Face Morphing Detection: An Approach Based on Image Degradation Analysis

Tom Neubert(✉)

Research Group Multimedia and Security, Otto-von-Guericke-University Magdeburg, P.O. Box 4120, 39016 Magdeburg, Germany
tom.neubert@iti.cs.uni-magdeburg.de

Abstract. In 2014 a novel identity theft scheme targeting specific application scenarios in face biometrics was introduced. In this scheme, a so called face morph melts two or more face images of different persons into one image, which is visually similar to multiple real world persons. Based on this non authentic image, it is possible to apply for an image based identity document to be issued by a corresponding authority. Thus, multiple persons can use such a document to pass image based person verification scenarios with a single document containing an artificially weakened template. Currently there is no reliable existing security mechanism to detect this attack.

This paper introduces a novel detection approach for face morphing forgeries based on a continuous image degradation. This is considered relevant because the degradation approach creates multiple artificial self-references and measures the "distance" from these references to the input. A small distance (significantly smaller than the one to be expected from a pristine image) could be considered as an anomaly here, indicating media manipulations (e.g. caused by morphing). Our degradation process is based on JPEG compression with different compression values. The evaluation results of our detection approach are classification accuracies of 90.1% under laboratory conditions and 84.3% under real world conditions.

Keywords: Digital image forensics · Detection of face morphing attacks

1 Introduction

The face is a widespread and well accepted biometric modality for many authentification scenarios. The identity verification of a person in such scenarios is often performed by using a face image in an identification document. Due to the wide spread usage of face image based authentification scenarios, they are in the focus of various identity theft schemes.

Ferrera et al. present in their paper "The magic passport" [1] a novel identity theft scheme for face biometrics, which describes an approach allowing two or more persons pass an identity verification scenario with only one artificially weakened template in form of a "magic" passport. For this attack they create a

© Springer International Publishing AG 2017
C. Kraetzer et al. (Eds.): IWDW 2017, LNCS 10431, pp. 93–106, 2017.
DOI: 10.1007/978-3-319-64185-0_8

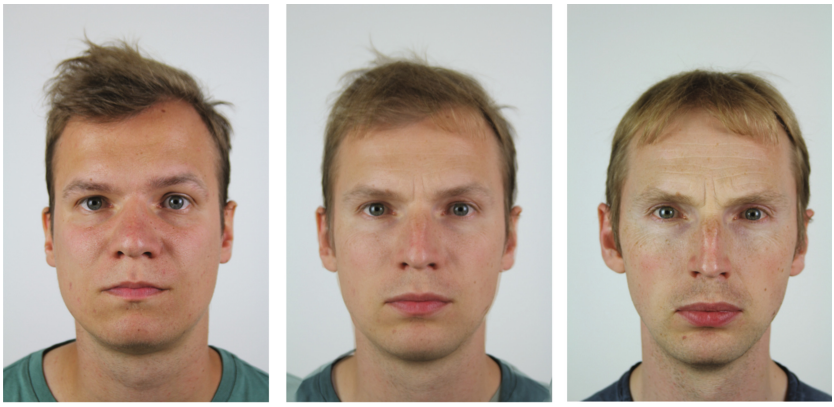

Fig. 1. Example of a manually created face morphing forgery of two different persons

so called face morph which melts two or more face images of different persons, so that it is similar to multiple real persons (see Fig. 1 for example). If this morphed image is used for the creation of an identification document, the document could successfully be used by multiple persons, whose faces are morphed in the face image integrated in the document.

Ferrera et al. figure out in [1] that the document successfully passes all optical and electronic authenticity and integrity checks. This reveals a weakness in official authentification checks, because currently there is no reliable existing security mechanism to detect this kind of attack.

In this paper, we introduce a novel detection approach for face morphing forgeries based on a continuous image degradation analysis, which can be seen as the main scientific contribution of our paper. For the image degradation process we perform a JPEG compression, with different compression values on a decompressed input file. To analyze the degradation process, we use a feature set derived from existing OpenCV (http://opencv.org) edge detecting methods. Afterwards, we compare the extracted feature values from the degraded images with the reference image (input) to describe the degradation. For genuine face images, we should observe a significant loss of edge-information in the face region because of the degradation. We assume that morphings create an anomaly here, because the loss of information through the degradation process should be significantly lower as a result of the blending operations in the morphing pipeline. These operations causes a loss of face details in the input image and the additional degradation should have a "smaller" influence on morphings than on genuine images.

Our work is structured as follows: Sect. 2 describes related work in forensics on face morphing attacks. In Sect. 3 we describe the concept for our degradation detection approach, including the feature space for our pattern recognition based detection. The next section gives an overview of our experimental dataset and

introduces the testing goals for our morphing detection experiment. Section 5 shows the results of our experiment and Sect. 6 concludes the paper with a summary and future work.

2 Related Work

In 2014 Ferrera et al. introduce in [1] a novel approach to attack face image based person verification systems with a so called face morphing attack. In their work they present a "magic passport" with a face morphed image on the photo ID document, which is created by a official authority and looks similar to multiple real world persons.

The vulnerability exploited in this attack is the fact, that in many countries self acquired photos are allowed to be submitted while document generation. So this passport could for example be successfully used by those multiple person on a border control because the document is absolutely authentic and will pass all optical and electronic authenticity and integrity checks. Ferrera et al. present no security mechanism to detect this attack and because of that it is important to find a detection mechanism for this easy to realize attack.

In [4] the relevance of the attack from [1] is confirmed. In this work Ferrera et al. analyze the performance of three automatic face recognition (AFR) systems to reject face morphed images. The results are frightening, the evaluated AFR systems are not able to distinguish between morphed and genuine faces.

The morphing attack from [1] uses manual generated morphed faces with GIMP/GAP (www.gimp.org), which makes the morphing process time consuming and allows only a small number of generated morphings. Therefore, they create an automated process for the generation of visually faultless facial morphings in [2]. This allows the generation of big experimental data, which is essential for the training of forensic detectors. The quality of these morphings is verified with an AFR (Luxand FaceSDK 6.1 [19]) system. The AFR system accepts "11.78% of morphings against any of genuine images at the decision threshold of 1% false acceptance rate". In addition we present a subjective experiment which demonstrates that humans ability to differ between these automatic generated morphings and genuine faces is close to random guessing. These results confirm that morphings are a serious issue for document security. This automated process is used in this work for the creation of morphings for training and test data sets. We also proposed a detection approach to automatically detect morphings making use of Benford features derived from quantized DCT coefficients of JPEG images. The evaluation reveals that the distribution of the coefficients shows an anomaly with morphed images, resulting from the image pre-processing steps.

In [3] the authors benchmark the robustness of the detection approach from [2] with different post-processing techniques and anti-forensic methods. Therefore, they have generated 86614 samples based on the Utrecht Face DB [18] to analyze the influence of the applied image processing to the AFR system and the forensic detector from [2]. The evaluation shows, that the performance of the forensic detector is very critical for some kind of processing techniques. For the biometric AFR system the processing has nearly no influence.

The authors of [7] focus on masking the gender information in a face image with respect to an automated gender estimation scheme, while retaining its ability to be used by a face matcher in their work. To do so they use a morphing scheme to create a mixed image of two facial inputs. The morphing process "can be used to progressively modify the input image, such that its gender information is progressively suppressed".

Schetinger et al. assert in [5] that CFA and double JPEG compression artifacts are plausible as traces for morphing detection.

Furthermore, Raghavendra et al. introduce in [6] a morph detection approach. The approach is based on binarized statistical image features used in conjunction with a linear SVM.

In [8] the authors have evaluated the vulnerability of two different face recognition system with respect to scanned morph face images. Additionally a comparative study on different currently proposed face morph detectors is introduced.

Gomez-Barrero et al. present in their paper [9] a new framework for the evaluation of the vulnerability of biometric system to morphing attacks. The analysis implies that biometric systems are vulnerable to different kind of attacks, depending on the verification threshold and the shape of the mated and non-mated score distributions.

Despite to the research released in this field, there exists, to the best of our knowledge, no absolutely reliable detection approach for face morphing forgeries and it is a novel and promissing idea to use a degradation process for the detection of face morphing forgeries.

3 Concept of Our Morphing Detection Approach Based on Image Degradation

In this section, we introduce our detection approach based on a continuous image degradation. Basically, the approach is not a native morphing detection approach, but rather an anomaly detection approach which detects anomalies resulting from the face morphing process. The approach is based on the idea that our proposed features react sensibly to the degradation of authentic images and not so sensibly to the degradation of morphed images. We use three different corner feature detectors in the face region. Due to the degradation, the number of detected corner features should decrease significantly for authentic images. We assume that morphings have an anomaly here, as a result of blending operations in the morphing pipeline. So, the degradation should not have such a significant impact on morphed images as on authentic images. The degradation process has 3 basic steps (Step I: Pre-Processing, Step II: Feature Extraction, Step III: Normalization of the Feature Vector) and is visualized in Fig. 2.

Before we start the process with the pre-processing, we decompress and store all used images in PNG image file format to have a homogeneous base for each used input file. We recommend this format because it is lossless and well known. As pre-processing (step I), prior to feature extraction (step II), the facial landmarks are extracted from *Img* by using the *dlib* programming library version

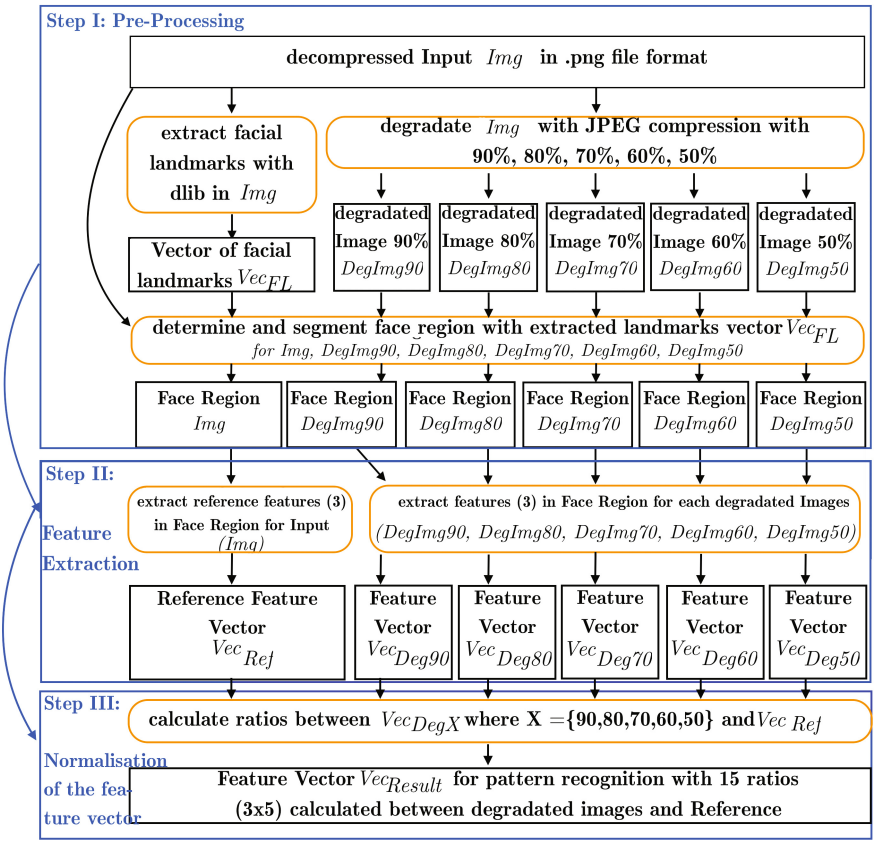

Fig. 2. Image degradation process of a single image

19.2 (http://dlib.net/). The coordinates of the facial landmarks are saved in a Vector Vec_{FL}. In parallel, we build five degradated images $DegImgX$ from Img with the following JPEG quality levels $X = \{90\%, 80\%, 70\%, 60\%, 50\%\}$.

In general, it is possible to degradate an image with other methods, for example different filtering methods, but we use the JPEG compression, because it is a standard and widespread method to degradate or compress images. Additionally, more JPEG quality parameters could be used to describe the degradation process more accurately, but we suppose that it leads to similar results. Afterwards, we use Vec_{FL} to determine and segment the convex hull of the facial landmarks for Img and $DegImgX$. Subsequently, we remove any image information outside of the determined convex hull of the face region for all used images (Img and $DegImgX$). Thus, the pre-processing results in 6 images (input Img and 5 degradated images $DegImgX$) containing only the face region of a person.

Then, the feature extraction (step II) is done in the face region of the input *Img* and of the degradated images *DegImgX*. We extract three features, the number of detected

- FAST [10],
- AGAST [11] and
- shiTomasi [12]

corner features (for example see Fig. 3). To extract these three features, we use existing methods from OpenCV version 3.1 with contributions (http://opencv.org/) with default parameterization. The extracted features from Img are used as a reference for the extracted features from the degradated images $DegImgX$. So, we save the 3 extracted features for each image in a separate feature vector (Vec_{Ref} and Vec_{DegX}). We use the corner feature detectors, because they react sensibly to the JPEG compression and seem to be well suited to describe the degradation process in images. Other feature detectors, for example SIFT [13] or SURF [14], are more robust to the degradation based on JPEG compression and therefore not well suited for our purpose.

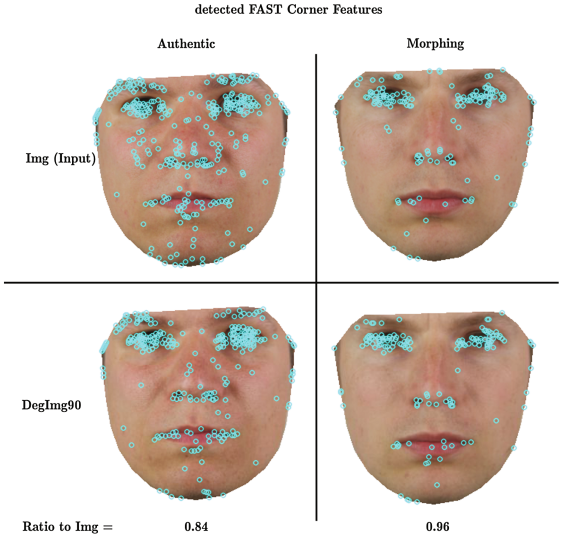

Fig. 3. Example of detected FAST corner features for an authentic sample and a morphed sample for Img and $DegImg90$

After feature extraction, the normalization of the feature vector follows in step III. Therefore, we use the absolute number of detected corner features for each of the 3 features. Basically, we calculate only the ratios between the feature vectors of the degradated images Vec_{DegX} and the reference feature vector Vec_{Ref} from the input $(\frac{Vec_{Deg90}.at(0)}{Vec_{Ref}.at(0)}, \ldots, \frac{Vec_{Deg50}.at(2)}{Vec_{Ref}.at(2)})$. In the end, we get 15

features (3 ratios for each of the 5 degradated images) for *Img*, which describe the degradation process. We intentionally get rid of further normalization steps (for example: normalization of the image resolution by dividing the number of detected corner features by the number of face pixels) in order to not distort the degradation process. The features are saved in a labeled ("Morphing" or "Authentic") feature vector Vec_{Result} for our pattern recognition based approach to detect morphed images. For the detection approach we train a two-class classification model Mod, by applying the described degradation process to all images in both classes. One class is for authentic face images and the other class for morphed face images. The experimental set up is described in Sect. 4.

4 Evaluation Goals and Setup

This section describes our pattern recognition based detection approach and gives an overview of our training and test data. Furthermore we define our evaluation goals.

4.1 Evaluation Goals

In order to evaluate our degradation process as a valid possibility to detect anomalies in morphed images, we define three evaluation goals:

- G_1 : Determine a reference accuracy of our classification model Mod for two exemplary attack realizations by a 10-fold cross validation to evaluate our designed feature space.
- G_2 : Analyze the impact of the degradation process to the feature space of Mod for authentic and morphed images.
- G_3 : Determine the detection accuracy of Mod for different test data sets, which have not been involved into training.

The three goals are addressed in three separate evaluation tests (T_1, T_2, T_3) described in the following subsection. The cross-validation in G_1 reproduces a laboratory test. Here the detector is tested under idealized conditions. We choose a 10-fold cross validation, because here the complete data of Mod is used for training and test data and it delivers more accurate results (especially with regards to outliers) than a single percentage split of the data. A higher number of folds during the cross validation is not suitable because it is more time consuming and delivers comparable results. G_2 checks the descriminatory power of the features of Mod to validate the feature space and G_3 aims at generalizing the detection accuracies of Mod under more realistic conditions with separate test sets, which are described in Subsect. 4.2.

4.2 Evaluation Setup

We use a pattern recognition based approach to analyze the degradation process and to detect morphed face images. Due to this, we train a classification model Mod with two classes

– class 1: *"Authentic"* (600 Samples) and
– class 2: *"Morphing"* (600 Samples),

and apply the introduced degradation process (see Fig. 2) to each sample, as mentioned in Sect. 3. The class *Authentic* contains self acquired non-modified face images, which represents our ground-truth, see Fig. 1 (Person 1 and Person 2). All these training images follow the ICAO standard [15] for images used in international passport documents to create a realistic passport setup. The class "Authentic" includes 600 samples of 50 different persons, so we use 12 face images for each person, which are acquired with 2 different cameras and different parameters. Additionally we use two different instances of both cameras. With that we try to create a diverse dataset for the training class *Authentic*. We assume that this could lead to more accurate results under realistic test conditions. The parameters and the used cameras are shown in Table 1.

Table 1. Used cameras and acquisition parameters for the training data in *Mod*

Camera	Resolution	ISO-value
2 ∗ Canon EOS 1200D	2304×3456	100,400
Lens: EF28-1005 f/4-5.6	1728×2592	100
2 ∗ Nikon Coolpix A100	1704×2272	100,400
	1200×1600	100

The second class *Morphing* of our classification model is trained with two different attack types of automatically generated face morphing images. These two morphing approaches are described in [2], see Sect. 2. The first attack type $Morph_{complete}$ could be seen as a result of warping and blending of complete facial images including hair, torso and background. The second attack type $Morph_{splicing}$ achieves a more realistic appearance by cutting facial regions, warp them and blend them to a mutual face and seamlessly stitch it back into one of the input images. An example to visualize these two attack types is given in Fig. 4. The clearly recognizable ghosting artefacts for $Morph_{complete}$ are negligible, because we are only using the convex hull of the face region for our approach and we are aware that an attacker would probably remove such clearly visible artefacts. Both attack types are thus well suited as training and test data, as they represent realistic faces almost entirely devoid of visual artefacts. The morphings are randomly created and selected from the 50 subject of the class *Authentic*. In order to train an unbiased classification model, we select 600 morphing samples for an equal distribution of both classes. For $Morph_{complete}$ we got 200 samples and for $Morph_{splicing}$ 400 samples, the higher number of samples for the latter attack type is intended to reflect the two morph targets (see Fig. 4).

Hence, *Mod* includes 1200 training samples to analyze our evaluation goals $(G_1 - G_3)$. In order to achieve these goals we perform three tests (T_1, T_2, T_3).

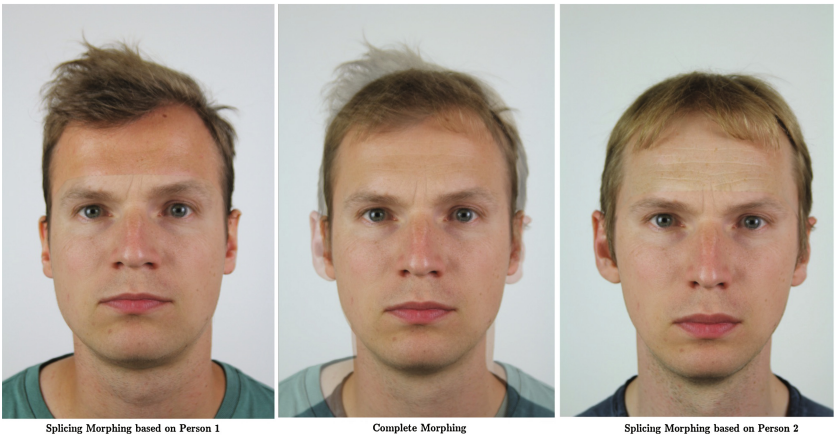

Fig. 4. Example of automatically created face morphing images ($Morph_{splicing}$ and $Morph_{complete}$)

- T_1 : To achieve G_1 we perform a 10-fold cross-validation to evaluate the reference accuracy of Mod, because the test is performed under optimized conditions. We use the open source data mining suite WEKA [16] version 3.8.0 with a Logistic Model Tree [17] (LMT) classifier with default parameterization. The LMT is a decision tree with logistic regression functions at the leaves. We have tested different alternative classifiers (for example: a pruned C4.5 decision tree, naive bayes, bagging predictors), but the LMT decision tree delivers the most accurate results for our performed tests.
- T_2 : For G_2 we investigate all extracted features of our feature space from both classes Mod. Therefore we build the mean value from each features for all 600 samples per class. With this data we are able to visualize to degradation process for the 3 extracted corner features (FAST,AGAST, shiTomasi) for morphed and authentic face images.
- T_3 : For G_3, we evaluate the classification accuracy of Mod under more realistic conditions with independent test sets. For the classification of the test datasets, we use also the LMT decision tree, to make the results comparable to T_1. With this test, we get an idea, how well our detection approach could work under real world conditions.

In order to perform T_3, we determine the classification accuracy of Mod for images from different origin. Therefore we create six separate and independent test datasets. Three of them are generated based on Utrecht ECVP [18], a publicly available face reference database. We use the non-smiling Utrecht genuine face images, to build $Morph_{complete}$ (1326 samples) and $Morph_{splicing}$ (2614 samples). Furthermore, we use 400 self-acquired genuine face images of the same 50 subjects as in the training data, but for this data we use two different cameras (2x Nikon D3300, Lens: Nikkor Lens: AF-S50mmf/1.8G) with different parameters (resolution: 2000×2992, 3000×4496 and ISO-values: 100, 400).

Table 2. Overview of used test datasets (independent from training data) in T_3

Name	Resolution	Type	Class	Samples	Base
$TDS_{Authentic-Utrecht}$	900×1200	Genuine	*Authentic*	73	Utrecht [18]
$TDS_{MorphSplicing-Utrecht}$	900×1200	$Morph_{splicing}$	*Morphing*	2614	Utrecht [18]
$TDS_{MorphComplete-Utrecht}$	900×1200	$Morph_{complete}$	*Morphing*	1326	Utrecht [18]
$TDS_{Authentic-AMSL}$	2000×2992	Genuine	*Authentic*	400	self-aquired
	3000×4496				
$TDS_{MorphSplicing-AMSL}$	2000×2992	$Morph_{splicing}$	*Morphing*	300	self-aquired
$TDS_{MorphComplete-AMSL}$	2000×2992	$Morph_{complete}$	*Morphing*	100	self-aquired

So, we acquire 8 images of each person. Based on this data, we generate complete und splicing Morphings for 2 separate test datasets. An Overview of the test datasets gives Table 2. We observe that the three self acquired test datasets are not completely independent from the training data because the 50 test persons are the same. But we assume, that the different acquisition parameters (Camera, Lens and Resolution) should make the test data unbiased to the training data. The evaluation results of the described three tests (T_1, T_2, T_3) are presented in the next section.

5 Evaluation Results

This section specifies the results of our three tests (Sect. 4.2). In addition we discuss, whether we could achieve our evaluation goals (Sect. 4.1).

In T_1 we evaluate the accuracy of our classification model Mod. This test determines a reference detection accuracy (G_1) under optimized conditions for our exemplary two morphing attack types ($Morph_{splicing}$ and $Morph_{complete}$). The results for T_1 are shown in Table 3.

Table 3. Results of the 10-fold cross validation for Mod with LMT classifier (T_1)

Authentic	Morphing	<− classified as
89.0%	11.0%	Authentic (Ground-Truth)
8.7%	**91.3**%	Morphing (Ground-Truth)

The reference classification accuracy of Mod is 90.2% (G_1). So, the degradation process does not have such a big impact on any authentic face image as we assumed. For example, the detection accuracy for "smooth" genuine faces is not as good as assumed, because the reduction of edge keypoints through the degradation process, is similarly low as for morphed face images.

To analyze the impact of the degradation process on morphed and authentic face images (G_2), we perform our second test T_2. For this, we compare the mean

Fig. 5. Impact of the image degradation process on morphed and authentic face images (T_2) for three corner feature detectors (determined by the mean values of the features from each class of the training data). Blue Class: *Authentic*, Red Class: *Morphing* (Color figure online)

values of all extracted features (based on the training samples of Mod) for each corner detector (FAST, AGAST, shiTomasi). Figure 5 shows that the impact of the degradation process is very different on authentic and morphed face images.

The influence of the process results in a higher quality loss for authentic face images than for morphed face images on all three corner features. The number of detected corner features for morphings for all 3 features on the lossy degradated images ($DegImg60$ and $DegImg50$) increases due to detected JPEG compression artifacts. But we also see that the shiTomasi corner detector is more robust to the degradation than the 2 other detectors. So, the shiTomasi features do not have such a descriminatory power as the features from the FAST and AGAST corner detectors. In the end we can assert, that the degradation process got a significant impact on genuine face images with the FAST and AGAST corner features, compared to the influence on morphed face images. So T_2 validates and justifies the selection of our feature space, but it also encourages to find more suitable features to describe the degradation process.

In T_3 we want to evaluate our classification model Mod under more realistic conditions. To do so, we determine the detection accuracies for Mod on 6 separate and independent test datasets (G_3), summarized in Table 2. The results for T_3 are shown in Table 4. T_3 shows acceptable detection accuracies for face

Table 4. Classification results of our model *Mod* with LMT classifier for independent test datasets (T_3)

Test dataset	Classification results	
	Authentic	Morphing
$TDS_{Authentic-Utrecht}$	**19.2**%	80.8%
$TDS_{MorphSplicing-Utrecht}$	16.9%	**83.1**%
$TDS_{MorphComplete-Utrecht}$	10.9%	**89.1**%
$TDS_{Authentic-AMSL}$	**77.5**%	22.5%
$TDS_{MorphSplicing-AMSL}$	3.7%	**96.3**%
$TDS_{MorphComplete-AMSL}$	10.0%	**90.0**%

morphing forgeries on independent test datasets for a first evaluation. Over all four morphing test datasets we could achieve a detection accuracy of 85.9% (3732 of 4340 correct classified samples). But the detection performance of the genuine face images is not as good as expected, the accuracy over both genuine test datasets is 68.4% (324 of 473). In the end, the approach has an overall detection accuracy of 84.3% (4056 of 4813) on all test samples.

The high number of incorrect classified samples for $TDS_{Authentic-Utrecht}$ can be explained. The samples of this dataset are already JPEG compressed multiple times. Because of that, the degradation has an influence on samples, that is more similar to the morphed images than to images taken directly from a camera. So, we recommend a strict compression policy for images used in international passport documents. Besides, the false alarm rate for $TDS_{Authentic-AMSL}$ is still high (22.5%), due to the reasons mentioned for T_1. We hope, the false alarm rate could be oppressed by other mechanisms that may support this approach in the future as a part of a security system. In the end, the results of the three tests (T_1, T_2, T_3) show that our degradation process is promissing for the detection of face morphing forgeries. The results are acceptable for a first evaluation and with more training data and a process with more particular degradation steps, the approach should lead to even better results.

6 Conclusion and Future Work

Our paper introduces a novel detection approach for face morphing forgeries based on image degradation. It is a promissing blind anomaly detection approach working on self-created artificial references. We present the design of our degradation process and perform a pattern recognition based detection approach. We implement a first test setup to evaluate the performance of our approach. Our experimental setup shows that the process works quite well under laboratory conditions. Here, we achieve an overall detection accuracy of 91.3% for face morphing forgeries with our classification model. Additionally the impact of the created degradation process is visualized and compared for morphed and for genuine face images. This comparison shows a significant difference of both types of

images, which validates our feature space. After this, we evaluate the accuracy of our classification model under more realistic conditions with six different test datasets. This evaluation shows detection accuracies for face morphings (85.9%), but struggles to classify authentic images correctly (68.4%). So, the false alarm rate is not acceptable for real world applications and has to be improved if the process should be a part of a real world application. All in all the degradation process is promissing to detect face morphings and encourages further research on this approach.

In future work, a bigger ground truth training dataset would be meaningful to train a more detailed classification model, which hopefully delivers more accurate evaluation results. Furthermore the granularity of the degradation process should be increased, to see whether it could lead to better classification results. Moreover the degradation process can be performed with other degradating procedures for example median filtering. Currently, our approach is based on three corner detectors which describe the degradation. It would be meaningful to expand the feature space by more degradation sensitive features.

Acknowledgments. The work in this paper has been funded in part by the German Federal Ministry of Education and Research (BMBF) through the research programme ANANAS under the contract no. FKZ: 16KIS0509K. The author would like to thank Jana Dittmann and Andrey Makrushin for the initial ideas as well as the joint work with both of them and Christian Kraetzer for discussions on the approach evaluated in this paper.

References

1. Ferrera, M., Franco, A., Maltoni, D.: The magic passport. In: Proceedings of the IEEE IEEE International Conference on Biometrics, Clearwater, Florida, pp. 1–7 (2014)
2. Makrushin, A., Neubert, T., Dittmann, J.: Automatic generation and detection of visually faultless facial morphs. In: Proceedings of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications (VISIGRAPP 2017). VISAPP, vol. 6, pp. 39–50 (2017). ISBN: 978-989-758-227-1
3. Hildebrandt, M., Neubert, T., Makrushin, A., Dittmann, J.: Benchmarking face morphing forgery detection: application of StirTrace for impact simulation of different processing steps. In: Li, C.-T. (ed.) Proceedings of the International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, University of Warwick, 4–5 April 2017
4. Ferrara, M., Franco, A., Maltoni, D.: On the effects of image alterations on face recognition accuracy. In: Bourlai, T. (ed.) Face Recognition Across the Imaging Spectrum, pp. 195–222. Springer, Cham (2016). doi:10.1007/978-3-319-28501-6_9
5. Schetinger, V., Iuliani, M., Piva, A., Oliveira, M.: Digital Image Forensics vs. Image Composition: An Indirect Arms Race. CoRR abs/1601.03239 (2016)
6. Raghavendra, R., Raja, K., Busch, C.: Detecting morphed facial images. In: Proceedings of 8th IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS 2016), Niagra Falls, USA, 6–9 September 2016

7. Othman, A., Ross, A.: Privacy of facial soft biometrics: suppressing gender but retaining identity. In: Agapito, L., Bronstein, M.M., Rother, C. (eds.) ECCV 2014. LNCS, vol. 8926, pp. 682–696. Springer, Cham (2015). doi:10.1007/978-3-319-16181-5_52
8. Scherhag, U., Raghavendra, R., Raja, K.B., Gomez-Barrero, M., Rathgeb, C., Busch, C.: On the vulnerability of face recognition systems towards morphed face attacks. In: Li, C.-T.(ed.) Proceedings of the International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, University of Warwick, 4–5 April 2017
9. Gomez-Barrero, M., Rathgeb, C., Scherhag, U., Busch, C.: Is your biometric system robust to morphing attacks? In: Li, C.-T. (ed.) Proceedings of the International Workshop on Biometrics and Forensics (IWBF 2017), Coventry, UK, University of Warwick, 4–5 April 2017
10. Rosten, E., Drummond, T.: Fusing points and lines for high performance tracking. In: IEEE International Conference on Computer Vision, vol. 2, pp. 1508–1511 (2005). doi:10.1109/ICCV.2005.104
11. Mair, E., Hager, G., Burschka, D., Suppa, M., Hirzinger, G.: Adaptive and Generic Corner Detection Based on the Accelerated Segment Test (2010). http://www6.in.tum.de/Main/Publications/Mair2010c.pdf. Access 7 Feb 2017
12. Shi, J., Tomasi, C.: Good features to track. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 593–600 (1994)
13. Low, D.: Object recognition from local scale-invariant features. In: Proceedings of the International Conference on Computer Vision (1999)
14. Bay, H., Tuytelaars, T., Gool, L.: SURF: speeded up robust features. In: Leonardis, A., Bischof, H., Pinz, A. (eds.) ECCV 2006, Part I. LNCS, vol. 3951, pp. 404–417. Springer, Heidelberg (2006). doi:10.1007/11744023_32
15. Wolf, A.: Portrait Quality (Reference Facial Images for MRTD). Version: 0.08 ICAO, Published by authority of the Secretary General (2017)
16. Hall, M., et al.: The WEKA data mining software: an update. SIGKDD Explor. **11**(1), 10–18 (2009)
17. Landwehr, N., Hall, M., Frank, E.: Logistic model trees. In: Proceedings in Machine Learning, pp. 161–205 (2005)
18. Hancock, P.: Psychological image collection at stirling (pics) - 2d face sets - Utrecht ECVP. http://pics.psych.stir.ac.uk/. Accessed 21 Apr 2017
19. Luxand, Inc.: Luxand - detect and recognize faces and facial features with luxand facesdk (2016). https://www.luxand.com/facesdk/. Accessed 6 June 2017