

# One-Class Face Anti-spoofing via Spoof Cue Map-Guided Feature Learning

Pei-Kai Huang<sup>1</sup>, Cheng-Hsuan Chiang<sup>1</sup>, Tzu-Hsien Chen<sup>1</sup>, Jun-Xiong Chong<sup>1</sup>, Tyng-Luh Liu<sup>2</sup>, and Chiou-Ting Hsu<sup>1</sup>

<sup>1</sup>National Tsing Hua University, Taiwan <sup>2</sup>Academia Sinica, Taiwan



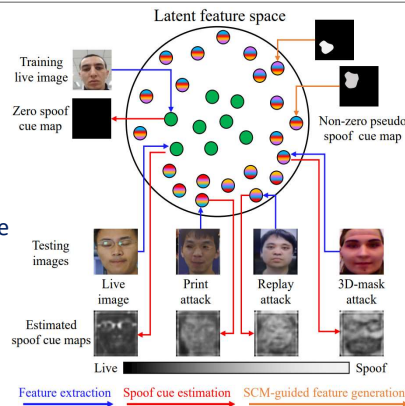
## One-Class Face Anti-spoofing (FAS)

### Challenges in one-class FAS

- Absence of spoof images
- Live and spoof images are visually similar
- Ever-evolving spoof attacks

### Goals

- Learn FAS discriminative features
  - Spoof Cue Map (SCM) guided generative feature learning
- Generate diverse spoof features
  - Probe unseen latent spoof features using memory bank



## One-Class Spoof Cue Map estimation Network (OC-SCMNet)

### Spoof features generation

- Conditional generator  $G$

$$\mathbf{z}^G \leftarrow G(\mathbf{n}|\hat{\mathbf{m}}; \theta_G)$$

- Generation loss

$$\mathcal{L}_G(\theta_G) = \sum_{\hat{\mathbf{m}} \in \mathcal{M}} \|E(G(\mathbf{n}|\hat{\mathbf{m}}; \theta_G)) - \hat{\mathbf{m}}\|_2^2$$

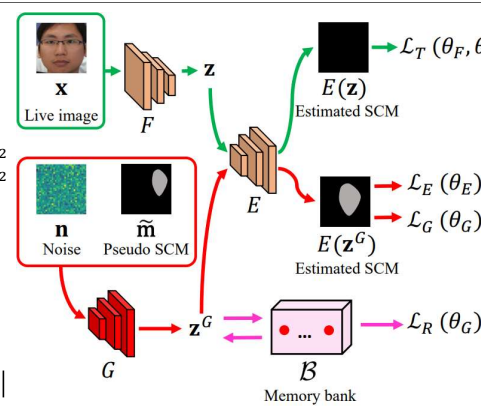
### Probing of spoof attacks

- Memory bank feature selection

$$\frac{1}{N_B} \sum_{j=1}^{N_B} |\cos(\mathbf{z}^G, \mathbf{z}_j^G)| < \delta$$

- Exploration loss

$$\mathcal{L}_R(\theta_G) = \sum_{\hat{\mathbf{m}} \in \mathcal{M}} \sum_{j=1}^{N_B} |\cos(\mathbf{z}^G, \mathbf{z}_j^G)|$$



### SCM training

- Live SCM constraint

$$\mathcal{L}_T(\theta_F, \theta_E) = \sum_{\mathbf{x} \in \mathcal{D}} \|E(\mathbf{z}; \theta_E)\|_2^2$$

- Spoof SCM constraint

$$\mathcal{L}_E(\theta_E) = \sum_{\hat{\mathbf{m}} \in \mathcal{M}} \|E(\mathbf{z}^G; \theta_E) - \hat{\mathbf{m}}\|_2^2$$

### Live/Spoof classification

- Summation of SCM as score

$$s(\mathbf{x}) = \frac{\sum_{d=1}^D \sum_{h=1}^H \sum_{w=1}^W |T(\mathbf{x})|}{D \cdot H \cdot W}$$

## Experiments

### Datasets

- OULU-NPU (O), SiW (S), HKBU-MARs (H), CASIA-SURF (U)

### Evaluation Metrics

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

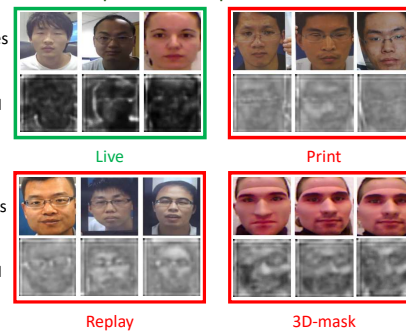
### Cross-Domain Testing w/ Unseen Attack

Training Data	Method	[O,S] → D		[O,S] → H		[O,S] → U	
		HTER	AUC	HTER	AUC	HTER	AUC
Live + Spoof	Auxiliary [16] (CVPR 18)	0.29	99.04	14.64	88.32	37.28	53.14
	NAS [28] (TPAMI 20)	<b>0.22</b>	99.31	15.13	88.91	37.68	<b>72.83</b>
	LDCN [9] (BMVC 22)	1.49	<b>99.91</b>	<b>8.75</b>	<b>95.60</b>	<b>33.54</b>	60.44
Live	IQM-GMM [17] (ICB 18)	43.83	43.43	19.14	80.53	38.18	66.18
	Baweja et al. [3] (IJCB 20)	37.86	45.8	35.65	68.90	41.74	49.85
	Lim et al. [14] (Access 20)	27.69	75.47	35.19	62.98	37.34	64.24
	AAE [10] (CCBR 21)	22.48	78.62	31.22	73.77	45.24	53.48
	OC-SCMNet (Ours)	<b>1.47</b>	<b>99.87</b>	<b>7.08</b>	<b>86.84</b>	<b>10.61</b>	<b>90.75</b>
Live + 1-Shot Spoof	OC-SCMNet (Ours)	1.19	99.77	0.0	100.0	8.43	92.66

### Cross-Domain Testing

Training Data	Method	C → I		I → C
		HTER	HTER	
Live + Spoof	Auxiliary [22] (CVPR 18)	27.6	28.4	
	STASN [39] (CVPR 19)	31.5	30.9	
	CDCN [42] (CVPR 20)	15.5	32.6	
	CIFL [5] (TIFS 21)	17.6	-	
	AENet [9] (ACPR 21)	24.7	30.9	
	PatchNet [32] (CVPR 22)	<b>9.9</b>	<b>26.2</b>	
Live	IQM-GMM [24] (ICB 18)	37.77	48.44	
	Baweja et al. [2] (IJCB 20)	46.29	29.44	
	Lim et al. [20] (Access 20)	37.36	39.78	
	AAE [15] (CCBR 21)	20.0	26.9	
	OC-SCMNet (Ours)	<b>7.29</b>	<b>17.44</b>	
Live + 1-Shot Spoof	OC-SCMNet (Ours)	2.14	1.11	

### Spoof Cue Map Visualization



### T-SNE Visualization

