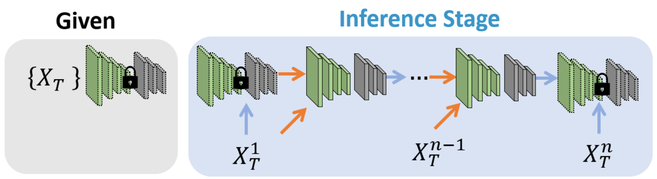
Test-Time Adaptation for Robust Face Anti-Spoofing

BMVC 2023 The 34th British Machine Vision Conference
20th - 24th November 2023, Aberdeen, UK

Pei-Kai Huang, Chen-Yu Lu, Shu-Jung Chang, Jun-Xiong Chong, and Chiou-Ting Hsu
National Tsing Hua University, Taiwan

Face Anti-Spoofing (FAS)

Fully Test-Time Adaptation (TTA)



~~$\{X_S, Y_S\}$: Label source dataset~~ → Training → Testing

$\{X_T\}$: Unlabeled target dataset $\{X_T\} = \{X_T^1, X_T^2, \ldots, X_T^n\}$

Challenges in TTA Setting

- Noisy pseudo-label problem
- Class imbalance within a batch of target data
- Unseen attack types

Goal

- To obtain reliable pseudo labels
  - ➢ Via fine-grained activation map
- To prevent overfitting to one dominant class
  - ➢ Via memory bank
- To detect unseen attack types
  - ➢ Associate unseen attacks with seen attacks

3A-TTA Framework

Activation-Based Pseudo-Labeling

- Pseudo label
- Similarity between liveness feature and class activation map

$$\bar{y} = \begin{cases} 1, if\ sim(\mathbf{f}, \mathbf{A}_l) \geq sim(\mathbf{f}, \mathbf{A}_s); \\ 0, if\ sim(\mathbf{f}, \mathbf{A}_l) < sim(\mathbf{f}, \mathbf{A}_s); \end{cases}$$

- Liveness loss

$$\mathcal{L}_l = -\sum \bar{y} log \mathbf{CF}(\mathbf{f}) + (1-\bar{y}) log(1-\mathbf{CF}(\mathbf{f}))$$

Anti-Forgetting Feature Learning

- Reliable feature selection

$$\gamma = \begin{cases} 1, & if \quad \begin{cases} \mathbf{CF}(\mathbf{f}) > \alpha \quad and \quad m_{sim} \geq \beta; \\ \mathbf{CF}(\mathbf{f}) < 1-\alpha \quad and \quad m_{sim} \leq -\beta; \end{cases} \\ 0, & otherwise \end{cases}$$

(Prediction Threshold: α; Activation Map Threshold: β)

- Anti-forgetting liveness loss

$$\mathcal{L}_{afl} = -\sum \hat{y} log \mathbf{CF}(\hat{\mathbf{f}}) + (1-\hat{y}) log(1-\mathbf{CF}(\hat{\mathbf{f}}))$$

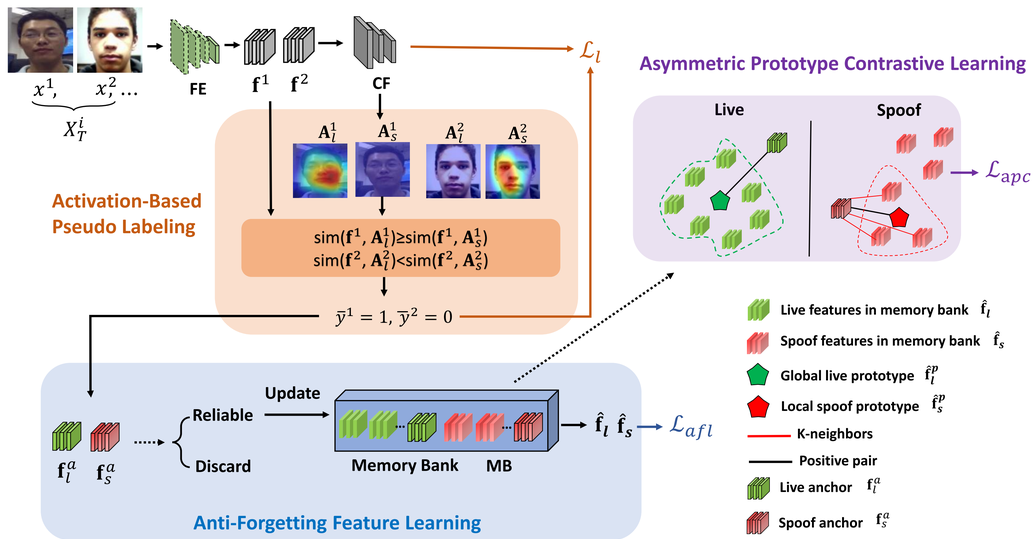
Asymmetric Prototype Contrastive Learning

- Asymmetric prototype contrastive loss

$$\mathcal{L}_{apc} = -\log \frac{\exp\left(sim(\mathbf{f}_s^a, \hat{\mathbf{f}}_s^p)\right)}{\sum_{j=\{\hat{\mathbf{f}}_s^p \cup N_s\}} \exp\left(sim\left(\mathbf{f}_s^a, \hat{\mathbf{f}}^j\right)\right)} - \log \frac{\exp(sim(\mathbf{f}_l^a, \hat{\mathbf{f}}_l^p))}{\sum_{j=\{\hat{\mathbf{f}}_l^p \cup N_l\}} \exp(sim\left(\mathbf{f}_l^a, \hat{\mathbf{f}}^j\right))}$$

Total Loss

$$\mathcal{L}_T = \mathcal{L}_l + \lambda_1 \mathcal{L}_{afl} + \lambda_2 \mathcal{L}_{apc}$$



Experiments

Datasets

- OULU-NPU (O), MSU-MFSD (M), CASIA-MFSD (C), Replay-Attack (I), 3DMAD (D), and HKBU-MARs (H)

Evaluation Metrics

- Half Total Error Rate (HTER) ↓
- Area Under Curve (AUC) ↑

Ablation Study

Method	Total Loss $\mathcal{L}_T$				pseudo-labeling Mechanisms			Feature Selection	[OMI] → D		[OMI] → C	
	$\mathcal{L}_l$	$\mathcal{L}_{afl}$	$\mathcal{L}_{apc}$	$\mathcal{L}_c$	Score based	Class Prototype based	Activation based		HTER	AUC	HTER	AUC
M0									26.86	87.83	28.78	86.26
M1	✓				✓				23.19	88.41	29.78	85.05
M2	✓					✓			27.72	88.28	30.24	86.05
M3	✓						✓		21.87	88.68	26.02	86.44
M4	✓	✓					✓		19.31	88.49	24.94	86.29
M5	✓	✓					✓	✓	18.15	89.47	24.33	87.07
M6	✓	✓		✓			✓	✓	18.20	87.78	26.00	86.56
M7	✓	✓	✓				✓	✓	**17.21**	**90.63**	**23.55**	**87.29**

Proposed TTA-FAS Benchmark

Protocol	Subset	Attack Type	Real data (V/I)	Attack data (V/I)	All data (V/I)
[O,C,I] → [M,D,H]	Source: OCI	print, replay	1280	5110	6390
	Target: MDH	print,replay,3D Mask	339	355	694
[O,M,I] → [C,D,H]	Source: OMI	print, replay	1200	4360	5560
	Target: CDH	print,replay,3D Mask	419	595	1014
[O,C,M] → [I,D,H]	Source: OCM	print, replay	1210	4620	5830
	Target: IDH	print,replay,3D Mask	409	845	1254
[I,C,M] → [O,D,H]	Source: ICM	print, replay	350	1360	1710
	Target: ODH	print,replay,3D Mask	1259	4105	5364

Experimental Comparisons

Method	[O,C,I] → [M,D,H]									[O,M,I] → [C,D,H]								
	O,C,I → M		O,C,I → D		O,C,I → H		Average		Time	O,M,I → C		O,M,I → D		O,M,I → H		Average		Time
	HTER	AUC	HTER	AUC	HTER	AUC	HTER	AUC		HTER	AUC	HTER	AUC	HTER	AUC	HTER	AUC	
No adaptation	26.67	94.49	19.55	88.11	22.15	84.33	22.79	88.98	0.50	28.78	86.26	26.86	87.83	23.47	84.91	26.37	86.33	0.62
Tent [42]	27.98	94.49	22.67	87.44	22.49	84.55	24.38	88.83	1.061	28.14	79.68	46.10	53.69	28.54	79.36	34.26	70.91	1.36
OAP [3]	26.41	94.49	19.79	88.09	22.15	84.35	22.78	87.35	0.55	29.34	86.03	26.86	87.78	22.95	85.86	25.38	86.55	0.70
3A-TTA	**26.21**	**94.53**	**16.26**	**92.03**	**20.89**	**84.74**	**21.12**	**90.43**	4.35	**23.55**	**87.29**	**17.21**	**90.63**	**20.33**	**86.99**	**20.36**	**88.30**	7.12
Method	[O,C,M] → [I,D,H]									[I,C,M] → [O,D,H]								
	O,C,M → I		O,C,M → D		O,C,M → H		Average		Time	I,C,M → O		I,C,M → D		I,C,M → H		Average		Time
	HTER	AUC	HTER	AUC	HTER	AUC	HTER	AUC		HTER	AUC	HTER	AUC	HTER	AUC	HTER	AUC	
No adaptation	30.36	71.22	25.27	83.89	19.93	90.08	25.19	81.73	0.71	37.73	81.95	25.80	**81.79**	34.93	83.88	32.82	**82.54**	2.28
Tent [42]	35.73	70.16	25.43	84.12	22.28	89.81	27.81	81.36	1.57	47.01	64.23	26.43	80.11	42.43	83.40	38.62	75.91	8.72
OAP [3]	29.69	71.15	25.15	83.81	19.93	90.09	24.92	81.68	0.81	31.21	78.50	25.62	81.55	35.41	83.65	30.75	81.23	2.28
3A-TTA	**28.11**	**72.45**	**21.78**	**86.28**	**16.99**	**90.36**	**22.29**	**83.03**	8.72	**25.62**	**82.25**	**24.35**	80.06	**30.71**	**84.41**	**26.89**	82.24	37.06

T-SNE Visualization