Deep Learning for Face Anti-Spoofing: A Survey

Zitong Yu, *Member, IEEE*, Yunxiao Qin, Xiaobai Li, *Member, IEEE*, Chenxu Zhao,
Zhen Lei, *Senior Member, IEEE* and Guoying Zhao, *Fellow, IEEE*

IEEE TPAMI 2022

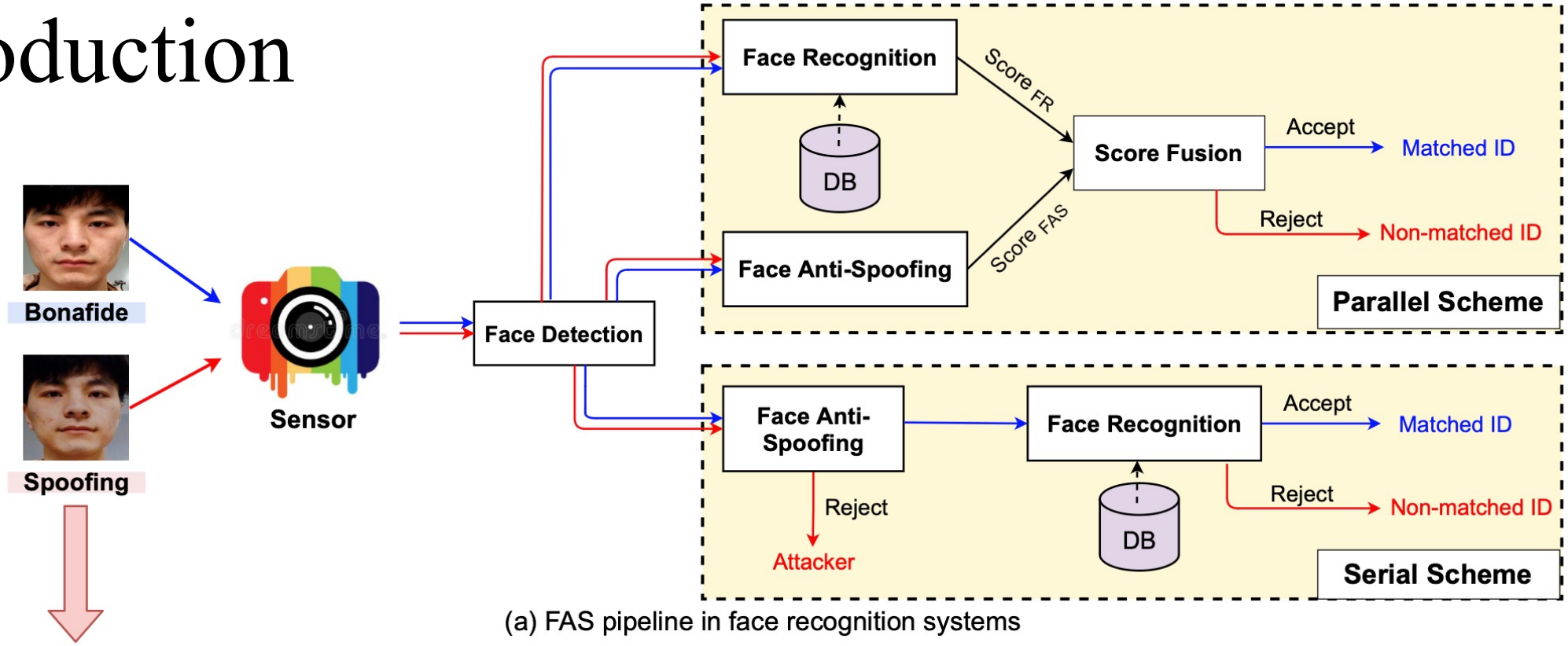
Presenter: Hao Wang

Advisor: Prof. Chia-Wen Lin

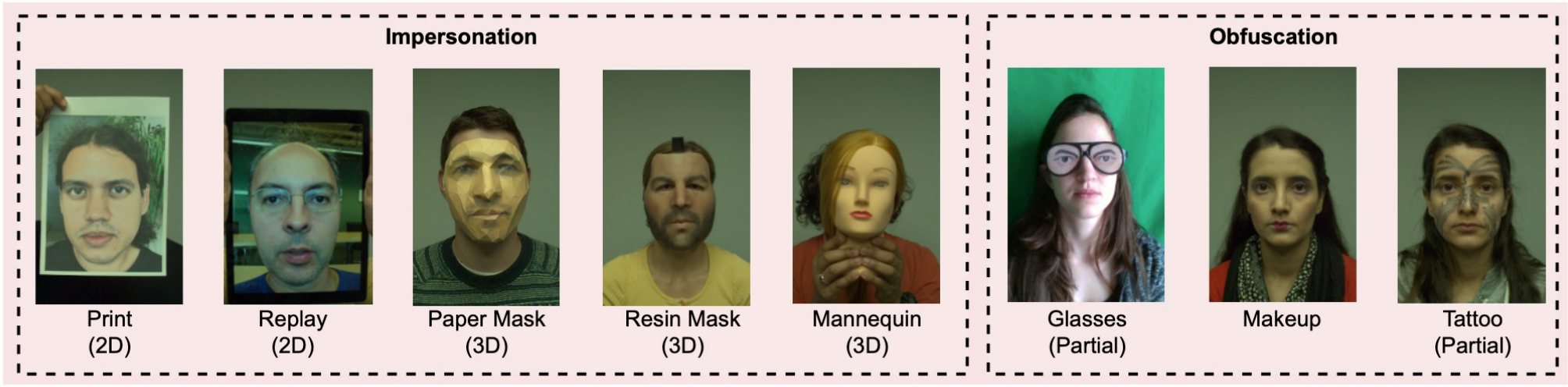
Outline

- Introduction
- Metrics
- Protocol & Dataset
- Recent paper protocol
- CVPRW challenge
- Conclusion

Introduction



(a) FAS pipeline in face recognition systems



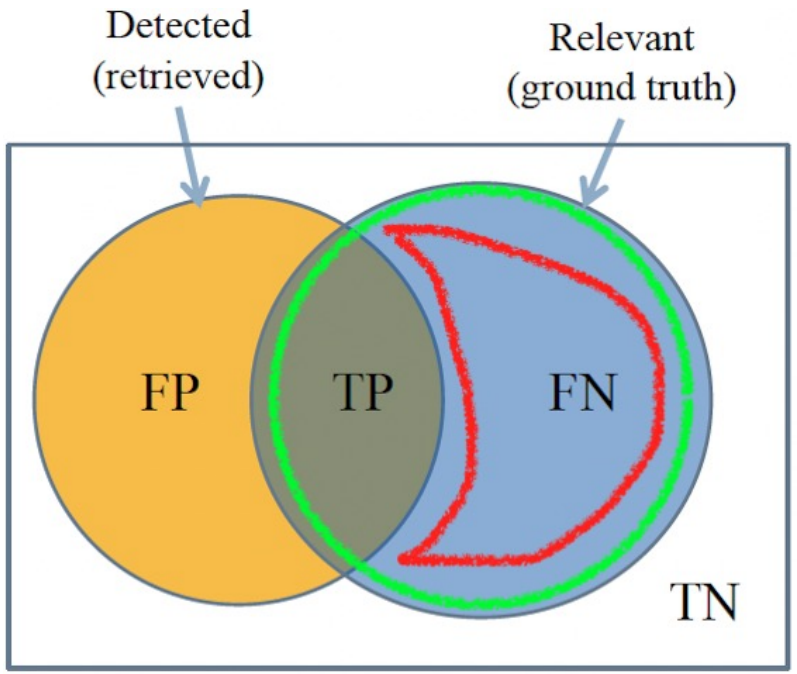
(b) Face spoofing attacks

Outline

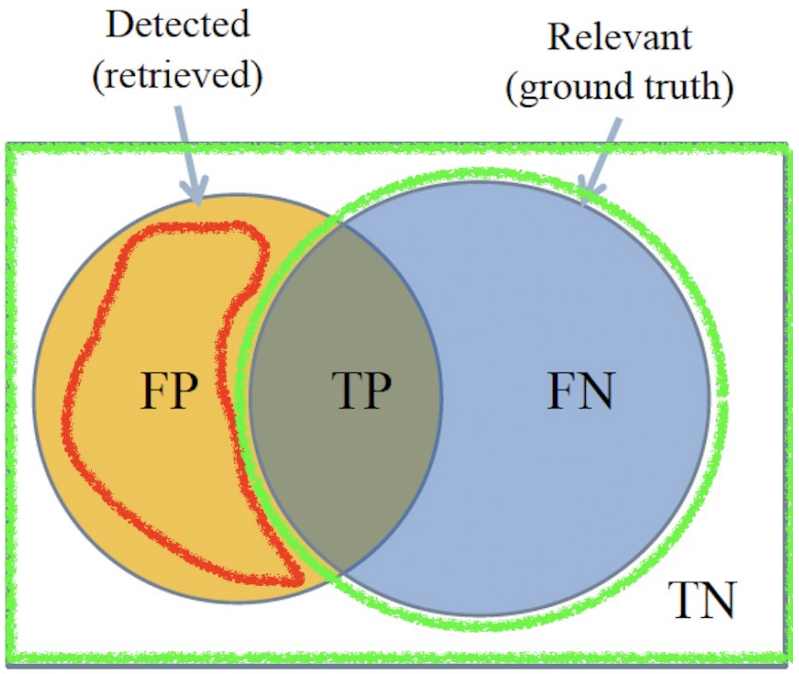
- Introduction
- Metrics
- Protocol & Dataset
- Recent paper protocol
- CVPRW challenge
- Conclusion

Metrics

$$\text{FRR} = \frac{\text{Number of false rejections}}{\text{Number of bonafide presentations}}$$

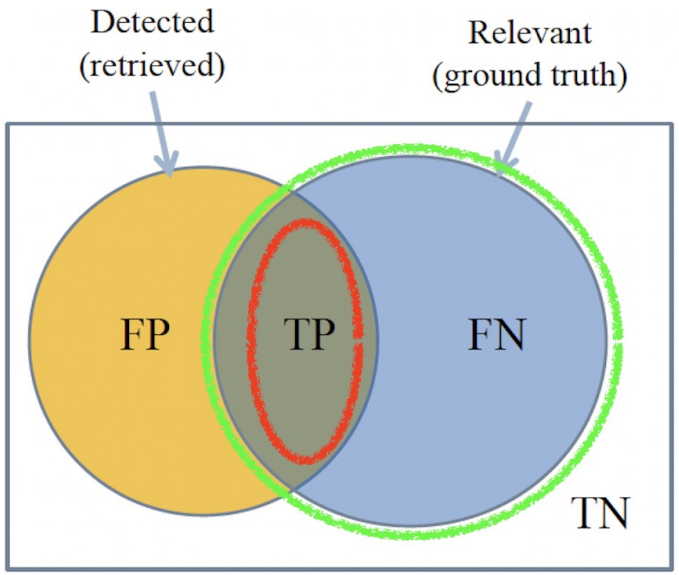


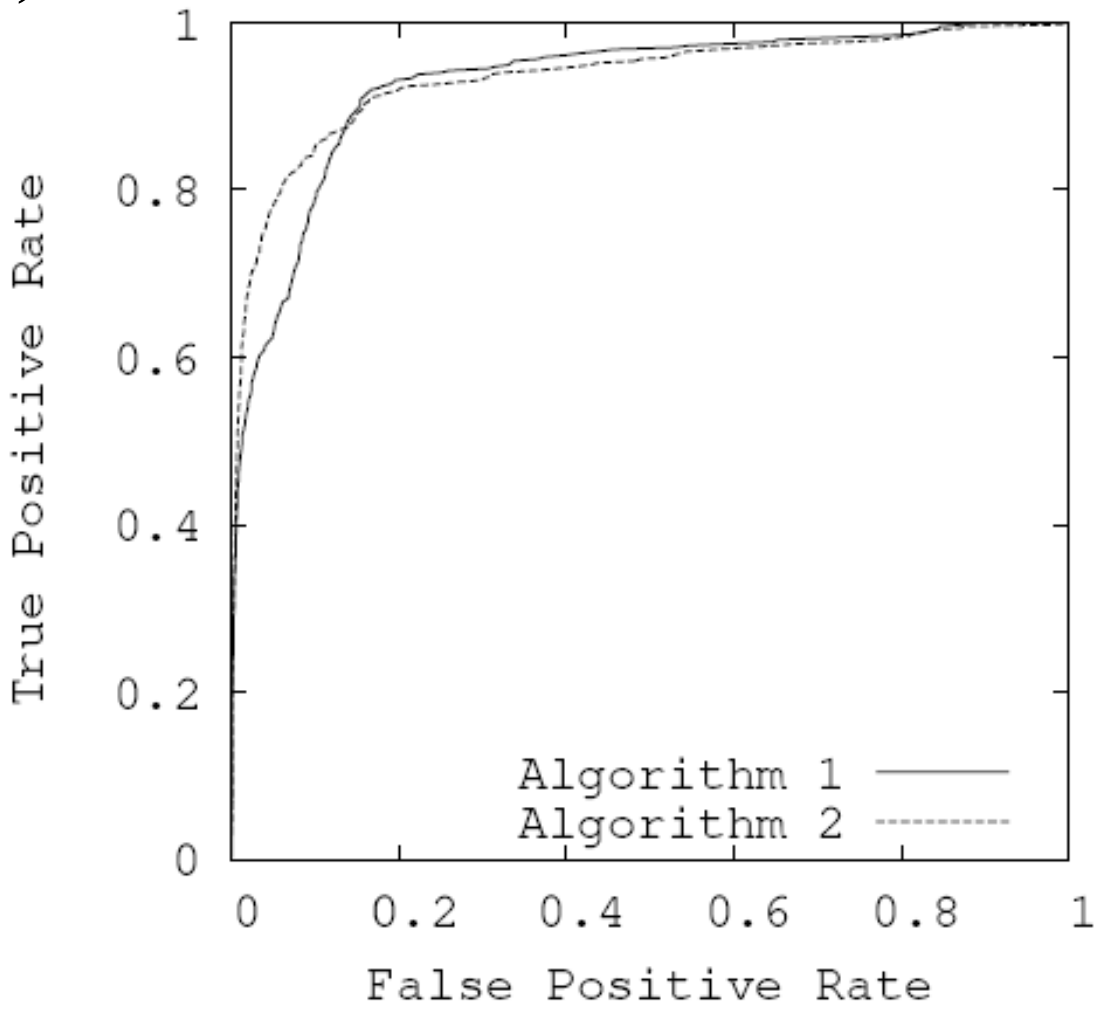
$$\text{FAR} = \frac{\text{Number of false acceptances}}{\text{Number of attack presentations}}$$

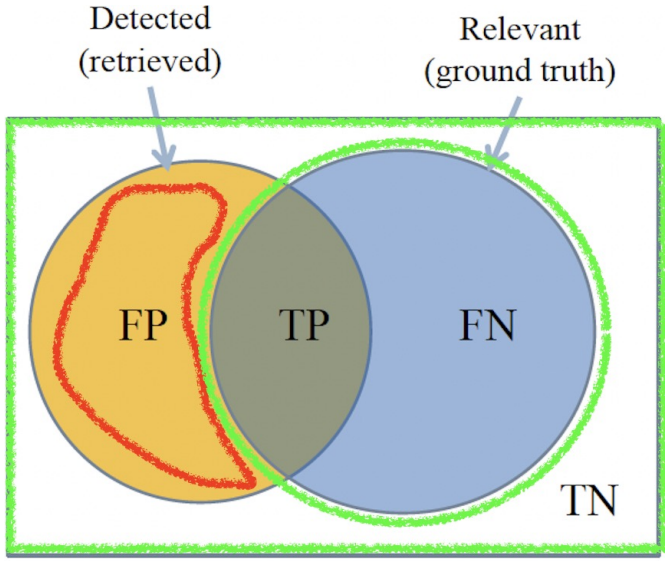


- HTER (ACER) is found out by calculating the average of FRR and FAR.
- EER is a specific value of HTER at which FAR and FRR have equal values.

Metrics (AUC)





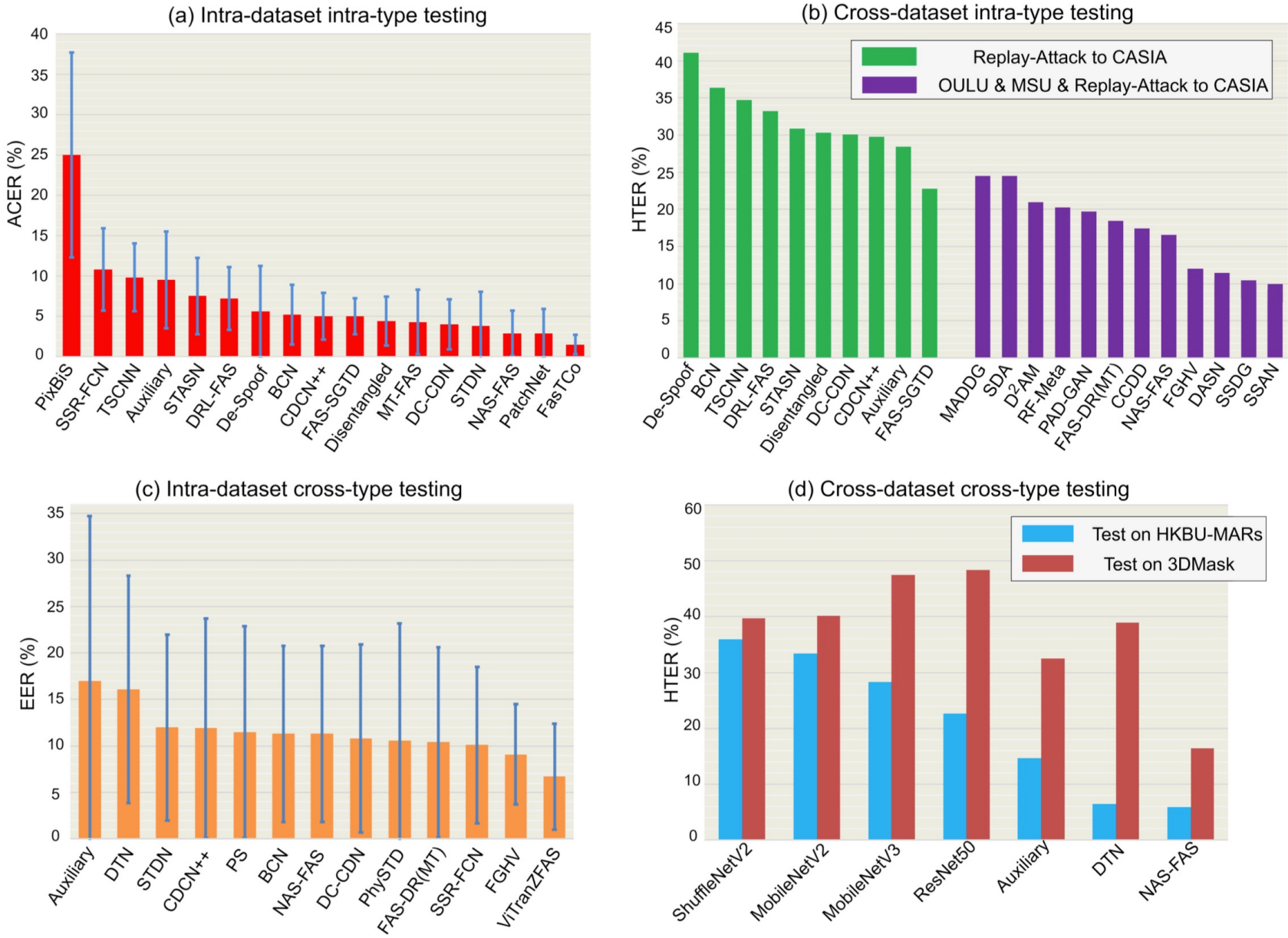


- Area Under the Curve (AUC)

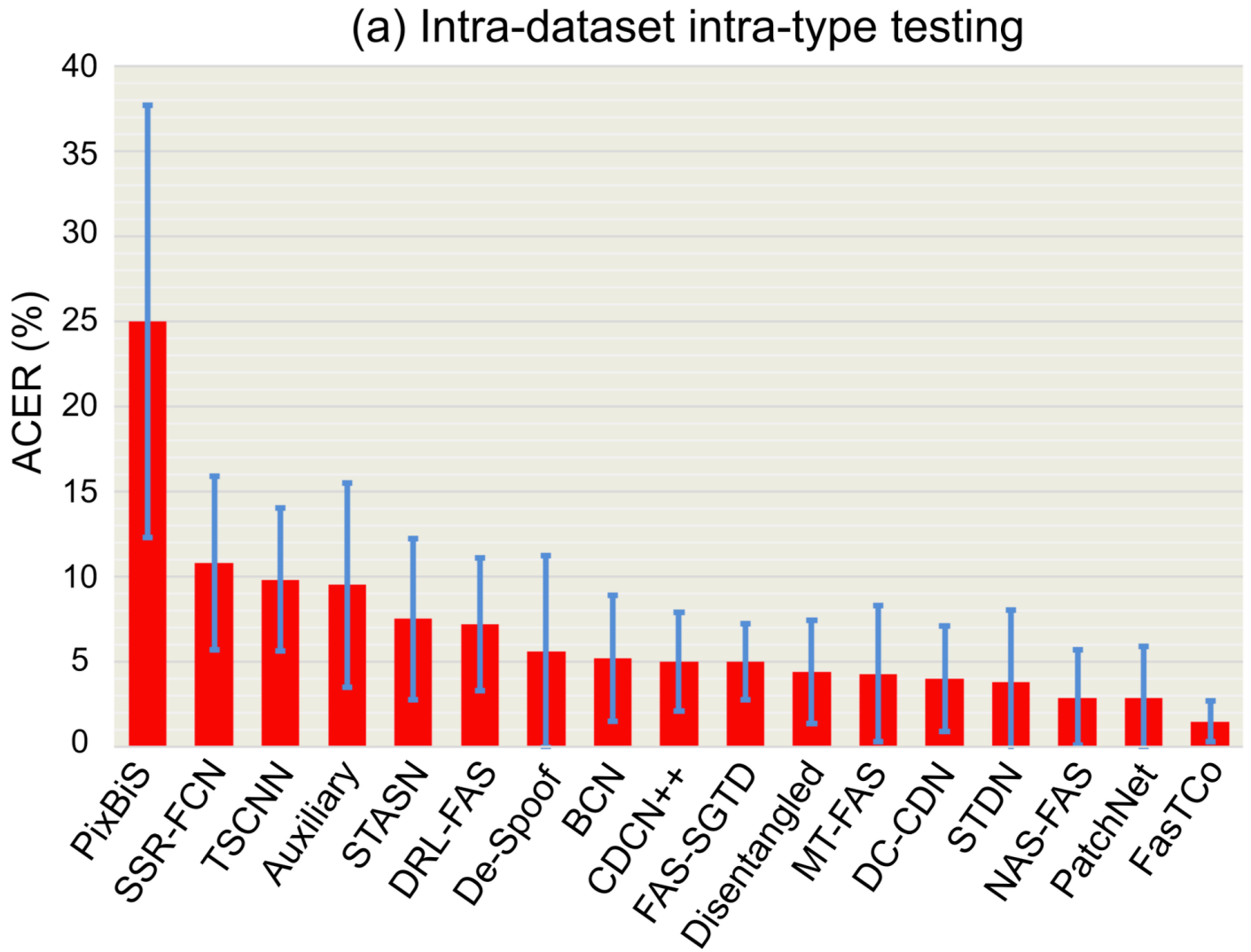
Outline

- Introduction
- Metrics
- Protocol & Dataset
- Recent paper protocol
- CVPRW challenge
- Conclusion

Performance of four evaluation protocols



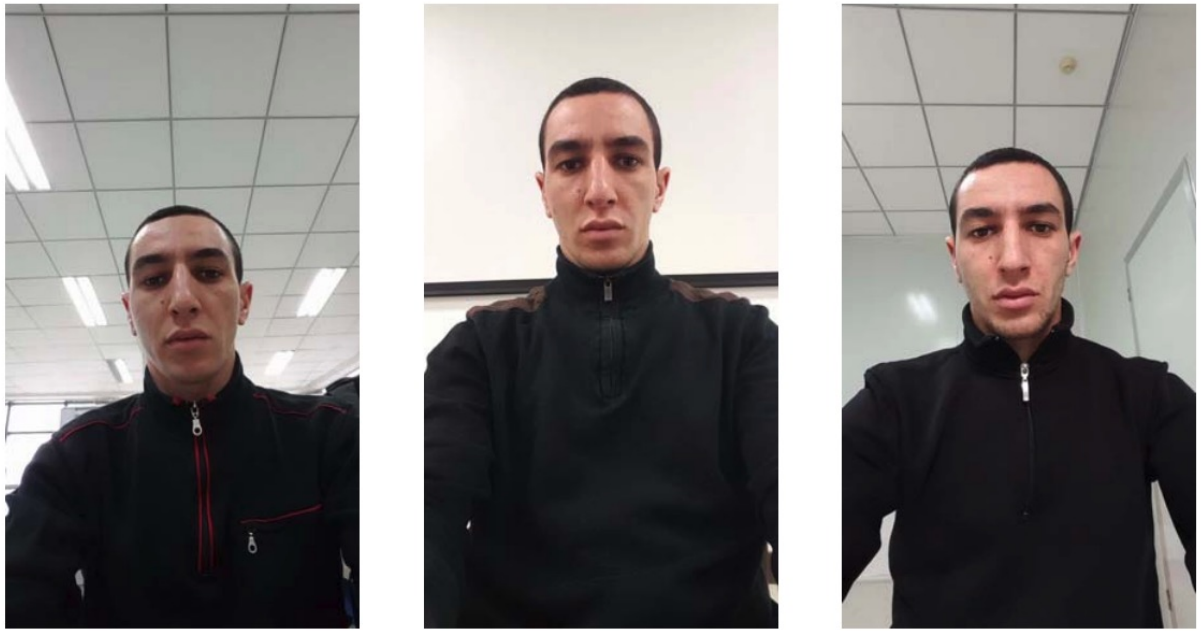
Protocol (a)



- With slight domain shift, as the training and testing data are sampled from the same datasets, they share similar domain distribution in terms of the recording environment, subject behavior, etc.

Protocol (a) dataset OULU-NPU

(a) Print 1 (b) Print 2 (c) Replay 1 (d) Replay 2

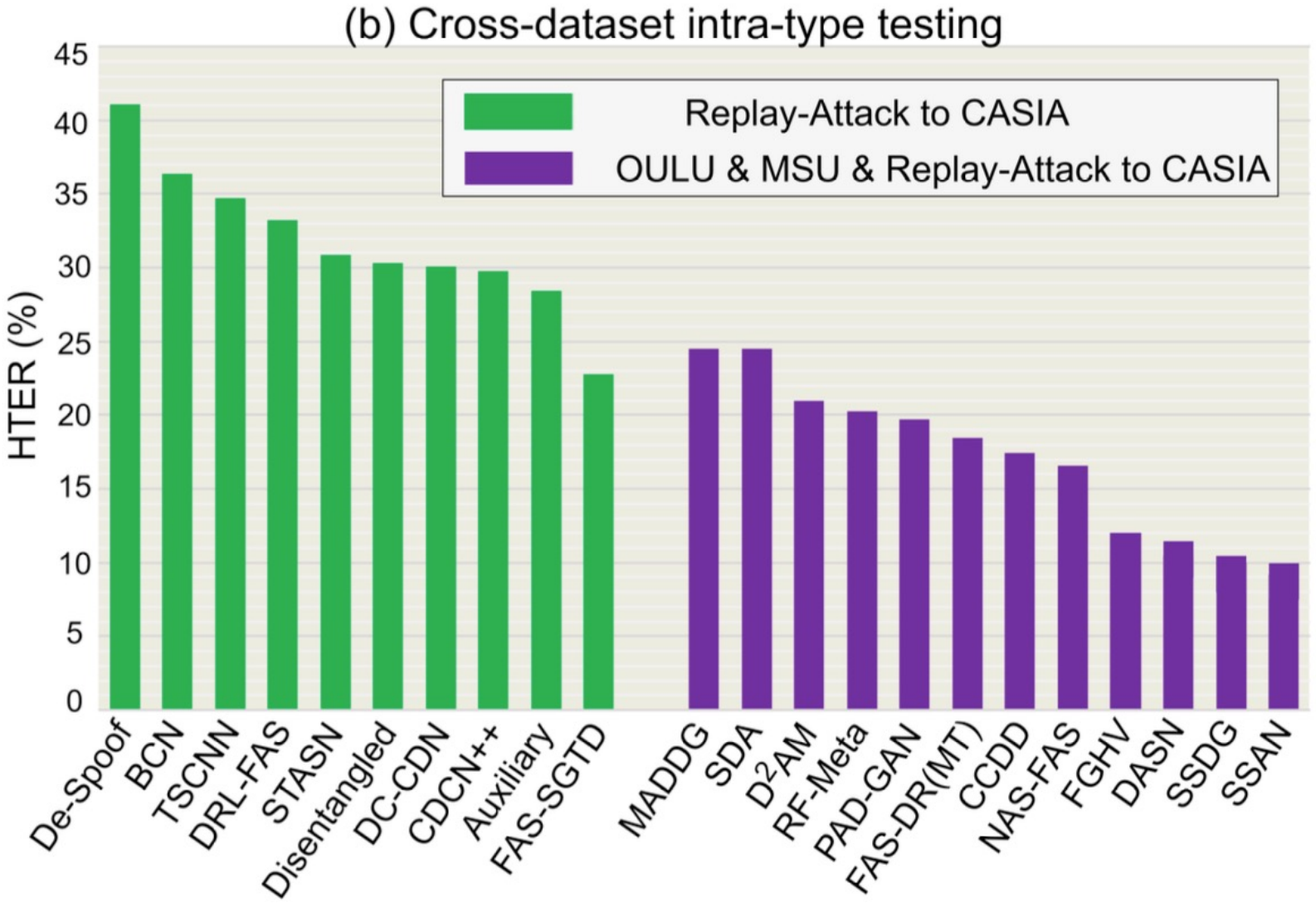


(a) Session 1 (b) Session 2 (c) Session 3

Protocol	Subset	Session	Phones	Users	Attacks created using	# real videos	# attack videos	# all videos
Protocol VI	Train	Session 1,2	5 Phones	1-20	Printer 1; Display 1	200	400	600
	Dev	Session 1,2	5 Phones	21-35	Printer 1; Display 1	150	300	450
	Test	Session 3	1 Phone	36-55	Printer 2; Display 2	20	40	60

720/2880(V)	55	VIS	Lighting & background in 3 sections	Print(flat), Replay(phone)

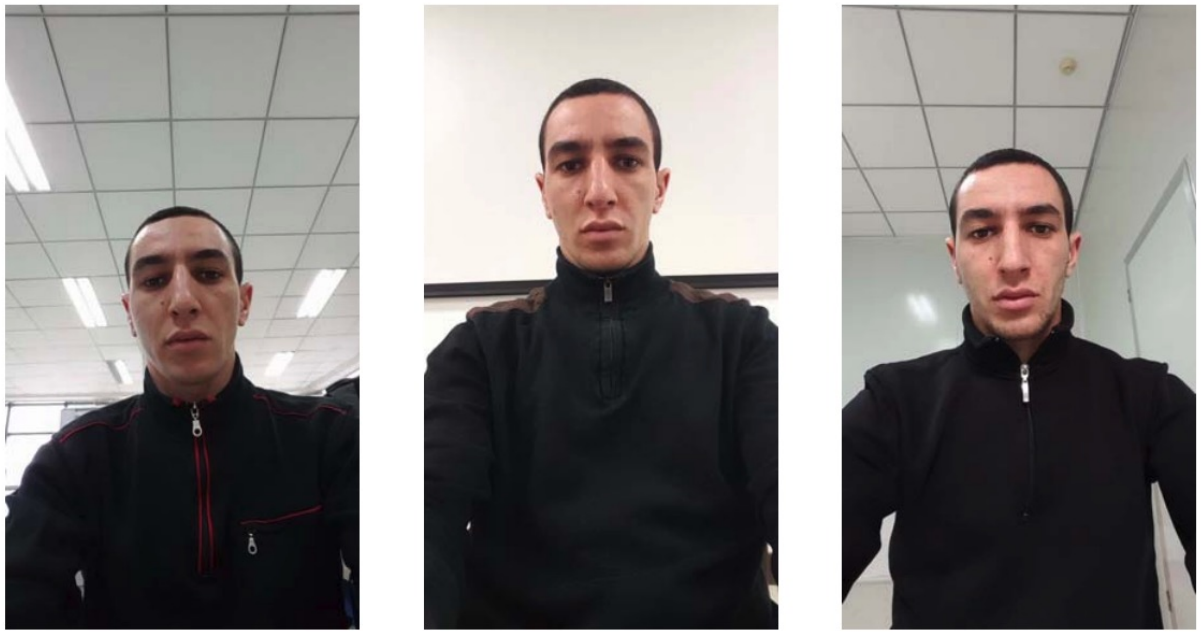
Protocol (b)



- Green bar
  - Train：Replay-Attack
  - Test：CASIA
- Purple bar
  - Train：Replay-Attack, OULU, MSU
  - Test：CASIA

Protocol (b.1) dataset OULU-NPU

(a) Print 1 (b) Print 2 (c) Replay 1 (d) Replay 2



(a) Session 1 (b) Session 2 (c) Session 3

720/2880(V)	55	VIS	Lighting & background in 3 sections	Print(flat), Replay(phone)

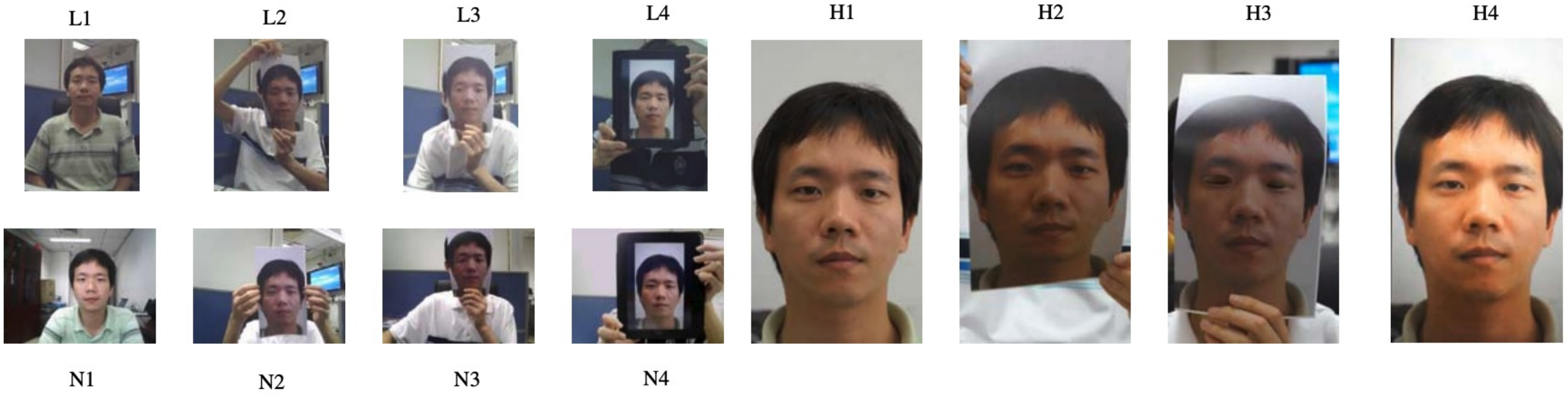
Protocol (b.1) dataset MSU-MFSD

70/210(V)	35	VIS	Indoor scenario; 2 types of cameras	Print(flat), Replay(tablet, phone)

Protocol (b.1) dataset REPLAY-ATTACK

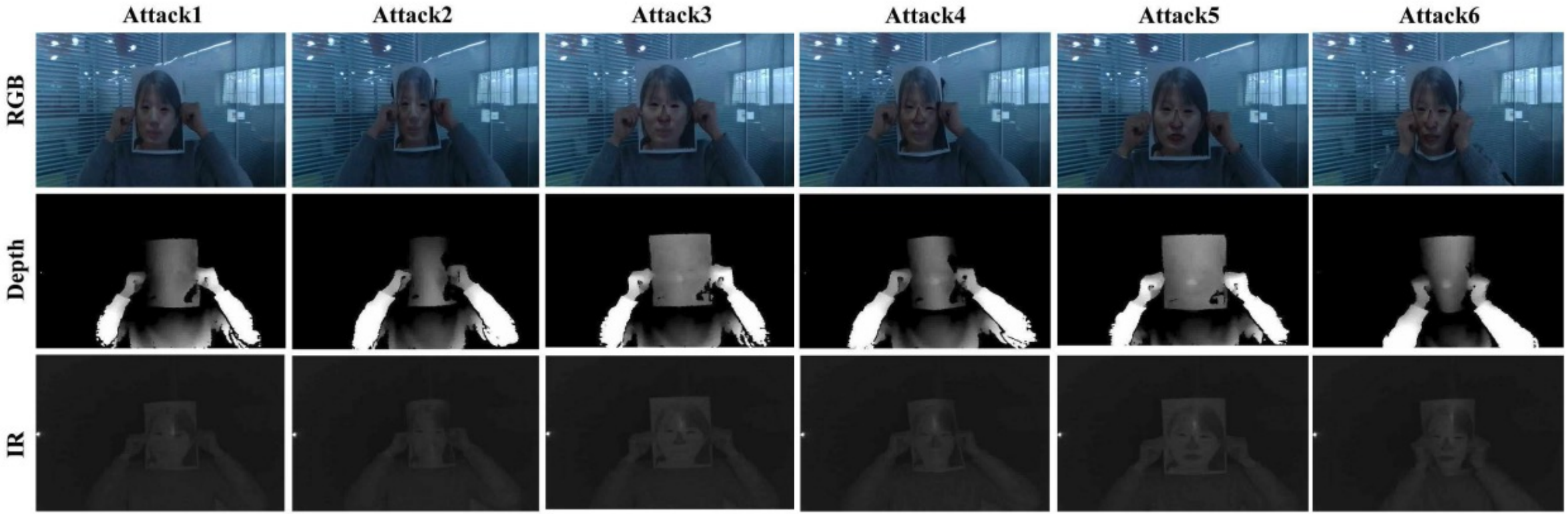
720/2880(V)	55	VIS	Lighting & background in 3 sections	Print(flat), Replay(phone)

Protocol (b.1) dataset CASIA-MFSD



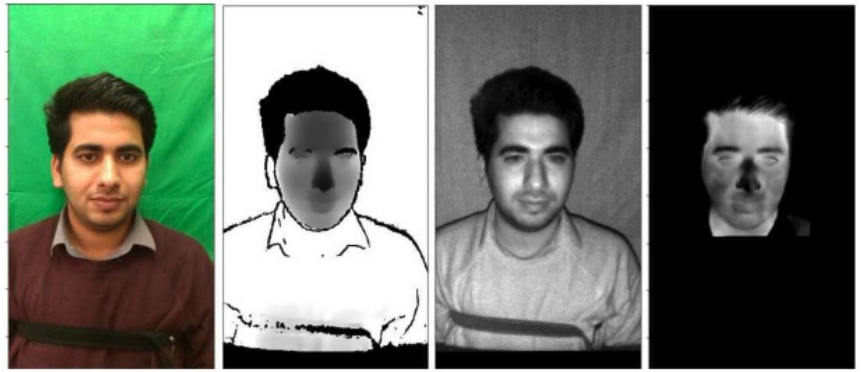
150/450(V)	50	VIS	7 scenarios and 3 image quality	Print(flat, wrapped, cut), Replay(tablet)

Protocol (b.2) dataset CASIA-SURF

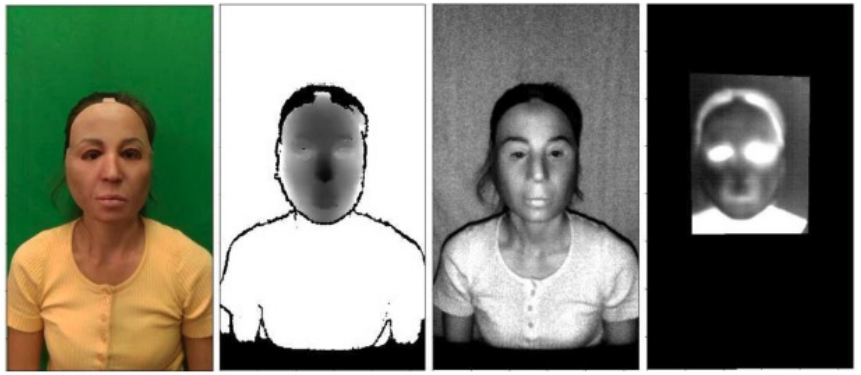


3000/ 18000(V)	1000	VIS, Depth, NIR	Background removed; Randomly cut eyes, nose or mouth areas	Print(flat, wrapped, cut)

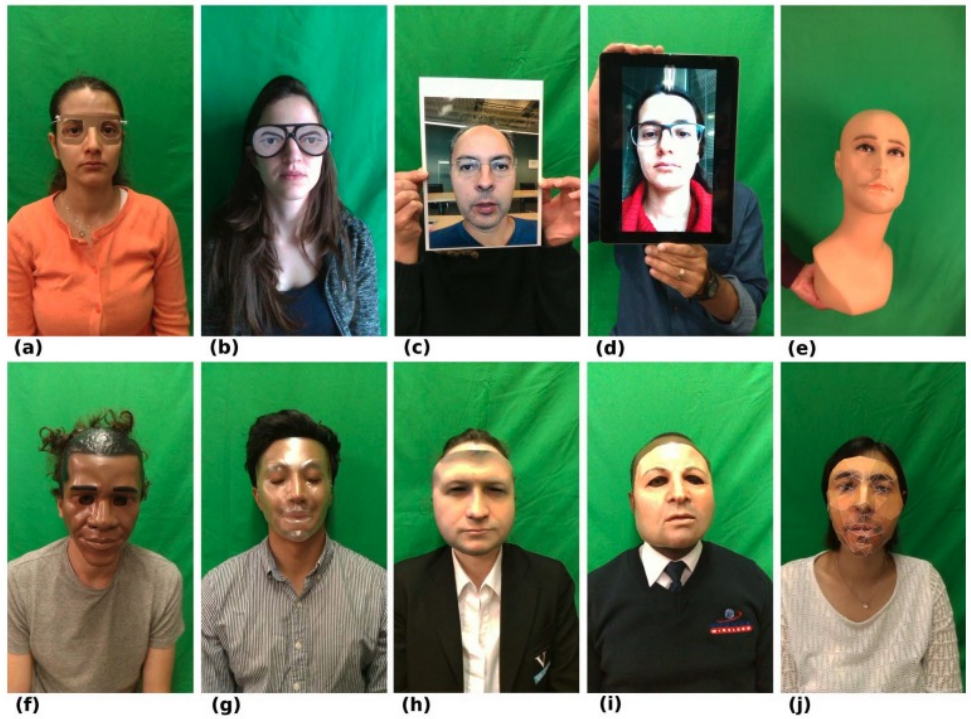
Protocol (b.2) dataset WMCA



(a)

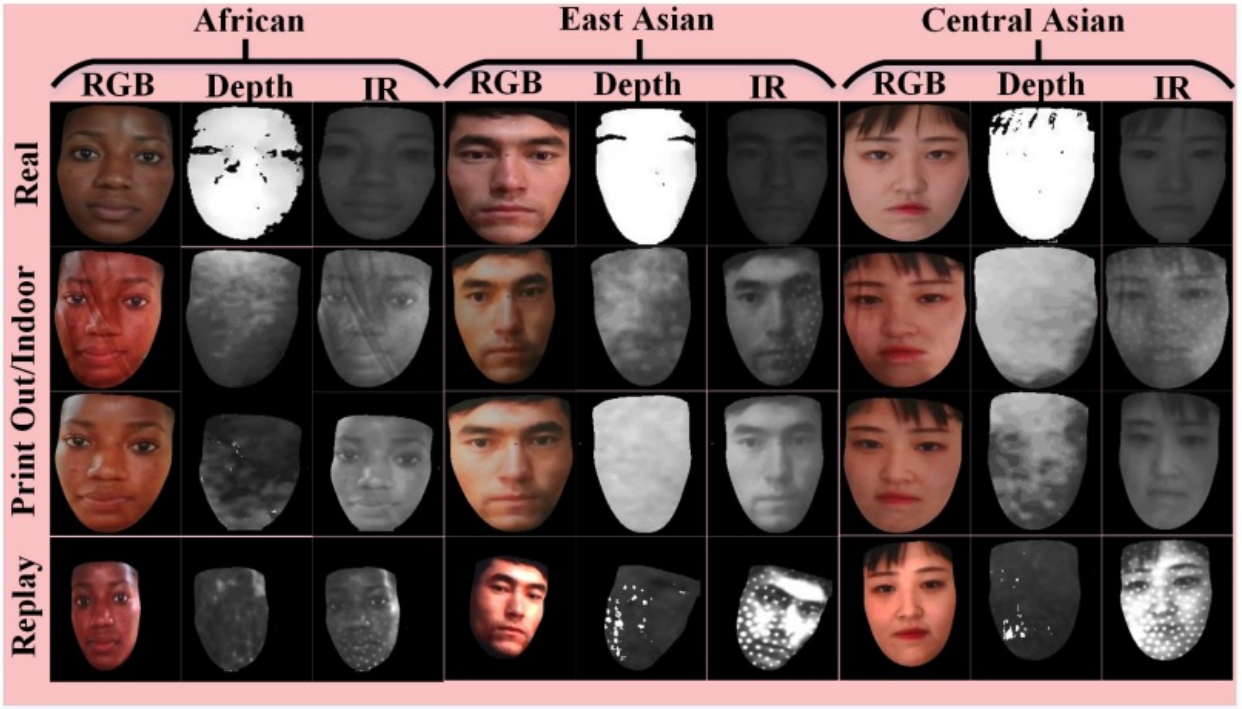


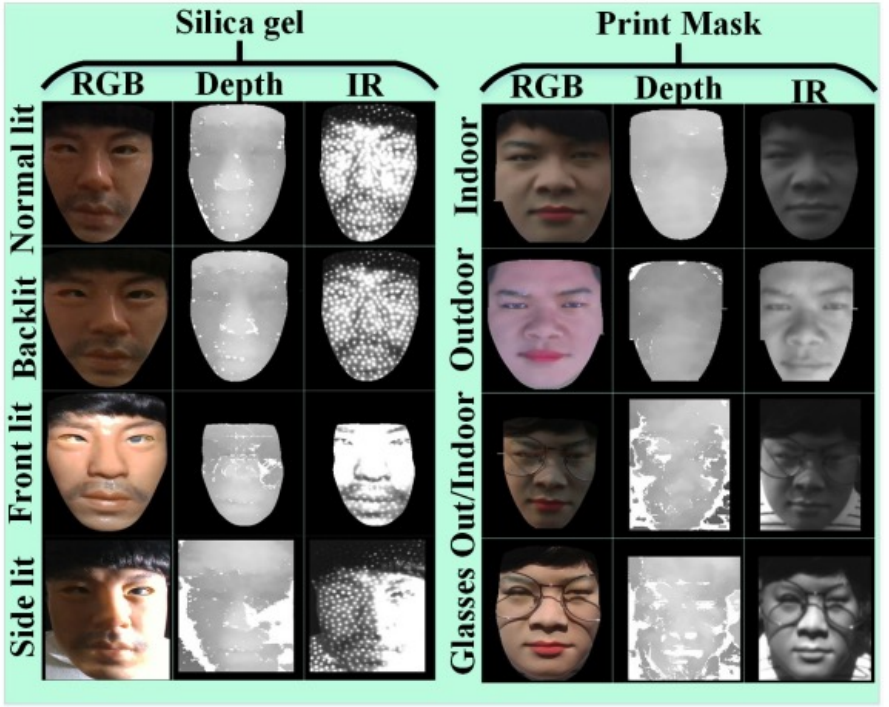
(b)



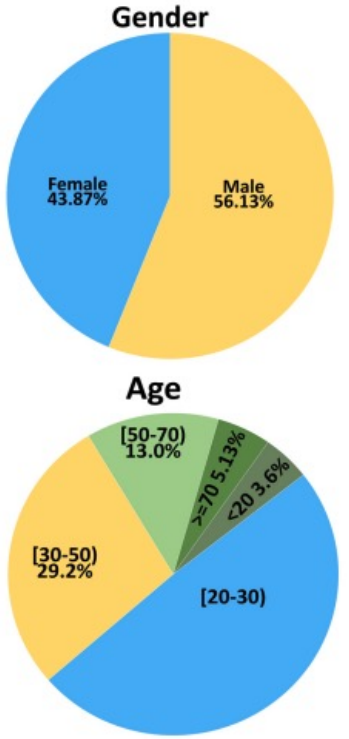
347/1332(V)	72	VIS, Depth, NIR, Thermal	6 sessions with different backgrounds and illumination; pulse data for bonafide recordings	Print(flat), Replay(tablet), Partial(glasses), Mask(plastic, silicone, and paper, Mannequin)

Protocol (b.2) dataset CASIA-CeFA





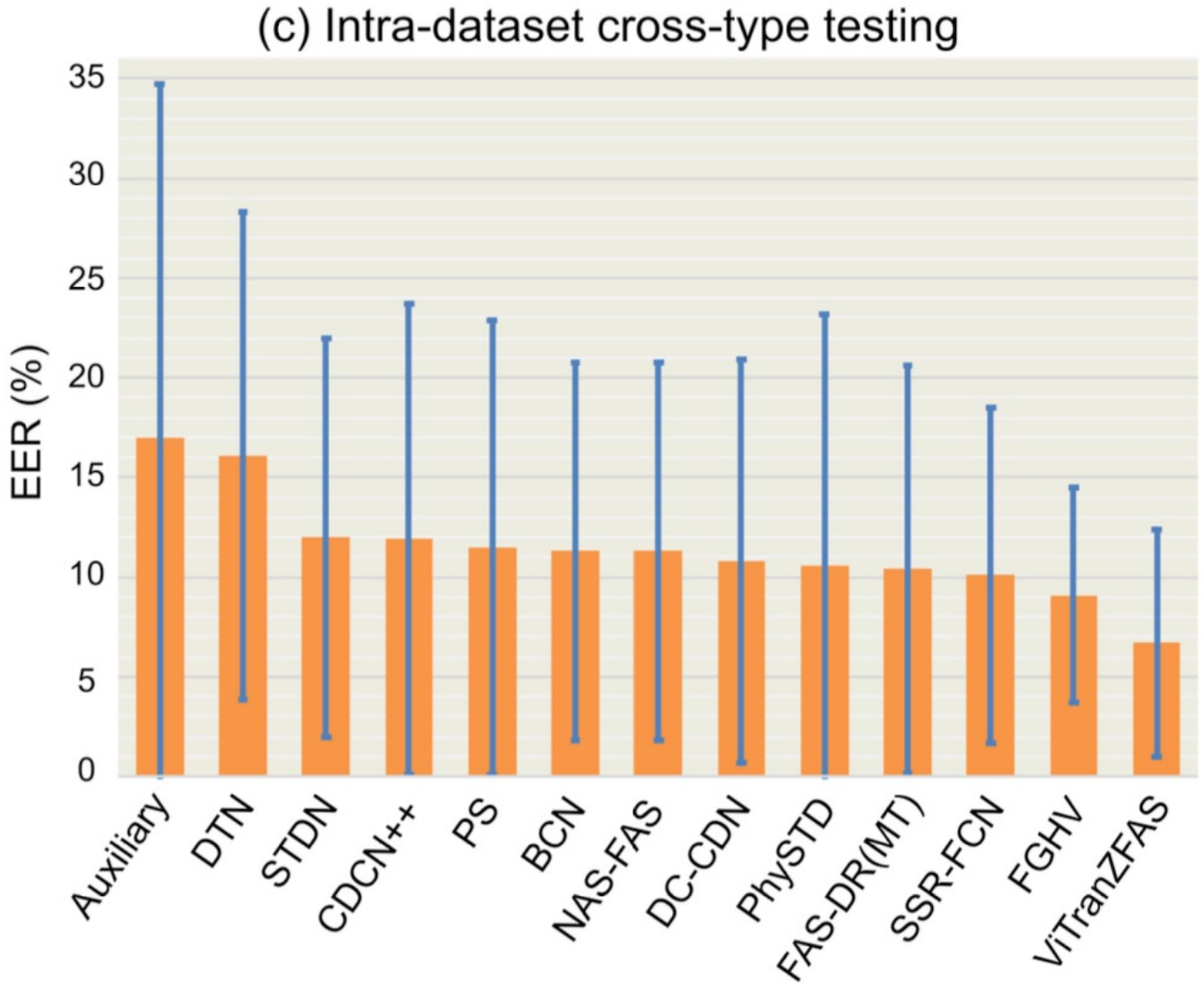
(a)



(b)

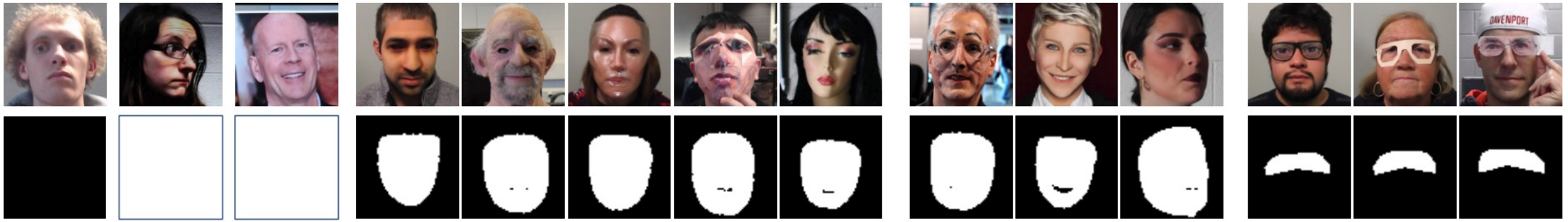
6300/ 27900(V)	1607	VIS, Depth, NIR	3 ethnicities; outdoor & indoor; decoration with wig and glasses	Print(flat, wrapped), Replay, Mask(3D print, silica gel)

Protocol (c)



- Intra-dataset cross-type testing on SiW-M with leave-one-type-out setting.

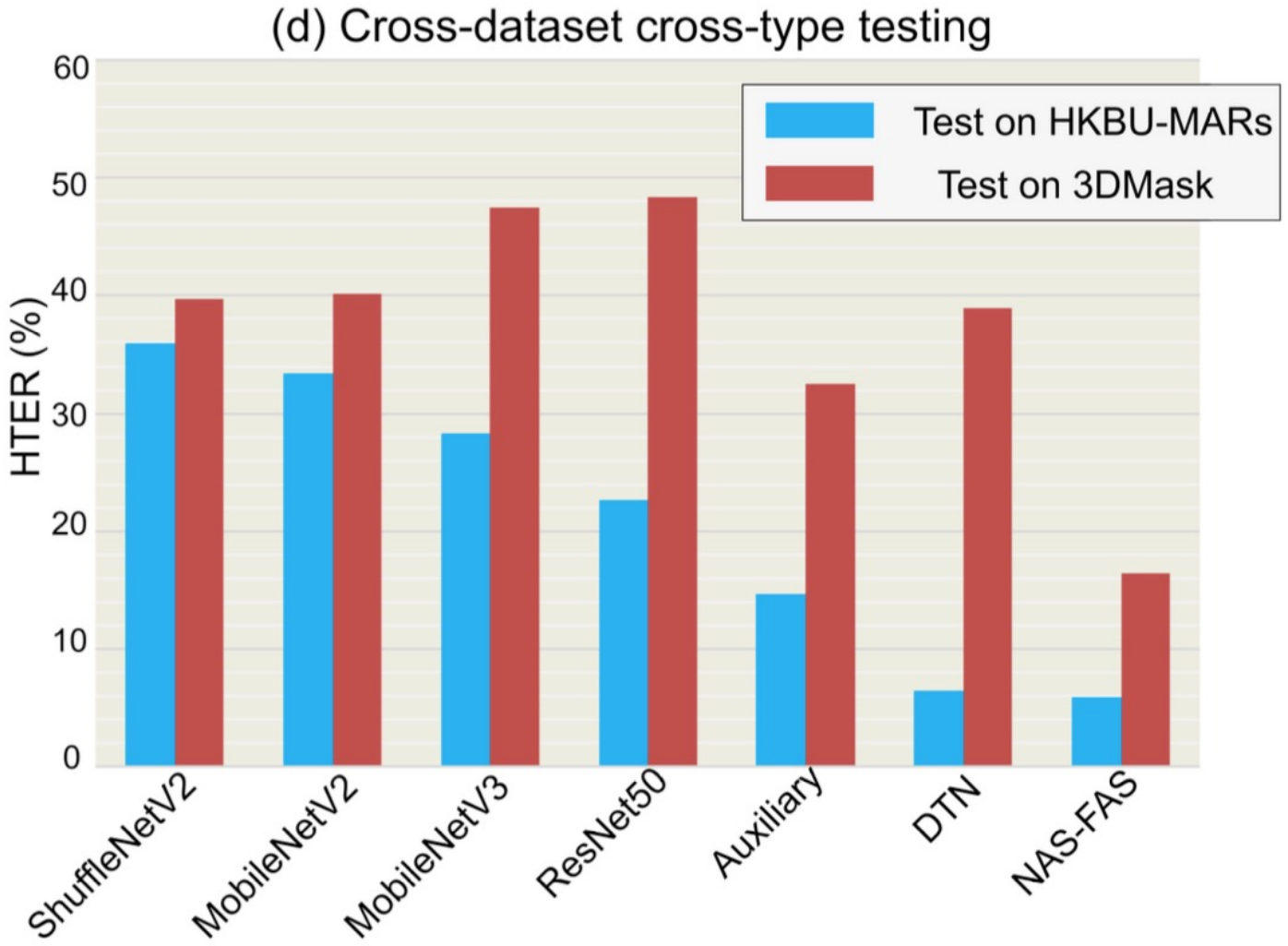
Protocol (c) dataset SiW-M



660/968(V)	493	VIS	Indoor environment with pose, lighting and expression variations	Print(flat), Replay, Mask(hard resin, plastic, silicone, paper, Mannequin), Makeup(cosmetics, impersonation, Obfuscation), Partial(glasses, cut paper)

complex recording conditions

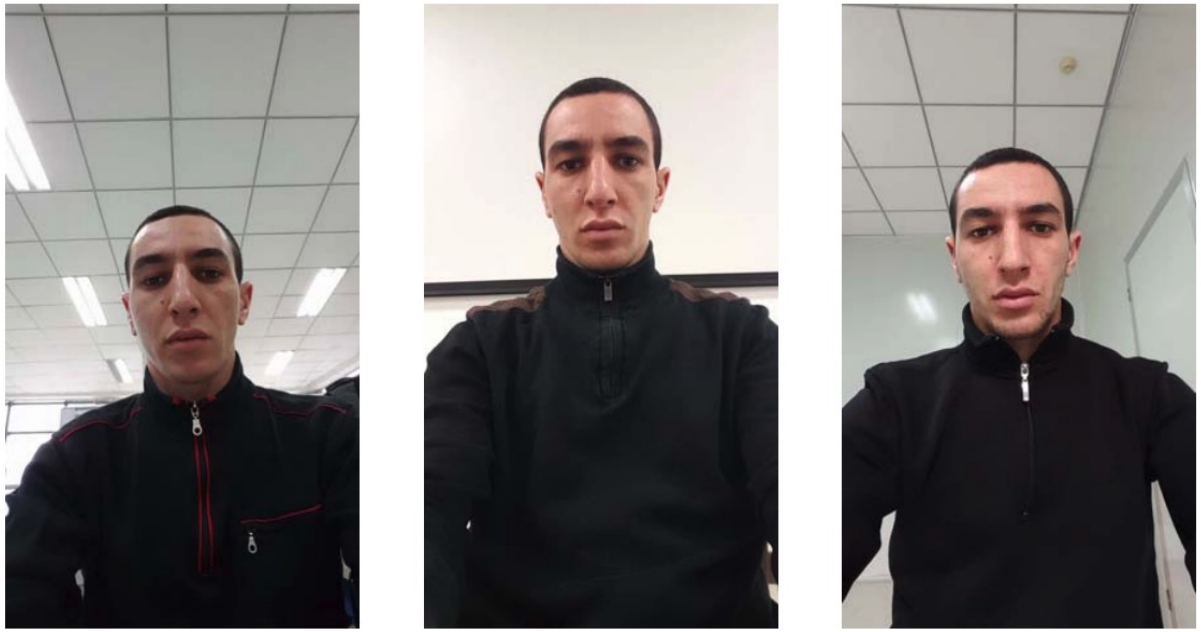
Protocol (d)



- Testing on 3D mask FAS datasets when training on datasets with only 2D attacks

Protocol (d) dataset OULU-NPU

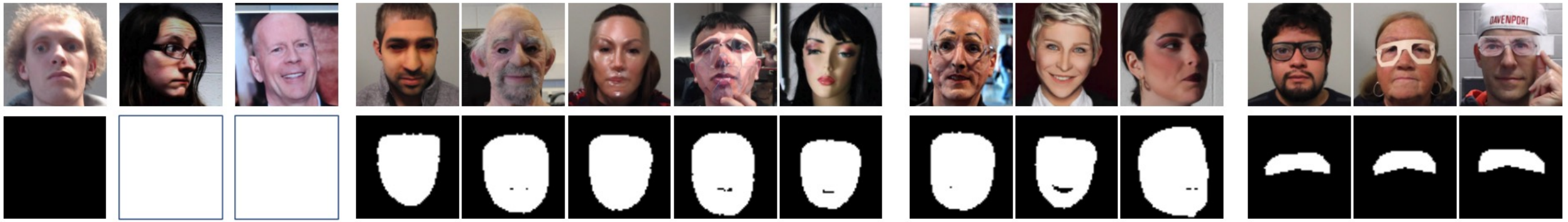
(a) Print 1 (b) Print 2 (c) Replay 1 (d) Replay 2



(a) Session 1 (b) Session 2 (c) Session 3

720/2880(V)	55	VIS	Lighting & background in 3 sections	Print(flat), Replay(phone)

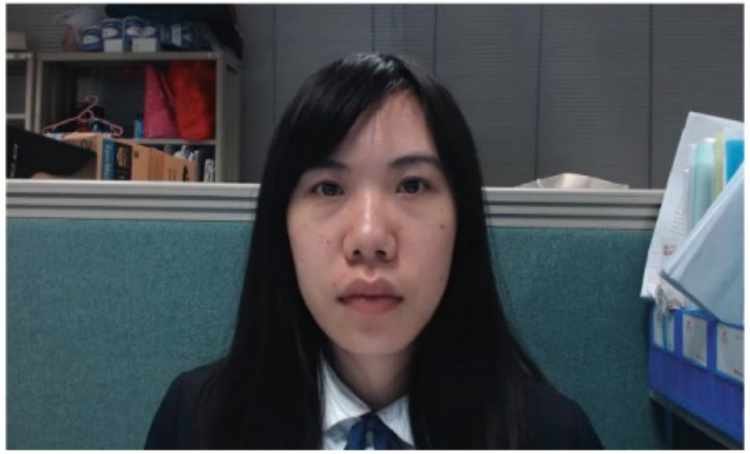
Protocol (d) dataset SiW-M



660/968(V)	493	VIS	Indoor environment with pose, lighting and expression variations	Print(flat), Replay, Mask(hard resin, plastic, silicone, paper, Mannequin), Makeup(cosmetics, impersonation, Obfuscation), Partial(glasses, cut paper)

complex recording conditions

Protocol (d) dataset HKBU-MARs V2



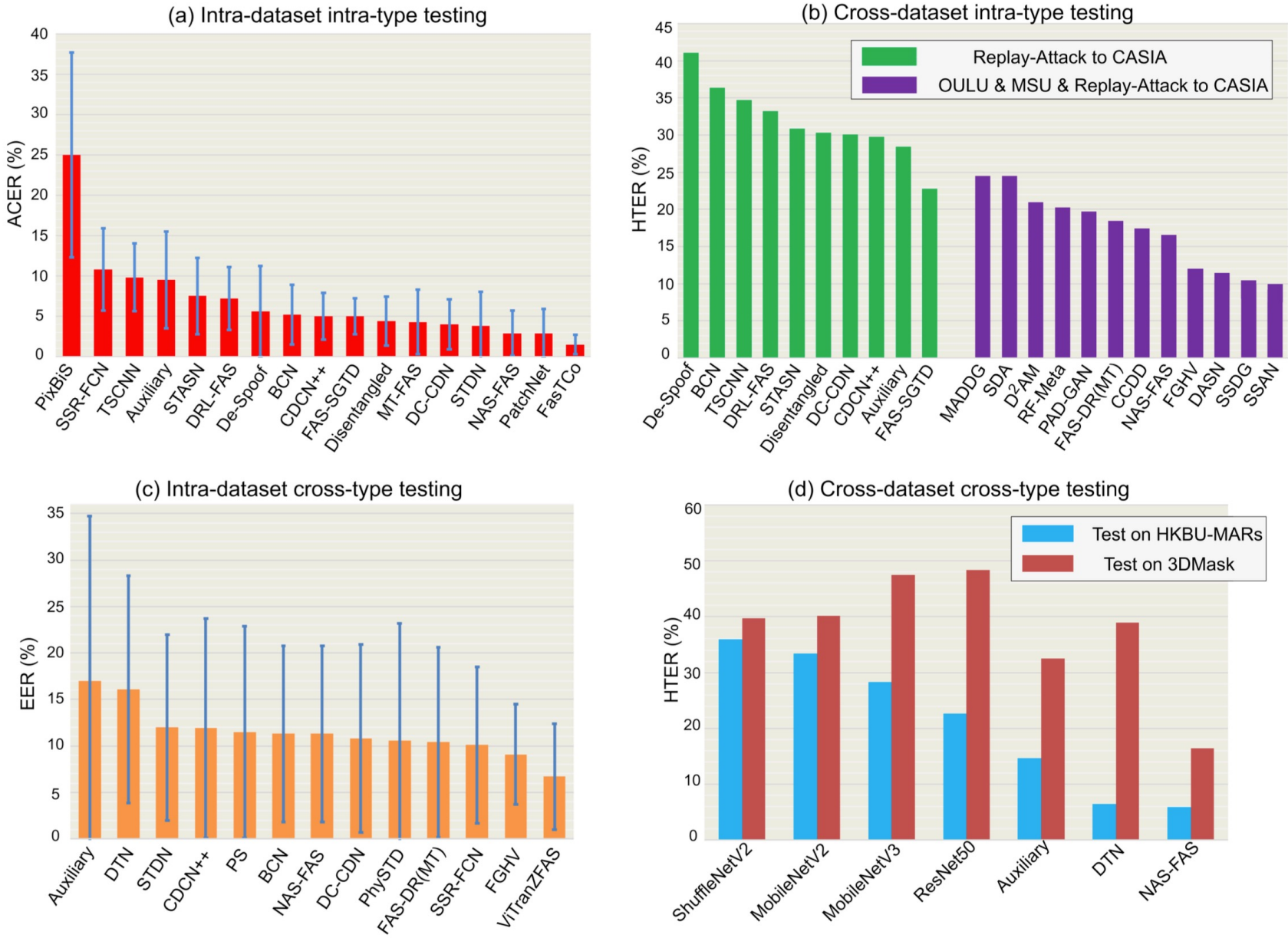
- Lab controlling dataset is low-fidelity.

504/504(V)	12	VIS	7 cameras from stationary and mobile devices and 6 lighting settings	Mask(hard resin) from Thatsmyface and REAL-f

Protocol (d) dataset CASIA-SURF 3DMask

288/864(V)	48	VIS	High-quality identity-preserved; 3 decorations and 6 environments	Mask(mannequin with 3D print)

Performance of four evaluation protocols



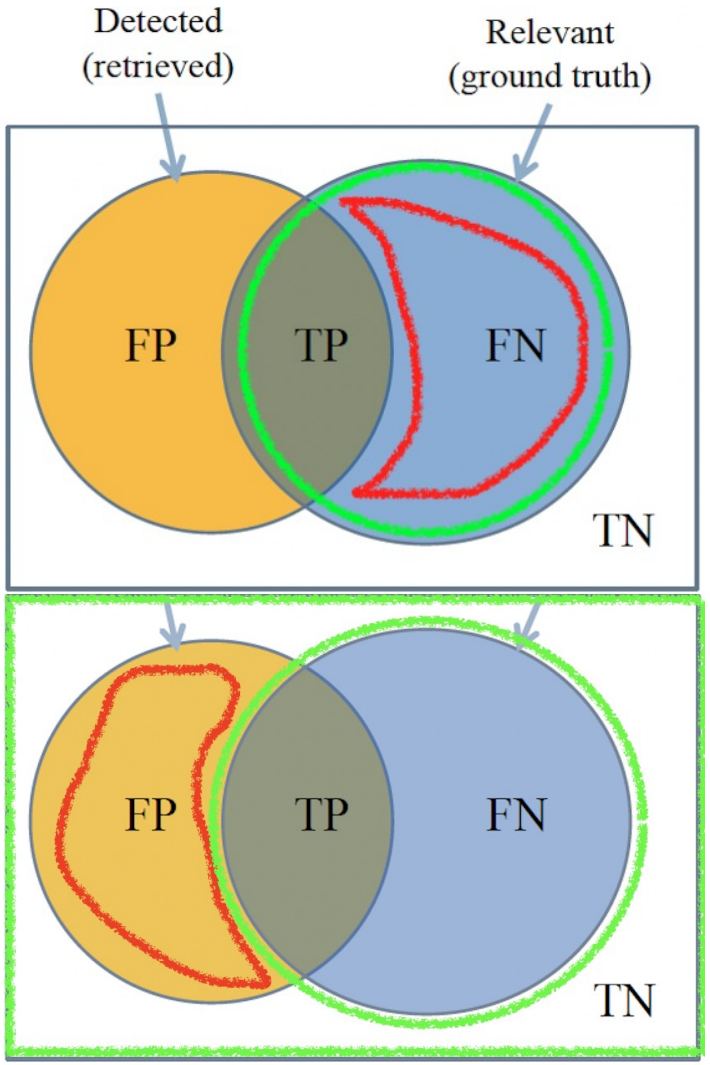
Outline

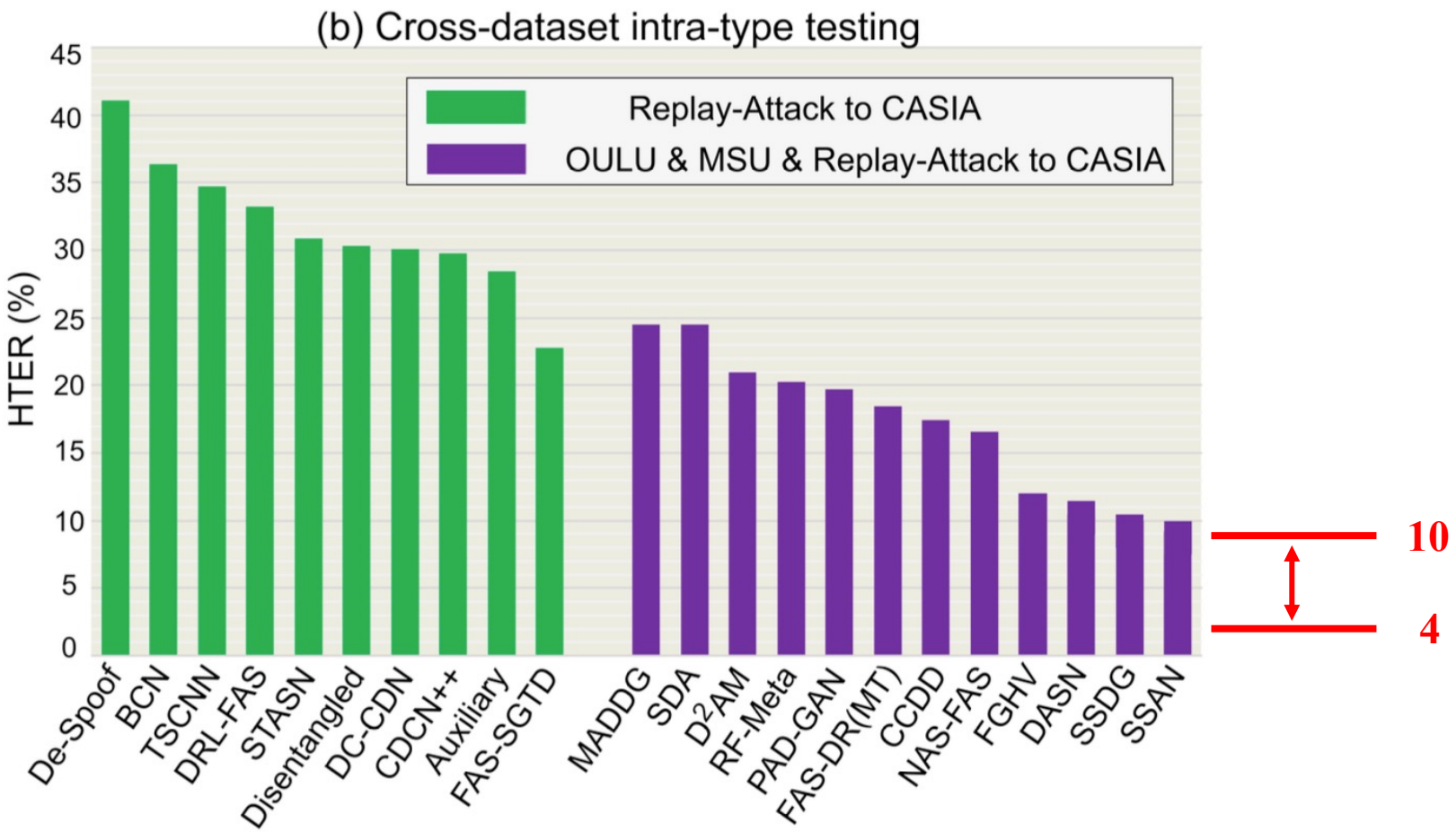
- Introduction
- Metrics
- Protocol & Dataset
- Recent paper protocol
- CVPRW challenge
- Conclusion

Recent paper protocol in CVPR 2024

- ~~Protocol (a)~~
- Protocol (b): Cross-dataset Intra-type
  - FLIP, CFPL-FAS, HPDR, TTDG, GAC-FAS
  - Multi-modal: MMDG
- Protocol (c)
  - HPDR
- Protocol (d)
  - GAC-FAS
- Special case
  - SCM-guided

Performance of paper in CVPR 2024





Outline

- Introduction
- Metrics
- Protocol & Dataset
- Recent paper protocol
- CVPRW challenge
- Conclusion

FAS Workshop and Challenge@CVPR2023

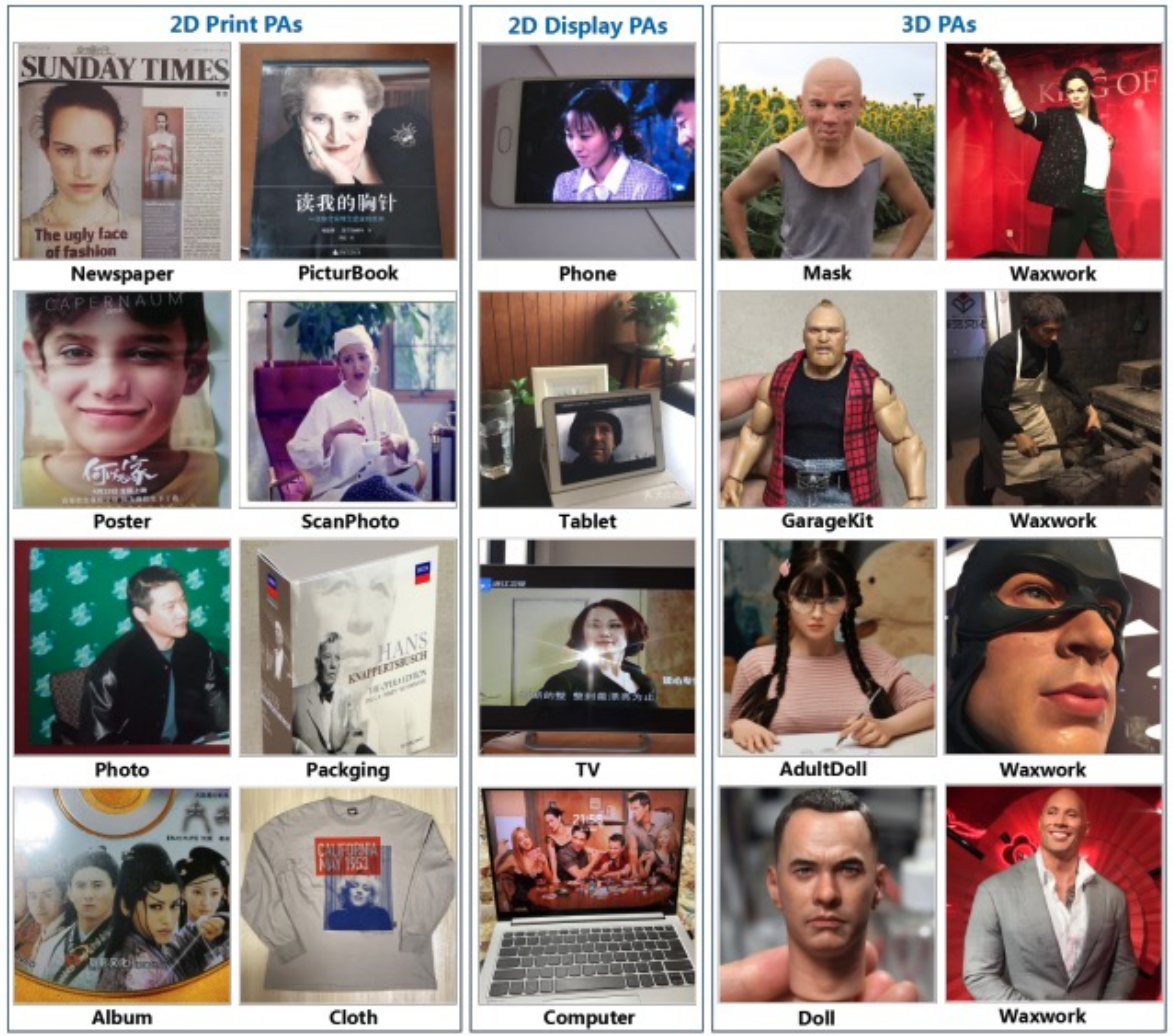
Existing FAS dataset	Surveillance scene based FAS dataset
	
Number of Subject: One	Number of Subject: : Many
Number of real or attack : One	Number of real or attack : Multiple real people and multiple types of attacks
Face Resolution : High resolution	Face Resolution : Low resolution
Posture and movement: Face the camera and remain still	Posture and movement: Not facing the camera and moving freely

Dataset, Year	#sub.	Distance (Long/Short)	Materials	Scenes	Light, Weather	Attacks	Devices	#Videos (#Live/#Fake)
SuHiFiMask (ours), 2022	101	**Long**	Resin, Plaster, Silicone, Paper	Security check lane, Theater, Parking lot [1]	Day/Night light, Sunny/Windy/ Cloudy/Snowy day	2D image, Video replay, 3D Mask	Surveillance cameras[2]	10,195* (10,195/10,195)

FAS Workshop and Challenge@CVPR2023

RESULTS							
#	User	Entries	Date of Last Entry	AUC ▲	APCER ▲	BPCER ▲	RANK<ACER> ▲
1	MateoH	14	03/04/23	98.1706	5.5044	3.4992	4.5018 (1)
2	CTEL_AI	17	03/04/23	98.2148	9.2130	1.9001	5.5565 (2)
3	horsego	18	03/04/23	96.9842	8.1093	4.3583	6.2338 (3)
4	hexianhua	15	03/04/23	97.8283	11.2076	2.9447	7.0762 (4)
5	buccellati	3	03/04/23	97.3799	9.1752	5.1275	7.1514 (5)
6	ew	11	03/04/23	97.5665	11.2793	3.0455	7.1624 (6)
7	OPDAI	14	03/04/23	97.1574	7.2058	8.4120	7.8089 (7)
8	wida	14	03/04/23	97.0104	12.3691	3.2614	7.8153 (8)
9	O-Sullivan	11	03/04/23	96.7046	10.4211	6.2086	8.3148 (9)
10	Ricardozzf	4	03/04/23	96.8995	10.0524	9.1157	9.5840 (10)

FAS Workshop and Challenge@CVPR2023



Category	PAs	Subjects	Images	Train	Dev	Test
2D-Print	Newspaper	9,046	14,425	✓		
	Poster	40,858	15,439	✓		
	photo	61,990	102,826	✓		
	Album	21,122	56,490	✓		
	PictureBook	118,355	349,232		✓	✓
	ScanPhoto	1,161	2,484		✓	✓
	Packaging	3,866	19,136		✓	✓
	Cloth	138	266		✓	✓
2D-Display	Phone	20,813	34,907	✓		
	Tablet	8,089	15,431	✓		
	TV	28,184	75,606		✓	✓
	Computer	13,938	25,291		✓	✓
3D	Mask	268	1,454	✓		
	GarageKit	1,488	4,505	✓		
	AdultDoll	165	12,021	✓		
	Doll	15,406	91,954		✓	✓
	Wax	2,283	6,843		✓	✓

FAS Workshop and Challenge@CVPR2023

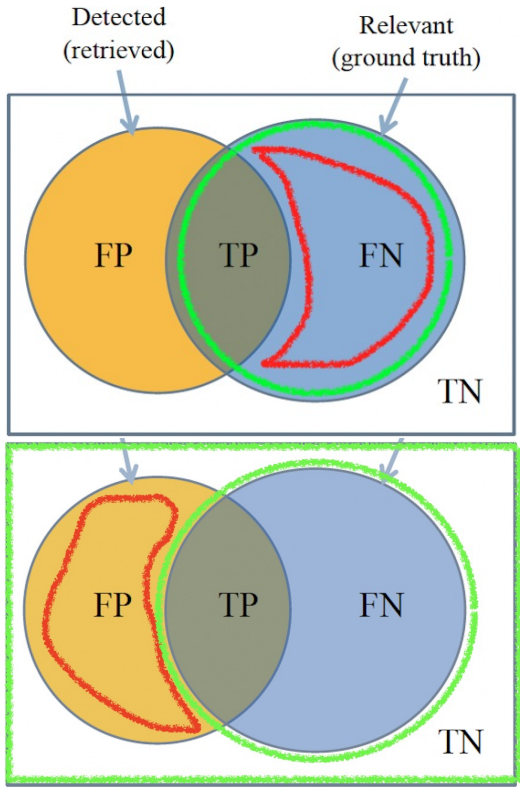
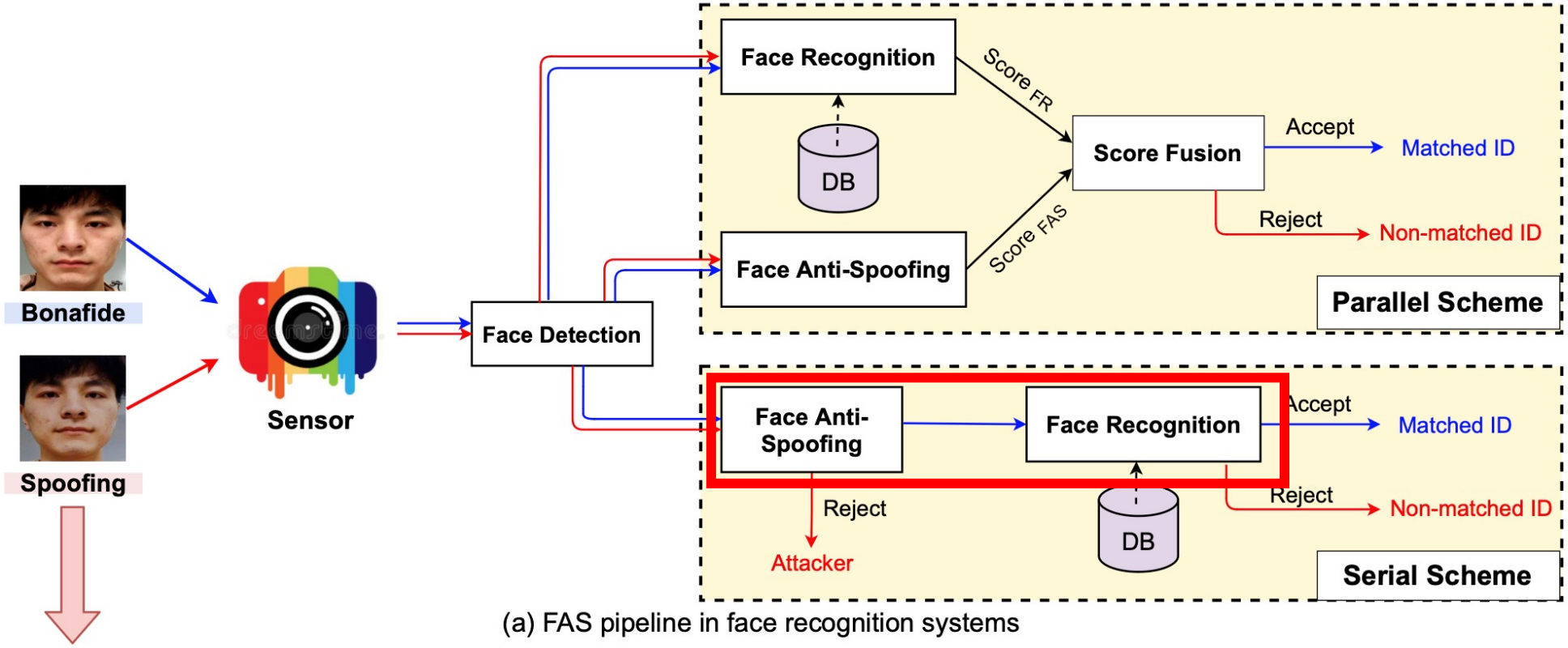


Table 4. The top-10 results of the Wild Face Anti-Spoofing Challenge at CVPR2023 workshop.

Rank	Affiliation	Team	ACER(%)	APCER(%)	BPCER(%)
1	ChinaTelecom	xuyaowen	**1.6010**	**1.2960**	**1.9060**
2	Meituan	hexianhua	2.2210	1.3770	3.0640
3	Netease	buccellati	2.5540	2.3390	2.7690
4	SCUT	xmj	2.8940	1.4440	4.3450
5	-	luoman	3.0700	1.7450	4.3950
6	-	Sicks	3.1450	1.7250	4.5640
7	KiwiTech	KiwiTech_LeoDu	3.1800	2.2060	4.1540
8	XMU	Iverson	3.1890	3.2890	3.0900
9	-	admin123	3.5300	2.7530	4.3060
10	SJTU	iKunCTRL	3.5430	3.2420	3.8440

Dataset	Year	Subjects	Quantity	Format	PAs
Our Dataset (WFAS)	2023	469,920	1,383,300	image	Print(newspaper, poster, photo, album, picture book, scan photo, packging, cloth), Display(phone, tablet, TV, computer), Mask, 3D Model(garage kit, doll, adult doll, waxwork)

FAS Workshop and Challenge@CVPR2024



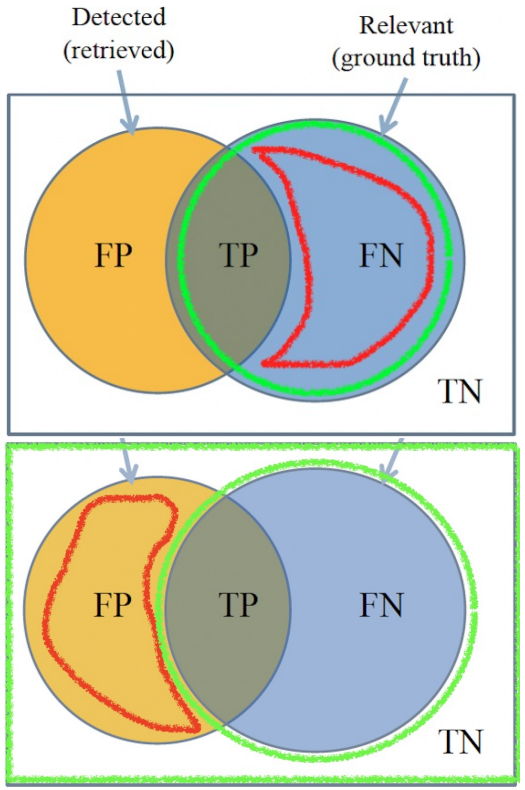
(a) FAS pipeline in face recognition systems

FAS Workshop and Challenge@CVPR2024

Figure 2: UniAttackData Dataset examples of all attack types corresponding to the same face ID. From top to bottom, they are Africans, Central Asians, and East Asians, respectively. The attack type of each sample is marked at the top.

UniAttackData (Ours)	**Complete**	**1 set: 29706 (V) (Live: 1800, Fake: 27906)**	**1800**	CASIA-SURF CeFA [Liu *et al.*, 2021a]	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 [Zou *et al.*, 2022]	1800 (V)
							ila_da [Yan *et al.*, 2022]	1800 (V)
							ssah [Luo *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)**

FAS Workshop and Challenge@CVPR2024



RESULTS

#	User	Entries	Date of Last Entry	AUC ▲	APCER ▲	BPCER ▲	RANK<ACER> ▲
1	Santosh	1	02/29/24	99.9992	1.7333	0.0903	0.9118 (5)
2	zry	4	03/02/24	99.9946	0.1778	0.2716	0.2247 (1)
3	jho-yonsei	4	03/02/24	99.9797	1.0963	0.3310	0.7136 (2)

Outline

- Introduction
- Metrics
- Protocol & Dataset
- Recent paper protocol
- CVPRW challenge
- Conclusion

Conclusion

- Introducing **various protocols** which provide a thorough assessment of FAS models, revealing strengths and weaknesses by testing on different datasets and attack scenarios.

- Showing **metrics** like HTER, EER, and AUC are essential for balanced evaluation, ensuring security and usability of FAS models.

- Recent advancements show progress in FAS, but challenges like domain shifts and robustness against diverse attacks persist.