# Analyzing eyebrow region for morphed image detection

Abdullah Zafar[1] and Christoph Busch[1]

Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

**Abstract.** Facial images in passports are designated as primary identifiers for the verification of travelers according to the International Civil Aviation Organization (ICAO) [9]. Hence, it is important to ascertain the sanctity of the facial images stored in the electronic Machine-Readable Travel Document (eMRTD). With the introduction of automated border control (ABC) systems that rely on face recognition for the verification of travelers [2], it is even more crucial to have a system to ensure that the image stored in the eMRTD is free from any alteration that can hinder or abuse the normal working of a facial recognition system. One such attack against these systems is the face-morphing attack. Even though many techniques exist to detect morphed images, morphing algorithms are also improving to evade these detections. In this work, we analyze the eyebrow region for morphed image detection. The proposed method is based on analyzing the frequency content of the eyebrow region. The method was evaluated on two datasets that each consisted of morphed images created using two algorithms. The findings suggest that the proposed method can serve as a valuable tool in morphed image detection, and can be used in various applications where image authenticity is critical.

**Keywords:** Morphed image detection · eyebrow region analysis · automatic border control (ABC) security.

## 1 Introduction

Face morphing is a real and live threat against the ABC systems which verify a person's identity by comparing the live image with the facial reference stored in the eMRTD [20]. Despite the simplicity of the solution of having the passport holder come to the center to take photographs, it is still not universally used due to financial reasons. Furthermore, many countries have adopted or are in the process of adopting web-based passport/visa applications for the ease of applicants where the user can upload a digital copy of the image to the web portal [13]. With technological advances, it is counter-intuitive for the general user to be asked to come to an office just to take a photograph. These things make the detection of a morphed image even more relevant in these times.

For simplicity, face morphing can be explained as an attack against face recognition systems where the images of two individuals are combined to create a

morphed image that is used as a reference image. This reference image produces a positive match against the images that were used in creating the morphed image. One serious application of such an attack is explained in [6] where face morphing enables an individual to travel on someone else's passport.

This paper will present a morphing attack detection (MAD) technique to detect morphed images during the enrollment phase. MAD methods can be divided into two categories i.e. single image MAD (S-MAD) and Differential MAD (D-MAD) [10]. S-MAD involves analyzing an image to determine whether the image is a morph or not. D-MAD involves analyzing the image and another trusted live source for detection. The approach presented in this paper is an S-MAD technique. However, the same technique can also be applied in a D-MAD scenario. S-MAD is more relevant for the passport application process because no trusted live source exists during the enrollment phase.

The approach is based on the analysis of the eyebrow region. The assumption is that the eyebrow region has a high-frequency content due to the presence of hairs. The idea is to analyze the possible reduction in this high-frequency information due to the smoothening effect that results from the averaging of two images in the creation of a morphed image. Furthermore, the eyebrow region is interesting because of its universality and importance in the performance of face recognition systems [15]. The rest of the paper is organized as: Section 2 will highlight some of the related work, Section 3 explains the methodology, Section 4 presents the results obtained, and Section 5 concludes with final remarks and discussion.

## 2 Prior Work

Morphing-based attacks against ABC systems were first identified by Ferrara et al. [6] where they demonstrated the hypothetical scenario of a malicious actor who travels on his friend's passport by means of a face morphing attack. After that, the topic of morphed image detection piqued the interest of researchers resulting in a number of studies presenting different kinds of morphed detection techniques. In this section, past works are presented where texture descriptors are used for morphing attack detection.

Ramachandra et al. [14] in 2016 proposed the first single image based morphed attack detection system. It relied on texture descriptor differences in bonafide and morphed images. The algorithm worked by obtaining a micro-texture variation using Binarized Statistical Image Features (BSIF) and then making the decision using a linear support vector machine. The same detection technique was tested in [17] against two databases of printed-scanned images. The reason for using print-scan images was to mimic the image quality in a visa application process as the visa application process in many countries requires submitting printed images that later get scanned to be saved in the system [16]. The results showed that the detection performance of this technique dropped compared to the digital images.

Spreeuwers et al. in [19] presented another MAD technique that was based on local binary patterns (LBD). Experiments were conducted on multiple databases and with different morphing algorithms to test the robustness of the proposed method. The results obtained were comparable to the BSIF-based method on one dataset, but the same performance could not be observed while testing on multiple datasets.

The application of Fourier spectrum analysis on different facial characteristics was first suggested by Ndeh de Mbah in [10]. This approach is based on analyzing the power density of six identified facial features. The decision of whether an image is morphed or bonafide is based on the total score obtained from the six classifiers. Experiments were conducted on two databases where the results varied greatly depending on the dataset used. However, the reasoning behind the difference in results was not addressed in the paper.

In this paper, we focus on analyzing the eyebrow region in the frequency domain to distinguish between a morphed and bonafide image. We use bonafide and morphed images from two different datasets containing ICAO-compliant printed scanned bonafide images and their morphs created using two morphing algorithms to test our approach. The proposed method is based on single-image detection that can also be used in a differential detection scenario.

## 3 The Proposed Method

The proposed method is a texture-based detection method where the smoothness property of the eyebrow region is studied to distinguish a morphed image from a bonafide image. The eyebrow region due to the presence of hairs is expected to have high-frequency content present in the Fourier domain. The study aims to find if this high-frequency content is lost due to the smoothening effect in a morphed image making it suitable to differentiate morphed images from bonafide images.

The experiments were based on developing a segmentation technique to crop the eyebrow region from a face image and then analyzing the segmented region in the frequency domain. The different steps of the experiment pipeline are described in the following subsections:

### 3.1 Eyebrow region segmentation

For eyebrow region segmentation, we used Dlib's facial landmark detector to locate the eyebrow region in a face image. The pre-trained shape predictor provided by Dlib was used in this study [4] which is based on the dataset from [8]. The Dlib shape predictor returns an array of length 68 containing coordinates of different facial features including the eyebrows. Eyebrows are marked by 10 array values with each eyebrow represented by 5 coordinates (Fig. 1a). These eyebrow coordinates are then used to find the limits of the eyebrow region and crop a rectangle around the region as shown in Fig. 1. This segmentation technique based on Dlib's landmark detector proved to be very effective for the ICAO-compliant images from the datasets.

(a) Sample image - Dlib landmarks

(b) Cropped eyebrow region

Fig. 1: Cropping the eyebrow region

### 3.2 Pre-processing

In this step, we prepare the cropped region for the frequency domain analysis. First, the image is converted to grayscale to be processed by the next stages. Converting the images to grayscale is important for the system to be used in a differential morph detection setting because some border control cameras only provide the trusted live capture image in grayscale [18].

After converting the images to grayscale, the contrast of the cropped eyebrow region is increased to enhance the variations in the cropped image. Contrast enhancement is done through black clipping and white clipping. It works by converting 1% percentage of the darkest grey pixels to black (black clipping) and 5% of the brightest grey pixels to white (white clipping), and then the rest of the gray pixels are scaled between the highest and the lowest values.

Since bonafide images are expected to have more variations, contrast enhancement is expected to further enhance these variations. Contrary to this, the morphed images because of their smoothened nature will be relatively less affected by this step. This phenomenon is also shown in the results in section 4.3. Fig. 2 shows the image after going through the pre-processing step.

(a) Cropped eyebrow region

(b) Enhanced grayscale image

Fig. 2: Preprocessing the cropped image

### 3.3 Fourier analysis

As explained earlier, the idea is to differentiate morphed images from bonafide images by observing the smoothening of eyebrows in morphed images. In a sharp

image, hairs in the eyebrows can be observed as edges separate from each other. These edges are represented by the high-frequency content in the frequency domain.

Next, 2D Fourier transform of the preprocessed image is calculated to get the frequency representation of the image. Since the interest here is in the strength of the frequency content, only the magnitude of the Fourier transform is considered in the analysis. Fig. 3 shows the averaged DFT magnitude spectra of the eyebrow region of bonafide images and morphed (FaceFusion) images from the FRGC dataset.

The plots are shifted to move the values associated with zero frequency to the middle so that the frequency increases as we move away from the origin. It can be observed from the DFT magnitude spectra that the outer circle for bonafide images is bigger than the morphed images indicating a wider spread out of high-frequency content in bonafide images. In our approach, we exploit this difference in the frequency content to distinguish between morphed and bonafide images.

(a) Bonafide (b) Morhped

Fig. 3: Averaged DFT magnitude spectra of eyebrow regions of bonafide and morphed images

### 3.4 Calculating frequency content

Once we have the Fourier spectrum, the next step is to establish a way of calculating the frequency content. We calculated the frequency content by taking the sum of the complete magnitude spectrum. The normalized sum calculated in our testing is expressed by the equation 1.

$$sum = \frac{1}{MN} \sum_{n=1}^{N} \sum_{m=1}^{M} f(n, m) \tag{1}$$

Here, f is an MxN array of the 2-dimensional DFT magnitude of the image, and M and N are the length and width of the cropped eyebrow region, respectively.

The sum of coefficients is divided by the number of pixels in the cropped region for generalizing because the size of the cropped region can vary among different people and images of different resolutions.

## 4 Experimental Results

In the following subsections, the datasets used in the experimentation, evaluation metrics, the experiment setup, and results are presented.

### 4.1 Datasets

The morphed and bonafide images used in this experimentation are taken from [18]. The bonafide images belong to two different datasets i.e. FERET [12] and FRGCv2 [11]. As described in [18], morphs are created by choosing the two subjects among the same dataset. In addition, the subjects are chosen based on their sex and whether they are wearing glasses.

622 bonafide images from the FERET dataset and 1440 images from the FRGC dataset were used in this experiment. Both the bonafide and morph images are post-processed by passing through a print and scan pipeline to mimic the post-processing steps followed in a passport application process.

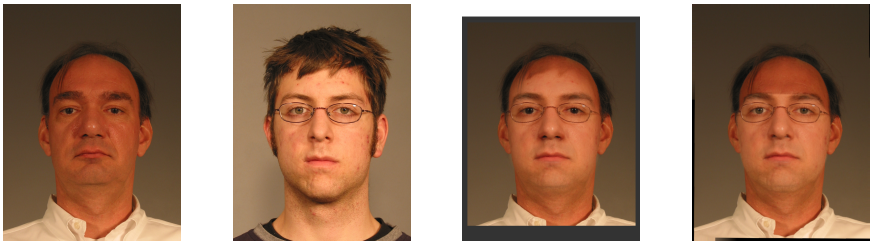
The morphed images are created using FaceFusion [5] and UBO Morpher [7]. More information about the images used is provided in the table 1. Figures 5 and 4 show sample images from FERET and FRGCv2 datasets and their morphs created using FaceFusion and UBO Morpher.

Table 1: Number of images in the datasets

| Dataset | Bonafide | FaceFusion | UBO Morpher |
|---|---|---|---|
| FERET | 622 | 529 | 529 |
| FRGCv2 | 1440 | 964 | 964 |

### 4.2 Evaluation metrics

The proposed solution is tested based on the metrics established by the ISO/IEC 30107-3 for performance assessment of presentation attack detection mechanisms i.e. attack presentation classification error rate (APCER) and bona fide presentation classification error rate (BPCER) [1]. APCER is a measure of falsely accepting the morphed images as bonafide images. Whereas, the BPCER is a measure of falsely rejecting the bonafide images by classifying them as morphed images. Here, the detection equal error rate (D-EER) point (where APCER=BPCER) is reported, along with the BPCER10 (where APCER = 10%) and BPCER20 (where APCER = 5%), as described in [3].



(a) Subject 1 (b) Subject 2 (c) Facefusion (d) UBO Morpher

Fig. 4: Sample images from FRGC subset and their morphs

(a) Subject 1 (b) Subject 2 (c) FaceFusion (d) UBO Morpher

Fig. 5: Sample images from FERET subset and their morphs

### 4.3 Experiment setup and results

The experiments were carried out under different settings and with various datasets to fine-tune and evaluate the reliability of the proposed method. The final results are hereby reported in this section.

**Effect of increasing contrast** For the preprocessing step, we experimented with increasing the contrast of the cropped eyebrow region. Since image contrast can be used to enhance the differentiation in the textures present in the image, the idea is that this can further increase the frequency content of the bonafide images as compared to the morphed images. Figure 6 shows the DET curves by varying the contrast on the FRGC images. The ISO metrics are presented in table 2 where it can be seen that the assumption is correct showing that increasing contrast helps improve the efficiency of the system.

Table 2: Effect of enhancing contrast on morph detection

| Image Enhancement | D-EER (%) | BPCER10 (%) | BPCER20 (%) |
|---|---|---|---|
| No | 8.5 | 7.3 | 13.9 |
| Yes (high contrast) | 6.5 | 4.2 | 9.6 |

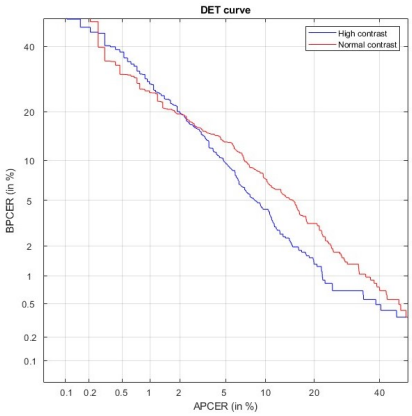



Fig. 6: DET curves by varying contrast

**Effect of cropping low-frequency content** Since the eyebrows are associated with the presence of high-frequency content, we experimented with cropping the low-frequency coefficients in the frequency spectrum. The experiments were conducted by ignoring 0%, 5%, and 10% of the low-frequency region from the calculations. The results are presented in table 3 which show that cropping the low-frequency region slightly reduces the performance of morphed image detection. Since the results are against the proposed idea, this step was not incorporated in the final proposed algorithm.

Table 3: Effect of ignoring low-frequency component

| Crop (%) | D-EER (%) | BPCER10 (%) | BPCER20 (%) |
|---|---|---|---|
| 0 | 6.5 | 4.2 | 9.6 |
| 5 | 6.6 | 3.8 | 9.9 |
| 10 | 6.7 | 4.1 | 9.8 |

**Final results on different datasets** Table 4 shows the results by applying the proposed scheme on the two datasets separately and then combining them. It can be seen that the proposed scheme gives a much better result with the FRGC dataset than with the FERET dataset. D-EER of 6.5% obtained with the FRGCv2 dataset is considerably lower than the D-EER of 22.2% on the FERET dataset.

On inspecting the images, it was found that the FERET images have lower quality compared to the FRGC dataset. This can also be attributed to the fact that the FERET images are relatively old (from 2011) compared to the FRGCv2

Table 4: Detection performance with different datasets

| Dataset | D-EER (%) | BPCER10 (%) | BPCER20 (%) |
|---|---|---|---|
| FRGCv2 | 6.5 | 4.2 | 9.6 |
| FERET | 22.2 | 38.2 | 51.7 |
| Combined | 14.2 | 17.02 | 23.2 |

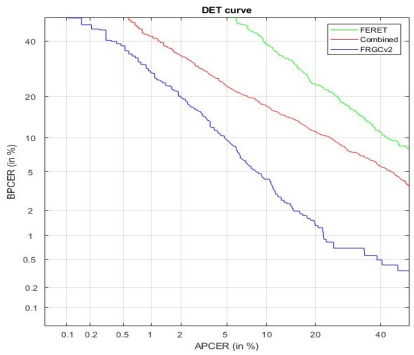



Fig. 7: DET curves obtained by applying the proposed scheme on different datasets

images (from 2014). Hence, due to the lower resolution of the images in the FERET dataset, it is harder to differentiate between a bonafide image and a morphed image. This claim is supported by the sizes of files from both datasets as shown in the table 5. These results are also supported by the findings in [18], where all MAD algorithms based on texture descriptors gave better results for the FRGC dataset compared to FERET.

Table 5: Bonafide image sizes among different datasets (in Kb)

| Dataset | Min | Max | Average |
|---|---|---|---|
| FRGCv2 | 704.4 | 1218.6 | 924.7 |
| FERET | 344.4 | 1065.8 | 722.2 |

**Comparison with previous work** In this section, the results will be presented by comparing them with the previous S-MAD techniques. For comparing the results with [10], experiments are performed on the FRGC dataset by dividing the dataset into training and testing subsets. The resulting error rates are presented in table 6. These also include ACER which is the average classification error rate [10]. These error rates are higher than the ones obtained in [10] showing that the proposed scheme does not improve the detection performance. However, if

we consider the overall performance on different datasets, the proposed scheme gives a lower D-EER of 22.2% in comparison with ACER of 38.24% in the other paper.

Table 6: BPCER, APCER, and ACER values with FRGC dataset

| Subjects | Total | Rightly classified | Wrongly classified | APCER | BPCER | ACER |
|---|---|---|---|---|---|---|
| Bonafide | 720 | 680 | 40 | 5.5 | 4.9 | 5.2 |
| Morphs | 964 | 916 | 48 | | | |

## 5 Conclusion and Discussion

The results indicate the effectiveness of the proposed method in detecting morphed images. The frequency spectrum analysis of the eyebrow region proves to be a promising approach for the detection of morphed images in light of the results. In addition to the S-MAD scenario, the proposed method can also be applied in a D-MAD system where a reduction in error rate is expected. Even though the detection capabilities were found to be dependent on the choice of dataset, these results were expected given the quality of images varied between the datasets, as explained in the results section. However, the detection capabilities were found to be robust against two different kinds of morphing techniques.

There are some limitations of using this approach that need to be investigated further. 1) People with certain diseases can not have eyebrows. Our datasets do not contain any such cases and hence the result of the segmentation method and frequency analysis in these cases needs can be studied for improving this method. 2) The morphed images used in the experiments are created from automated morphing algorithms. For an attacker to conduct a successful attack, a manually generated image is sufficient. So, further analysis can be made to study the possibility of altering a morphed image to bypass the proposed detection scheme.

## References

1. Biometrics, I.: Iso/iec 30107-1: 2016. information technology biometric presentation attack detection. Part 1 Fram. Int. Organ. Stand (2016)
2. Carlos-Roca, L.R., Torres, I.H., Tena, C.F.: Facial recognition application for border control. In: 2018 International Joint Conference on Neural Networks (IJCNN). pp. 1–7. IEEE (2018)
3. Debiasi, L., Rathgeb, C., Scherhag, U., Uhl, A., Busch, C.: Prnu variance analysis for morphed face image detection. In: 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS). pp. 1–9. IEEE (2018)
4. dlib.net/face_landmark_detection.py.html. http://dlib.net/face_landmark_detection.py.html, (Accessed on 04/30/2023)

5. Facefusion - have fun mixing faces together! - home of the best face fusion app for iphone and ipad. http://www.wearemoment.com/FaceFusion/, (Accessed on 05/08/2023)
6. Ferrara, M., Franco, A., Maltoni, D.: The magic passport. IEEE International Joint Conference on Biometrics pp. 1–7 (2014)
7. Ferrara, M., Franco, A., Maltoni, D.: Decoupling texture blending and shape warping in face morphing. In: 2019 international conference of the biometrics special interest group (BIOSIG). pp. 1–5. IEEE (2019)
8. ibug - resources - facial point annotations. https://ibug.doc.ic.ac.uk/resources/facial-point-annotations/, (Accessed on 04/28/2023)
9. ICAO, D.: 9303-machine readable travel documents-part 9: Deployment of biometric identification and electronic storage of data in emrtds. International Civil Aviation Organization (ICAO) **123** (2015)
10. Ndeh de Mbah, E.Y.: Morphed Image Detection using Local Spectrum Analysis. B.S. thesis, University of Twente (2021)
11. Phillips, P.J., Flynn, P.J., Scruggs, T., Bowyer, K.W., Chang, J., Hoffman, K., Marques, J., Min, J., Worek, W.: Overview of the face recognition grand challenge. In: 2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05). vol. 1, pp. 947–954. IEEE (2005)
12. Phillips, P.J., Wechsler, H., Huang, J., Rauss, P.J.: The feret database and evaluation procedure for face-recognition algorithms. Image and vision computing **16**(5), 295–306 (1998)
13. Raja, S.V.R.R.K., Busch, C.: Face morphing attack generation & detection: A comprehensive survey
14. Ramachandra, R., Raja, K., Busch, C.: Detecting morphed face images. In: 8th IEEE International Conference on Biometrics Theory, Applications and Systems, BTAS. pp. 1–7 (2016)
15. Sadr, J., Jarudi, I., Sinha, P.: The role of eyebrows in face recognition. Perception **32**(3), 285–293 (2003)
16. Scherhag, U., Budhrani, D., Gomez-Barrero, M., Busch, C.: Detecting morphed face images using facial landmarks. In: Image and Signal Processing: 8th International Conference, ICISP 2018, Cherbourg, France, July 2-4, 2018, Proceedings 8. pp. 444–452. Springer (2018)
17. 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: 2017 5th international workshop on biometrics and forensics (IWBF). pp. 1–6. IEEE (2017)
18. Scherhag, U.J.: Face Morphing and Morphing Attack Detection. Ph.D. thesis (2020)
19. Spreeuwers, L., Schils, M., Veldhuis, R.: Towards robust evaluation of face morphing detection. In: 2018 26th European Signal Processing Conference (EUSIPCO). pp. 1027–1031. IEEE (2018)
20. Zhang, L.B., Peng, F., Long, M.: Face morphing detection using fourier spectrum of sensor pattern noise. In: 2018 IEEE international conference on multimedia and expo (ICME). pp. 1–6. IEEE (2018)