Regularized Fine-grained Meta Face Anti-spoofing

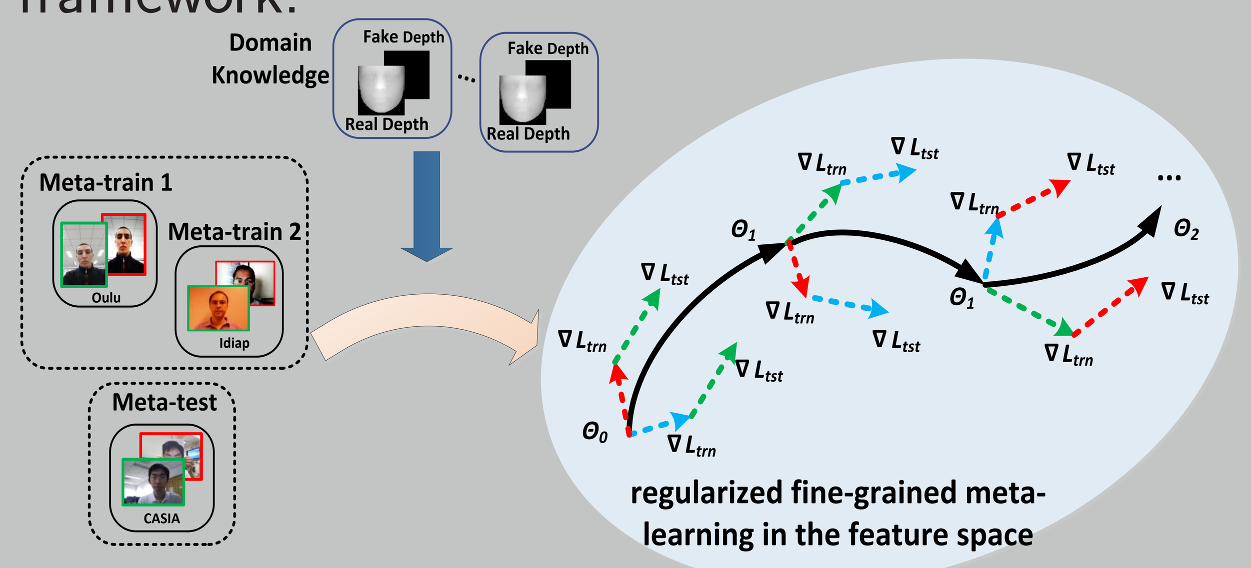
Rui Shao, Xiangyuan Lan, Pong C. Yuen

Department of Computer Science, Hong Kong Baptist University

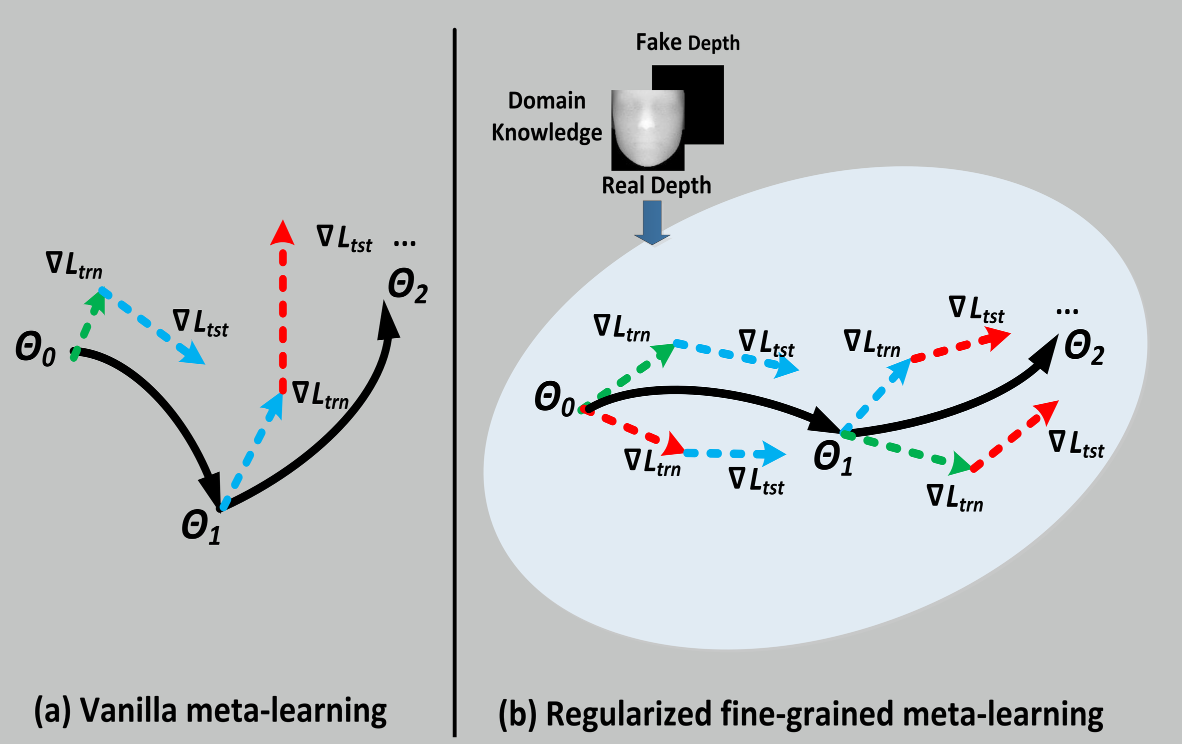
DEPARTMENT OF COMPUTER SCIENCE 計算機科學系

Objective

1. Improve the generalization ability of face anti-spoofing method to unseen attacks.
2. Cast face anti-spoofing as a domain generalization (DG) problem and address it in a meta-learning framework.

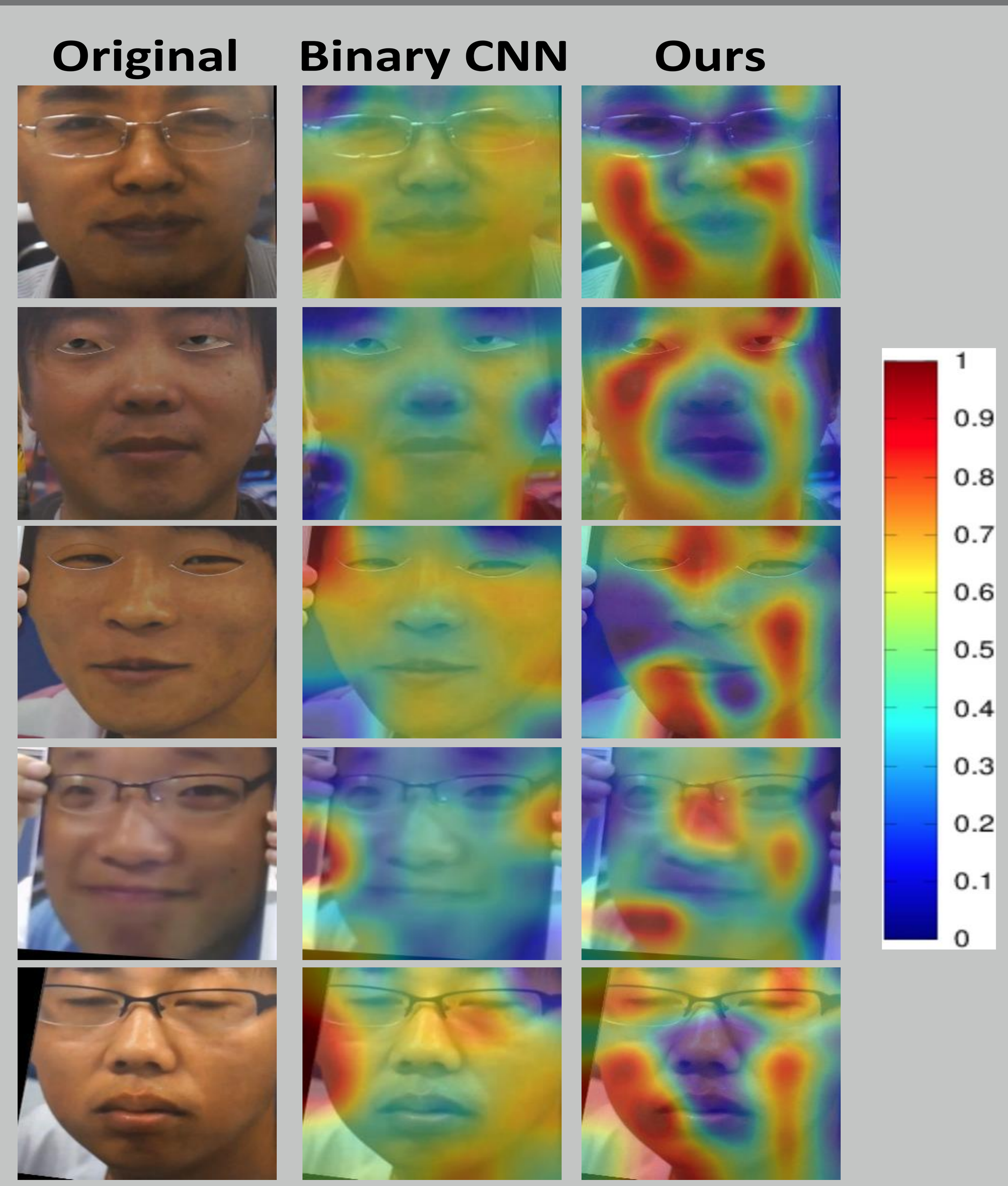


Idea



- Two issues: 1) Learning directions in the meta-train and meta-test steps are arbitrary and biased; 2) Only a single domain shift scenario is simulated
- Solution: 1) Incorporate domain knowledge as regularization to conduct regularized meta-learning; 2) Fine-grained learning strategy divides source domains into multiple meta-train and meta-test domains

Attention Map Visualization



- Bianry CNN pays most attention to extracting the differentiation cues in the background or on paper edges/holding fingers
- Our method focuses on the region of internal face for searching differentiation cues

Method

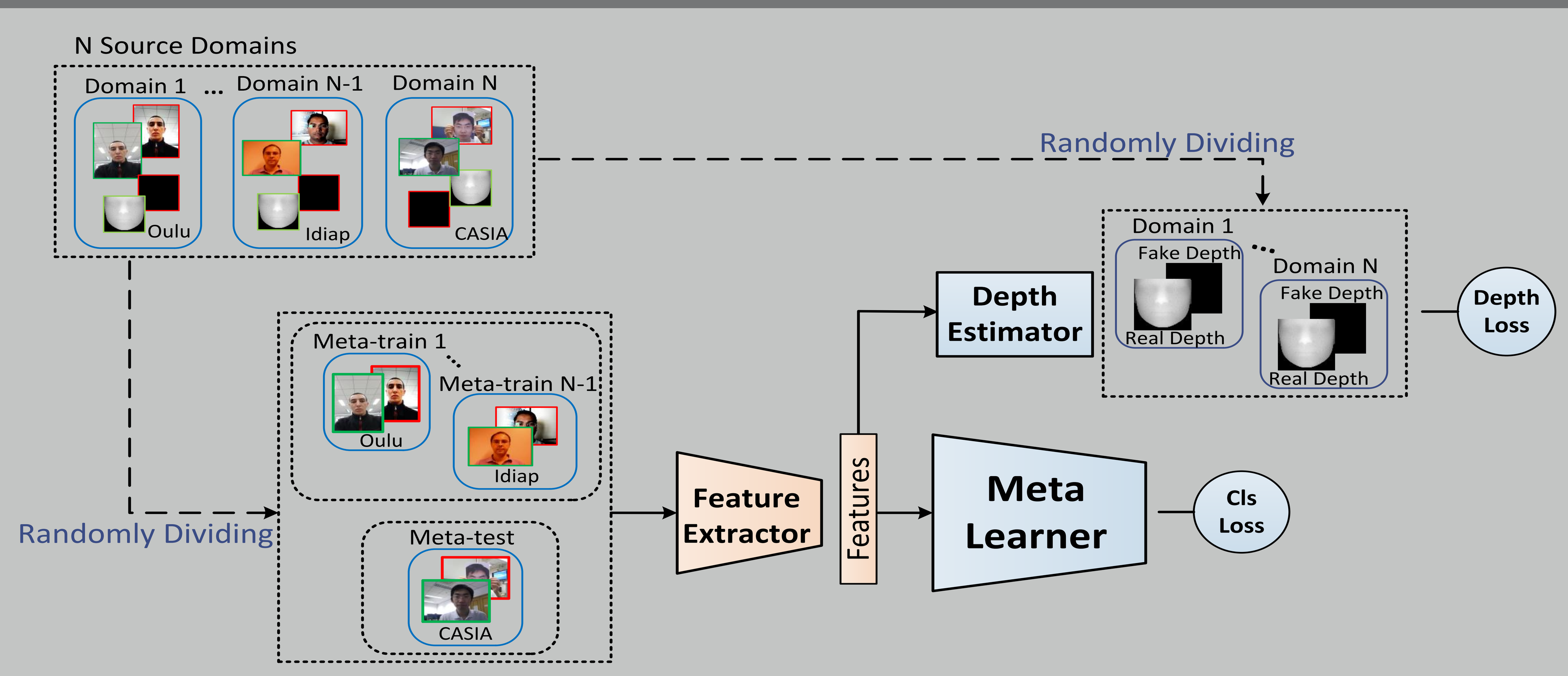


Figure 1:Framework of the proposed method.

- Meta-Train:

$$\begin{aligned} &\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_F,\theta_M) \\ &= \sum_{(x,y)\sim\bar{\mathcal{T}}_i} y\log M(F(x)) + (1-y)\log(1-M(F(x))) \\ &\mathcal{L}_{Dep(\bar{\mathcal{T}}_i)}(\theta_F,\theta_D) = \sum_{(x,I)\sim\bar{\mathcal{T}}_i} \|D(F(x)) - I\|^2 \\ &\theta_{M_i}' = \theta_M - \alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_F,\theta_M) \end{aligned} \tag{1}$$

- Meta-Test:

$$\begin{aligned} &\sum_{i=1}^{N-1}\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_F,\theta_{M_i}') = \\ &\sum_{i=1}^{N-1}\sum_{(x,y)\sim\tilde{\mathcal{T}}} y\log M_i'(F(x)) + (1-y)\log(1-M_i'(F(x))) \\ &\mathcal{L}_{Dep(\tilde{\mathcal{T}})}(\theta_F,\theta_D) = \sum_{(x,I)\sim\tilde{\mathcal{T}}} \|D(F(x)) - I\|^2 \end{aligned} \tag{2}$$

- Meta-Optimization:

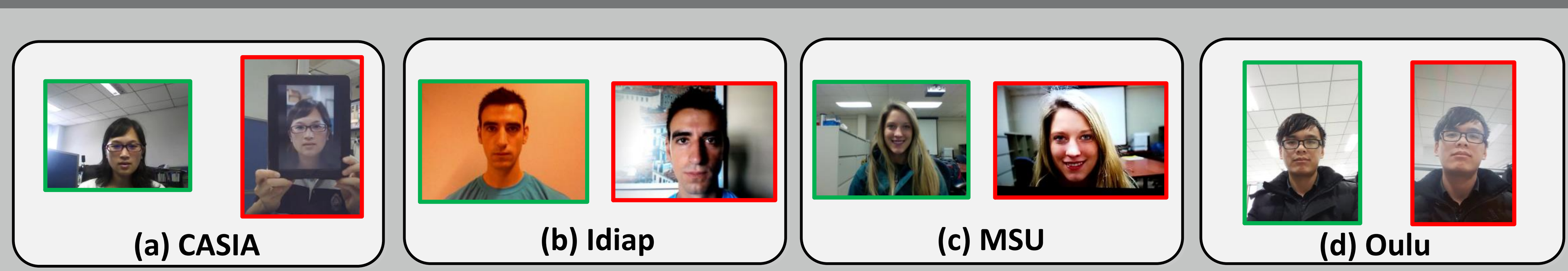
$$\begin{aligned} &\theta_M \leftarrow \theta_M - \beta\nabla_{\theta_M}\Big(\sum_{i=1}^{N-1}\big(\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_F,\theta_M) + \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_F,\theta_{M_i}')\big)\Big) \\ &\theta_F \leftarrow \theta_F - \beta\nabla_{\theta_F}\Big(\mathcal{L}_{Dep(\tilde{\mathcal{T}})}(\theta_F,\theta_D) + \sum_{i=1}^{N-1}\big(\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_F,\theta_M) + \mathcal{L}_{Dep(\bar{\mathcal{T}}_i)}(\theta_F,\theta_D) + \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_F,\theta_{M_i}')\big)\Big) \\ &\theta_D \leftarrow \theta_D - \beta\nabla_{\theta_D}\Big(\mathcal{L}_{Dep(\tilde{\mathcal{T}})}(\theta_F,\theta_D) + \sum_{i=1}^{N-1}\big(\mathcal{L}_{Dep(\bar{\mathcal{T}}_i)}(\theta_F,\theta_D)\big)\Big) \end{aligned} \tag{3}$$

- Analysis:

$$\begin{aligned} &\min_{\theta_M}\sum_{i=1}^{N-1}\big(\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_M) + \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_{M_i}')\big) \\ &\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_{M_i}') = \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M - \alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_M)) = \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M) + \nabla_{\theta_M}\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M)^T(-\alpha\nabla_{\theta_M}\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_M)) \\ &\min_{\theta_M}\sum_{i=1}^{N-1}\big(\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_M) + \mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M) - \alpha(\nabla_{\theta_M}\mathcal{L}_{Cls(\bar{\mathcal{T}}_i)}(\theta_M)^T\cdot\nabla_{\theta_M}\mathcal{L}_{Cls(\tilde{\mathcal{T}})}(\theta_M))\big) \end{aligned} \tag{4}$$

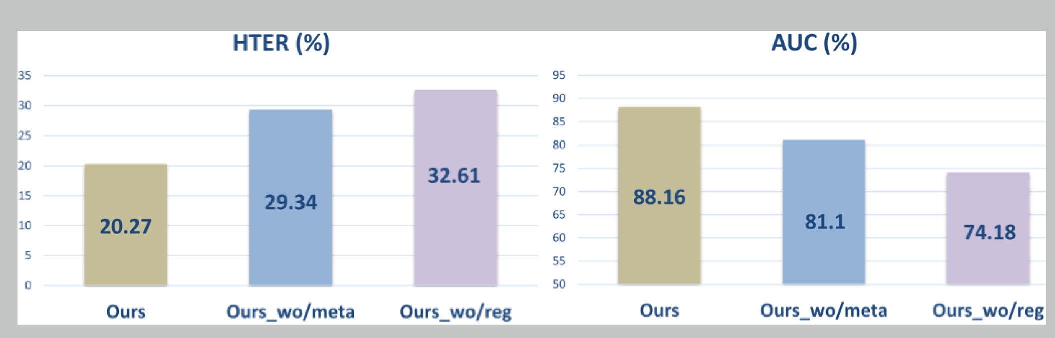
- Above objective is conducted in feature space regularized by the domain knowledge
- Above objective is conducted between $N-1$ pairs of meta-train and meta-test domains

Results



Comparison to face anti-spoofing methods for domain generalization on face anti-spoofing

Methods	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HETR	AUC	HETR	AUC	HETR	AUC	HETR	AUC
MS_LBP	29.76	78.50	54.28	44.98	50.30	51.64	50.29	49.31
B_CNN	29.25	82.87	34.88	71.94	34.47	65.88	29.61	77.54
IDA	66.67	27.86	55.17	39.05	28.35	78.25	54.20	44.59
CT	28.09	78.47	30.58	76.89	40.40	62.78	63.59	32.71
LBPTOP	36.90	70.80	42.60	61.05	49.45	49.54	53.15	44.09
Auxiliary	22.72	85.88	33.52	73.15	29.14	71.69	30.17	77.61
MMD_AAE	27.08	83.19	44.59	58.29	31.58	75.18	40.98	63.08
MADDG	17.69	88.06	24.5	84.51	22.19	84.99	27.98	80.02
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**



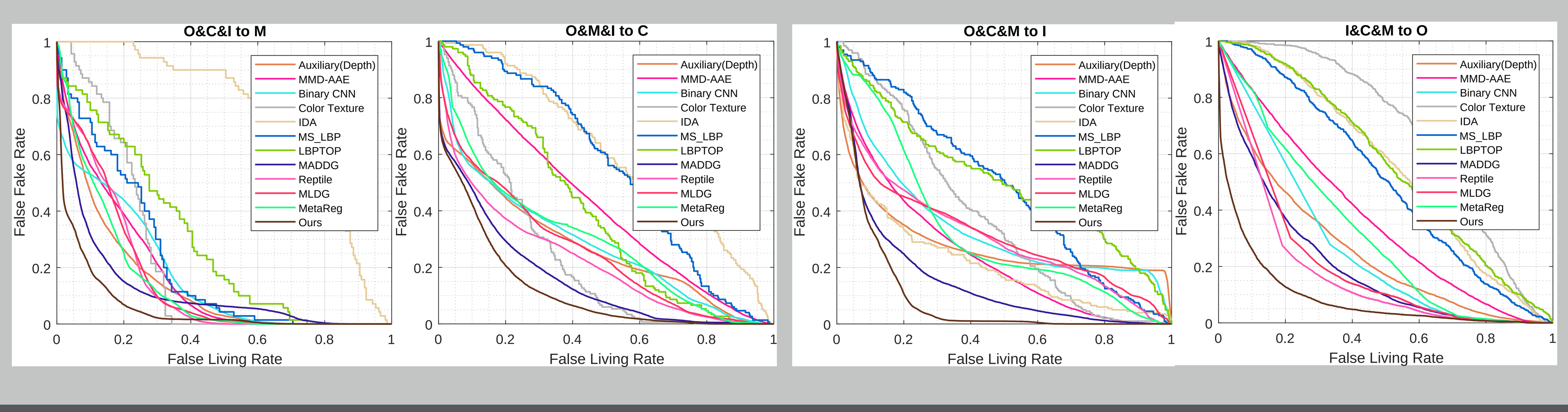
Evaluation of different components of proposed method in O&M&I to C set for face anti-spoofing

Comparison to meta-learning for domain generalization on face anti-spoofing

Methods	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HETR	AUC	HETR	AUC	HETR	AUC	HETR	AUC
Reptile	23.64	85.06	30.38	78.10	36.13	69.01	22.88	82.22
MLDG	23.91	84.81	32.75	74.51	36.55	68.54	25.75	79.52
MetaReg	21.17	86.11	35.66	70.83	32.28	67.48	37.72	68.71
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**

Effectiveness of fine-grained learning strategy and second-order derivative information

Methods	O&C&I to M		O&M&I to C		O&C&M to I		I&C&M to O	
	HETR	AUC	HETR	AUC	HETR	AUC	HETR	AUC
Ours (Aggregation)	14.54	92.87	24.28	85.29	20.07	88.13	17.94	90.69
Ours (First-order)	17.93	87.36	27.47	82.17	26.24	79.32	19.24	87.82
Ours	**13.89**	**93.98**	**20.27**	**88.16**	**17.3**	**90.48**	**16.45**	**91.16**



ruishao@comp.hkbu.edu.hk