Morphing Attack Detection using Laplace operator based features

Ulrich Scherhag[1], Daniel Fischer[1], Sergey Isadskiy[1], Jonas Otte[2], and Christoph Busch[1]

da/sec – Biometrics and Internet Security Research Group, Hochschule Darmstadt, Germany
{ulrich.scherhag, daniel.fischer, christoph.busch}@h-da.de, isadskiy@googlemail.com
Technical University of Denmark
jonas.soerensen.84@gmail.com

Abstract

The vulnerability of facial recognition systems through morphing attacks is a known problem. Since the first publication about this vulnerability of facial recognition systems, a variety of morphing attack detection methods have been presented, promising an automated detection of such fraudulent attacks. In this work, a new approach is presented attempting to distinguish bona fide from morphed images based on information about the edges in the image extracted by the Laplace operator. It can be demonstrated that the features employed contain information that can contribute to the detection of morphed face images.

1 Introduction

Image morphing techniques can be used to combine information from two (or more) images into one image. Morphing techniques can also be used to create a morphed facial image from the biometric face images of two individuals, of which the biometric information is similar to that of both individuals. Realistically looking morphed face images can be generated by unskilled users applying readily available tools [17].

In most countries, the passport photo is provided by the applicant in digital or analogue form when applying for a passport. This allows a wanted criminal to create a morphed passport photo with the help of an accomplice, with which the accomplice can then apply for a passport. Since most morphed passport photos are capable of deceiving a human observer as well as face recognition systems [3, 14], the wanted criminal can authenticate himself with the passport of his accomplice and, e.g., use the passport to cross borders. This problem can be reduced to a large extent by a supervised enrolment during the passport application process, as is done in Norway. However, as long as not all countries whose passports are accepted introduce supervised enrolment processes, all countries will have to check at the border for morphed passport photos in the passports of other countries as well.

Due to the great attack potential, there is a growing interest in reliable methods to detect morping attacks. The methods for detecting morping attacks can be divided into two classes. *Single image* Morphing Attack Detection (MAD) and *differential* MAD. With *single image* MAD, the algorithm only has the potential morph at its disposal, for example the passport photo at the handover during the passport application. In the *differential* MAD scenario, however, the algorithm has access to an additional trusted live capture of the subject, for example the sample image the eGate captures during passport control during border crossing of the subject. Most algorithms proposed to date are based on the *single image* scenario. This scenario is easier to reproduce by databases and the algorithms are easier to implement. *Differential* MAD algorithms, however, have the capability to achieve higher recognition performance and

Table 1: Overview of most relevant differential MAD algorithms.

Reference	Approach	Category	Morphing method	Source face DB
Scherhag *et al.* [18]	Differences in deep face features with SVM	Feature comparison	4 different Methods	FERET [13], FRGCv2 [12]
Scherhag *et al.* [16]	Differences in BSIF features with SVM	Feature comparison	triangulation + blending	FRGCv2 [12]
Scherhag *et al.* [15]	Differences in angles of landmark pairs with SVM	Feature comparison	triangulation + blending	ARface [10]
Damer *et al.* [2]	Directed distances of landmarks with SVM	Feature comparison	triangulation + blending (+ swapping)	FERET [13]
Ferrara *et al.* [4]	Demorphing	Morphing reversion	triangulation + blending, GIMP/GAP	ARface [10]
Ferrara *et al.* [5]	Demorphing	Morphing reversion	triangulation + blending, GIMP/GAP	ARface [10], CAS-PEAL-R1 [6]
Peng *et al.* [11]	GAN-based Demorphing	Morphing reversion	triangulation + blending [9]	in-house

robustness due to the additional information provided by trusted live capture. In this paper a *differential* MAD algorithm is proposed.

Table 1 lists the relevant *differential* MAD algorithms. The algorithms can be divided into two categories. Feature comparison and morphing reversion. Feature comparison algorithms are based on the comparison of features extracted from the potential morph and the trusted live capture. These can be explicit features like texture features extracted by BSIF [16] or landmark features [15], or implicit features extracted by deep learning [18].

Morphing reversion, on the other hand, follows the approach that the (possibly) performed morphing process for the passport photo is reversed using the trusted live capture. The idea is that after the revision of the morphing in case of a morph, the second subject appears, but if no other subject is present (bona fides passport photo), the subject remains in the passport photo after the revision.

The approach proposed in this publication is based on feature comparison. It is assumed that the number and intensity of edges in the image is reduced by the averaging process during the morphing of two images. The approach aims to make these parameters measurable using the Laplace operator. To achieve independence of the algorithm from the facial characteristics of the subject, the number and intensity of edges in the trusted live capture is subtracted from those in the potential morph.

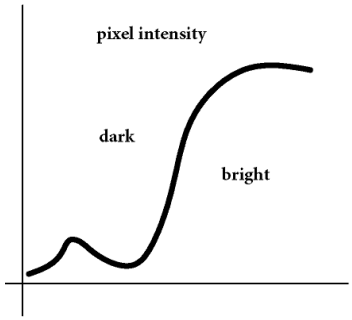
2 Laplace operator

The Laplace operator highlights regions of intensity discontinuities and is usually used in image processing to find edges or other fine details on a dark background. It could be interpreted as an extension of the Sobel operator [8]. Since edges represent significant local changes of intensity in an image, the Sobel operator calculates the first-order derivative of the intensity function (the grayscale-values of the image), that reaches its local maximum in the edge regions. Figure 1c to 1e illustrates the behaviour of the Sobel operator for edges in the grayscale image. In the second derivation, a corner leads to zero crossings, as shown in Figure 1e.

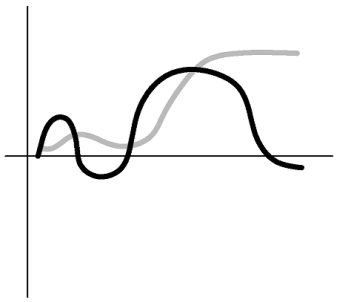
The Laplace operator approximates the second derivative of the Sobel operator, whereby edges in the original image are reflected as bright areas in the Laplace image. For example, the corner of the mouth (indicated by a circle in figure 1a), which leads to a bright region in

(a) Crop of faceimage. An example for an edge is highlighted by a red circle

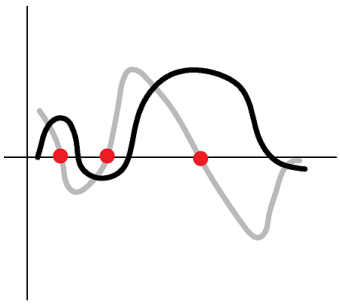
(b) Sobel operator on cropped faceimage



(c) Example of Sobel operator on edges



(d) Example of first derivative of the Sobel operator on edges



(e) Example of second derivative of the Sobel operator on edges. Zero crossings are highlighted

Figure 1: Example for the principle of the Laplace operator

Figure 1b.

Mathematically the Laplace operator (Δ) for 2-dimensional space in a Cartesian coordinate system is defined as the dot product of the two gradient vectors of the image:

$$\Delta f = \begin{bmatrix} \frac{\partial f}{\partial x} \frac{\partial f}{\partial y} \end{bmatrix} \begin{bmatrix} \frac{\partial f}{\partial x} \\ \frac{\partial x}{\partial y} \end{bmatrix} = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} \tag{1}$$

Due to the fact, that the Laplace operator approximates a second derivative measurement on the image, the result of the transformation is very sensitive to noise. To handle this, a Gaussian blur is applied to the original image, since it reduces the high frequency noise components to the differentiation step, leading to the so-called Laplacian of Gaussian (LoG) filter.

3 Proposed system

The proposed algorithm for morphing attack detection is based on the LoG operator, which can be divided into the Gaussian and the Laplace filter.

Gaussian filter:
To reduce noise, the image is processed by smoothing with a Gaussian filter. In the proposed method the kernel size of 3 is chosen for facial images cropped as depicted in Figure 1a and scaled to 320×320 pixels. Larger kernel would lead to a higher smoothing effect, reducing unwanted noise artefacts, but also the number of zero crossings would drop, reducing the capabilities of the Laplace filter.

Laplace filter:
As described in equation 1 the two-dimensional Laplace operator is composed of the second derivative in x and y dimension. These derivatives can be approximated by filter operations of size 3×3:

$$\partial^2 x = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -2 & 1 \\ 0 & 0 & 0 \end{bmatrix} \quad \partial^2 y = \begin{bmatrix} 0 & 1 & 0 \\ 0 & -2 & 0 \\ 0 & 1 & 0 \end{bmatrix} \tag{2}$$

According to equation 1 the resulting Laplace operator can be written as:

$$\Delta = \begin{bmatrix} 0 & 0 & 0 \\ 1 & -2 & 1 \\ 0 & 0 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 & 0 \\ 0 & -2 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix} \tag{3}$$

The edges of the image can be determined using the zero crossings of the Laplace function, as shown in figure 1. To detect these, regions with sign changes are searched for in the Laplace image. To form the feature vector, the intensities of the determined zero crossings are transferred into a histogram, which is subsequently normalized.

To achieve the differential detection scenario, the histograms of probe and corresponding reference are subtracted and z-normalized, so that the differential histogram is used as a classifier input [16]. A number of support vector machines (SVM) with radial basis function (RBF) kernel, which is frequently used in SVM classification [1], are trained on the pre-processed input data.

4 Experiments

The Experiments are performed on the MAD database, introduced in [18], which consists of images from the FRGCv2 [12] and color FERET [13] face database. The morphs are created, by applying four different automated morphing tools:

1. **FaceFusion**[1], a proprietary morphing algorithm. Originally being an iOS app, we deployed an adaptation for Windows which uses the 68 landmarks of Dlib and Delaunay triangles. After the morphing process, certain regions (eyes, nostrils, hair) of the first face image are blended over the morph to hide artefacts. The corresponding landmarks of upper and lower lips can be reduced as described in [9] to avoid artefacts at closed mouths. The created morphs have a high quality and low to no visible artefacts.

2. **FaceMorpher**[2], an open-source implementation using Python. In the version applied for this work, the algorithm uses STASM for landmark detection. Delaunay triangles,

[1] www.wearemoment.com/FaceFusion/
[2] github.com/alyssaq/face_morpher

which are formed from the landmarks, are wrapped and blended. The area outside the landmarks is averaged. The generated morphs show strong artefacts in particular in the area of neck and hair.

3. **OpenCV**, a self-made morphing algorithm derived from "Face Morph Using OpenCV"[3]. This algorithm works similar to FaceMorpher. Important differences between the algorithms are that for landmark detection Dlib is used instead of STASM and that additional landmarks are positioned at the edges of the image, which are also used to create the morphs. Thus, in contrast to FaceMorpher, the outer facial area does not consist of an averaged image, but like the rest of the image, of morphed triangles. However, visible artefacts outside the face area can be observed, which is mainly due to missing landmarks.

4. **UBO-Morpher**, the morphing tool of University of Bologna, as used, e.g., in [4]. Dlib landmarks were used for this algorithm. The morphs are generated by triangulation, averaging and blending. To avoid the artefacts in the area outside the face, the morphed face is copied to the background of one of the original images. Even if the colors are adjusted at boundaries, visible edges may appear at the transitions.

The SVMs were trained on the images originating from FRGCv2 and subsequently evaluated on the FERET, and vice versa. Thus, a strict separation of training and test data is achieved, as well as a high variance in the data between these sets. The test and training sets only consist of images, created with one of the four morphing tools, mentioned above. As an example, the data trained on FRGC with FaceFusion is evaluated on FERET with OpenCV.

The accuracy of the detection algorithm is reported using the Detection Equal Error Rate (D-EER), i.e., at the decision threshold where the proportion of attack presentations incorrectly classified as bona fide presentations (APCER) is as high as the proportion of bona fide presentations incorrectly classified as presentation attack (BPCER). For APCER and BPCER the definitions of ISO IEC 30107-3 [7] for measuring accuracy of presentation attack detection are used:

APCER: proportion of attack presentations incorrectly classified as bona fide presentations in a specific scenario

BPCER: proportion of bona fide presentations incorrectly classified as presentation attacks in a specific scenario

The results determined on the database are shown in table 2. It can be seen that the presented approach is basically suitable to recognize morphed images, which confirms that the Laplace filter is able to extract useful information. However, the error rates also show that the approach needs further improvement before it is able to produce error rates that can be compared to other differential MAD methods. In particular, the results achieved on the basis of deep features [18] are significantly better.

The results show that the morphs generated by the more advanced morphing algorithms (FaceFusion and UBO-Morpher) tend to be more difficult to detect with the Laplace operator-based approach than the images morphed with the simpler algorithms. For example, after training on FaceFusion Morphs, the FaceMorpher Morphs of the FERET database can be recognized with a D-EER of 20.9%, whereas the FaceFusion Morphs themselves can only be recognized with a D-EER of 27.3%.

[3] www.learnopencv.com/face-morph-using-opencv-cpp-python/

Table 2: Performance results of Laplace operator based MAD

Train DB	Train MA	Test MA	D-EER (in %)
FERET	FaceFusion	FaceFusion	35.05
		FaceMorpher	28.10
		OpenCV	32.01
		UBO-Morpher	33.65
	FaceMorpher	FaceFusion	32.68
		FaceMorpher	21.78
		OpenCV	27.27
		UBO-Morpher	28.88
	OpenCV	FaceFusion	32.62
		FaceMorpher	23.15
		OpenCV	27.73
		UBO-Morpher	29.58
	UBO-Morpher	FaceFusion	31.16
		FaceMorpher	22.06
		OpenCV	26.82
		UBO-Morpher	28.46
FRGC	FaceFusion	FaceFusion	27.31
		FaceMorpher	20.88
		OpenCV	23.14
		UBO-Morpher	25.41
	FaceMorpher	FaceFusion	28.57
		FaceMorpher	21.73
		OpenCV	23.99
		UBO-Morpher	25.54
	OpenCV	FaceFusion	28.54
		FaceMorpher	22.62
		OpenCV	24.65
		UBO-Morpher	26.17
	UBO-Morpher	FaceFusion	28.54
		FaceMorpher	22.24
		OpenCV	24.15
		UBO-Morpher	26.01

The approach proposed in this publication is based on feature comparison. It is assumed that the number and intensity of corners in the image is reduced by the averaging process during the morphing of two images. The approach aims to make these parameters measurable using the Laplace operator.

5 Conclusion

Morphing attacks remain a serious threat to the proper functioning of facial recognition systems.Especially in the area of automatic border control via eGates, a solution for the robust recognition of morphed images is needed to ensure a secure operation. In this paper it is demonstrated, that information about edges in the image extracted by the Laplace operator

can contribute to the detection of these attacks. Although the results obtained so far do not allow the use of these feature extractors in a solitary system, they motivate further research towards these feature extractors, whether to further refine this approach or to combine it with other approaches to achieve a more robust overall system.

6 Acknowledgments

This research work has been funded by the German Federal Ministry of Education and Research and the Hessian Ministry of Higher Education, Research, Science and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

References

[1] Yin-Wen Chang, Cho-Jui Hsieh, Kai-Wei Chang, Michael Ringgaard, and Chih-Jen Lin. Training and testing low-degree polynomial data mappings via linear svm. *Journal of Machine Learning Research*, 11(4), 2010.

[2] Naser Damer, Viola Boller, Yaza Wainakh, Fadi Boutros, Philipp Terhörst, Andreas Braun, and Arjan Kuijper. Detecting face morphing attacks by analyzing the directed distances of facial landmarks shifts. In *Proceedings of the 40th German Conference of Pattern Recognition (GCPR)*, 2018.

[3] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. On the effects of image alterations on face recognition accuracy. In *Face Recognition Across the Imaging Spectrum*, pages 195–222. Springer International Publishing, 2016.

[4] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. Face demorphing. *IEEE Transactions on Information Forensics and Security*, 13(4):1008–1017, apr 2018.

[5] Matteo Ferrara, Annalisa Franco, and Davide Maltoni. Face demorphing in the presence of facial appearance variations. In *Proceedings of the 26th European Signal Processing Conference (EUSIPCO)*, 2018.

[6] Wen Gao, Bo Cao, Shiguang Shan, Delong Zhou, Xiaohua Zhang, and Debin Zhao. The CAS-PEAL large-scale chinese face database and baseline evaluations. Technical Report JDL-TR-04-FR-001, Chinese Academy of Sciences, May 2004.

[7] ISO/IEC JTC1 SC37 Biometrics. Information technology – biometric presentation attack detection – part 3: Testing and reporting. ISO ISO/IEC IS 30107-3:2017, International Organization for Standardization, Geneva, Switzerland, 2017.

[8] N. Kanopoulos, N. Vasanthavada, and R.L. Baker. Design of an image edge detection filter using the sobel operator. *IEEE Journal of Solid-State Circuits*, 23(2):358–367, apr 1988.

[9] Andrey Makrushin, Tom Neubert, and Jana Dittmann. 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*. SCITEPRESS - Science and Technology Publications, 2017.

[10] Aleix Martinez and Robert Benavente. The AR face database. Technical Report 24, Computer Vision Center (CVC), June 1998.

[11] Fei Peng, Le-Bing Zhang, and Min Long. FD-GAN: Face de-morphing generative adversarial network for restoring accomplice's facial image. *IEEE Access*, 7:75122–75131, 2019.

[12] P.J. Phillips, P.J. Flynn, T. Scruggs, K.W. Bowyer, J. Chang, K. Hoffman, J. Marques, J. Min, and W. Worek. Overview of the face recognition grand challenge. In *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, 2005.

[13] P.Jonathon Phillips, Harry Wechsler, Jeffery Huang, and Patrick J. Rauss. The FERET database and evaluation procedure for face-recognition algorithms. *Image and Vision Computing*, 16(5):295–306, apr 1998.

[14] David J. Robertson, Andrew Mungall, Derrick G. Watson, Kimberley A. Wade, Sophie J. Nightingale, and Stephen Butler. Detecting morphed passport photos: a training and individual differences approach. *Cognitive Research: Principles and Implications*, 3(1), jun 2018.

[15] Ulrich Scherhag, Dhanesh Budhrani, Marta Gomez-Barrero, and Christoph Busch. Detecting morphed face images using facial landmarks. In *Proceedings of the 2018 International Conference on Image and Signal Processing (ICISP)*, pages 444–452. Springer International Publishing, 2018.

[16] Ulrich Scherhag, Christian Rathgeb, and Christoph Busch. Towards detection of morphed face images in electronic travel documents. In *2018 13th IAPR International Workshop on Document Analysis Systems (DAS)*. IEEE, apr 2018.

[17] Ulrich Scherhag, Christian Rathgeb, Johannes Merkle, Ralph Breithaupt, and Christoph Busch. Face recognition systems under morphing attacks: A survey. *IEEE Access*, 7:23012–23026, 2019.

[18] Ulrich Scherhag, Christian Rathgeb, Johannes Merkle, and Christoph Busch. Deep face representations for differential morphing attack detection. *IEEE Transactions on Information Forensics and Security*, 15:3625–3639, 2020.