TeSLA: Test-Time Self-Learning With Automatic Adversarial Augmentation

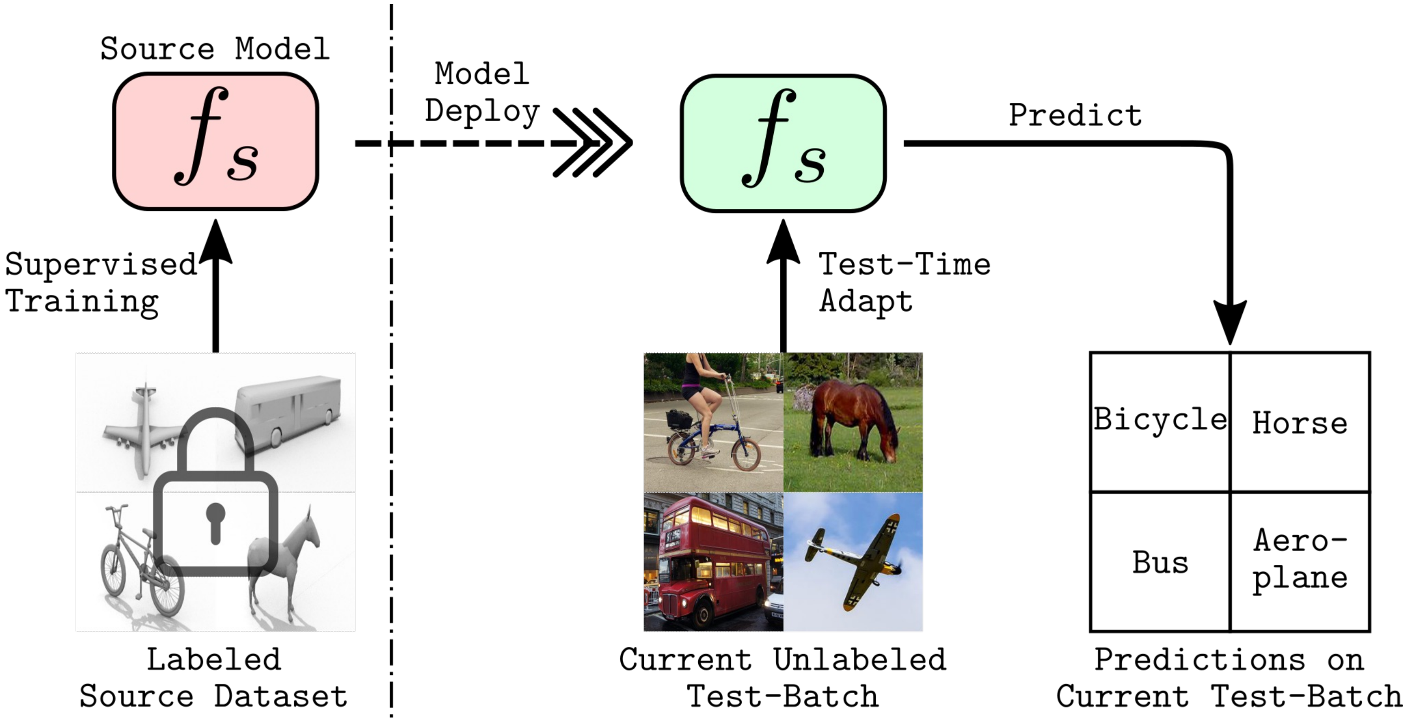
Join us in the poster session: THU-AM-367

[1]Devavrat Tomar, [1]Guillaume Vray, [1,2]Behzad Bozorgtabar, [1,2]Jean-Philippe Thiran

[1]EPFL, Switzerland [2]CHUV, Switzerland

Test-Time Adaptation (TTA)

- Adapt the pre-trained **source model** to the *distributionally shifted* test domain
- Access to the **source** *training dataset* is restricted

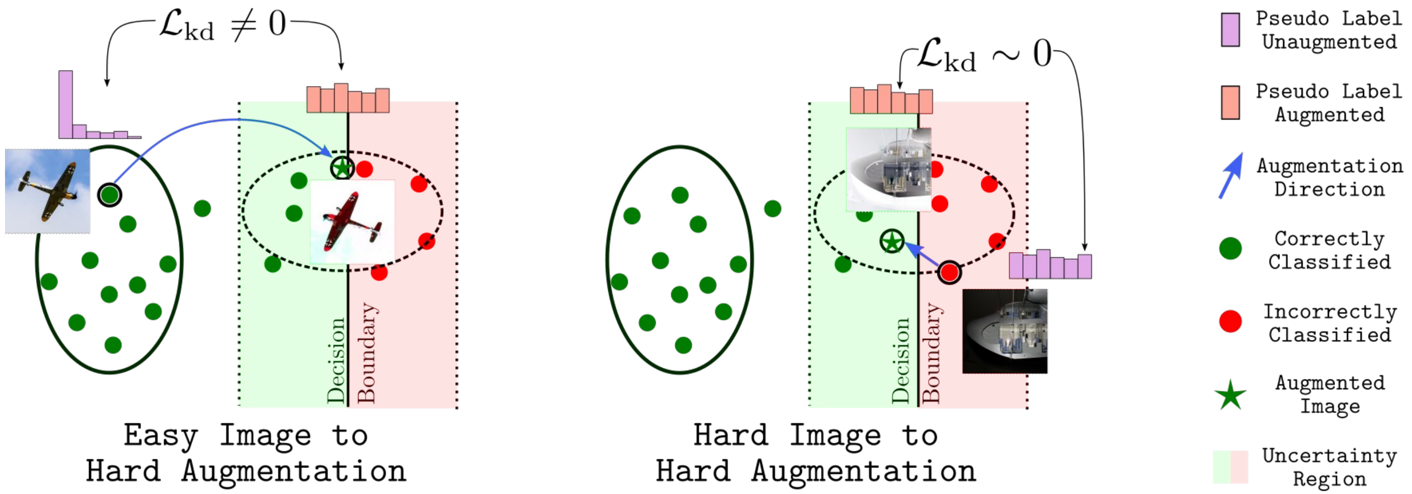


TTA: shortcomings of current methods

- Poor model calibration
- Special model architectures and source training strategies
- Dataset and task-specific methods

TeSLA: motivation

- Simulate hard-to-classify images using adversarially augmented test images



TeSLA: summary of results

Class avg. error rates (%) on classification task

Method	Protocol	Common Image Corruptions: CIFAR10-C O	CIFAR10-C M	CIFAR100-C O	CIFAR100-C M	ImageNet-C O	ImageNet-C M	Syn-to-Real: VisDA-C O	VisDA-C M	Measurement Shift: Kather-16 O	Kather-16 M
Source	N	29.1		60.4		81.8		51.5		32.0	
BN	N	15.6	15.4	43.7	43.3	67.7	67.6	35.4	35.0	18.3	18.2
TENT	N	14.1	12.9	39.0	36.5	57.4	54.2	33.5	29.3	16.2	12.0
SHOT	N	13.9	14.2	39.2	38.7	68.7	68.2	29.4	24.5	14.7	12.0
AdaContrast	N	-						23.1	20.2	-	
TTT++	Y	15.8	9.8	44.4	34.1	59.3	-	35.2	34.1	16.7	7.9
TTAC	Y	13.4	**9.4**	41.7	33.6	58.7	-	32.2	31.1	9.6	5.5
TeSLA	N	12.5	9.7	38.2	32.9	55.0	**51.5**	**17.8**	**13.5**	**9.2**	3.3
TeSLA-s	Y	**12.1**	9.7	**37.3**	**32.6**	**53.1**	-	24.0	17.9	9.9	**3.1**

Class avg. dice score (%) on MRI segmentation task

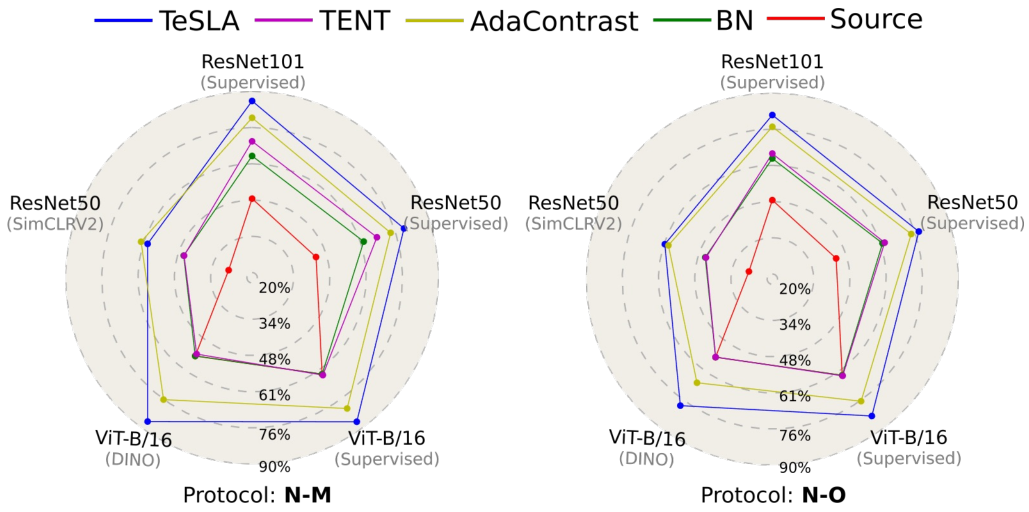
Protocol		Source	BN	TENT	PL	OptTTA	TeSLA
Spinal Cord `Site{1}` → `Sites{2,3,4}`							
N	O	76.0±11.8	81.6±8.3	81.1±9.1	81.7±8.6	84.1±4.8	**85.3**±5.8
N	M		84.3±4.8	84.4±4.7	84.3±4.7	84.3±4.4	**85.4**±4.4
Prostate `Sites{A,B}` → `Sites{D,E,F}`							
N	O	60.5±27.0	72.1±15.2	74.7±17.9	72.4±15.2	83.1±7.7	**83.5**±6.5
N	M		73.1±18.0	81.2±9.3	81.1±9.2	83.4±7.7	**84.3**±5.8

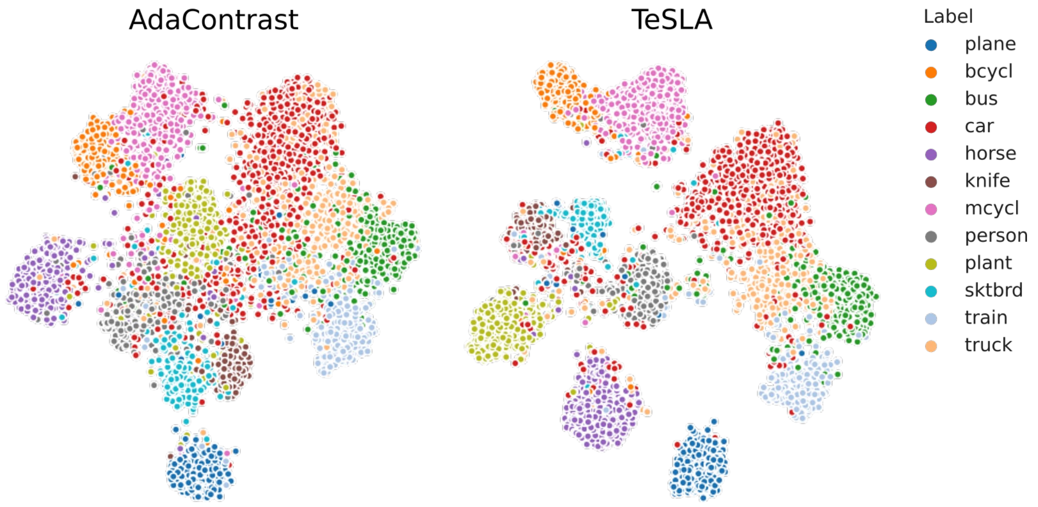
Class avg. mIoU (%) on VisDA-S segmentation task

Protocol		Source	BN	TENT	PL	CoTTA	TeSLA
N	O	35.3	36.7	38.3	38.8	37.0	**44.5**
N	M		38.4	39.2	38.6	39.9	**46.0**

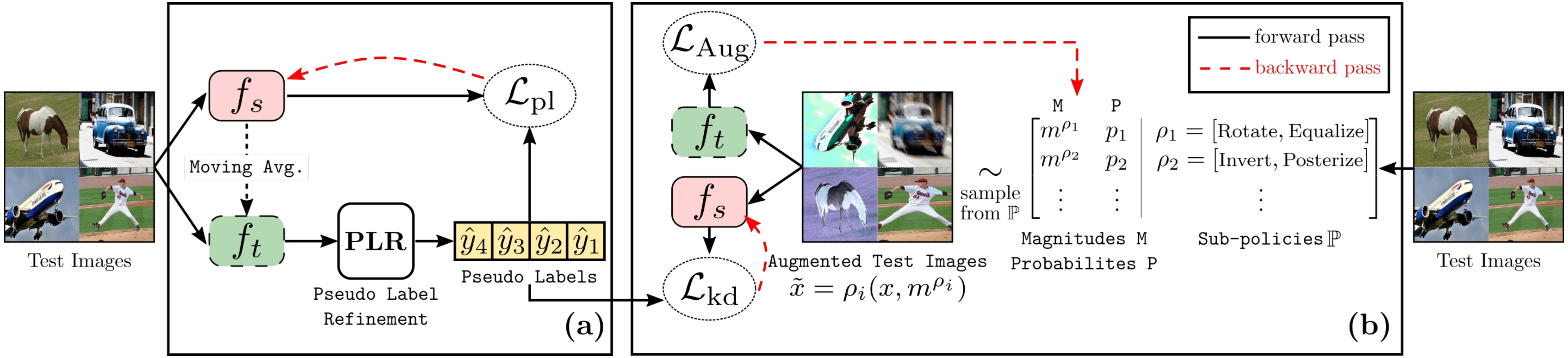
TeSLA: summary of results

- Agnostic to model architectures and source training strategies
- Better class-wise feature separability



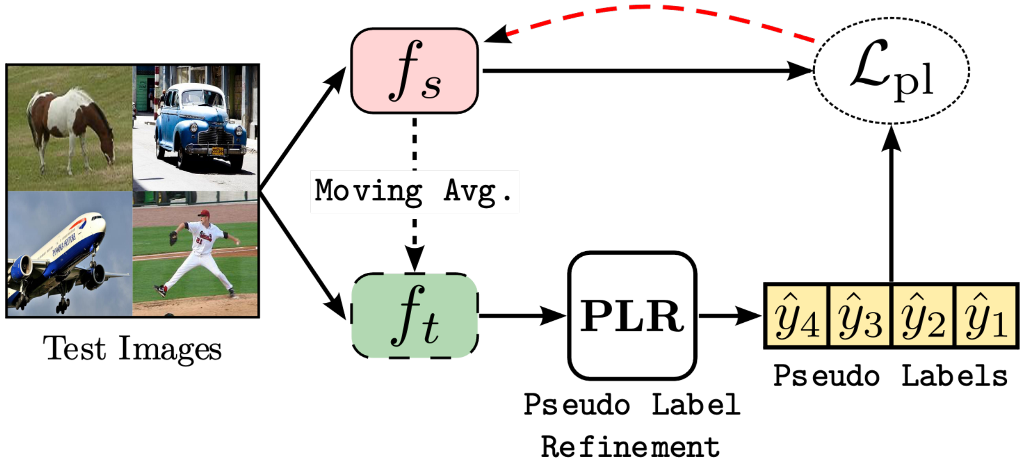


TeSLA: overview



Test-time objective

- Flipped cross entropy f-CE as a proxy to teacher-guided mutual information maximization



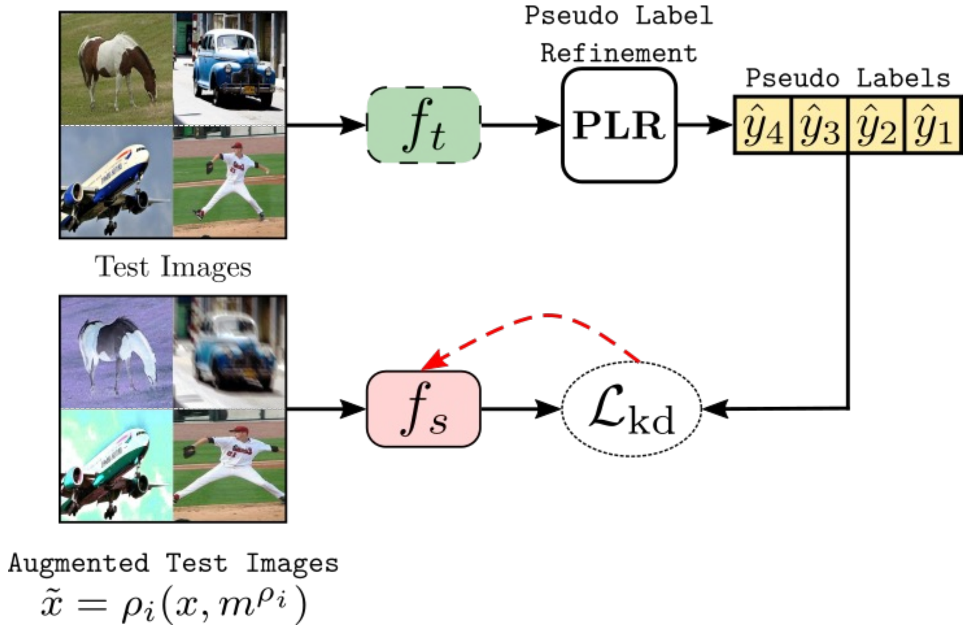
$$\underbrace{\mathcal{H}\left(\mathbf{Y};\hat{\mathbf{Y}}\mid\mathbf{X}\right)}_{f\text{-}\mathbb{CE}}-\mathcal{H}\left(\mathbf{Y}\right)=-\underbrace{\mathcal{I}\left(\mathbf{Y};\mathbf{X}\right)}_{\text{Mutual Info.}}+\mathcal{D}_{\mathrm{KL}}\left(\mathbf{Y}\parallel\hat{\mathbf{Y}}\mid\mathbf{X}\right)$$

$$\mathcal{L}_{\mathrm{pl}}(X,\hat{Y})=-\frac{1}{B}\sum_{i=1}^{B}\sum_{k=1}^{K}\left(f_s(x_i)_k\log((\hat{y}_i)_k)+\hat{f}_s(X)_k\log(\hat{f}_s(X))_k\right)$$

Test-time objective

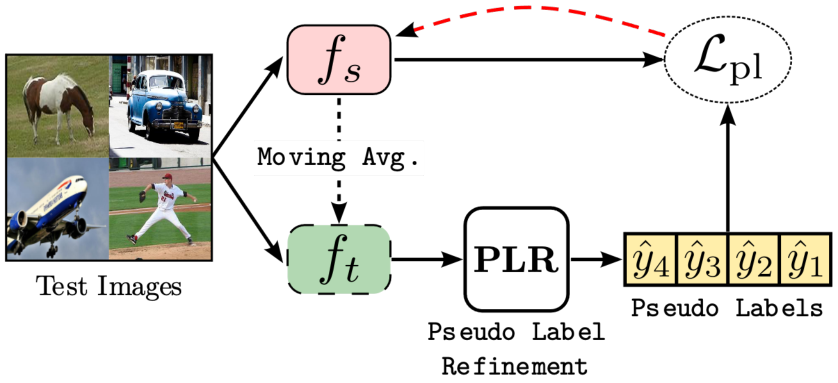
- Knowledge distillation from the teacher to the student using adversarial augmentation

$$\mathcal{L}_{\text{kd}}(\tilde{x}, \hat{y}) = \mathcal{D}_{\text{KL}}(\hat{y} \| f_s(\tilde{x}))$$

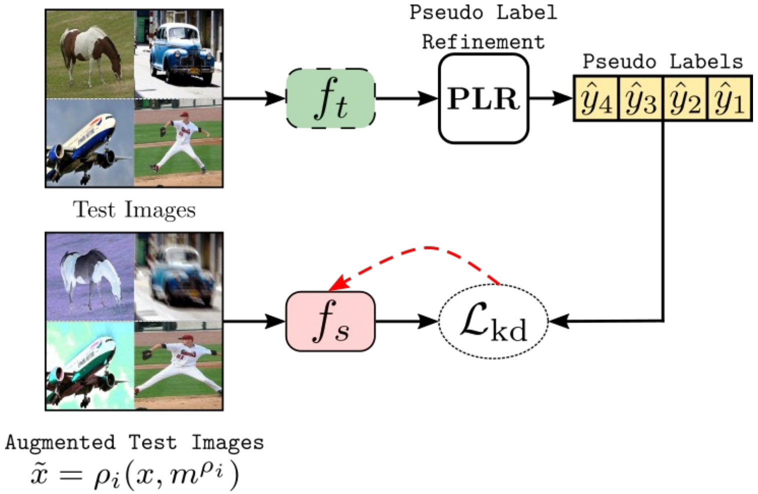


Test-time objective

- Overall test-time objective:



+



$$\mathcal{L}_{\text{TeSLA}}(X, \tilde{X}, \hat{Y}) = \mathcal{L}_{\text{pl}}(X, \hat{Y}) + \frac{\lambda_2}{B} \sum_{i=1}^{B} \mathcal{L}_{\text{kd}}(\tilde{x}_i, \hat{y}_i)$$

PLR (Pseudo Label Refinement)

- Average teacher's predictions on weakly augmented views *stored* in an online balanced queue Q.

$$\mathbf{z}_t, \mathbf{y}_t \leftarrow \mathbb{E}_{\mathbf{u}\in\rho_w(x)}[g_t(\mathbf{u}), h_t(g_t(\mathbf{u}))]$$

$$\mathbf{Q}[\arg\max(\mathbf{y}_t)].\mathrm{append}(\{\mathbf{z}_t, \mathbf{y}_t\})$$

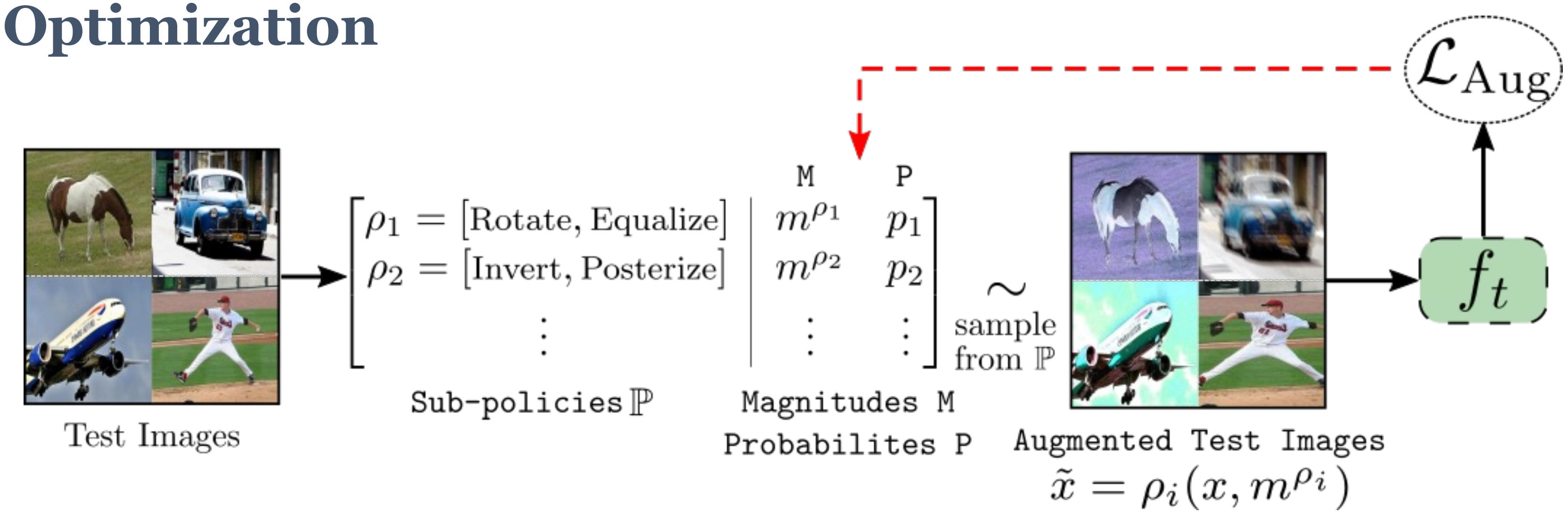
where, ρ_w denotes weak augmentations, g_t is the encoder, and h_t is the classifier

- Refine pseudo-labels by averaging the soft-pseudo labels of k-nearest neighbors from Q.

$$\hat{y} = \frac{1}{n}\sum \mathcal{N}_{\mathbf{Q},n}(\mathbf{z}_t)$$

Automatic adversarial augmentations

- **Policy Search Space**
- **Policy Evaluation**
- **Policy Optimization**

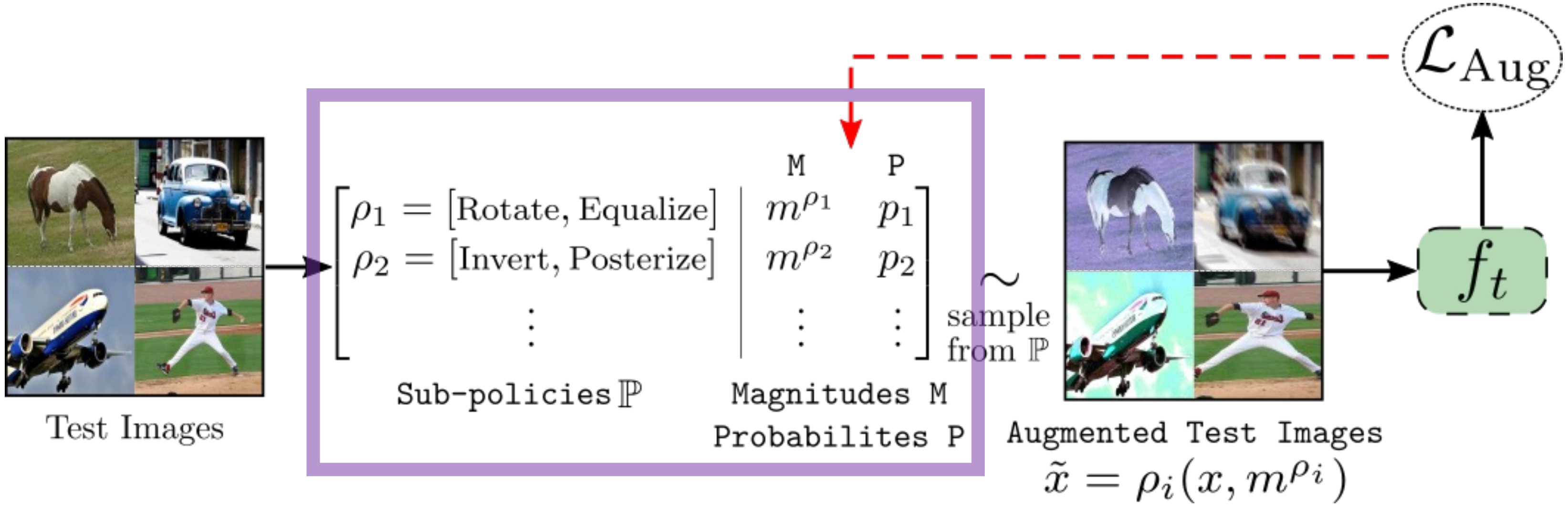


Automatic adversarial augmentations

Policy Search Space $\mathbb{P}$

Sub-policy (ρ): *A combination of N=2 image operations and characterized by their magnitudes* m^{ρ}.

All possible sub-policies with their corresponding magnitudes constitute policy search space.

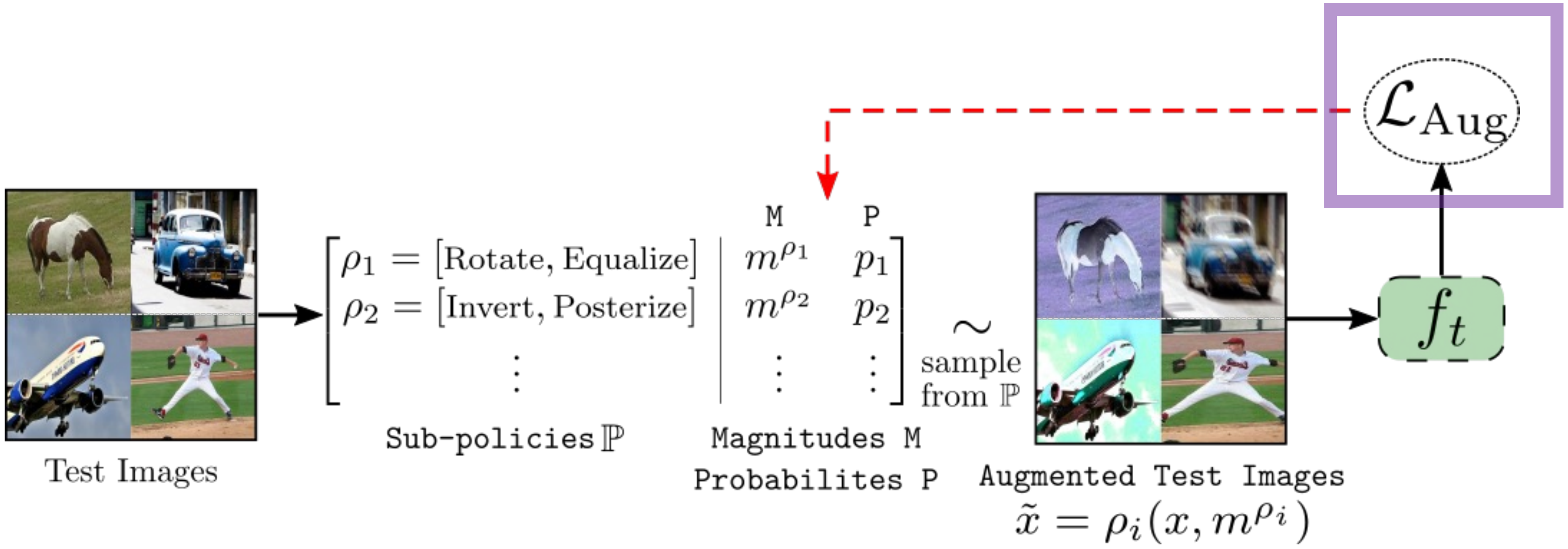


Automatic adversarial augmentations

Policy Evaluation

Given teacher f_t, a sub-policy ρ with magnitude m^{ρ} is evaluated by following loss:

$$\mathcal{L}_{\text{aug}}(\boldsymbol{x}, \rho) = \sum_{k=1}^{K} f_t\left(\tilde{\boldsymbol{x}}\right) \log\left(f_t\left(\tilde{\boldsymbol{x}}\right)\right) + \lambda_1 r(\tilde{\boldsymbol{x}}, \boldsymbol{x}) \quad \textit{where,} \quad \tilde{\boldsymbol{x}} = \rho\left(\boldsymbol{x}, m\right)$$

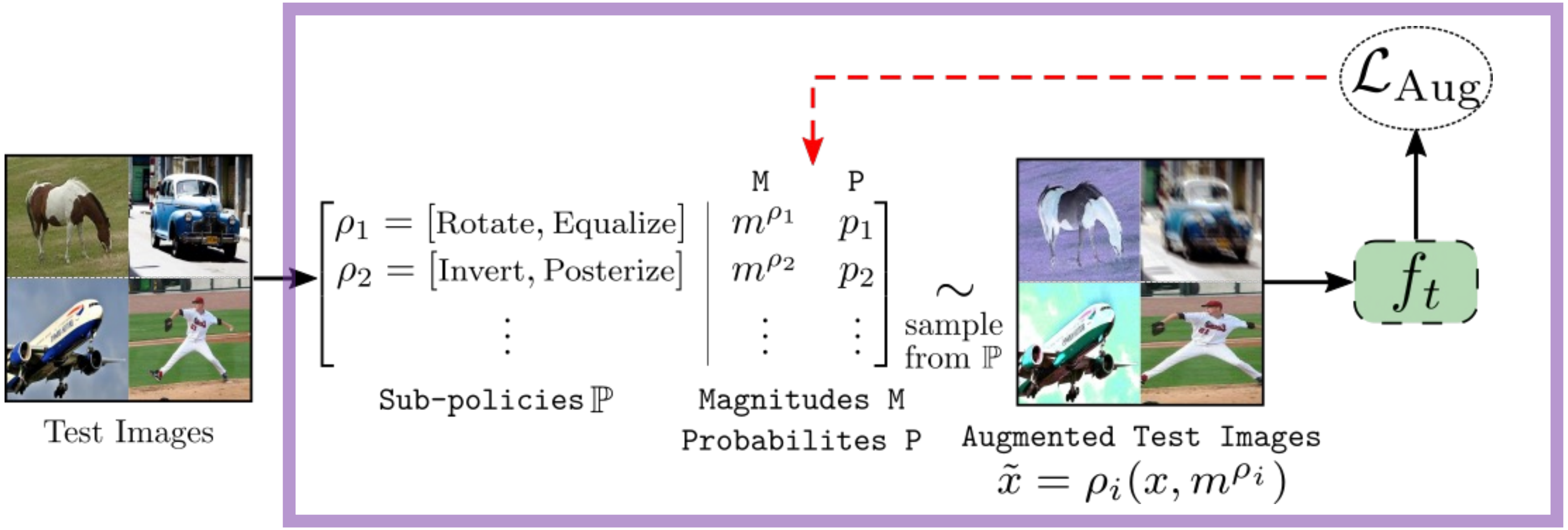


Automatic adversarial augmentations

Policy Optimization

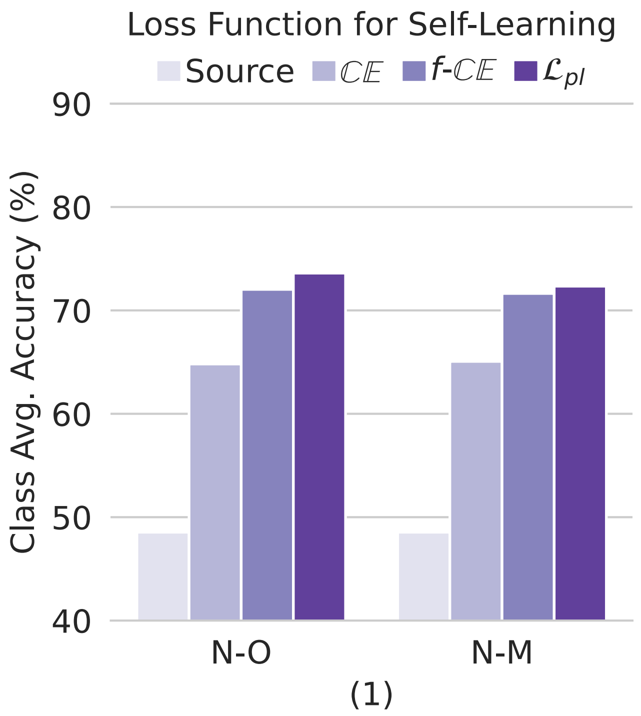
$$\mathbb{E}[\mathcal{L}_{\text{aug}}(x)] = \sum_{i=1}^{||\mathbb{P}||} p_i \cdot \mathcal{L}_{\text{aug}}(x, \rho_i)$$

$$\hat{\delta}(x, \rho_i) = \nabla \mathcal{L}_{\text{aug}}(x, \rho_i) + \mathcal{L}_{\text{aug}}(x, \rho_i) \cdot \nabla \log p_i$$



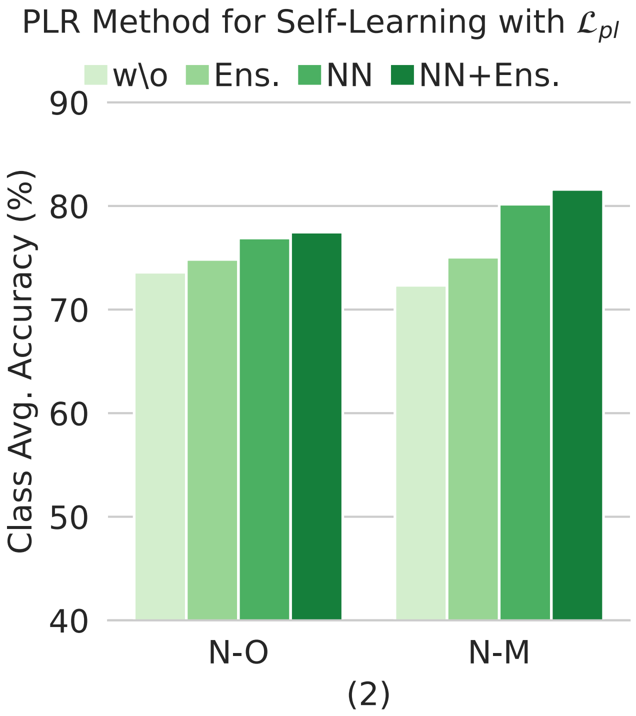
Ablation studies: test-time objective

- Our test-time objective outperforms other test-time objectives.



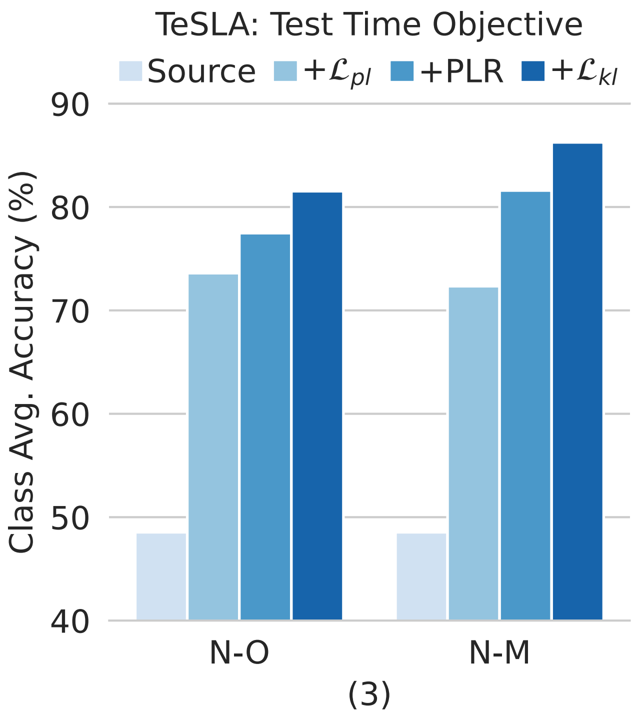
Ablation studies: PLR

- Our soft-pseudo label refinement module helps to get refined pseudo-labels



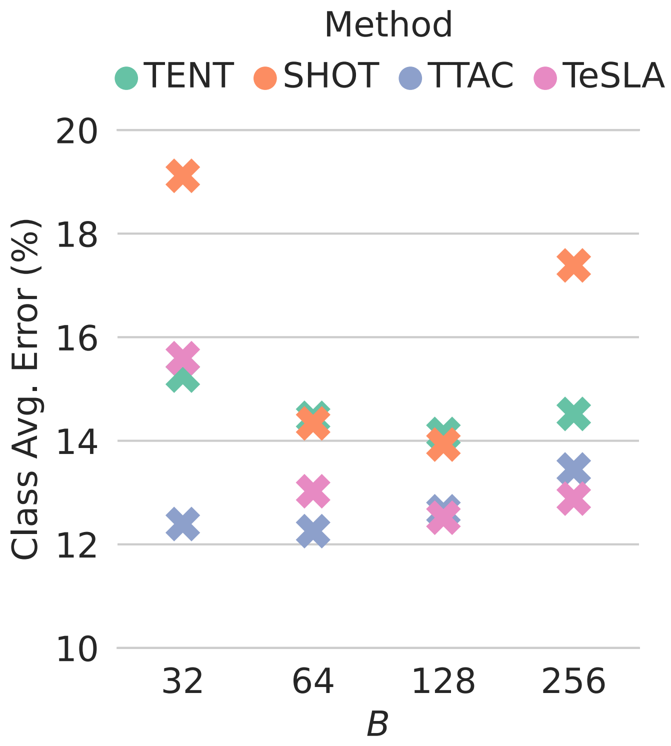
Ablation studies: individual components

- We study the effect of individual loss term on performance below.

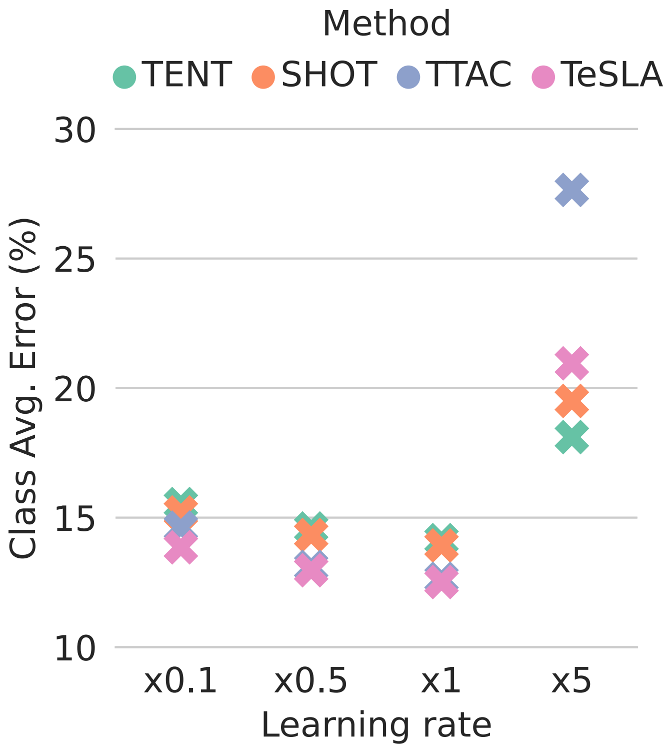


Ablation studies: sensitivity tests

- TeSLA is stable to the change in test-time **(a) batch size** and **(b) learning rate** hyperparameters compared to competing baselines.



(a)



(b)

TeSLA: summary and limitations

- Novel self-learning TTA method utilizing efficient automatic adversarial augmentations
- Agnostic to model architectures and source training strategies
- Superior performance from common image corruption to measurement shifts in medical imaging

- Assumes test images are class-wise IID distributed!

Thank You!

Project page: https://behzadbozorgtabar.com/TeSLA.html