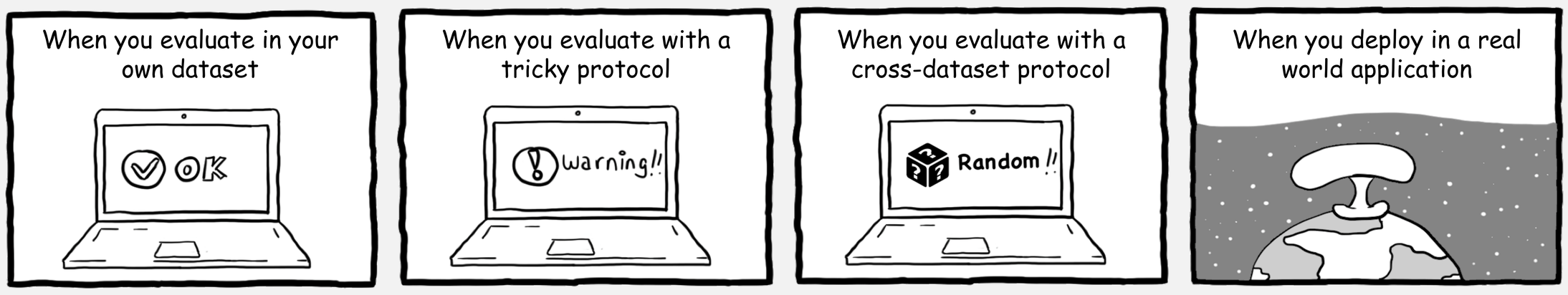
GENERALIZED PRESENTATION ATTACK DETECTION
A FACE ANTI-SPOOFING EVALUATION PROPOSAL

Artur Costa-Pazo[1,2], David Jimenez-Cabello[1], Esteban Vazquez-Fernandez [1],
José L. Alba-Castro[2] , Roberto J. López-Sastre[3]
{acosta, djcabello, evazquez}@gradiant.org, jalbla@gts.uvigo.es, robertoj.lopez@uah.es
[1]GRADIANT (SPAIN), [2]University of Vigo (SPAIN), [3]University of Alcalá (SPAIN)

Motivation



Main Contributions

- We provide the **largest aggregated dataset** with a common categorization in two levels to represent four key aspects in anti-spoofing: attacks, lighting, capture devices and resolution.
- We release **an open-source evaluation framework**, introducing an unified benchmark for GPAD.
- We provide an evaluation of state-of-the-art methods in the proposed benchmark. We demonstrate the limitation of current dataset evaluation procedures (generalization, cross-domain evaluation, etc.), while showing the benefits of the proposed unified framework. All the experiments will be reproducible.
- Using the novel evaluation tool, **we introduce two novel protocols for the GPAD problem**.

Reproducible Research

https://github.com/Gradiant/bob.paper.icb2019.gradgpad

GitHub python

GRAD-GPAD Framework

Generalization Representation over Aggregated Datasets for Generalized Presentation Attack Detection

Aggregate Dataset

Dataset	Year	Num Identities	Num samples real | attack	Spoof atacks
CASIA-FASD	2012	50	150 | 450	Print, Replay
REPLAY-ATTACK	2012	50	200 | 1000	Print, 2 Replay
3DMAD	2013	17	170 | 85	Mask (rigid)
MSU-MFSD	2015	35	110 | 330	Print, 2 Replay
UVAD	2015	404	808 | 16268	7 Replay
REPLAY-MOBILE	2016	40	390 | 640	Print, Replay
HKBU (v1)	2016	8	70 | 40	Mask (rigid)
OULU-NPU	2017	55	1980 | 3960	2 Print, 2 Replay
ROSE-YOUTU	2018	20	897 | 2600	2 Print, 2 Replay, 2 Mask(paper)
SIW	2018	165	1320 | 330	2 Replay, 4 Replay
CSMAD	2018	14	88 | 220	Print, Mask (silicone)

Table. 1 List of existing databases for anti-spoofing based on videos and their main characteristics.

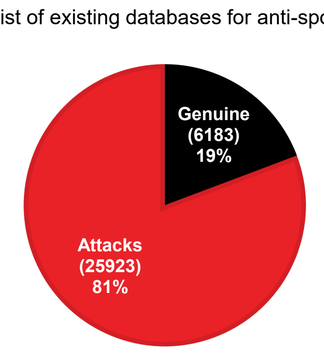


Figure. 1 Aggregate Dataset samples distribution

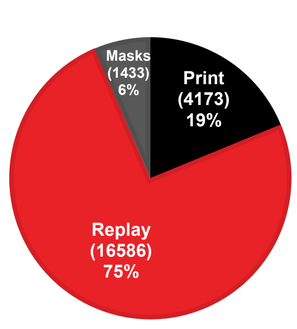


Figure. 2 Aggregate Dataset attacks distribution (PAIs).

Common Taxonomy

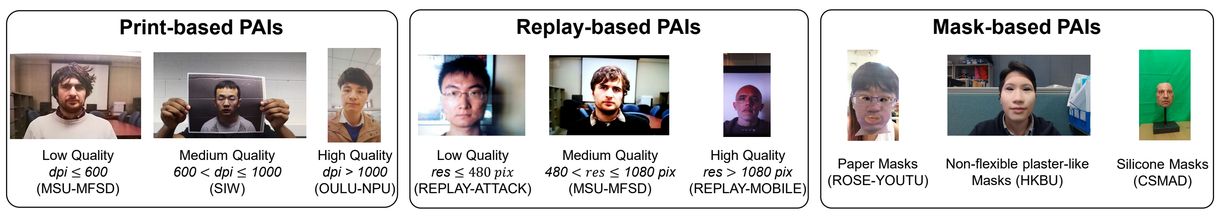


Figure. 3 Sample of Common PAIs (Presentation Attack Instruments).

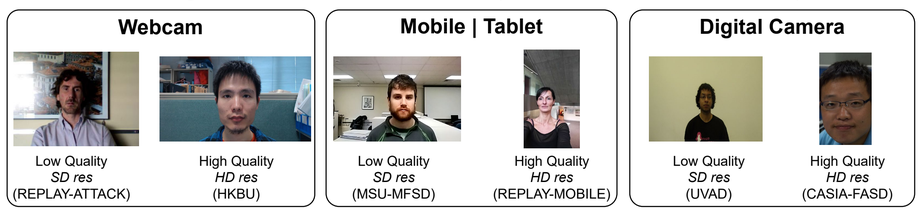


Figure. 4 Samples of Common Capture Devices.

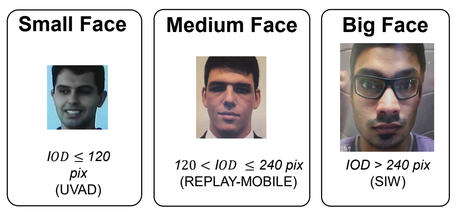


Figure. 5 Samples of Common Face Resolution. *IOD stands for Interocular Distance.*

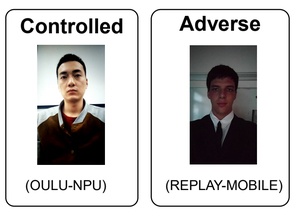
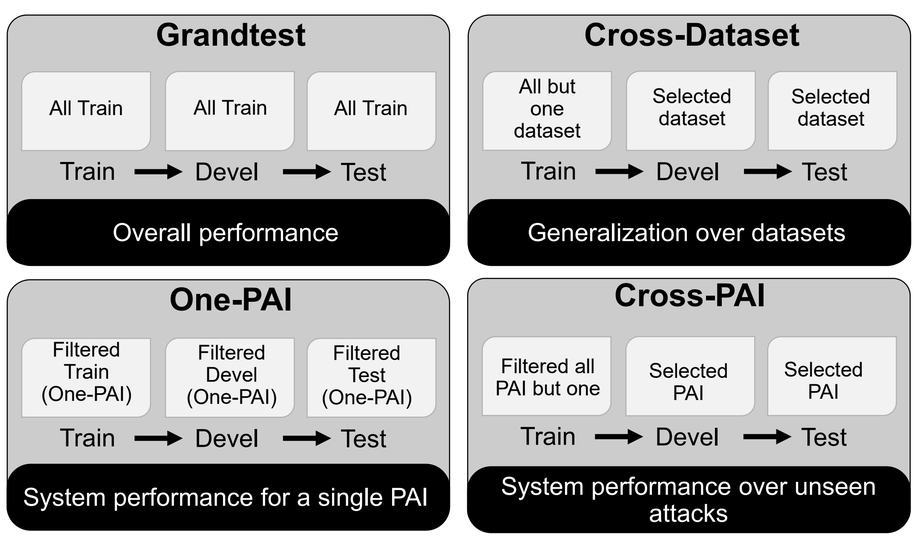


Figure. 6 Samples of Common Lighting.

Protocols

Extended classical Protocols



Novel Protocols

[1] **Optimal conditions:** high quality capture devices, low and medium quality PAIs, paper masks and both controlled and no info lighting conditions.
[2] **Adverse conditions:** low quality capture devices, high quality PAIs, silicon and non-flexible plaster-like mask, and adverse lighting conditions

Experiments

Baseline	HTER (%)	ACER (%)	APCER (%)	BPCER (%)
Quality-Based [1]	17.03	25.25	34.09	16.41
Color-Based [2]	6.33	10.22	13.86	6.58

Table. 2 Results for **Grandtest** protocol.

Baseline	Cross-Device Protocol	HTER (%)	ACER (%)	APCER (%)	BPCER (%)
Quality-Based [1]	DigitalCamera-Test	24.85	52.27	86.67	17.89
	Webcam-Test	28.55	53.57	29.52	47.62
	MobileTablet-Test	21.11	25.76	29.33	22.19
Color-Based [2]	DigitalCamera-Test	7.42	16.26	26.76	5.75
	Webcam-Test	12.16	31.90	48.98	14.83
	MobileTablet-Test	9.08	12.30	15.07	9.54

Table. 3 Results for **Cross-Device** protocol

Tested on	HTER (%)	ACER (%)	APCER (%)	BPCER (%)
CASIA-FASD	41.57	48.98	81.11	16.85
REPLAY-ATTACK	27.61	34.06	33.96	34.17
3DMAD	29.00	29.00	0.00	58.00
MSU-MFSD	31.11	46.66	46.66	46.66
REPLAY-MOBILE	26.89	28.19	34.37	22.02
HKBU	45.00	45.00	90.0	0.00
OULU-NPU	34.68	41.11	75.27	6.94
ROSE-YOUTU	37.88	45.81	42.40	49.22
SIW	31.97	48.40	53.07	43.74
CSMAD	40.51	40.51	10.20	70.83

a) Result Using Quality-Based [1] face-PAD.

Tested on	HTER (%)	ACER (%)	APCER (%)	BPCER (%)
CASIA-FASD	15.45	16.75	17.78	15.73
REPLAY-ATTACK	25.11	33.35	31.25	35.44
3DMAD	0.00	0.00	0.00	0.00
MSU-MFSD	17.78	35.00	56.66	13.33
REPLAY-MOBILE	18.30	22.99	23.96	22.02
HKBU	0.00	0.00	0.00	0.00
OULU-NPU	34.27	37.78	72.22	3.33
ROSE-YOUTU	27.42	34.78	25.25	44.32
SIW	9.90	22.06	30.43	13.69
CSMAD	40.05	40.05	55.10	

b) Result Using Color-Based [2] face-PAD.

Table. 4 Results for **Cross-Dataset** protocol

Baseline	Cross-FaceResolution Protocol	HTER (%)	ACER (%)	APCER (%)	BPCER (%)
Quality-Based [1]	LargeFaces-Test	24.48	51.86	86.21	17.52
	SmallFaces-Test	29.98	48.79	50.00	47.58
Color-Based [2]	LargeFaces-Test	8.33	15.81	27.50	4.12
	SmallFaces-Test	25.47	29.62	12.20	47.04

Table. 5 Results for **Cross-FaceResolution** protocol

Baseline	Cross-Conditions Protocol	HTER (%)	ACER (%)	APCER (%)	BPCER (%)
Quality-Based [1]	Adverse-Test	36.62	40.48	72.50	8.46
	Optimal-Test	45.50	66.06	96.67	35.46
Color-Based [2]	Adverse-Test	41.13	45.43	86.25	4.61
	Optimal-Test	34.37	55.12	93.33	16.91

Table. 6 Results for **Cross-Conditions** protocol

References:
[1] Z. Boulkenafet et al. Face spoofing detection using colour texture analysis. IEEE Transactions on Information Forensics and Security (TIFS), 2016.
[2] O. Nikisins et al.. On effectiveness of anomaly detection approaches against unseen presentation attacks in face anti-spoofing. In ICB, 2018.