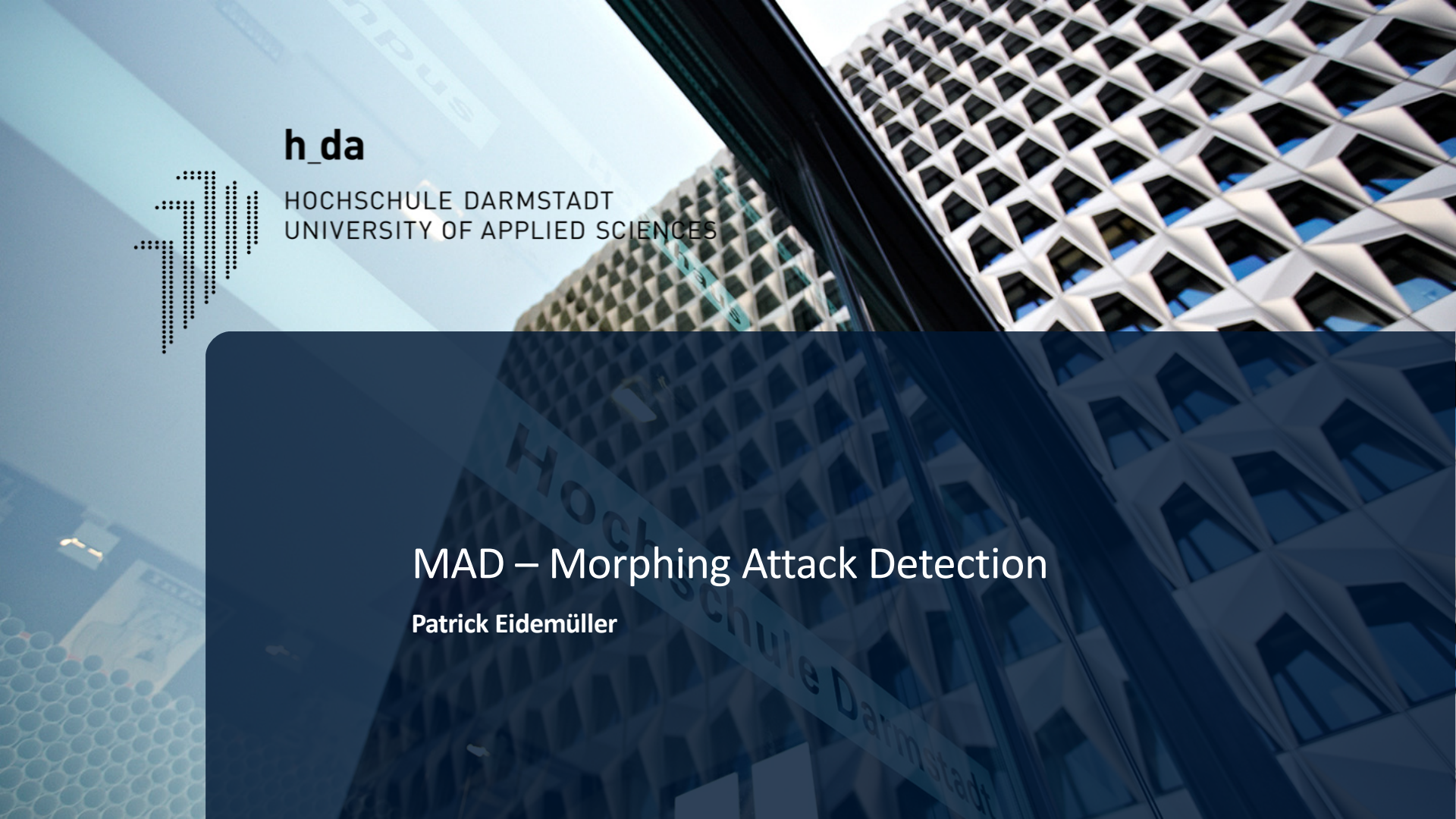


h_da

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

MAD – Morphing Attack Detection

Patrick Eidemüller

Face Morphing

Figure 1: Example of face morphed image

Detecting Moprhed Face Images: R. Raghavendra, Kiran B. Raja, Christoph Busch

h_da

Face Morphing

Subject 1

Subject 2

Morphed Face

match

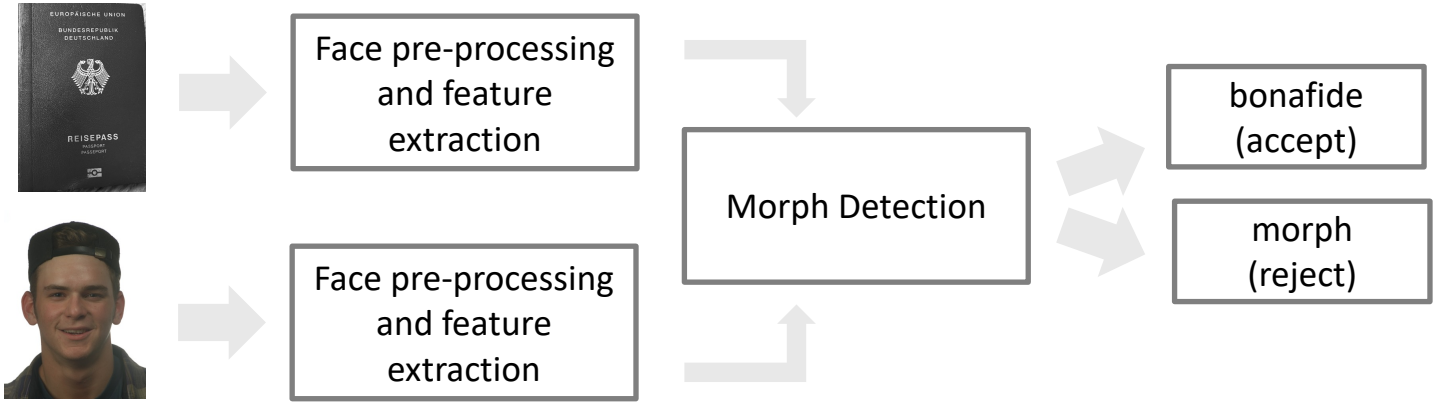
Subject 1 live face

match

Subject 2 live face

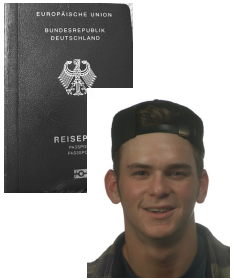
Prof. Dr. Vorname Nachname
Hochschulkommunikation
Hochschule Darmstadt

Morphing Attack Detection Categories



Handbook of Digital Face Manipulation and Detection: Ulrich Scherhag, Christian Rathgeb, and Christoph Busch

Morphing Attack Detection Categories



Face pre-processing and feature extraction

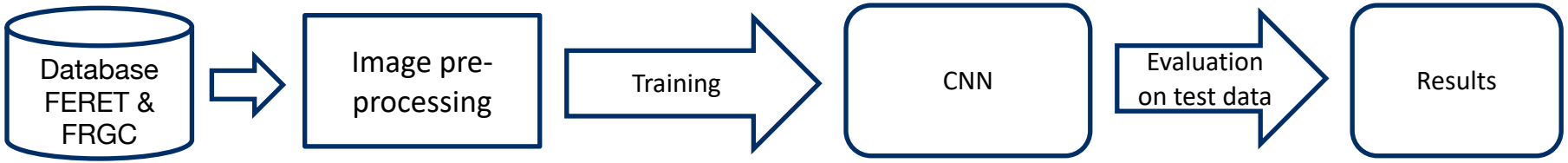
Morph Detection

bonafide (accept)

morph (reject)

Handbook of Digital Face Manipulation and Detection: Ulrich Scherhag, Christian Rathgeb, and Christoph Busch

Self trained Model

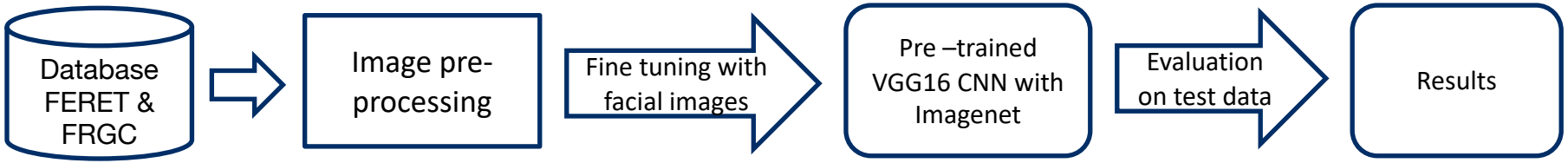


- Face Cropping
- Data Augmentation
- Data Normalization

- Hyper parameter tuning

- ISO/ IEC IS 30107-1

Transfer Learning Approach



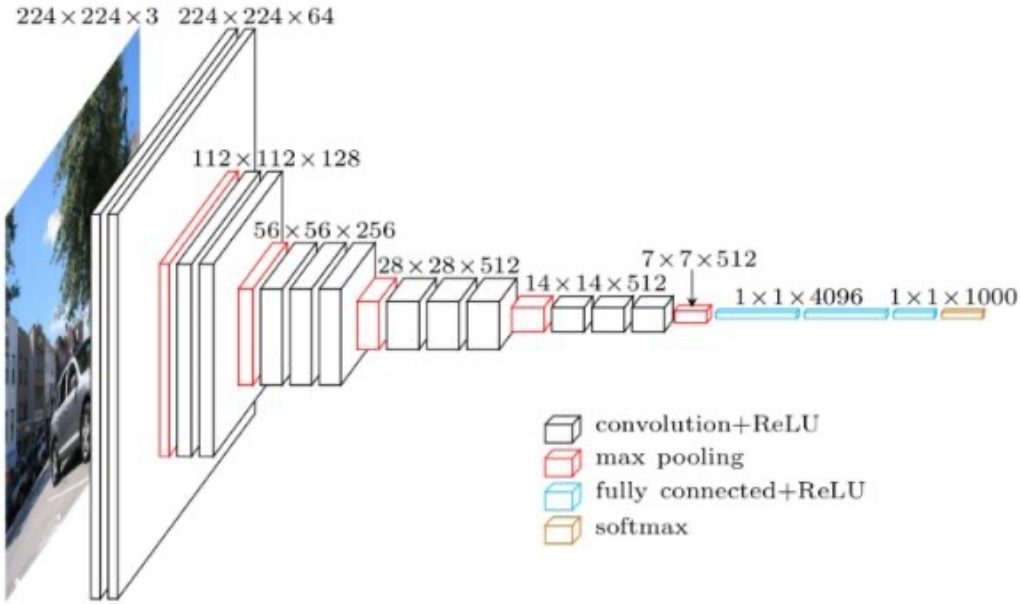
- Face Cropping
- Data Augmentation
- Data Normalization

- Hyper parameter tuning

- ISO/ IEC IS 30107-1

h_da

VGG16 Architecture



Prof. Dr. Vorname Nachname
Hochschulkommunikation
Hochschule Darmstadt

Transfer Learning

Layer (type)	Output Shape	Param #
Conv2d-1	[-1, 64, 224, 224]	1,792
ReLU-2	[-1, 64, 224, 224]	0
Conv2d-3	[-1, 64, 224, 224]	36,928
ReLU-4	[-1, 64, 224, 224]	0
MaxPool2d-5	[-1, 64, 112, 112]	0
Conv2d-6	[-1, 128, 112, 112]	73,856
ReLU-7	[-1, 128, 112, 112]	0
Conv2d-8	[-1, 128, 112, 112]	147,584
ReLU-9	[-1, 128, 112, 112]	0
MaxPool2d-10	[-1, 128, 56, 56]	0
Conv2d-11	[-1, 256, 56, 56]	295,168
ReLU-12	[-1, 256, 56, 56]	0
Conv2d-13	[-1, 256, 56, 56]	590,080
ReLU-14	[-1, 256, 56, 56]	0
Conv2d-15	[-1, 256, 56, 56]	590,080
ReLU-16	[-1, 256, 56, 56]	0
MaxPool2d-17	[-1, 256, 28, 28]	0
Conv2d-18	[-1, 512, 28, 28]	1,180,160
ReLU-19	[-1, 512, 28, 28]	0
Conv2d-20	[-1, 512, 28, 28]	2,359,808
ReLU-21	[-1, 512, 28, 28]	0
Conv2d-22	[-1, 512, 28, 28]	2,359,808
ReLU-23	[-1, 512, 28, 28]	0
MaxPool2d-24	[-1, 512, 14, 14]	0
Conv2d-25	[-1, 512, 14, 14]	2,359,808
ReLU-26	[-1, 512, 14, 14]	0
Conv2d-27	[-1, 512, 14, 14]	2,359,808
ReLU-28	[-1, 512, 14, 14]	0
Conv2d-29	[-1, 512, 14, 14]	2,359,808
ReLU-30	[-1, 512, 14, 14]	0
MaxPool2d-31	[-1, 512, 7, 7]	0
AdaptiveAvgPool2d-32	[-1, 512, 7, 7]	0
Linear-33	[-1, 4096]	102,764,544
ReLU-34	[-1, 4096]	0
Dropout-35	[-1, 4096]	0
Linear-36	[-1, 4096]	16,781,312
ReLU-37	[-1, 4096]	0
Dropout-38	[-1, 4096]	0
Linear-39	[-1, 4096]	16,781,312
ReLU-40	[-1, 4096]	0
Dropout-41	[-1, 4096]	0
Linear-42	[-1, 1]	4,097
Sigmoid-43	[-1, 1]	0

Total params: 151,045,953
Trainable params: 16,785,409
Non-trainable params: 134,260,544

Input size (MB): 0.57
Forward/backward pass size (MB): 218.87
Params size (MB): 576.19
Estimated Total Size (MB): 795.64

freeze

Fine-tune

Prof. Dr. Vorname Nachname
Hochschulkommunikation
Hochschule Darmstadt

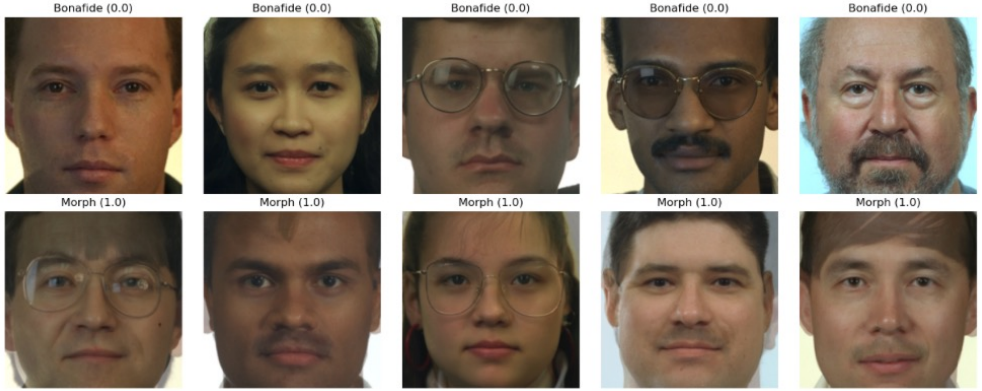
Transfer Learning

- AdaptiveAvgPool
- Linear
- Dropout
- Sigmoid

```
AdaptiveAvgPool2d-32            [-1, 512, 7, 7]               0
           Linear-33                 [-1, 4096]     102,764,544
             ReLU-34                 [-1, 4096]               0
          Dropout-35                 [-1, 4096]               0
           Linear-36                 [-1, 4096]      16,781,312
             ReLU-37                 [-1, 4096]               0
          Dropout-38                 [-1, 4096]               0
           Linear-39                 [-1, 4096]      16,781,312
             ReLU-40                 [-1, 4096]               0
          Dropout-41                 [-1, 4096]               0
           Linear-42                    [-1, 1]           4,097
          Sigmoid-43                    [-1, 1]               0
================================================================
Total params: 151,045,953
Trainable params: 16,785,409
Non-trainable params: 134,260,544
----------------------------------------------------------------
Input size (MB): 0.57
Forward/backward pass size (MB): 218.87
Params size (MB): 576.19
Estimated Total Size (MB): 795.64
----------------------------------------------------------------
```

Database

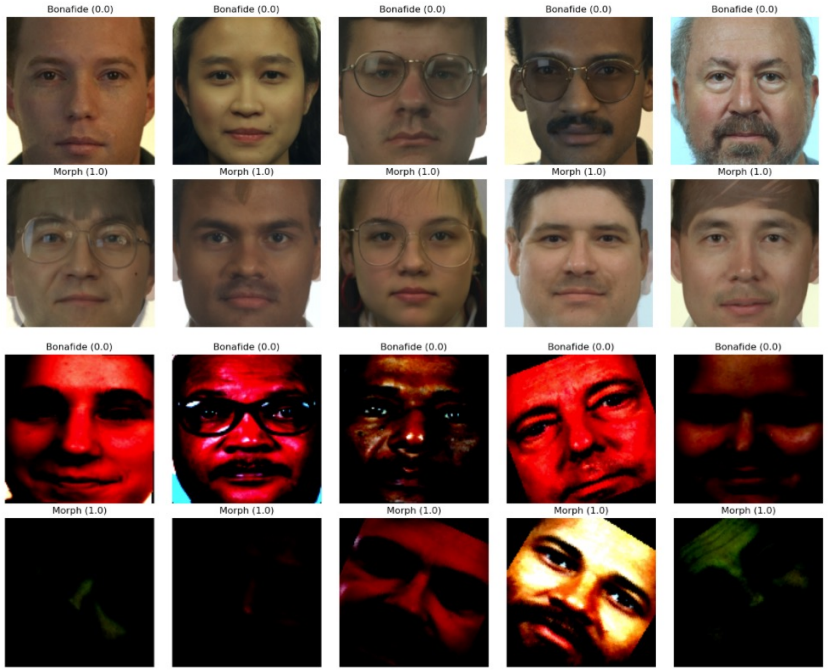
- DATABASE
  - FERET (1410 bonafide; 2121 morphs)
  - FRGC (3167 bonafide; 3861 morphs)
    - bonafide_probe
    - bonafide_reference
    - morphs_facefusion
    - morphs_facemorpher
    - morphs_opencv
    - morphs_ubo



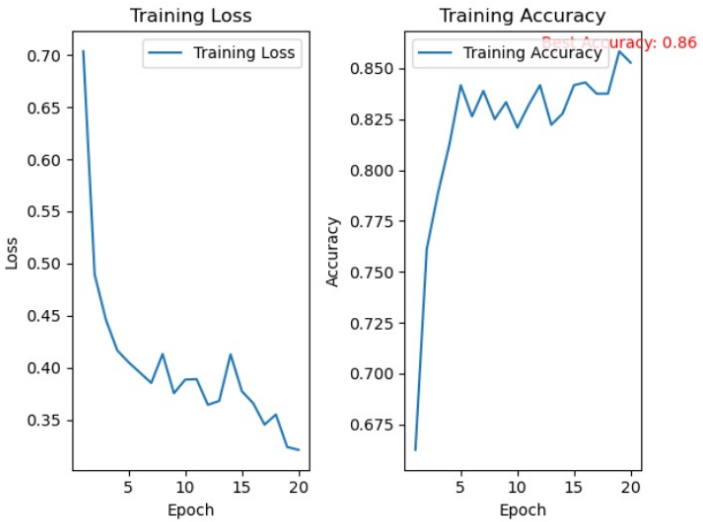
h_da

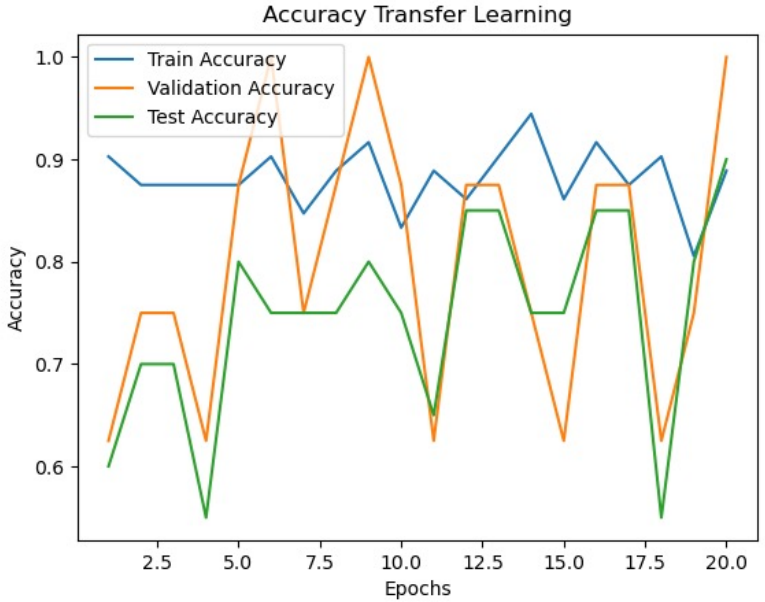
Data Preprocessing

- Face Cropping
  - Random Crop
  - Center Crop
  - Haar Cascade Face Classifier
- Data Augmentation
  - Random Rotation
  - Random Flip
- Data Normalization
  - Scaling Pixels [0,1]



Training the vggface

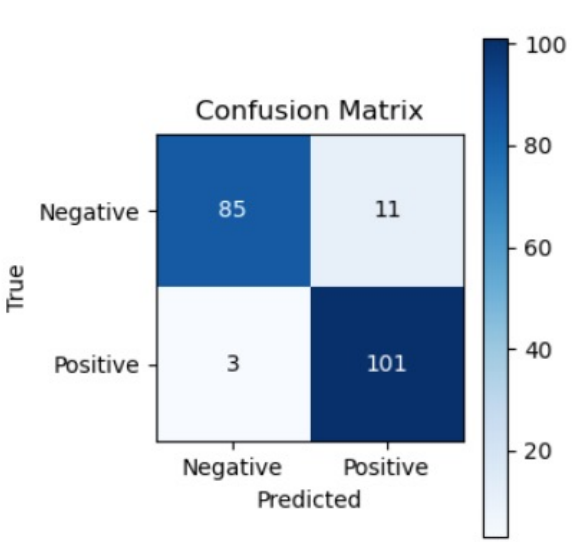


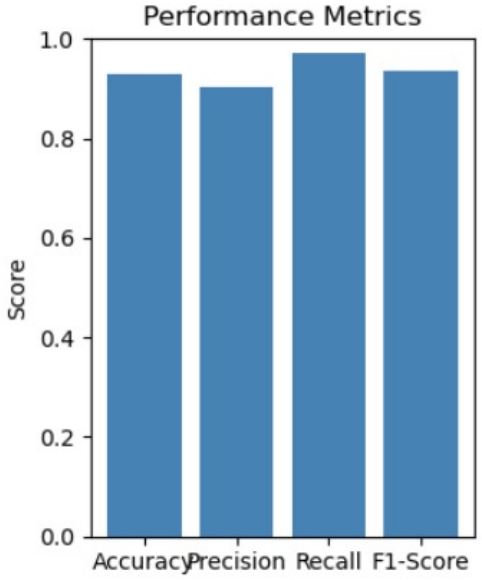


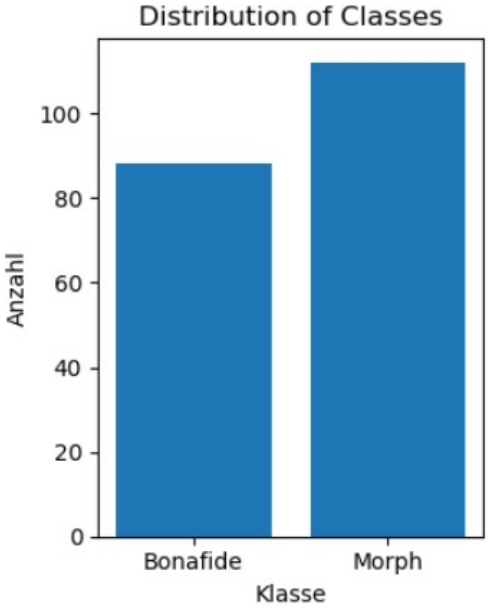
Prof. Dr. Vorname Nachname
Hochschulkommunikation
Hochschule Darmstadt

h_da

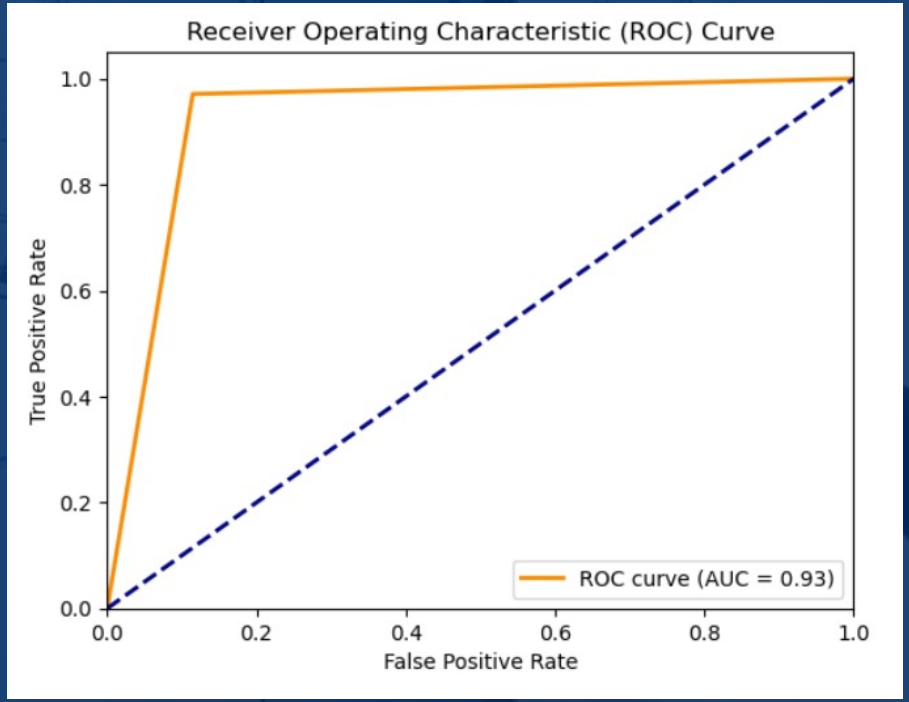
Results


Confusion Matrix
Negative
Positive
True
85
11
3
101
Negative
Positive
Predicted
100
80
60
40
20


Performance Metrics
Score
1.0
0.8
0.6
0.4
0.2
0.0
Accuracy
Precision
Recall
F1-Score

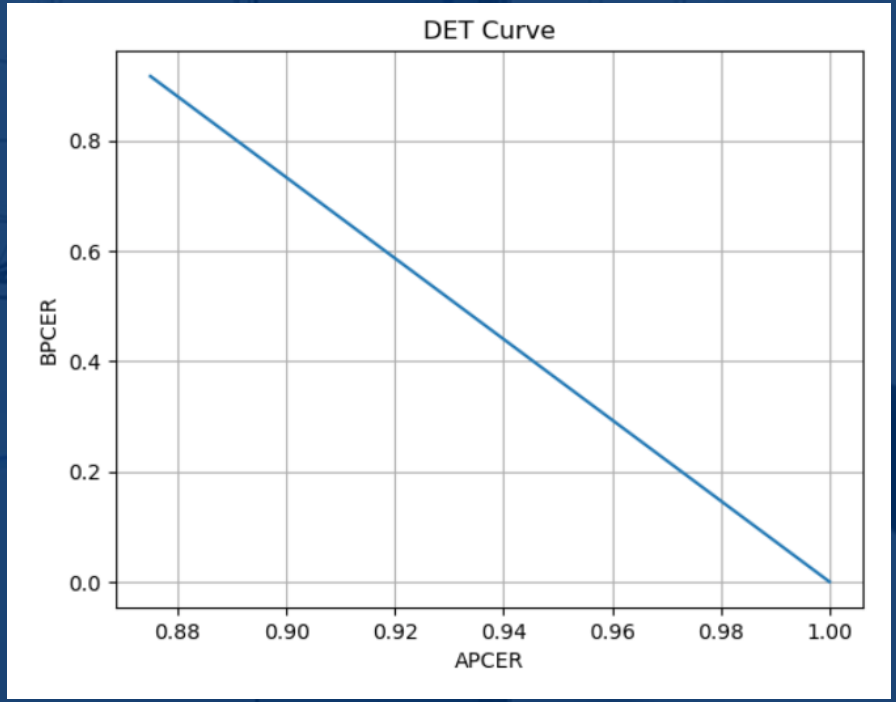

Distribution of Classes
Anzahl
100
80
60
40
20
0
Bonafide
Morph
Klasse

ROC



Prof. Dr. Vorname Nachname
Hochschulkommunikation
Hochschule Darmstadt

DET



Prof. Dr. Vorname Nachname
Hochschulkommunikation
Hochschule Darmstadt