Learning to Augment via Implicit Differentiation for Domain Generalization

Tingwei Wang, Da Li, Kaiyang Zhou, Tao Xiang and Yi-Zhe Song
1. University of Surrey 2. Samsung AI Center 3. Nanyang Technology University

Abstract

In this paper, we propose a novel augmentation-based DG approach, dubbed AugLearn. Different from existing data augmentation methods, our AugLearn views a data augmentation module as hyper-parameters of a classification model and optimizes the module together with the model via meta-learning.

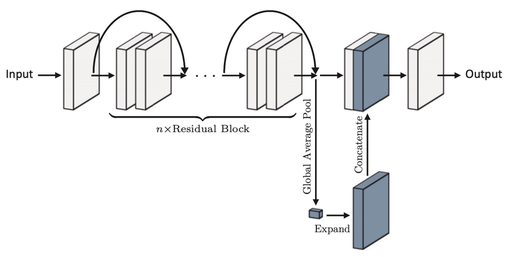
Motivation


original

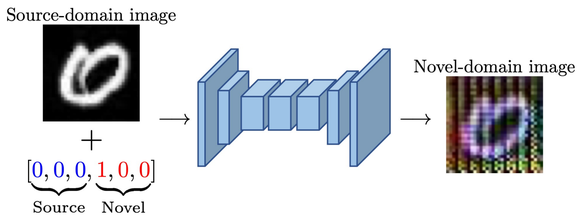

flip


crop


jitter



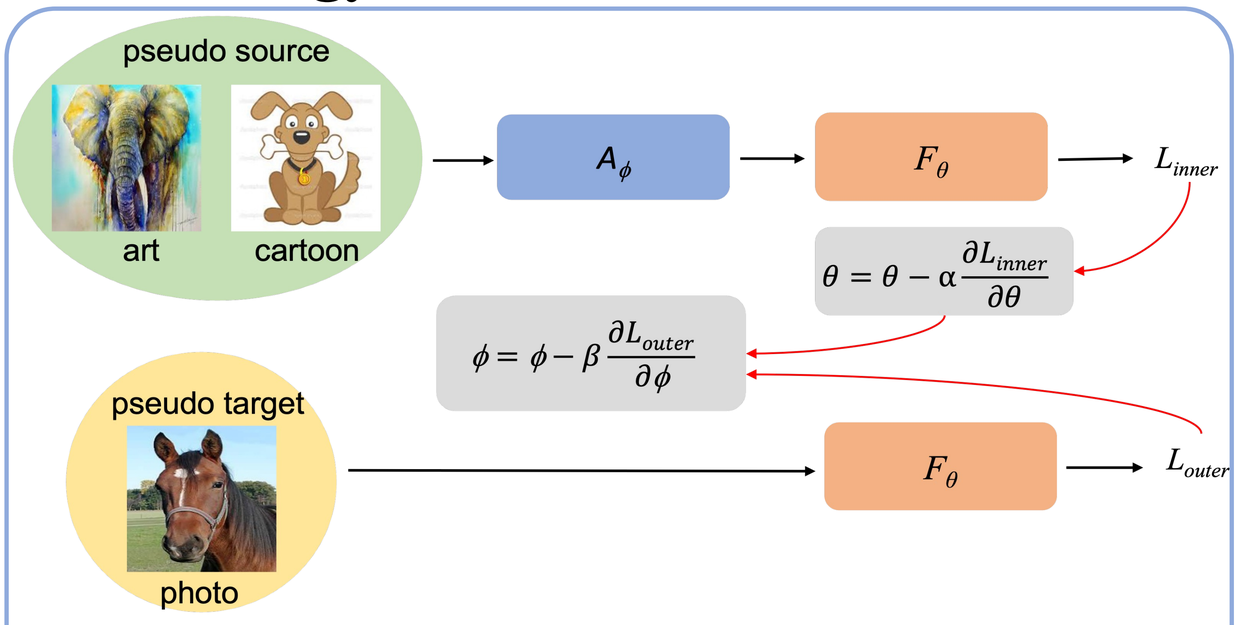
DDAIG



L2A-OT

Existing augmentation DG methods are non-optimizable or normally require some complicated design of learning objectives. There is no guarantee that the augmented images, when used for training the main classification model, can ensure the model generalizes well to an unseen domain.

Methodology



Inner loop optimization

$$\theta^* = \arg\min_{\theta} \frac{1}{|\mathcal{D}^{\hat{p}src}|} \sum_{x,y \sim \mathcal{D}^{\hat{p}src}} \ell_{ce}(F_\theta(\mathcal{A}_\phi(x)), y), \quad (1)$$

outer loop optimization

$$\phi = \arg\min_{\phi} \frac{1}{|\mathcal{D}^{\hat{p}trg}|} \sum_{x,y \sim \mathcal{D}^{\hat{p}trg}} \ell_{ce}(F_{\theta^*}(\phi(x)), y). \quad (2)$$

$\mathcal{A}$ is the augmentation module, and F is the classification model.

Augmentation in frequency space

$$\theta^* = \arg\min_{\theta} \frac{1}{|\mathcal{D}^{\hat{s}rc}|} \sum_{x,y \sim \mathcal{D}^{\hat{s}rc}} \ell_{ce}(F_\theta(\mathcal{T}_{inv}(\mathcal{A}_\phi(\mathcal{T}(x)))), y) \quad (3)$$

$\mathcal{T}$ is DCT, and $\mathcal{T}_{inv}$ is inverse DCT.

Experiments

A. Main results

Method	PACS					Office-Home				
	Art	Cartoon	Photo	Sketch	Average	Artistic	Clipart	Product	Real World	Average
ERM	78.5	75.2	96.2	67.9	79.5	58.4	49.2	74.1	76.3	64.5
CCSA	80.5	76.9	93.6	66.8	79.4	59.9	49.9	74.1	75.7	64.9
MMD-AAE	75.2	72.7	96.0	64.2	77.0	56.5	47.3	72.1	74.8	62.7
CrossGrad	79.8	76.8	96.0	70.2	80.7	58.4	49.4	73.9	75.8	64.4
JiGen	79.4	75.3	96.0	71.6	80.5	53.0	47.5	71.5	72.8	61.2
DDAIG	**84.2**	77.0	95.3	83.1	74.7	59.2	52.3	74.6	76.0	65.5
L2A-OT	83.3	78.2	**96.2**	82.8	73.6	**60.6**	50.1	**74.8**	**77.0**	65.6
MixStyle	84.1	78.8	96.1	75.9	83.7	58.7	53.4	74.2	75.9	65.5
ERM+AugLearn	82.9	78.8	94.5	80.1	84.1 (+4.6)	58.9	53.3	74.3	76.0	65.6 (+1.1)
ERM+AugLearn-F	81.9	**79.2**	95.3	80.7	84.3 (+4.8)	58.5	**54.2**	73.2	75.1	65.3 (+0.8)
MixStyle+AugLearn	84.1	79.0	95.2	**81.5**	**85.0** (+1.3)	59.3	53.5	74.6	76.0	**66.0** (+0.5)
MixStyle+AugLearn-F	83.9	**79.2**	95.4	81.0	84.9 (+1.2)	59.8	52.7	**74.8**	75.6	65.7 (+0.2)

Table 1: Leave-one-domain-out generalization results on PACS and Office-Home.

AugLearn (-F) outperforms the ERM method by a clear margin on both PACS and Office-Home datasets. In addition, AugLearn (-F) is complementary to other DG method (e.g. MixStyle).

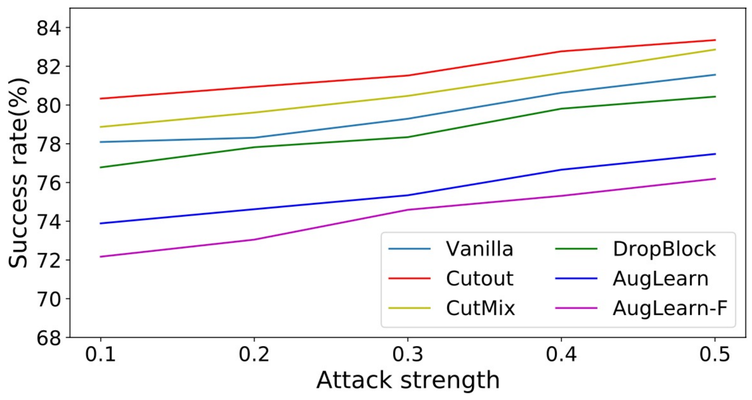
B. Ablation study

Method	Art	Cartoon	Photo	Sketch	Avg.
ERM	78.5	75.2	96.2	67.9	79.5
AugLearn	82.9	78.8	94.5	80.1	84.1
- w/o ML	81.6	76.3	93.8	79.0	82.7
AugLearn-F	81.9	79.2	95.3	80.7	84.3
- w/o ML	81.2	76.5	94.2	79.9	83.0

Table 2: Ablation study results on PACS

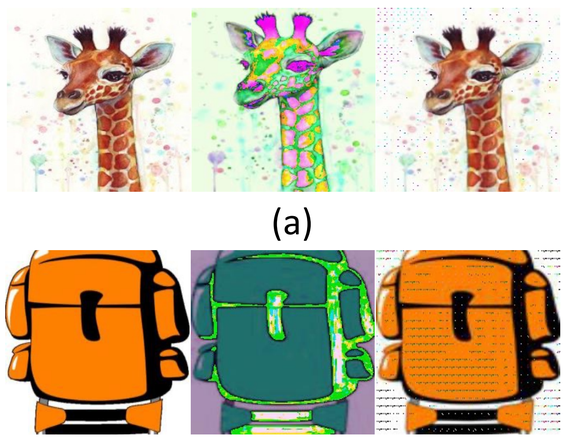
Results show that learning the model with meta-learning is crucial to improve the generalization ability.

C. Adversarial attack



Augmenting the input images in the frequency space during training gives more robustness to the trained classification model against potential adversarial attacks.

D. Visualization


(a)

(b)

Left: original, middle: AugLearn, right: AugLearn-F

AugLearn changes the original images dramatically while AugLearn-F do not change much from the original images. AugLearn-F still can improve the model performance clearly, which shows it is more effective to augment images in frequency space than that in time space.

Conclusion

We have presented a novel data augmentation based DG method, termed AugLearn. AugLearn treats the augmentation module as the model hyperparameters and optimizes it with meta learning. Our AugLearn is light-weight, model-agnostic and applicable to any base DG methods (verified with two different DG methods). More inherently, our AugLearn module is capable of augmenting data in both the time and frequency spaces.

UNIVERSITY OF SURREY
DDAIG: Deep Domain-Adversarial Image Generation for Domain Generalisation
L2A-OT:Learning to Generate Novel Domains for Domain Generalization
BMVC 2022