A2XP: Towards Private Domain Generalization

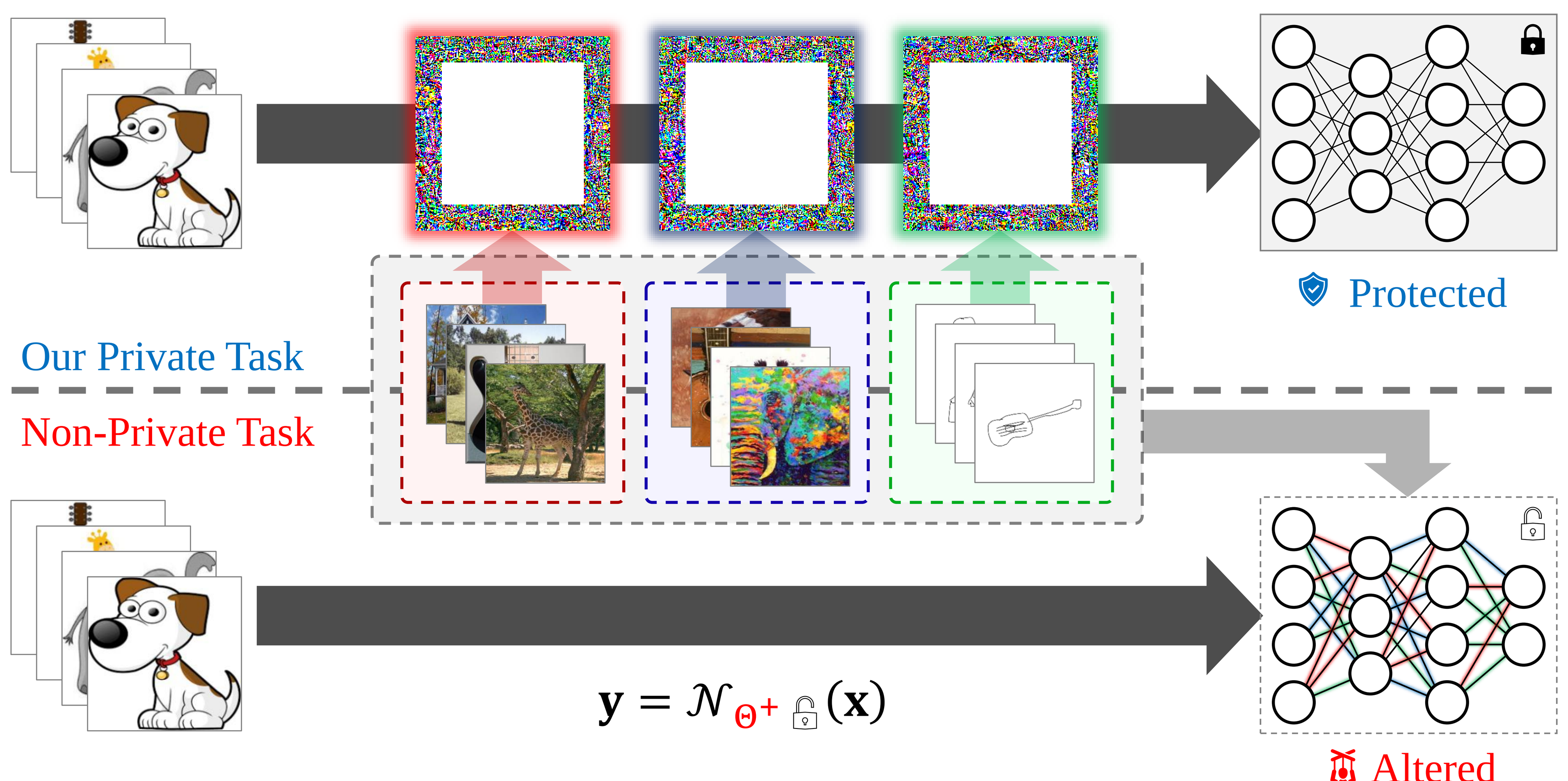
Geunhyeok Yu Hyoseok Hwang

KYUNG HEE UNIVERSITY

CVPR JUNE 17-21, 2024 SEATTLE, WA

I. Private Domain Generalization

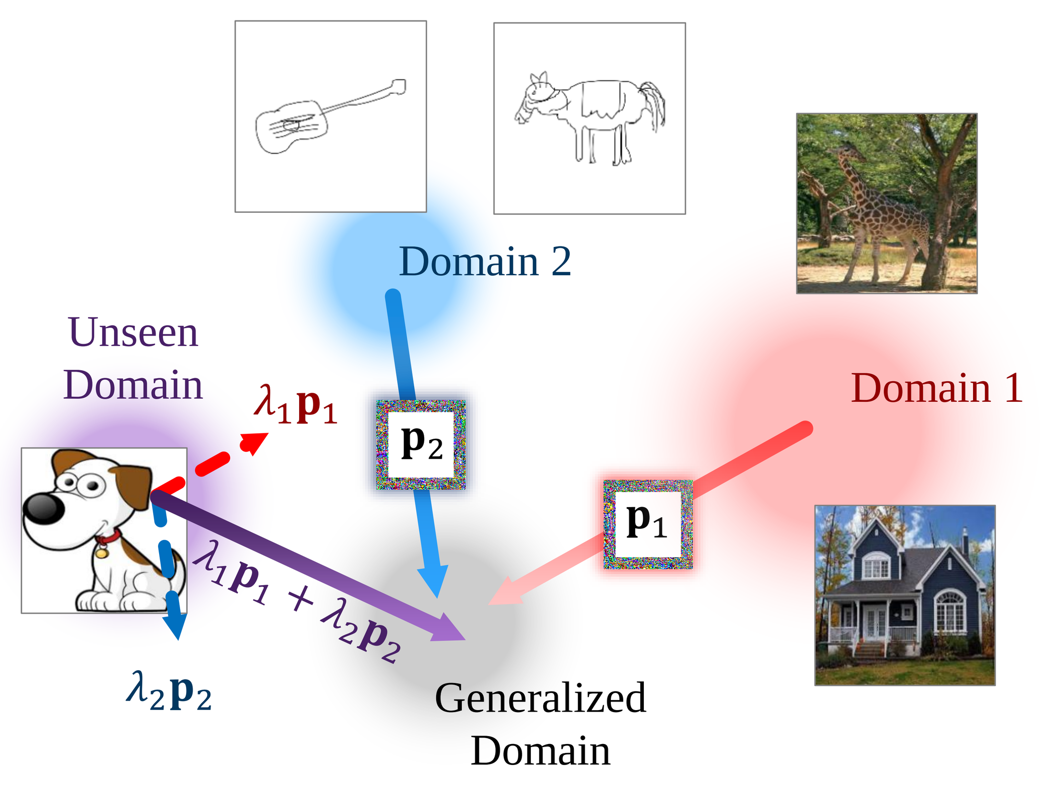
$$\mathbf{y} = \mathcal{N}_{\Theta}(\mathbf{x}^{+})$$



$$\mathbf{y} = \mathcal{N}_{\Theta^{+}}(\mathbf{x})$$

We **generalize** an objective network.
Previous methods modify while **ours does not modify**
neither **the architecture** nor **the parameters** of the network.

II. Problem Formulation



$$\mathbf{p}_{N+1} = \sum_{i=1}^{N} \lambda_i \mathbf{p}_i\,, \qquad \lambda_i = \Lambda(\mathbf{p}_i | \mathbf{x} \in X_i)$$

$$J(\lambda_i) = \mathrm{KL}(\mathcal{N}(\mathbf{x}_{N+1} + \mathbf{p}_{N+1}) \| \mathcal{D}_{N+1})$$

$$L(\mathcal{D}_{N+1} | \mathcal{N}(\mathbf{x}_{N+1} + \mathbf{p}_{N+1})) \in e^{-J(\lambda_i)}$$

$$J(\lambda_i) \propto -\log L(\mathcal{D}_{N+1} | \mathcal{N}(\mathbf{x}_{N+1} + \mathbf{p}_{N+1}))$$

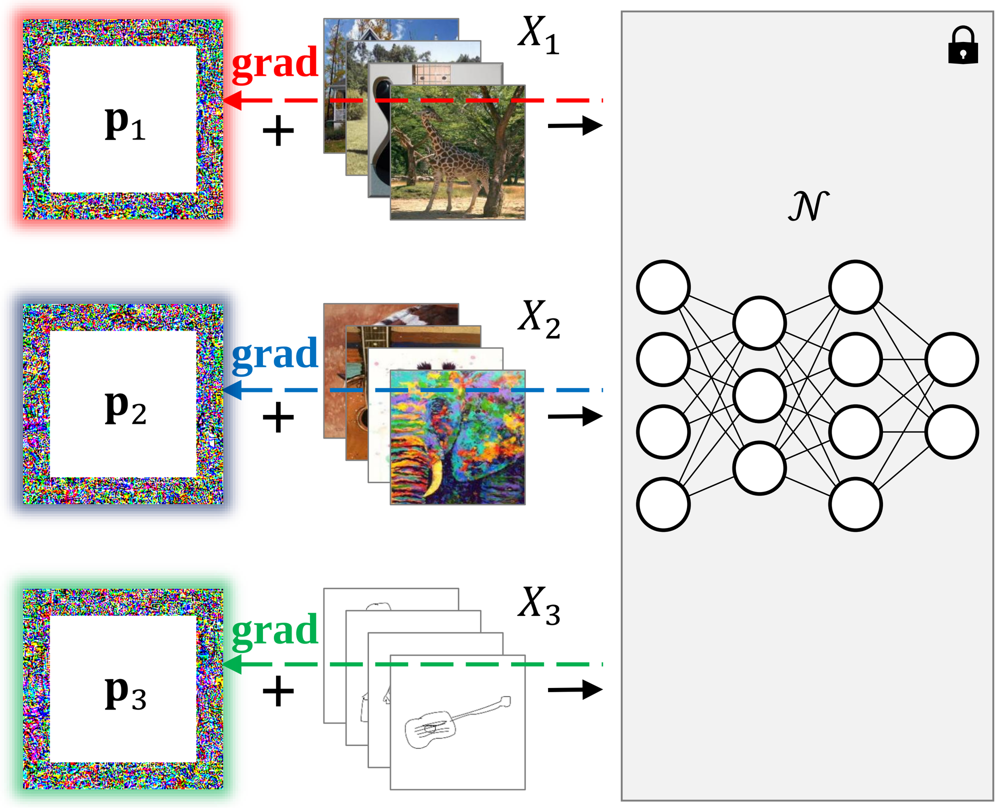
∴ ***minimizing J** by optimizing Λ*
*is equivalent to **maximizing***
***likelihood L**.*

III. The Proposed Attend to eXpert Prompts (A2XP)

Two-Phase Approach

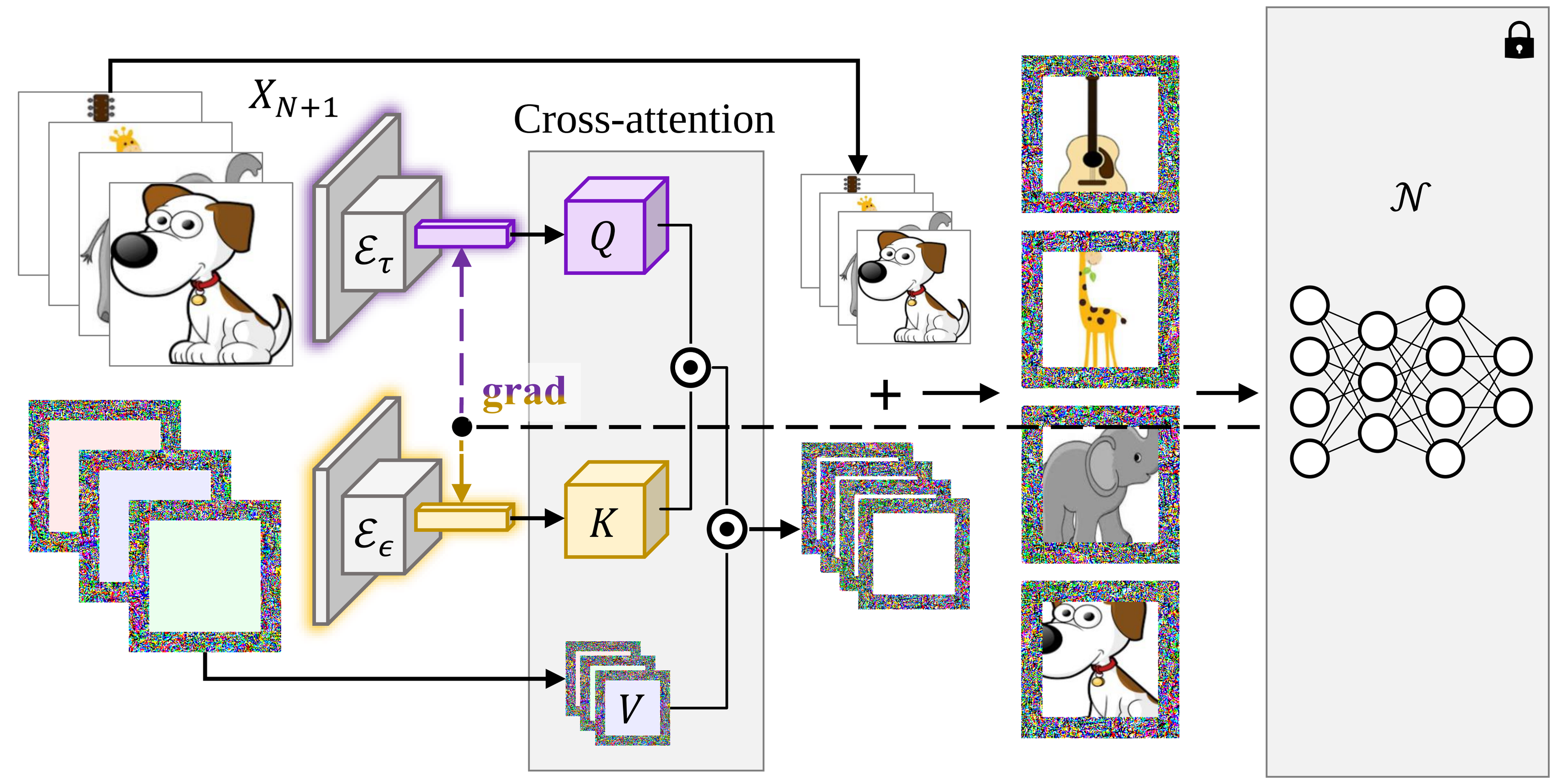
i. Expert Adaptation

$$\mathbf{p}_i = \underset{\mathbf{p}}{\arg\min}\ \mathrm{KL}(\mathcal{N}(\mathbf{x} + \overset{\text{grad}}{\mathbf{p}}), \mathbf{y})\,, (\mathbf{x}, \mathbf{y}) \in X_i$$

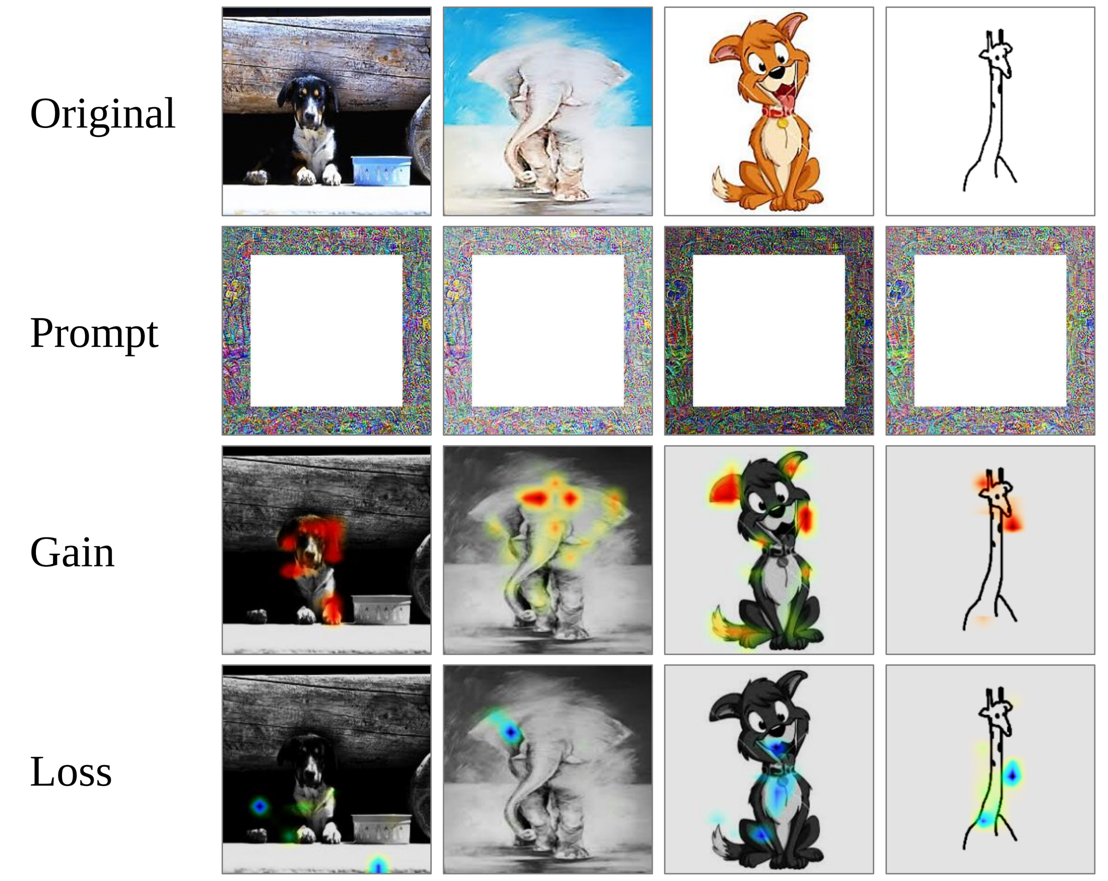


ii. Attention-based Generalization

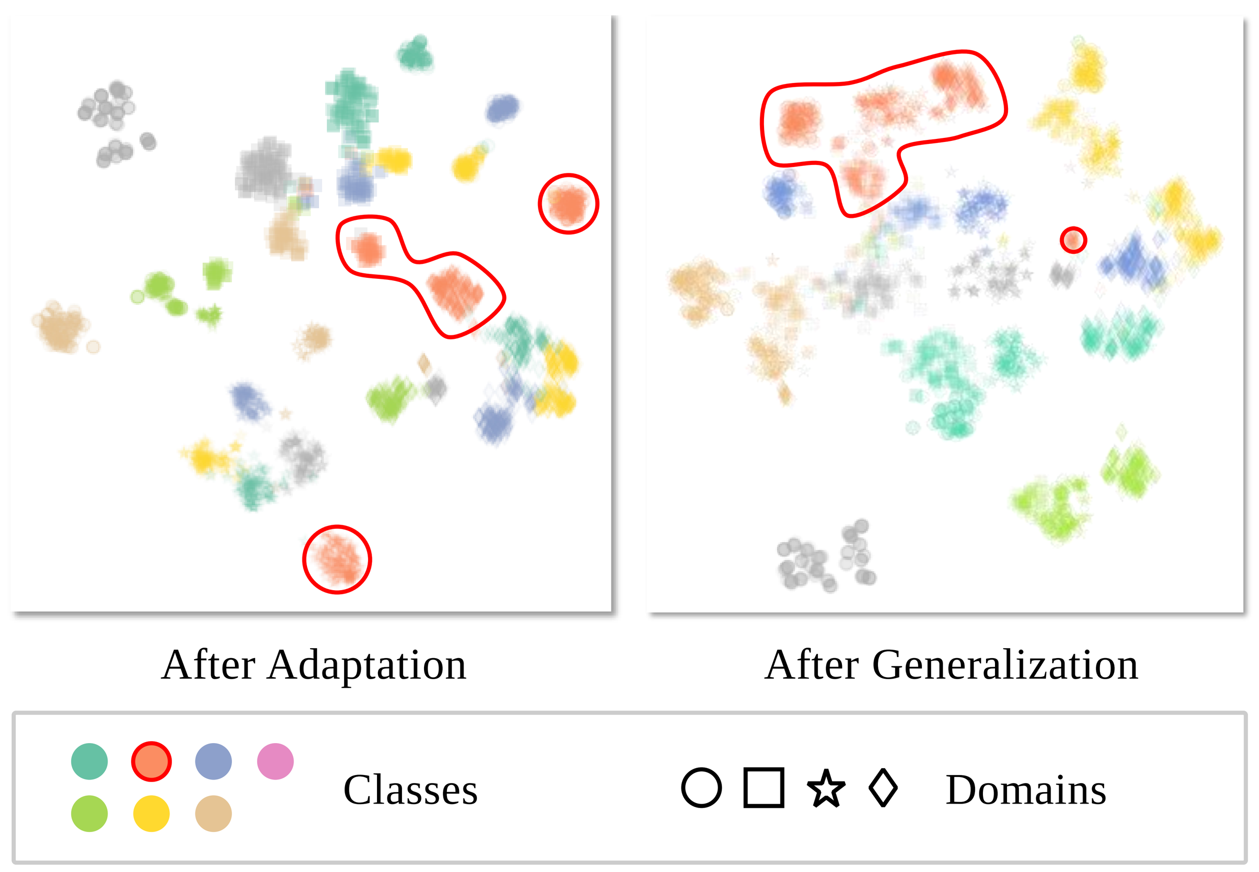
$$(\Theta_{\mathrm{T}}, \Theta_{\mathrm{E}}) = \underset{(\tau,\epsilon)}{\arg\min}\ \Sigma_{i=1}^{N} J\left(\overset{\text{grad}}{\mathcal{E}_\tau}(\mathbf{x})\overset{\text{grad}}{\mathcal{E}_\epsilon}(\mathbf{p}_i)^{\mathrm{T}}\right), \mathbf{x} \in X_{N+1}$$



IV. Qualitative Results



Activation: Visualization of gain and loss of Grad-CAM.



Manifold: t-SNE result of the manifold space after each phase.

V. Quantitative Results

PACS [2]	Picture	Art	Cartoon	Sketch	Avg.
ERM [4]	97.08	87.19	86.25	82.38	88.22
DANN [5]	97.68	89.93	86.41	81.11	88.78
MIRO [6]	96.48	90.79	90.46	83.59	90.33
A2XP (ours)	**99.07**	**95.27**	**98.07**	**87.85**	**95.07**

VLCS [3]	VOC 2007	LabelMe	Caltech101	SUN09	Avg.
ERM [4]	75.60	64.47	97.08	77.49	78.66
DANN [5]	77.86	66.97	98.59	73.53	79.24
MIRO [6]	78.05	66.68	97.53	71.97	78.56
A2XP (ours)	**84.07**	**68.72**	**99.62**	**80.19**	**83.15**

Comparison: Other methods in the target domain. DART [4] was applied to the baselines (not ours) for their best performance.

Adaptation	A → A	C → C	P → P	R → R	Avg.
Zero	21.18	38.95	61.93	43.10	41.29
Uniform	21.63	32.94	44.92	46.71	36.55
Normal	28.92	32.51	40.17	23.36	31.24
Meta [7]	**47.05**	**54.39**	**69.66**	**52.03**	**56.35**

Generalization	CPR → A	APR → C	ACR → P	ACP → R	Avg.
Zero	67.57	57.98	66.55	71.29	65.85
Uniform	67.41	58.33	67.27	71.77	66.20
Normal	67.74	58.35	67.83	71.22	66.29
Meta [7]	**77.42**	**65.73**	**81.93**	**83.15**	**77.06**

Analysis: Impact of meta [7] initialization in Office-Home [8].

※ Contributions ※

- ✓ A novel and simple DG method that **preserves privacy, inspired by VP [1]**.
- ✓ Mathematically **analyze** the **DG task** as an optimization of a **linear combination**.
- ✓ **Demonstrate the effectiveness** and characteristics of A2XP through **extensive experiments**.
- ✓ A2XP achieves **SOTA** with **significantly lower computational resource requirements**.

[1] Bahng et al. "Exploring visual prompts for adapting large-scale models." arXiv:2203.17274. [2] Da et al. "Deeper, broader and artier domain generalization." ICCV 2017. [3] Antonio et al. "Unbiased look at dataset bias." CVPR 2011. [4] Vladimir N. "An overview of statistical learning theory." IEEE ToNNs (1999). [5] Ganin et al. "Domain-adversarial training of neural networks." JMLR 17.59 (2016). [6] Cha et al. "Domain generalization by mutual-information regularization with pre-trained models." ECCV 2022. [7] Huang et al. "Diversity-aware meta visual prompting." CVPR 2023. [8] Venkateswara et al. "Deep hashing network for unsupervised domain adaptation." CVPR 2017.