
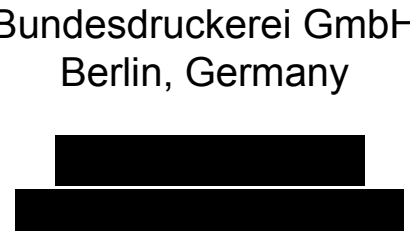



# DISTRIBUTED AND GDPR/IPR COMPLIANT BENCHMARKING OF FACIAL MORPHING ATTACK DETECTION SERVICES



Advanced Multimedia and Security Lab  
Otto-von-Guericke University of Magdeburg  
Magdeburg, Germany




Bundesdruckerei GmbH  
Berlin, Germany



DERMALOG Identification Systems GmbH  
Hamburg, Germany



Fraunhofer HHI  
Berlin, Germany



Fraunhofer IPK  
Berlin, Germany

**International Conference on Biometrics for Borders**  
**October 10, 2019, Warsaw, Poland**

## Project „ANANAS“

**ANANAS:** Anomalie-Erkennung zur Verhinderung von Angriffen auf  
gesichtsbildbasierte Authentifikationssysteme

- *Anomaly Detection to Prevent Attacks on Facial Image Based Authentication Systems* -

*Project Duration: June 2016 – May 2020*

*Funding:*



*Consortium members:*



*Eine Forschungsinitiative zur „Erkennung und Aufklärung von IT-Sicherheitsvorfällen“ im Rahmen des Förderprogramms „IKT 2020 – Forschung für Innovationen“*

# Motivation

- Human examiners
    - Prone to errors with “unknown” faces
    - Unable to detect high-quality morphs
  - Automated face recognition (AFR) systems
    - Very high acceptance rates when comparing morphed face images with a “live” image/stream
- ⇒ **Need for morphing detection algorithms**

# Motivation

- Protection from face morphing attacks (FMA) is a **young research field**
- Several research groups have already designed and prototypically implemented a bunch of morphing attack detection (MAD) approaches
  - At least **five research groups**
- Challenge: **GDPR/IPR compliant** benchmarking of MAD approaches
- GDPR = **General Data Protection Regulation**
  - Handling personal/biometric data
- IPR = **Intellectual Property Rights**
  - Sharing a proprietary software

## GDPR challenge

- Facial photographs, in particular those of a high quality, are regarded as **personal biometric data** which is protected by GDPR
  - **Written consent** from face image donors
  - Sharing data with third parties is prohibited by the European law warranting the image donors' **right to request image removal at any moment**
  - Photographs must be **stored on a protected media** disabling the option of copying the data to any uncontrolled media
- ⇒ Putting the data into a public domain is not possible
- A standard solution is not to grant access to the database, but to ask the developers of MAD approaches to submit their algorithms for evaluation

## IPR challenge

- Source code cannot be shared
  - Algorithms are developed
    - for different platforms
    - using different programming languages
    - using proprietary libraries
    - with different requirements to hardware
- ⇒ Compiling executables for a particular platform is not always possible
- Benchmarking is conducted by an independent body ensuring that algorithms are not
    - disassembled
    - used for tasks other than benchmarking
    - offered to third parties without consent of the owner

## State of the art

- Existing benchmarks can be assigned to one of two categories:
  - **Public benchmarks** with the data unknown to MAD developers for independent, unbiased comparison
  - **Individual benchmarks** with self-collected or public data aiming at understanding the characteristics of MAD approaches and improving their performance

## State of the art

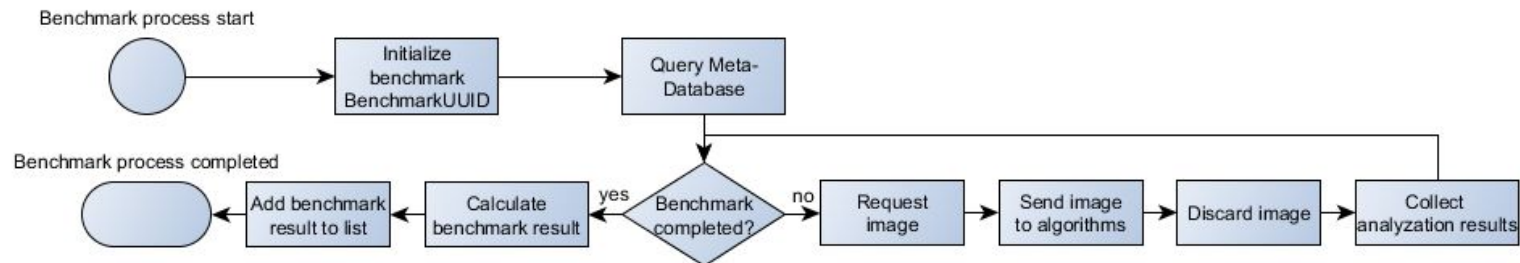
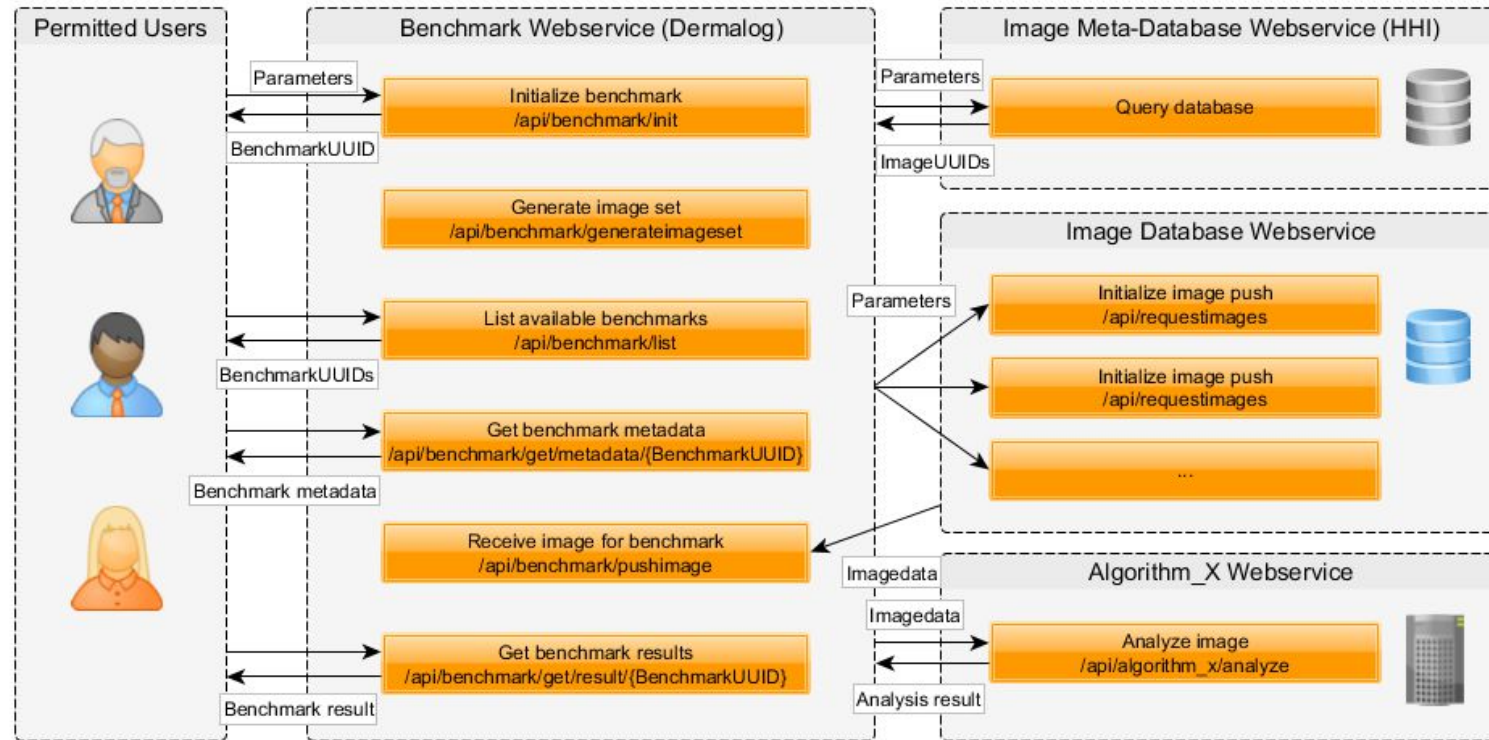
- Public benchmarks
  - FVC-onGoing Face Morphing Challenge maintained by the UNIBO
  - FRVT MORPH maintained by the NIST
- Both challenges provide i/o interfaces and encourage the potential participants to submit MAD solutions that are **compliant to the given runtime environment specifications**
- Contributions are supposed to be **executed on local servers of the organizers** with undisclosed genuine and morphed face images
- Benchmarking results are supposed to be publicly reported
- Issues
  - MAD algorithms have to be re-implemented to comply with the very restrictive run-time environment
  - Numbers of submissions and test runs per participant are limited
  - Composition of the test dataset cannot be influenced, which restricts the understanding of how specific image characteristics influence the error rates of a MAD algorithm



# ANANAS benchmarking infrastructure

- Based on Representational state transfer (REST)
  - POST requests with attached JSON objects
  - HTTPS for secure communication
  - Processed images are in a protected volatile memory
- Our network of RESTful Web services incl.
  - Services for automated generation of high-quality morphed face images
  - MAD services
  - Private face image databases
  - Meta-database of image IDs
- Benchmarking Web service (a core part of the framework)
  - Users communicates with the benchmarking Web service only
  - All components of the framework and the communication between them remain hidden
  - A User defines criteria for image selection and chooses MAD services to test
  - Request image IDs that meet certain criteria from the meta-database
  - Images are derived from one of the image databases and sent to the MAD services
  - Responses of MAD services are stored in the benchmarking log

# ANANAS Benchmark



## Hosts of Web services

Benchmark Web service	- DERMALOG Identification Systems GmbH (Dermalog)
Meta-Database Web service	- Fraunhofer Heinrich-Hertz Institut (HHI)
Image Database Web services	<ul style="list-style-type: none"> <li>- DERMALOG Identification Systems GmbH (Dermalog)</li> <li>- Fraunhofer Heinrich-Hertz Institut (HHI)</li> <li>- Fraunhofer Institute for Production Systems and Design Technology (IPK)</li> <li>- Otto-von-Guericke University of Magdeburg (OVGU)</li> </ul>
Algorithm_X Web services	<ul style="list-style-type: none"> <li>- Fraunhofer Heinrich-Hertz Institut (HHI)</li> <li>- Fraunhofer Institute for Production Systems and Design Technology (IPK)</li> <li>- Otto-von-Guericke University of Magdeburg (OVGU)</li> </ul>
Morphing Web services	<ul style="list-style-type: none"> <li>- Fraunhofer Heinrich-Hertz Institut (HHI)</li> <li>- Fraunhofer Institute for Production Systems and Design Technology (IPK)</li> <li>- Otto-von-Guericke University of Magdeburg (OVGU)</li> </ul>

## Benchmark test run

- Exemplary benchmarking run lasting from November 1st to December 3rd, 2018
- PUT face database [1]
- 680 genuine images (605 male / 75 female)
- 12000 morphed face images with two algorithms, 6000 each
- Morphing algorithms are deployed as Web services
  - OVGU [2]: 5321/679 male/female morphs
  - Fraunhofer HHI [3]: 5730/270 male/female morphs
- All morphed face images were compared with constituent face images using the Dermalog Face Recognition software [4]
  - The requirement for the inclusion of a morphed face image into the dataset is that both comparison scores exceed 80% similarity
- 6 MAD algorithms: *FaceNet-based* [5], *GoogLeNet-based* [3], *High-Dim LBP* [5], *VGG19-based (naive)* [6], *benford* [7], and *keypoints* [8].

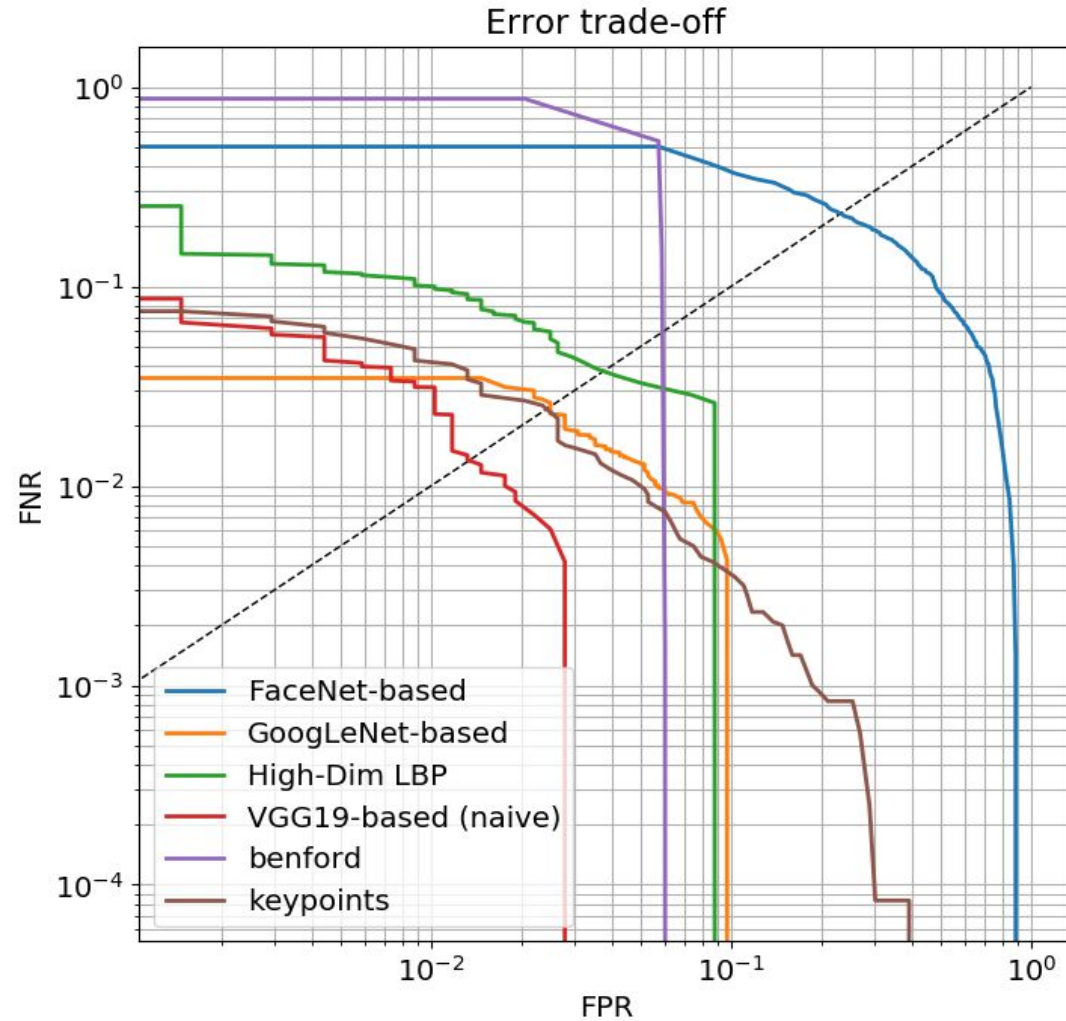
## Evaluation metrics

- Morphing detection is a standard detection problem with **morphed images as positive examples**
- Algorithms provide a score from 0 to 1 (1 for morph)
- The standard performance metrics:
  - **False Positive Rate (FPR)** giving a ratio of falsely detected **genuine** images  
(false positive = false alarm)
  - **False Negative Rate (FNR)** giving a ratio of falsely missed **morphed** images  
(false negative = miss)
- With evaluation set
  - DET curves
  - **Equal Error Rate (EER)**
  - FNR at a certain level of FPR (0.01%, 0.1%, 1%, 10%)

# Results

**FNR = APCER [9]**

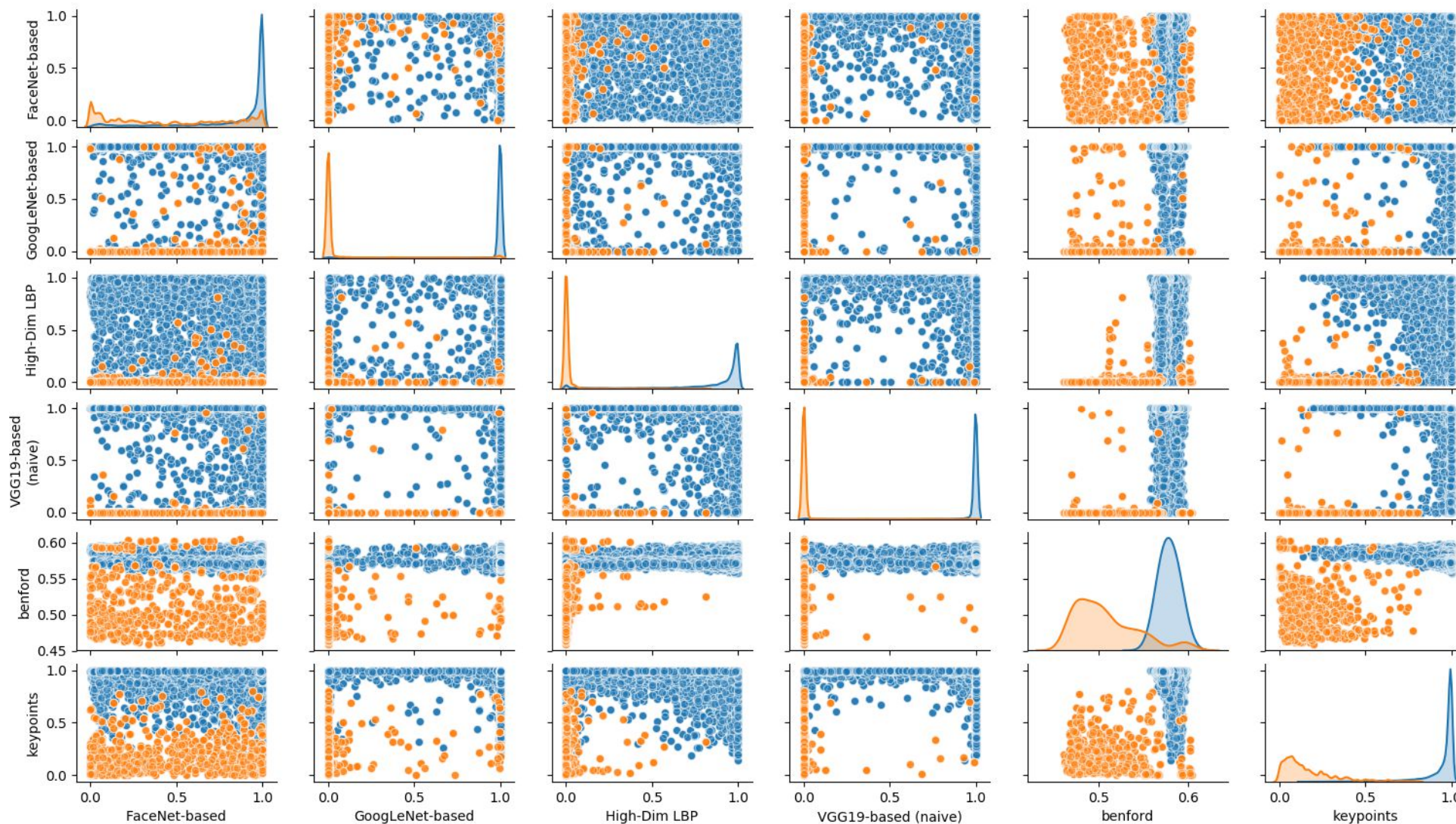
**FPR = BPCER [9]**





# Results

● morph  
● genuine



## Results

	FPR	FNR	FNR @ 0.01% FPR	FNR @ 0.1% FPR	FNR @ 1% FPR	FNR @ 10% FPR	EER
<i>FaceNet-based</i>	43.53%	12.54%	59.23%	59.09%	57.69%	37.65%	23.21%
<i>GoogLeNet-based</i>	3.97%	1.52%	<b>4.06%</b>	<b>4.03%</b>	3.66%	0.30%	2.53%
<i>High-Dim LBP</i>	0.15%	18.02%	25.96%	25.53%	10.03%	1.45%	3.77%
<i>VGG19-based (naive)</i>	1.03%	2.75%	10.29%	9.24%	<b>3.13%</b>	<b>0.00%</b>	<b>1.36%</b>
<i>benford</i>	53.09%	0.00%	99.94%	99.38%	93.82%	0.00%	5.97%
<i>keypoints</i>	4.71%	1.14%	7.93%	7.66%	4.19%	0.36%	2.43%

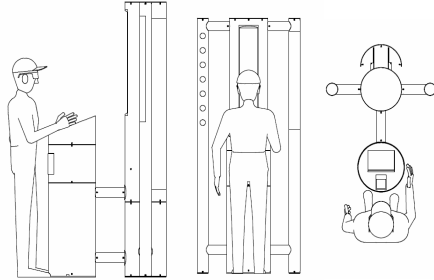


## Final remarks

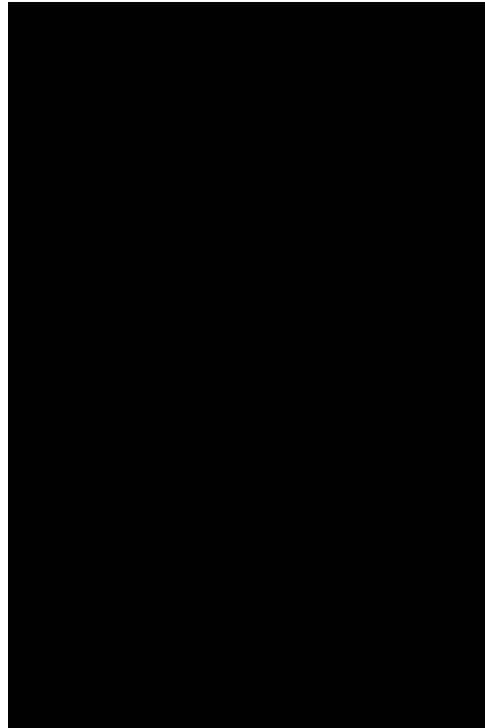
- REST technology allows for GDPR/IPR compliant evaluation of MAD approaches
- MAD services can be used not only as a part of the framework, but also individually
- Benchmarking results are reproducible and transparent for the benchmark users
- The demonstrated benchmarking run does not cover all capabilities of the framework, but gives an idea how the benchmark can be configured and how the results can be visualized
- More flexibility for developers of MAD approaches as well as more transparency in test image datasets
- Parties interested in benchmarking MAD approaches are invited to contact the authors in order to register as users of the framework so that they can browse through existing benchmarks as well as configure and run own ones
- Currently, the MAD Web services are integrated into the ABC reference environment of Bundesdruckerei (German official document printing agency)

# ANANAS Demonstrator

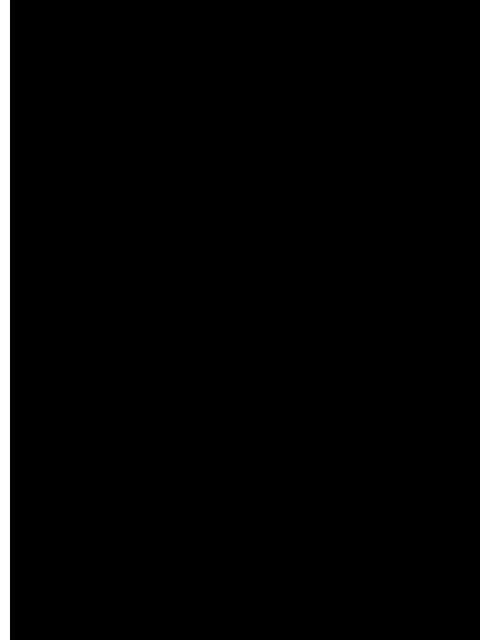
**2016**



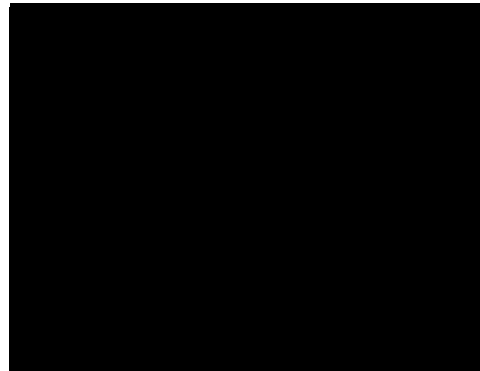
**2017**



**2018**



**2019**

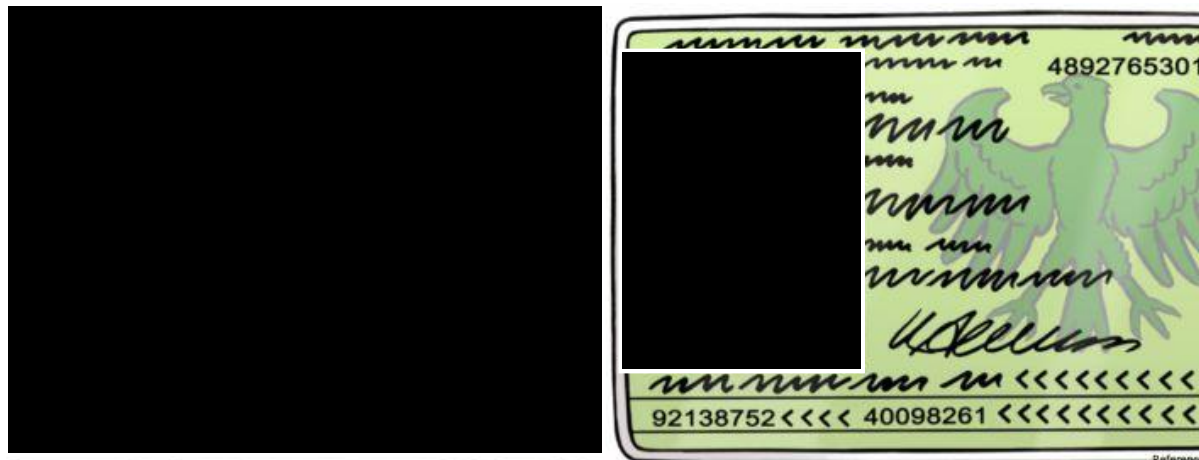


## References

- [1] A. Kasinski, A. Florek, and A. Schmidt, "The PUT face database," Image Processing and Communications 13:59-64, 2008
- [2] T. Neubert et al., "Extended StirTrace Benchmarking of Biometric and Forensic Qualities of Morphed Face Images," IET Biometrics 7(4):325–332, 2018
- [3] C. Seibold, W. Samek, A. Hilsmann, and P. Eisert, "Detection of Face Morphing Attacks by Deep Learning," Proc. 16th Int. Workshop on Digital Forensics and Watermarking (IWDW'17), pp. 107–120, 2017
- [4] Dermalog Face Recognition, <https://www.dermalog.com/products/software/face-recognition>, online, 02.10.2019
- [5] L. Wandzik, G. Kaeding, and R. Vicente-Garcia, "Morphing Detection Using a General-Purpose Face Recognition System," Proc. EUSIPCO'18, pp 1012–1016, 2018
- [6] C. Seibold, W. Samek, A. Hilsmann, P. Eisert, "Accurate and Robust Neural Networks for Security Related Applications Exemplified by Face Morphing Attacks," CoRR abs/1806.04265, 2018
- [7] A. Makrushin, C. Kraetzer, T. Neubert and J. Dittmann, "Generalized Benford's Law for Blind Detection of Morphed Face Images," Proc. IH&MMSec'18, pp. 49-54, 2018
- [8] C. Kraetzer et al., "Modeling Attacks on Photo-ID Documents and Applying Media Forensics for the Detection of Facial Morphing," Proc. IH&MMSec'17, pp 21-32, 2017
- [9] ISO/IEC JTC1 SC37 Biometrics. ISO/IEC IS 30107-3:2017, IT – Biometric presentation attack detection – Part 3: Testing and Reporting

## The End

Thank you for your attention!



„match“ or „no match“ 😊