5th Face Anti-Spoofing Workshop and Challenge@CVPR2024

Jun Wan, Ajian Liu, Jiankang Deng, Shengjin Wang, Ya-Li Li,

Sergio Escalera, Hugo Jair Escalante, Isabelle Guyon, Zhen Lei

2024.6.17

sergio.escalera.guerrero@gmail.com

Background

Print photo attack

Bending the print attack

3D Mask attack

Video replay attack

Face recognition systems can be attacked in different ways

Previous Competitions

- IJCB 2011
  - 2D Attacks (RGB)
  - Dataset: Relayattack
- ICB 2013
  - 2D Attacks (RGB)
  - Dataset:Relayattack
- IJCB 2017
  - 2D Attacks (RGB)
  - Dataset: Oulu-NPU

Idiap

Figure 1: Examples of real accesses and attacks in different scenarios. In the top row, samples from *controlled* scenario. In the bottom row, samples from *adverse* scenario. Columns from left to right show examples of real access, printed photograph, mobile phone and tablet attacks.

Relayattack

(a) Samsung (b) HTC (c) MEIZU (d) ASUS (e) Sony (f) OPPO

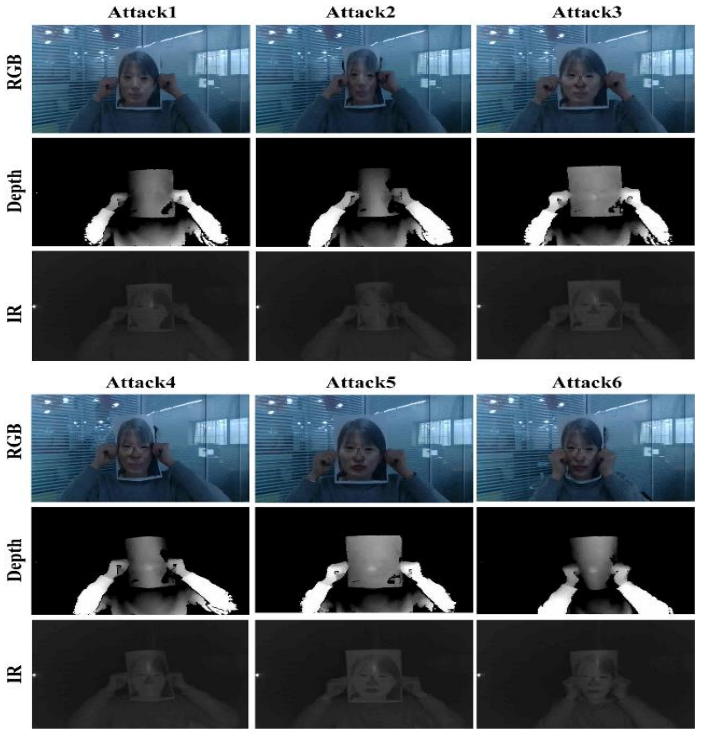
Fig. 3: Sample images showing the image quality of the different camera devices.

Oulu-NPU

Previous Competitions@CVPR2019

- CVPR workshop 2019
  - Multi-modal Attacks (RGB,depth, infraed)
  - dataset: **CASIA-SURF**

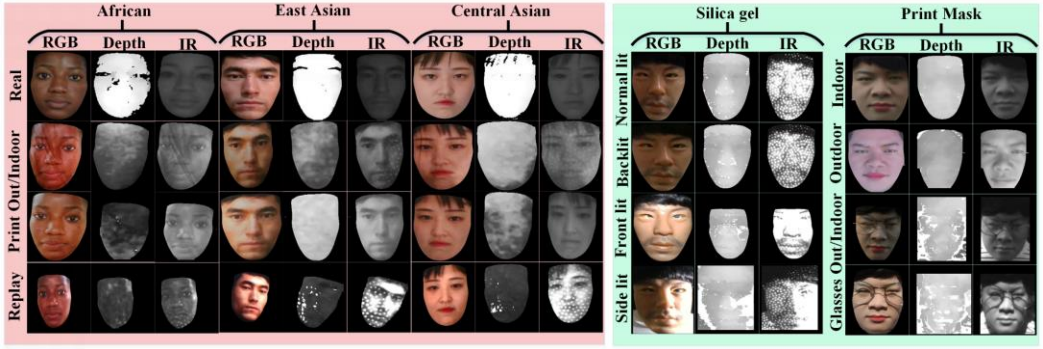
Figure 2. Keynote Speakers: IEEE Fellow Stan Z. Li (CASIA), Abdenour Hadid (University of Oulu), Xiaoming Liu (MSU), Guodong Guo (IDL, Baidu).



CASIA-SURF

Previous Competitions@CVPR2020

- CVPR workshop 2020
  - Multi-modal Attacks (RGB, depth, infraed)
  - Multi-ethnic Attacks (African, East/ Central Asian)
  - dataset: CASIA-SURF CeFA



- Intel RealSense SR300
- Covering 3 ethnicities, 3 modalities, 1, 607 subjects, and 2D plus 3D attack types.
- Five protocols are introduced to measure the affect under varied evaluation conditions.

- Protocol 1 (cross-ethnicity)
- Protocol 2 (cross-PAI)
- Protocol 3 (cross-modality)
- Protocol 4 (cross-ethnicity & PAI)

Protocol of the challenge used

Ethnicity	Real & Attack styles	# RGB	# Depth	# IR	Subtotal
African East Asian Central Asian	Real	500	500	500	6000 6000 6000
	Cloth-indoor attack	500	500	500	
	Cloth-outdoor attack	500	500	500	
	Replay attack	500	500	500	
Total: 1500 subjects, 18000 videos					

3D Mask Attack	Attack styles	# RGB	# Depth	# IR	Subtotal
Print mask 99 Subjects & 6 Lighting	Only mask	594	594	594	5346
	Wig without glasses	594	594	594	
	Wig with glasses	594	594	594	
Silica gel mask 8 Subjects & 4 Lighting	Wig without glasses	32	32	32	192
	Wig with glasses	32	32	32	
Total: 107 subjects, 5538 videos					

Statistics of the 2D/3D attack subset

Previous Competitions@ICCV 2021

- **ICCV workshop 2021**
  - The largest 3D face mask dataset
  - Dataset: **CASIA-SURF HiFiMask**

- Protocol 1 (Seen)
- Protocol 2 (Unseen)
- **Protocol 3 (cross-modality)**

Table 2. Statistical information for each protocol of the proposed HiFiMask dataset. Note that 1, 2 and 3 in the fourth column mean Transparent, Plaster and Resin mask, respectively.

Pro.	Subset	subject	Masks	# live	# mask	# all
1	Train	45	1&2&3	8,108	24,406	32,514
	Dev	6	1&2&3	1,084	3,263	4,347
	Test	24	1&2&3	4,335	13,027	17,362
2_1	Train	45	2&3	8,108	16,315	24,423
	Dev	6	2&3	1,084	2,180	3,264
	Test	24	1	4,335	4,326	8,661
2_2	Train	45	1&3	8,108	16,264	24,372
	Dev	6	1&3	1,084	2,174	3,258
	Test	24	2	4,335	4,350	8,685
2_3	Train	45	1&2	8,108	16,233	24,341
	Dev	6	1&2	1,084	2,172	3,256
	Test	24	3	4,335	4,351	8,686

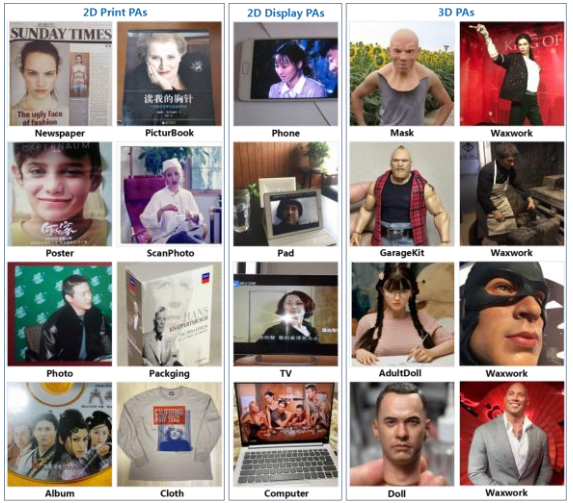
Previous Competitions@CVPR 2023

- **CVPR Workshop 2023**
  - **CASIA-SURF SuHiFiMask:** The first real surveillance scenes dataset
  - **WFAS:** A large-scale, diverse FAS dataset collected in unconstrained settings.

➢ **Protocol 3 (generalizable protocol)**

Prot.	SubSet	#Subj.	Mask	Score	#Live	#Mask	#Others	#All
3	Train	101	1∼4	[0.4,1]	64,276	35,898	58,889	159,063
	Dev	101	1∼4	[0.3,0.4)	37,990	24,031	27,255	89,276
	Test	101	1∼4	[0,0.3)	83,181	43,087	35,614	161882

CASIA-SURF SuHiFiMask



WFAS

5th Chalearn Face Anti-spoofing Workshop and Challenge@CVPR2024

Track 1: Unified Physical-Digital Face Attack Detection Challenge

- **UniAttackData Dataset**

Dataset	Attack Type (each ID)	# Datasets / Data	# ID	Physical Attacks		Digital Attacks		
				Dataset Name	No.	# Categories	Methods	No.
GrandFake	Incomplete	6 sets: 789412 (I) (Live: 341738, Fake: 447674)	96817	SiW-M [Liu *et al.*, 2019b]	128112 (I)	Adv (6)	FGSM [Goodfellow *et al.*, 2015]	19739 (I)
							PGD [Madry *et al.*, 2019]	19739 (I)
							DeepFool [Moosavi-Dezfooli *et al.*, 2016]	19739 (I)
							AdvFaces [Deb *et al.*, 2019]	19739 (I)
							GFLM [Dabouei *et al.*, 2018]	17946 (I)
							SemanticAdv [Qiu *et al.*, 2020]	19739 (I)
						DeepFake (6)	FaceSwap [Kowalski, 2018]	14492 (I)
							Deepfake [Korshunov and Marcel, 2018]	18165 (I)
							Face2Face [Thies *et al.*, 2016]	18204 (I)
							StarGAN [Choi *et al.*, 2018]	45473 (I)
							STGAN [Liu *et al.*, 2019a]	29983 (I)
							StyleGAN2 [Karras *et al.*, 2020]	76604 (I)
JFSFDB	Incomplete	9 sets: 27172 (V) (Live: 5650, Fake: 21522)	356	SiW [Liu *et al.*, 2018]	3173 (V)	DeepFake (4)	Face2Face [Thies *et al.*, 2016]	1000 (V)
				3DMAD [Erdogmus and Marcel, 2014]	85 (V)		FaceSwap [Kowalski, 2018]	1000 (V)
				HKBU [Liu *et al.*, 2016]	588 (V)		NeuralTextures [Thies *et al.*, 2019]	1000 (V)
				MSU [Wen *et al.*, 2015]	210 (V)			
				3DMask [Yu *et al.*, 2020a]	864 (V)		Deepfake [Korshunov and Marcel, 2018]	10752 (V)
				~~ROSE [Li *et al.*, 2018]~~	~~2850 (V)~~			
UniAttackData (Ours)	**Complete**	**1 set:** **29706 (V)** **(Live: 1800, Fake: 27906)**	**1800**	CASIA-SURF CeFA [Liu *et al.*, 2020]	6400 (V)	Adv (6)	advdrop [Duan *et al.*, 2021]	1706 (V)
							alma [Rony *et al.*, 2021]	1800 (V)
							demiguise [Wang *et al.*, 2021c]	1800 (V)
							fgtm [Luo *et al.*, 2022]	1800 (V)
							ila_da [Yan *et al.*, 2022]	1800 (V)
							ssah [Zhong *et al.*, 2022]	1800 (V)
						DeepFake (6)	FaceDancer [Rosberg *et al.*, 2023]	1800 (V)
							InsightFace [Heusch *et al.*, 2020]	1800 (V)
							SimSwap [Chen *et al.*, 2020]	1800 (V)
							SAFA [Wang *et al.*, 2021a]	1800 (V)
							DaGAN [Hong *et al.*, 2022]	1800 (V)
							OneShotTH [Wang *et al.*, 2021b]	1800 (V)
						summary	**12**	**21506 (V)**

Table 1: Comparison of our multimodal facial attack datasets with Grandfake and JFSFDB. Our UniAttackData dataset covers all attack types, containing advanced forgery methods from 2020 to 2023, using the same ID as the existing dataset CASIA-SURF CeFA. Images in UniAttackData of the amount of $2,526,432$ are 3 times more than GrandFake. [Keys: I=Image, V=Video]

UniAttackData Dataset

- Each ID in UniAttackData contains a complete set of attack types.
- UniAttackData incorporates of the most advanced and comprehensive attack methods
- UniAttackData is the largest joint physical and digital attack dataset.

Unified Physical-Digital Face Attack Detection Challenge

Statistics of teams

- **Participates Teams (registered): 136**
- **Code submissions: 13 Teams**

Ranking	Team Name	Leader Name, Affiliation
1	MTFace	Xianhua He, Meituan
2	SeaRecluse	Minzhe Huang, Akuvox
3	duileduile	Jiaruo Yu, INTSIG Information Co. Ltd
4	BSP-Idiap	Anjith George, Idiap Research Institute
5	VAI-Face	Vu Minh Quan, Viettel AI
6	L&L&W	Tongming Wan, Central South University
7	SARM	Jun Lan, SARM
8	M2-Purdue	Shu Hu, Purdue University
9	Cloud Recesses	Peipeng Yu, Nanyang Technological Univeristy
10	ImageLab	Sabari Nathan, Couger Inc., Sethu Institute of Technology, Thiagarajar college of engineering
11	BOVIFOCR-UFPR	Bernardo Biesseck, Federal University of Paraná
12	Inria-CENATAV-Tec	Luis Santiago Luévano García, Inria, CENATAV, Tecnologico de Monterrey
13	Vicognit	Manoj Sharma, Bennett Univeristy

Unified Physical-Digital Face Attack Detection Challenge

Challenge winners:

Rank	Leader Name	Team	Affiliation	ACER(%)	AUC	APCER	BPCER
1	hexianhua	MTFace	MEITUAN	2.3396	99.6923	0.9259	3.7533
2	minzhe.huang	SeaRecluse	Akuvox	3.4369	96.5631	0.3999	6.4737
3	Jiaruo Yu	duileduile	INTSIG Information Co. Ltd	5.5111	98.6830	5.5185	5.5037

workshop Paper:

[1] Joint Physical-Digital Facial Attack Detection Via Simulating Spoofing Clues, CVPRW, 2024
[2] A visualization method for data domain changes in CNN networks and the optimization method for selecting thresholds in classification tasks, CVPRW, 2024
[3] Unified Face Attack Detection with Micro Disturbance and a Two-Stage Training Strategy, CVPRW, 2024

Track 2: Snapshot Spectral Imaging Face Anti-spoofing Challenge

- **HySpeFAS Dataset** Main organizer: Shengjin Wang, TsingHua University

Live faces | 2D print attacks | 3D HiFi masks

- **The dataset contains 6760 hyperspectral images (HSIs) of 10 live subjects and 60 spoof subjects (50 3D masks and 10 2D printed posters) recontructed from SSI images by TwIST algorithm.**
- **The 50 3D masks include 22 different materials, such as silicone, resin, latex, plastic, nylon, paper, and metals.**

Track 2: Snapshot Spectral Imaging Face Anti-spoofing Challenge

Statistics of teams

- **Participates Teams (registered): 70**
- **Final Round Teams： 26**

Rank	Username	Team	Affiliation	ACER(%)	APCER(%)	BPCER(%)
1	yiyao_scb	Ant	AntGroup	0.00	0.00	0.00
1	CTEL_AI	CTEL_AI	ChinaTelecom	0.00	0.00	0.00
3	SeaRecluse	SeaRecluse	Akuvox	0.03	0.06	0.00
4	hexianhua	MTFace	Meituan	0.18	0.37	0.00
5	Ricardozzf	-	-	0.22	0.212	0.32
6	ctyun-ai	ctyun-ai	ChinaTelecom	0.47	0.31	0.64
7	galileo	-	-	0.63	0.31	0.96
8	ZTT	ZTTTeam	CMBChina	0.69	0.74	0.64
9	DXAI	-	-	0.72	0.80	0.64
10	stella0831	AIM_Lab	Hanbat National University	0.95	0.31	1.60

Challenge Winners

R	Team Name	Team Leader	Affiliation	ACER（%）
1	Ant Security Lab	yiyao.scb	AntGroup	0.00
2	CTEL_AI	ZhaoFan Zhou	China Telecom	0.00
3	SeaRecluse	minzhe.huang	Akuvox	0.03

Acknowledgments

- **Awards Sponsor**

- **Data Sponsor**

References

- [1]Fang H, Liu A, Wan J, et al. Unified Physical-Digital Face Attack Detection. IJCAI, 2024.

This paper introduces the UniAttackData dataset.

- [2] Yuan H, Liu A, Wan J, et al. Unified Physical-Digital Attack Detection Challenge. CVPRW, 2024.

This paper introduces the face anti-spoofing attack challenge-track1, including winners methods information.

Thanks!

Agenda

- Time: 8:30 AM - 12:00 AM

- Location: Arch 201
  - 8:30 - 8:40 Opening of the contest, Overview of results;
  - **8:40 - 9:10 Keynote Speaker#1 (Lizhuang Ma)**
  - **9:10 -9:25 Team: MTFace (Track 1, 1st: MTFace)**
  - **9:25 - 9:40 Team: Ant Security Lab (Track 2, 1st: Ant Security Lab)**
  - **9:40 - 10:10 Keynote Speaker#2 (Karthik Nandakumar)**
  - **10:10 - 10:25 Team: SeaRecluse (Track 1, 2nd & Track 2, 3rd: SeaRecluse)**
    - **10:25 - 10:50 Coffe Break**
  - **10:50 - 11:20 Keynote Speaker#3 (Xiang Xu)**
  - **11:20 - 11:35 Team: CTEL_AI (Track 2, 2nd: CTEL_AI)**
  - **11:35 - 11:50 Team: duileduile (Track 1, 3rd: duileduile)**
  - **11:50 - 12:00 Closing**