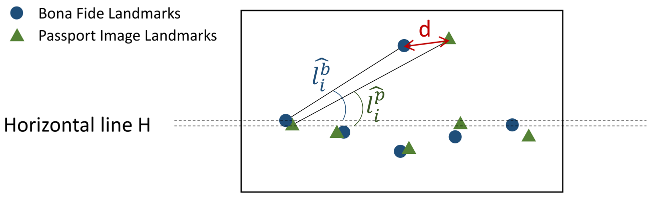


Fig. 4: Landmark based feature extraction

returning a positive difference between 0° and 180°. The resulting feature vector has a length of length 68 and will be referred to as angles features.

During this work, multiple classifiers have been tested. It turned out, that the classification task can not be solved by linear classifiers, e.g. linear Support Vector Machine (SVM). Therefore, and in order to have a more comprehensive evaluation, three different classifiers are employed:

Random Forest with 500 estimators.
SVM without kernel
SVM with a Radial Basis Function (RBF) kernel

The best performance could be achieved employing an SVM with RBF kernel.

3 Databases

The databases created for previous works are either non-public, or do not comprise enough independent bona fide images to carry out a fair evaluation. Thus, for this work, a new database was constructed utilising two different morphing techniques. The new database builds upon the publicly available ARface database [16], which comprises 136 subjects. In order to generate realistic morphs, all frontal faces with neutral expression are selected[3]. The selected 493 images from 120 subjects are processed according to the recommendations of the International Civil Aviation Organisation (ICAO) [2]. For the normalization process, the landmark detection algorithm of dlib [15] is employed to determine the centers of the eyes, according to which the images are horizontally aligned. Subsequently, the image is cropped according to [17] and downsized to 720 × 960 pixels, which is 5 times higher than the minimal required resolution for passport images.

For the experiments, the subjects are divided into two subsets: training and testing, each comprising 60 subjects. While the first image of each subject is reserved for the morphing attack creation, the remaining images are utilized as bona fide samples. The

[3] In order to support reproducible research, the mapping of the images will be provided via `URLisremovedforthereviewprocess`.

Table 1: Composition of created database

#	Training	Testing
Subjects	60	60
Bona Fide	215	223
Morphs	2703	2098

total composition of the database is depicted in Table 1. The morphs are generated utilizing the dlib landmark detector [15] and delaunay triangulation and referred to as OpenCV Morphs.

4 Experiments and results

The experiments conducted in this work are evaluated according the metrics for presentation attack detection defined in ISO/IEC 30107-3 [8]:

Attack Presentation Classification Error Rate (APCER): proportion of attack presentations using the same Presentation Attack Instrument (PAI) species incorrectly classified as bona fide presentations in a specific scenario.

Bona fide Presentation Classification Error Rate (BPCER): proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario.

In addition, the following metrics are reported:

BPCER10: BPCER observed at a fixed APCER of 10%.
Detection Equal Error Rate (D-EER): the operating point in which APCER and BPCER are equal.

In addition to the aforementioned metrics and in order to evaluate the quality of the generated database, the Mated Morph Presentation Match Rate as well as the Relative Morph Match Rate (RMMR) [18] were calculated, which indicates the vulnerability of the FRS with respect to the attack. Employing the Cognitec FaceVACS-SDK [19] a ProdAvg-MMPMR of 96.7% ProdAvg-RMMR of 97.7% was computed for testing and training set.

Due to the fact that we employ a differential morphing detection scheme, we obtain many more distance-scores than samples. The number of bona fide comparisons is 315 for the testing set. The number of morph comparisons, which could be much higher, is limited to 300 to obtained a balanced classifier.

The error rates (D-EER and BPCER10) for the classifiers are summarised in Table 2. Furthermore, the Detection Error Tradeoff (DET) curves [20] are depicted in Figure 5.

In the DET-plot (Figure 5), higher error rates can be observed for the distance features compared to the angle features. The linear SVM yields slightly higher error rates compared to the SVM with RBF kernel, indicating a non-linearity of the problem.

Table 2: Performance of the proposed system

Classifier	**Features**	**D-EER**	**BPCER10**
Random Forest	Distance	45.3%	76.6%
	Angle	41.2%	67.3%
SVM (lin)	Distance	44.7%	83.0%
	Angle	43.9%	87.0%
SVM (rbf)	Distance	44.1%	84.9%
	Angle	32.7%	61.7%

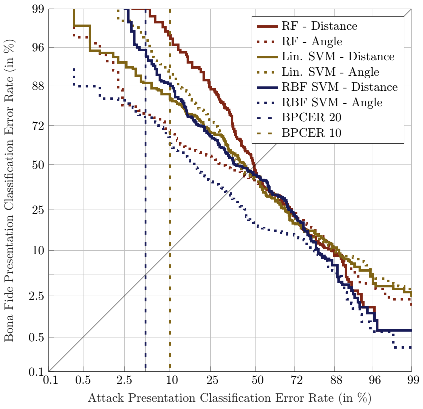


Fig. 5: Performance Evaluation of the analyzed detection algorithms

The best detection performance for all operating points is achieved by the SVM with RBF kernel, yielding a D-EER of 32.7% and BPCER10 of 61.7%. The results indicate, that some information about the morphing process can be derived from the landmarks, but due to the low overall performance, the algorithms presented in this work are still not applicable for real world applications. Thus our future work, will fuse landmark based information with complementary information derived from the image texture.

5 Conclusions

In this work a novel approach for morphed face image detection has been presented. Unlike previous detection methods, this work utilizes, in addition to the passport image submitted, a trusted bona fide facial image from the claimed data subject. Employing a Random Forest classifier, the differences of the angles between certain landmarks of passport and bona fide image are compared, yielding a D-EER of 32.7%, a fusion of both approaches might lead to lower error rate. The results achieved in this work are not suited for operational deployment, but it is a first step towards reference based morphed face image detection.

References

1. International Organization for Standardization: Information technology – Vocabulary – Part 37: Biometrics. ISO/IEC 2382-37:2012, JTC 1/SC 37, Geneva, Switzerland (2012)
2. International Civil Aviation Organization: Machine readable passports – part 9 – deployment of biometric identification and electronic storage of data in emrtds (2015)
3. Ferrara, M., Franco, A., Maltoni, D.: The magic passport. In: Proc. IEEE Int. Joint Conf. on Biometrics, IEEE (sep 2014)
4. Ferrara, M., Franco, A., Maltoni, D.: On the Effects of Image Alterations on Face Recognition Accuracy. In: Face Recognition Across the Imaging Spectrum. Springer Int. Pub. (2016)
5. Raghavendra, R., Raja, K.B., Busch, C.: Detecting Morphed Face Images. In: Proc. 8th IEEE Int. Conf. on Biometrics: Theory, Applications, and Systems. (2016)
6. Scherhag, U., Ramachandra, R., Raja, K.B., Gomez-barrero, M., Rathgeb, C., Busch, C.: On the Vulnerability and Detection of Digital Morphed and Scanned Face Images. In: Proc. Int. Workshop on Biometrics and Forensics (IWBF). (2017)
7. Gomez-Barrero, M., Rathgeb, C., Scherhag, U., Busch, C.: Is Your Biometric System Robust to Morphing Attacks? In: Proc. Int. Workshop on Biometrics and Forensics (IWBF), Coventry, IEEE (2017)
8. International Organization for Standardization: Information Technology – Biometric presentation attack detection – Part 3: Testing and reporting. ISO/IEC FDIS 30107-3:2017, JTC 1/SC 37, Geneva, Switzerland (2017)
9. Kannala, J., Rahtu, E.: BSIF: Binarized statistical image features. 21st Int. Conf. on Pattern Recognition (ICPR) (2012)
10. Ferrara, M., Franco, A., Maltoni, D.: Face demorphing. IEEE Transactions on Information Forensics and Security **13**(4) (April 2018) 1008–1017
11. Scherhag, U., Rathgeb, C., Busch, C.: Towards detection of morphed face images in electronic travel documents. In: 13th IAPR Workshop on Document Analysis Systems (DAS). (2018) 1–6
12. Hildebrandt, M., Neubert, T., Makrushin, A., Dittmann, J.: Benchmarking face morphing forgery detection: Application of stirtrace for impact simulation of different processing steps. In: Proc. Int. Workshop on Biometrics and Forensics (IWBF). (2017) 1–6
13. Kraetzer, C., Makrushin, A., Neubert, T., Hildebrandt, M., Dittmann, J.: Modeling attacks on photo-ID documents and applying media forensics for the detection of facial morphing. In: Proc. Workshop on Information Hiding and Multimedia Security (IH& MMSec). (2017) 21–32
14. Shi, J., Samal, A., Marx, D.: How effective are landmarks and their geometry for face recognition? Comput. Vis. Image Underst. **102**(2) (May 2006)
15. King, D.E.: Dlib-ml: A machine learning toolkit. Journal of Machine Learning Research **10** (2009)
16. Martinez, A.: The AR face database. Technical report, CVC Tech. Report (1998)
17. International Organization for Standardization: Information technology – Biometric data interchange formats – Part 5: Face image data. ISO/IEC 19794-5:2011, JTC 1/SC 37, Geneva, Switzerland (2011)
18. Scherhag, U., Nautsch, A., Rathgeb, C., Gomez-Barrero, M., Veldhuis, R., Spreeuwers, L., Schils, M., Maltoni, D., Grother, P., Marcel, S., Breithaupt, R., Raghavendra, R., Busch, C.: Biometric systems under morphing attacks: Assessment of morphing techniques and vulnerability reporting. In: Int. Conf. of the Biometrics Special Interest Group (BIOSIG). (2017) 1–12
19. Cognitec: FaceVACS-SDK. http://www.cognitec.com Accessed: 2017-04-28.
20. Martin, A., et al.: The DET Curve in Assessment of Detection Task Performance. Proc. Eurospeech (1997)