

# Reducing the False Alarm Rate for Face Morph Detection by a Morph Pipeline Footprint Detector

1<sup>st</sup> Tom Neubert, 2<sup>nd</sup> Christian Kraetzer, 3<sup>rd</sup> Jana Dittmann

*Research Group Multimedia & Security*

*Dept. of Computer Science*

*Otto-von-Guericke University of Magdeburg*

PO Box 4120, 39016 Magdeburg, Germany

{tom.neubert, christian.kraetzer, jana.dittmann}@iti.cs.uni-magdeburg.de

**Abstract**—In this paper, we introduce a novel multi-level process to reduce the false alarm rate (FAR) of existing state-of-the-art face morph detectors, designed to counter the threat that face morphing attacks represent for face image based authentication scenarios. Therefore, we design a novel morph pipeline footprint detector and a novel verification engine to validate the classification results of these existing detectors. The detectors are based on Benford features derived from JPEG DCT coefficients (in the face region of the image and background) and local derivative pattern features. We evaluate the morph pipeline footprint detector with more than 30,000 images and our morph verification engine with false classified authentic images of state-of-the-art approaches. The evaluation shows that our approach is able to reduce the false alarms by 83.67%.

**Index Terms**—face morphing, image forensics

## I. INTRODUCTION

Face Morphing is a recent image tampering attack introduced in 2014 by Ferrara et al. in [1]. It melts two or more face images of different persons, so that it is similar to multiple real persons. This attack is easy to implement and targets all face image based authentication scenarios, combining characteristics of template space and presentation attacks on biometric systems. Since it was introduced, different morph creation and detection approaches have been published by the signal processing community. Currently, there exists no reliable morph detector which is suitable for all types of morphs, because different morph pipelines result in different image artifacts (so called “footprints”). So, different morph detectors deliver different morph detection accuracies and different false alarm rates (FAR) for any morph pipeline. Due to this, it is valuable to know what type of face morph pipeline (FMP) is used for the morph creation to verify the detection result and to decrease the FAR of these detectors. Currently, the FAR of the state-of-the-art morph detectors is too high for real world applications (mostly more than 10%). Of course although the false missing rate (FMR) is, from a security point of view, the more severe error case, but the number of false alarms has to be considered to be a crucial factor to whether the system will be used at all. For example: if the FAR of a face morph detector would be 0.1%, there would be more than 1000 false alerts per day, on the worlds most busiest airport in Atlanta, USA [2]. So, the FAR has

to be significantly decreased for the current state-of-the-art morph detectors. Hence, this paper introduces a concept to verify images which are already classified as morph from existing morph detectors (1st level morph detectors). To reduce the FAR, we introduce a 2nd level morph pipeline footprint detector, which recognizes the morph pipeline used to create a morphed image. Afterwards, the image goes into a 3rd level morph validator, which verifies if this image belongs to the morph pipeline or establishes that it is an authentic image, that was wrongfully flagged at the 1st level. Every authentic image, which is classified as an authentic one by the morph validator, would reduce the FAR of the 1st level morph detector.

Our **contributions** can be summarized as follows:

- a novel multi-level process reducing the FAR by redesigning the state-of-the-art morph detection pipelines,
- a novel morph pipeline footprint detector is introduced and evaluated to form a 2nd level component in the introduced detection pipeline to accompany existing first level detection approaches,
- a novel verification engine is designed and evaluated as 3rd level component to validate the classification result of the 1st level detector with the knowledge derived at the 2nd level,
- an empirical evaluation with more than 30,000 images is performed to evaluate the 2nd level morph pipeline footprint detector and an evaluation of false classified authentic images shows the benefit of the novel multi-level process in terms of a reduced FAR.

## II. STATE OF THE ART

In this section, we introduce three selected face morph pipelines (FMP), which are used in this work for footprinting to reduce the false alarm rate (FAR) for face morph detectors. The three FMP are a representative subset of known automated morphing strategies in the literature. Manual morphing pipelines are not considered yet, this has to be done in future work. Furthermore, we give a short overview about the related work on face morph detection, to show that the FAR for these approaches is too high to use them in real world applications.

### A. Face Morph Pipelines (FMP)

The 3 FMP address the issue of generating training and test data to evaluate designed face morph detection approaches. All morph pipelines are based on warping and subsequent alpha-blending as proposed in [3]. The alpha blending is set to 0.5 to make it equal to averaging between both input images. The warping process is based on a triangulation which uses 68 facial landmarks localized with dlib (www.dlib.net). These landmarks describe parts of the face such as eyes, nose, mouth and face contour. The result of these 3 FMP are visualized in Fig. 1.

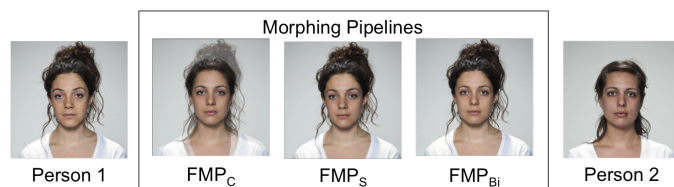


Fig. 1. Example of the three state-of-the-art Face Morph Pipelines  $FMP_C$  [4] and  $FMP_S$  [4] and  $FMP_{Bi}$  [5]

1) *Complete Morph ( $FMP_C$ )*: The *complete morph* is introduced in [4] and it could be seen as a result of warping and blending of complete facial images (including hair, torso and background). The only addition to the steps above (see Section II-A) is that the set of 68 facial landmarks is extended by additionally adding 20 landmarks on the image borders, as proposed in [6] to cover the complete image. In the end, a complete morph has an average geometry and an average texture of the original faces. On the one hand, this leads to a high biometric quality, as asserted in [4]. But on the other hand, a complete morph usually has clearly visible ghosting artifacts as a result of blending operations (see Fig. 1).

2) *Splicing Morph ( $FMP_S$ )*: The *splicing morph* is also introduced in [4] and has a more realistic appearance than morphs generated with  $FMP_C$ , because they are designed to avoid ghosting artifacts. For splicing morphs, facial regions are cut, warped and blended to a mutual face and seamlessly stitched back into one of the input images. This leads to fewer visible artifacts, but also to a lower biometric quality [4].

3) *Combined Morph ( $FMP_{Bi}$ )*: The *combined morph* is designed to avoid shortcomings of the aforementioned pipelines  $FMP_C$  and  $FMP_S$  and is introduced in [5]. The important difference to  $FMP_C$  and  $FMP_S$  is an alignment of original images prior to the warping process. This ensures that warping does not lead to a drastic distortion of the face geometry. Thus, the warped face has a more realistic appearance and can be used as a target for face splicing. The morph generated with  $FMP_{Bi}$  has no major artifacts and the skin color has no influence on the visual quality. So, this pipeline has a high visual quality as well as a high biometric quality as mentioned in [5].

### B. Face Morph Detection Approaches (possible examples for 1st stage detection)

1) *Benford-Detector*: The detector published in [4] is based on Benford features of JPEG DCT coefficients. The assumption is that natural and artificially generated images have significantly different distributions of DCT coefficients. Hence, the Benford features should be differently distributed for original and morphed images. The evaluation of this detector shows a FAR of 3.5% on the test dataset.

2) *Keypoint-Detector*: In [7] a face morph detector is introduced based on texture describing keypoint features in the face region. It uses the assumption that the blending operation in the morph process causes a reduction of these keypoint features. So, the number of detected keypoints should be significantly lower on morphed images. In the evaluation a FAR of 18.7% is determined for this detector.

3) *Degradation-Detector*: For the detection approach in [8], an image is continuously degraded by JPEG compression and the loss of details in the face region is measured. It is based on the idea, that an authentic image should have a more significant degradation in the face region than a morphed one because of the already applied blending operations. The evaluation determines an average FAR of 31.6%.

### III. CONCEPT OF OUR NOVEL MULTI-LEVEL DETECTOR AND VALIDATION PROCESS

We introduce a novel multi-level detection and validation process to reduce the false alarm rate of the current state of the art morph detectors [4], [7] and [8]. We visualize the multi-level process in Fig. 2. The process is divided into 3-levels.

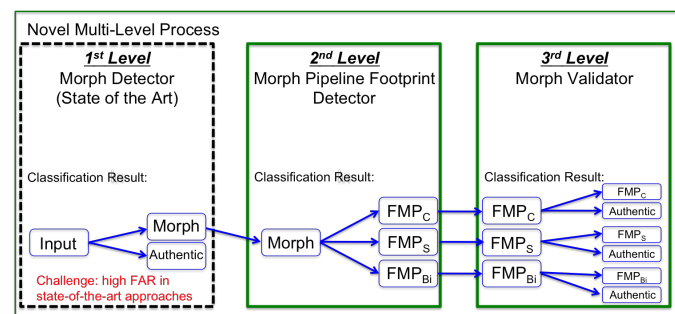


Fig. 2. The novel multi-level detection and validation process to reduce the FAR of state-of-the-art face morph detectors

- The 1st level component is a state-of-the-art morph detector, which delivers a classification result (“Morph” or “Authentic”) for an input face image.
- The 2nd level component is our novel morph pipeline footprint detector, which determines a state-of-the-art face morph pipeline (complete morph  $FMP_C$ , splicing morph  $FMP_S$  or combined morph  $FMP_{Bi}$ , see Section II-A) if an image is already classified as “Morph” by 1st level component.
- The 3rd level component is a verification engine to validate the classification result from the 1st level with the

knowledge derived at the 2nd level. It decides between the determined morph pipeline and an authentic image.

We are aware of that an incorrectly classified authentic image in 1st level has no footprint for the 2nd level and the detector has to made an incorrect decision here, but we renounce consciously an “authentic” class of images for this level to avoid an increasing false missing rate. This concept addresses the research challenge of the high false alarm rates for the current state-of-the-art morph detectors. With the novel introduced multi-level detection and verification process, we reduce the false alarm rate for the morph detectors significantly.

#### IV. CONCEPT OF OUR IMAGE PROCESSING PIPELINE FOR 2ND AND 3RD LEVEL DETECTION

The concept of our morph pipeline footprint detector (2nd Level) is based on the idea, that all morph pipelines create different artifacts, especially outside of the face region. The artifacts inside the face region are for all three morph pipelines nearly the same, caused by the blending and warping operations in the face region. Due to this, we focus on artifacts in the background. Our proposed image processing pipeline has 7 steps and is visualized in Fig 3.

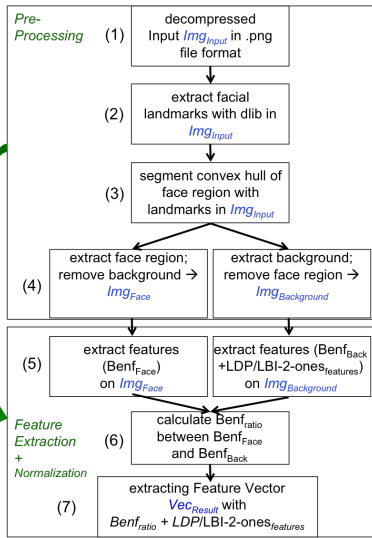


Fig. 3. Proposed image processing and feature extraction pipeline

Before we start, all used images are decompressed and stored in PNG image file format to have a homogeneous base for each used input file  $Img_{Input}$  (1). We start our image processing with extracting the facial landmarks from  $Img_{Input}$  (2) by using the *dlib* programming library version 19.2 (<http://dlib.net>). With these landmarks we are able to segment the convex hull of the face region in  $Img_{Input}$  (3). This gives us the opportunity to extract the face and to remove the background ( $Img_{Face}$ ) and the other way around ( $Img_{Background}$ ) (4). After the pre-processing, we start the feature extraction on  $Img_{Face}$  and on  $Img_{Background}$  (5). We extract JPEG DCT coefficients on  $Img_{Face}$  as well as on  $Img_{Background}$ . For this step we convert both images from the PNG image file

format to the JPEG file format (with 100% image quality). We describe the distribution of the DCT coefficients for all 3 color channels (Y, Cb, Cr) with the known nine benford features as suggested in [9] for  $Img_{Face}$  with the vector  $Benf_{Face}$  and for  $Img_{Background}$  with  $Benf_{Background}$ . Furthermore, we calculate the 1st (for four directions) and 2nd order (for four directions) local derivative pattern (LDP, as suggested in [10]) based on  $Img_{Background}$  (in PNG file format). Thus, we calculate two features for each LDP:

- the percentage share of pixels not null and
- and the average pixel intensity in the background.

So, we obtain 16  $LDP_{Features}$  derived from the 8 LDPs. Additionally, we calculate a local binary image (LBI) on  $Img_{Background}$  and extract the percentage share of so called LBI-2-ones (8  $LBI-2-ones_{features}$ ) as suggested in [11]. We assume to detect the ghosting artifacts from  $FMP_C$  as well as the warping artifacts in the background from  $FMP_{Bi}$  based on the 8 LDPs.

After the feature extraction we calculate the ratio between the 9 Benford features from  $Benf_{Face}$  and  $Benf_{Background}$  (6) in  $Benf_{ratio}$ . We assume that this ratio describes the significantly different treatment between the face and the background. For  $FMP_C$  the background is warped and blended, for  $FMP_S$  the background is untouched and for  $FMP_{Bi}$  the background is warped. In the end, we extract 33 features (9  $Benf_{ratio}$ , 16  $LDP_{Features}$  and 8  $LBI-2-ones_{features}$ ) which should significantly differ between the three morph pipelines and which are saved in labeled feature vectors (7), which can be used for a pattern recognition based detection approach. The same features are used for the 3rd level morph validator, because they should also significantly differ between authentic images and morphed images.

#### V. EVALUATION SETUP AND GOALS

To evaluate our concept we use a pattern recognition based approach. Here, we operate with the open source data mining suite WEKA [12] (version 3.8.1) with SMO classifier.

##### A. Evaluation Setup for Morph Pipeline Footprint Detector (2nd Level)

1) **Training Data (self acquired):** For the morph pipeline footprint detector we train a 3-class-training-model  $Mod_{FMP}$ , with one class for each state-of-the-art FMP. For the training data we use self acquired ground-truth data from 85 different persons. We have acquired each person with 3 different cameras (Canon EOS 1200D, Nikon D3300 and Nikon Coolpix A100) with 3 different resolutions and ISO values per camera. We manually select one visually good looking shot from every person and apply the 3 state of the art morph pipelines to these 85 images. Afterwards, we randomly select 2,500 images for each class in  $Mod_{FMP}$ . To create a realistic passport scenario, all these training images follow the ICAO standard [13] for images used in passport documents.

2) **Test Data** (from [14] and [15]): The test data to evaluate the performance of our 2nd level morph pipeline footprint detector is based on 2 publicly available face reference databases (LondonDB [14] and UtrechtDB [15]). We apply all three morph pipelines on all 102 non-smiling faces of the LondonDB and on all 73 non-smiling faces of the UtrechtDB. So, we create 3 test datasets for both face reference databases  $\{Lon_{FMP_C}, Lon_{FMP_S}, Lon_{FMP_{Bi}}, Utr_{FMP_C}, Utr_{FMP_S}, Utr_{FMP_{Bi}}\}$ , see Table I. Overall, our morph pipeline footprint detector is tested with 31,094 images.

TABLE I  
OVERVIEW OF USED TEST DATA (INDEPENDENT FROM THE TRAINING DATA IN SECTION V-A1) FOR MORPH PIPELINE FOOTPRINT DETECTOR

Name	Resolution	Type	Samples	Base
$Lon_{FMP_C}$	1350x1350	FMP <sub>C</sub>	5,050	LondonDB [14]
$Lon_{FMP_S}$	1350x1350	FMP <sub>S</sub>	9,352	LondonDB [14]
$Lon_{FMP_{Bi}}$	1350x1350	FMP <sub>Bi</sub>	10,100	LondonDB [14]
$Utr_{FMP_C}$	900x1200	FMP <sub>C</sub>	1,326	UtrechtDB [15]
$Utr_{FMP_S}$	900x1200	FMP <sub>S</sub>	2,614	UtrechtDB [15]
$Utr_{FMP_{Bi}}$	900x1200	FMP <sub>Bi</sub>	2,652	UtrechtDB [15]

### B. Evaluation Setup for Morph Validator (3rd Level)

1) **Training Data** (self acquired): For the morph validator we train 3 training models  $Mod_{MV.FMP_C}$ ,  $Mod_{MV.FMP_{Bi}}$  and  $Mod_{MV.FMP_S}$  (one for each face morph pipeline) with 2 classes (FMP<sub>Type</sub> and “Authentic”), where “Type” is the corresponding morphing pipeline (C, S or Bi). For the class “Authentic” we use self acquired ground truth images, directly from the camera. These authentic images, are based on the same data as mentioned in Section V-A1 and 2,500 images were randomly selected (minimum: 30 images per person, all with 3 different resolutions and 3 different ISO-values per camera) too. For the morph pipelines we use the same data as described in Section V-A1. Due to this, all 3 training models include 5,000 images (2,500 per class).

2) **Test Data** (from [4], [7] and [8]): To evaluate our morph validator and to see if our approach is able to reduce the false alarm rate (FAR), we take all false classified authentic images (false alarms FAs) from the three mentioned state-of-the-art detection approaches (see section II-B). Subsequently, we put these images, into our 2nd level morph pipeline footprint detector and depending on which FMP is classified, the corresponding  $Mod_{MV.FMP_{Type}}$  is used to verify the image as a morphed image or an authentic image. Furthermore, we have to evaluate, if our morph validator increases the false missing rate (FMR), by a false classification of morphed images, which are flagged as “Morph” by the 1st level. Therefore, we use all 31,094 morphings from V-A2 (see Table II).

### C. Evaluation Goals

In order to evaluate our novel multi-level detection and validation process to reduce the FAR of the state-of-the-art face morph detectors, we define two evaluation goals for the 2nd level and two goals for the 3rd level of the process.

TABLE II  
OVERVIEW OF USED TEST DATA (INDEPENDENT FROM THE TRAINING DATA IN SECTION V-B1) FOR MORPH VALIDATOR

Name	Type	Samples	Base
FAs[4]	Authentic	14	[4]
FAs[7]	Authentic	28	[7]
FAs[8]	Authentic	56	[8]
FMP <sub>all</sub>	Morph	31,094	[14] and [15]

#### 1) Goals for Morph Pipeline Footprint Detector (2nd Level):

- **G1**: Determine a reference accuracy of our 2nd level training model  $Mod_{FMP}$  by a 10-fold cross validation on the training data to evaluate the designed feature space.
- **G2**: Determine the detection accuracy of  $Mod_{FMP}$  for different test data sets from Table I, which have not been involved into training (31,094 test samples).

#### 2) Goals for Morph Validator to lower FAR (3rd Level):

- **G3**: Determine reference accuracies of our 3rd level training models  $Mod_{MV.FMP_C}$ ,  $Mod_{MV.FMP_S}$  and  $Mod_{MV.FMP_{Bi}}$  by a 10-fold cross validation on the training data to evaluate the designed feature space.
- **G4**: Determine whether the 3rd level morph validator decreases the FAR and not increases the FMR.

## VI. EVALUATION RESULTS

We structure this section according to the evaluation goals in Section V-C.

### A. Evaluation Results for G1:

For evaluation goal **G1** we determine a reference accuracy for the training model  $Mod_{FMP}$  under optimized conditions, to see if our designed feature space is able to distinguish between the three state-of-the-art FMP. The classification accuracy of the 10-fold cross validation is 99.84% (12 out of 7,500 samples are incorrect classified). Thus, we can assume that our feature space is suitable to distinguish between the three FMP under optimized conditions.

### B. Evaluation Results for G2:

With the evaluation goal **G2**, we evaluate our 2nd level morph pipeline footprint detector under more realistic conditions with 6 test datasets which are not involved into training. The test data for G2 is described in Section V-A2. The detection accuracies are summarized in Table III.

TABLE III  
CLASSIFICATION RESULTS OF TRAINING MODEL  $Mod_{FMP}$  WITH SMO CLASSIFIER FOR INDEPENDENT TEST DATASETS (G2);

Test Dataset	Classification Results		
	FMP <sub>C</sub>	FMP <sub>S</sub>	FMP <sub>Bi</sub>
$Lon_{FMP_C}$	<b>5,001</b>	49	0
$Lon_{FMP_S}$	0	<b>9,352</b>	0
$Lon_{FMP_{Bi}}$	522	4,838	<b>4,740</b>
$Utr_{FMP_C}$	<b>1,275</b>	0	51
$Utr_{FMP_S}$	0	<b>2,614</b>	0
$Utr_{FMP_{Bi}}$	16	4	<b>2,632</b>

We determine an average detection accuracy for  $Mod_{FMP}$  of 82.37% (25,614 out of 31,094 correct classified samples)

over all test datasets. The vast majority of created morphs from the UtrechtDB are correctly classified (only 71 errors). We have to mention that these results cannot be generalized for the LondonDB. Here, a lot of samples from the  $FMP_{Bi}$  pipeline are classified as  $FMP_S$ . This mismatch between the performances while applying the same model for different test databases implies an overfitting to the training data used.

### C. Evaluation Results for G3:

In G3, we determine the reference accuracy of the morph validator training models  $Mod_{MV.FMPC}$ ,  $Mod_{MV.FMPS}$  and  $Mod_{MV.FMPBi}$  to see if the designed feature space is also able to distinguish between an authentic image and morphed face images from the corresponding FMP. The results for G3 are summarized in Table IV. 96.02% of the images are correctly classified (7,201 of 7,500). Hence, our feature space is suitable to distinguish between morphed and authentic images.

TABLE IV

RESULTS OF THE 10-FOLD CROSS VALIDATION FOR  $Mod_{MV.FMPC}$ ,  $Mod_{MV.FMPS}$  AND  $Mod_{MV.FMPBi}$  WITH SMO CLASSIFIER (G3)

Training Model	Authentic	$FMP_C$	<- classified as
$Mod_{MV.FMPC}$	<b>2,487</b>	13	Authentic (Ground-Truth)
	12	<b>2,488</b>	$FMP_C$ (Ground-Truth)
Training Model	Authentic	$FMP_S$	<- classified as
$Mod_{MV.FMPS}$	<b>2,471</b>	29	Authentic (Ground-Truth)
	3	<b>2,497</b>	$FMP_S$ (Ground-Truth)
Training Model	Authentic	$FMP_{Bi}$	<- classified as
$Mod_{MV.FMPBi}$	<b>2,384</b>	116	Authentic (Ground-Truth)
	126	<b>2,374</b>	$FMP_{Bi}$ (Ground-Truth)

### D. Evaluation Results for G4:

For G4 we evaluate 3 different test datasets with false classified authentic images from 3 state-of-the-art morph detectors ([4], [7] and [8]), see Section V-B2. The results are presented in Table V. It shows, that 82 (14 + 22 + 46) of the false alarms are classified as "Authentic" (out of 98 images), that means that our approach is able to reduce the FAR by 83.67%. Furthermore, we evaluate, if our approach increases the false missing rate (FMR) by false classification of morphed images as "Authentic". The results show that 3,569 (1,710 + 68 + 1,791) morphed samples out of 31,094 are incorrectly classified. Hence, the FMR increases by 11.47%. But we have to mention again, that a low FAR is a crucial factor to whether a system will be used or not. Since throughput is the main goal for automatic detection systems on airport gates, it is necessary to sacrifice a very high detection rate for a more practical system and a low FAR.

## VII. CONCLUSION AND FUTURE WORK

In this work, we present a novel multi-level process to reduce the false alarm rate (FAR) of face morph detectors. To do so, we use a pattern recognition based approach with features based on local derivative and local binary patterns and the distribution of JPEG DCT coefficients. The presented approach is able to reduce the FAR significantly (83.67%) in our experiments. In future work we would like to evaluate the influence of other morph pipelines on our approach.

TABLE V  
DETECTION RESULTS FOR THE 3RD LEVEL MORPH VALIDATOR (G4);  
TRAINING MODEL FOR 2ND LEVEL IS  $Mod_{FMP}$

Test Dataset	2nd Level		=>	3rd Level		Summary
	Info	Results		Training Model	Results	
$FAs[4]$	14 false alarm samples	$1 FMP_C$	$\Rightarrow$	$Mod_{MV.FMPC}$	0 $FMP_C$ 1 <b>Authentic</b>	14 of 14 false alarms detected
		$1 FMP_S$	$\Rightarrow$	$Mod_{MV.FMPS}$	0 $FMP_S$ 1 <b>Authentic</b>	
		$12 FMP_{Bi}$	$\Rightarrow$	$Mod_{MV.FMPBi}$	0 $FMP_{Bi}$ 12 <b>Authentic</b>	
$FAs[7]$	28 false alarm samples	$0 FMP_C$	$\Rightarrow$	$Mod_{MV.FMPC}$	-	22 of 28 false alarms detected
		$26 FMP_S$	$\Rightarrow$	$Mod_{MV.FMPS}$	6 $FMP_S$ 20 <b>Authentic</b>	
		$2 FMP_{Bi}$	$\Rightarrow$	$Mod_{MV.FMPBi}$	0 $FMP_{Bi}$ 2 <b>Authentic</b>	
$FAs[8]$	56 false alarm samples	$1 FMP_C$	$\Rightarrow$	$Mod_{MV.FMPC}$	0 $FMP_C$ 1 <b>Authentic</b>	46 of 56 false alarms detected
		$51 FMP_S$	$\Rightarrow$	$Mod_{MV.FMPS}$	10 $FMP_S$ 41 <b>Authentic</b>	
		$4 FMP_{Bi}$	$\Rightarrow$	$Mod_{MV.FMPBi}$	0 $FMP_{Bi}$ 4 <b>Authentic</b>	
$FMP_{all}$	31,094 morphed samples	$6,840 FMP_C$	$\Rightarrow$	$Mod_{MV.FMPC}$	5,130 $FMP_C$ 1,710 <b>Authentic</b>	3,569 (11.47%) false misses triggered
		$16,791 FMP_S$	$\Rightarrow$	$Mod_{MV.FMPS}$	16,723 $FMP_S$ 68 <b>Authentic</b>	
		$7,462 FMP_{Bi}$	$\Rightarrow$	$Mod_{MV.FMPBi}$	5,671 $FMP_{Bi}$ 1,791 <b>Authentic</b>	

## ACKNOWLEDGMENT

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.

## REFERENCES

- [1] M. Ferrara, A. Franco, and D. Maltoni, "The magic passport.," in *IJCB*, pp. 1–7, IEEE, 2014.
- [2] D. of The Port Authority of NY & NJ, "Airport traffic report," 2018.
- [3] G. Wolberg, "Image morphing: a survey,," in *Visual Computer* 14(8), pp. 360-372., 1998.
- [4] A. Makrushin, T. Neubert, and J. Dittmann, "Automatic generation and detection of visually faultless facial morphs,," in *Proceedings of the 12th International Joint Conference on Computer Vision, VISAPP*, 2017.
- [5] T. Neubert, A. Makrushin, M. Hildebrandt, C. Kraetzer, and J. Dittmann, "Extended stirtrace benchmarking of biometric and forensic qualities of morphed face images,," *IET Biometrics*, 2018.
- [6] S. Mallick, "Face morph using opencv - c++ / python,," *J http://www.learnopencv.com/face-morph-using-opencv-cpp-python/ last accessed: 2017/07/07.*
- [7] C. Kraetzer, A. Makrushin, T. Neubert, M. Hildebrandt, and J. Dittmann, "Modeling attacks on photo-id documents and applying media forensics for the detection of facial morphing,," in *Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security, IHMMSec '17*, (New York, NY, USA), pp. 21–32, ACM, 2017.
- [8] T. Neubert, "Face morphing detection: An approach based on image degradation analysis,," in *Digital Forensics and Watermarking*, pp. 93–106, Springer International Publishing, 2017.
- [9] D. Fu, Y. Q. Shi, and W. Su, "A generalized benford's law for jpeg coefficients and its applications in image forensics,," in *Proc. SPIE EI 6505, San Jose, CA*, 2007.
- [10] N. I. Evdokimova and A. Kuznetsov, "Copy-move detection algorithm based on local derivative pattern,," *CEUR Workshop Proceedings; 1638: 304-312.*, 2016.
- [11] A. Asaad and S. Jassim, "Topological data analysis for image tampering detection,," in *Digital Forensics and Watermarking* (C. Kraetzer, Y.-Q. Shi, J. Dittmann, and H. J. Kim, eds.), (Cham), pp. 136–146, Springer International Publishing, 2017.
- [12] M. Hall, "The weka data mining software: An update.,," in *SIGKDD Explorations*, 2009.
- [13] A. Wolf, "Portrait quality (reference facial images for mrted). version: 0.06,," *Published by authority of the Secretary General*, 2016.
- [14] L. M. DeBruine and B. C. Jones, "Face research lab london set,," *figshare doi: 10.6084/m9.figshare.5047666*, 2017.
- [15] P. Hancock, "Psychological image collection at stirling (pics) - 2d face sets - utrecht ecvp, <http://pics.psych.stir.ac.uk/> last accessed: 2018/06/06,,"