PRIME: A few primitives can boost robustness to Common Corruptions.

Apostolos Modas*, Rahul Rade*, Guillermo Ortiz-Jiménez, Seyed-Mohsen Moosavi-Dezfooli and Pascal Frossard

EPFL ETH zürich ECCV TEL AVIV 2022

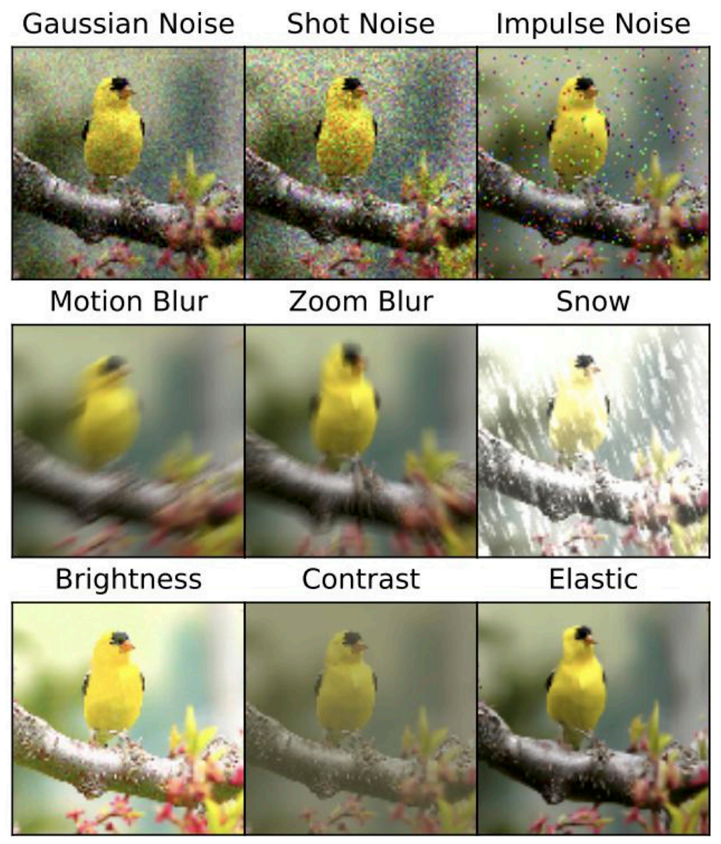
How to build classifiers that are robust to Common Corruptions?

Usually through very complicated methods.

Is there a simpler and more principled way?

Yes! Data augmentation with max-entropy transformations!

Common Corruptions (CC).



All possible distortions that can occur during **acquisition**, **storage** or **processing** of an image.

An ill-posed problem: evaluate on standard benchmarks.

Common Corruptions Benchmark by Hendrycks et al. [1]

Prior Art.

Most common approach: **Data Augmentation**

AugMix [2]
- **unintuitive** transformations
- **not good** on ImageNet

DeepAugment (DA) [3]
- **black-box**: Im2Im DNNs
- **heavy**: only offline

Current **SOTA** on CC: **DA + AugMix**
- very **heavy**
- hard to **adapt** to new datasets
- lacks **ablation** studies

*How to design a **simple** but **principled** augmentation method?*

PRIME Augmentations.

General model of visual corruptions

Linear **combination** of **compositions** of transformation **primitives**

$$\mathcal{T}_{\boldsymbol{x}} = \left\{ \sum_{i=1}^{n} \lambda_i \; g_1^i \circ \cdots \circ g_m^i(\boldsymbol{x}) : \; g_j^i \in \{\omega, \tau, \gamma\}, \lambda_i \in \mathbb{R} \right\}$$

Transformation primitives

τ : **spatial** (diffeomorphisms)

ω : **spectral** (filtering)

γ : **color** (jittering)

Principle of maximum-entropy

$$\max_{\mu} H(\mu) = -\int \mathrm{d}\mu(g) \log(\mu(g))$$

with $g \sim \mu$

PRImitives of Maximum Entropy

Robustness to Common Corruptions.

SOTA Robustness
- **Simpler**
- **Principled**
- **Faster** than DA

Dataset	Method	Clean Acc (↑)	CC Acc (↑)
CIFAR-10	Standard	95.0	74.0
	AugMix	95.2	88.6
	PRIME	94.2	**89.8**
CIFAR-100	Standard	76.7	51.9
	AugMix	78.2	64.9
	PRIME	78.4	**68.2**
ImageNet	Standard	76.1	38.1
	AugMix	77.5	48.3
	DA	76.7	52.6
	PRIME	77.0	**55.0**
	DA+AugMix	75.8	58.1
	DA+PRIME	75.5	**59.9**

Contribution of Transformations.

Ablation study on **ImageNet-100**

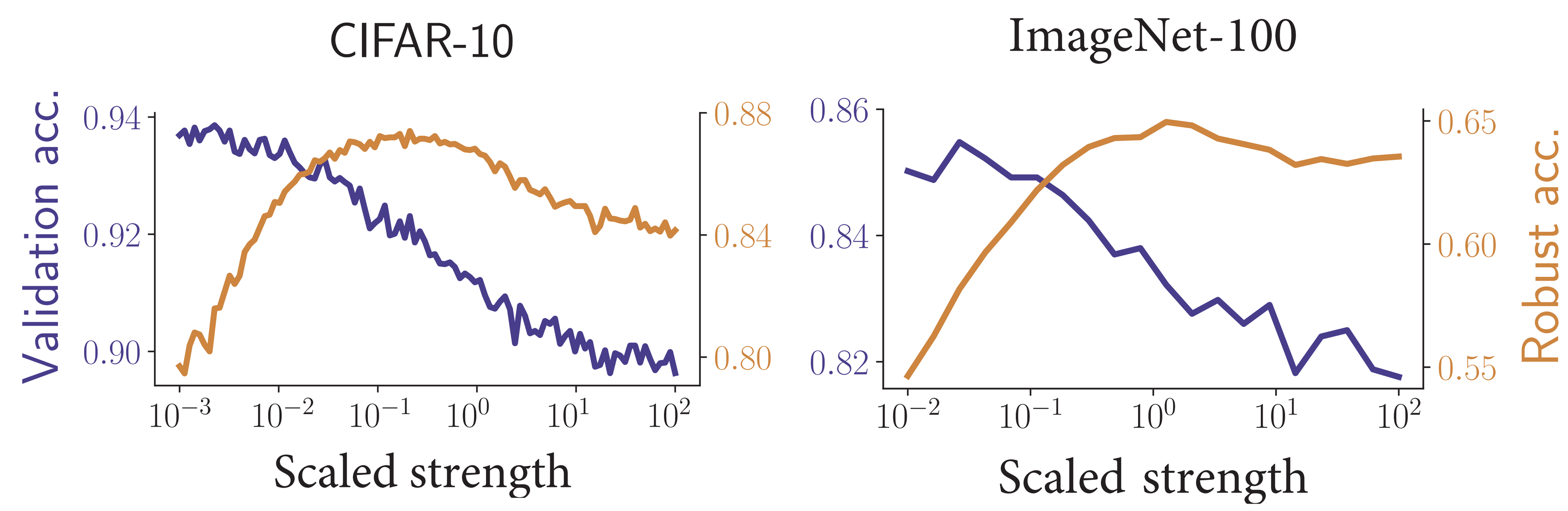
Trans.	CC	Noise	Blur	Weather	Digital
ω	64.1	60.7	55.4	66.6	72.9
τ	53.8	30.1	56.2	57.6	65.4
γ	59.9	67.4	52.6	54.4	67.1
ω+τ	64.5	58.5	57.3	**66.8**	73.9
ω+γ	67.5	77.2	55.7	65.3	74.2
τ+γ	63.3	74.7	57.4	56.2	67.8
ω+τ+γ	**68.8**	**78.8**	**58.3**	66.0	**74.8**

Primitives help **individually**

Best: combined

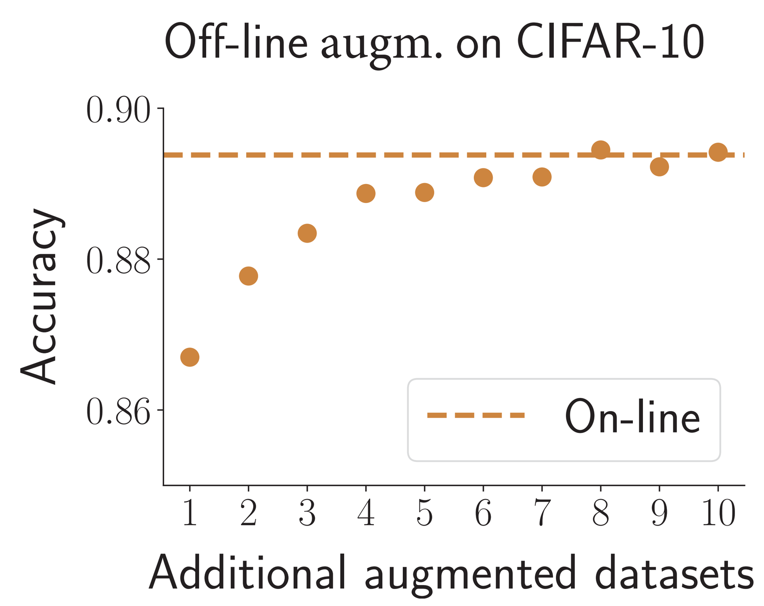
Robustness/Accuracy trade-off.

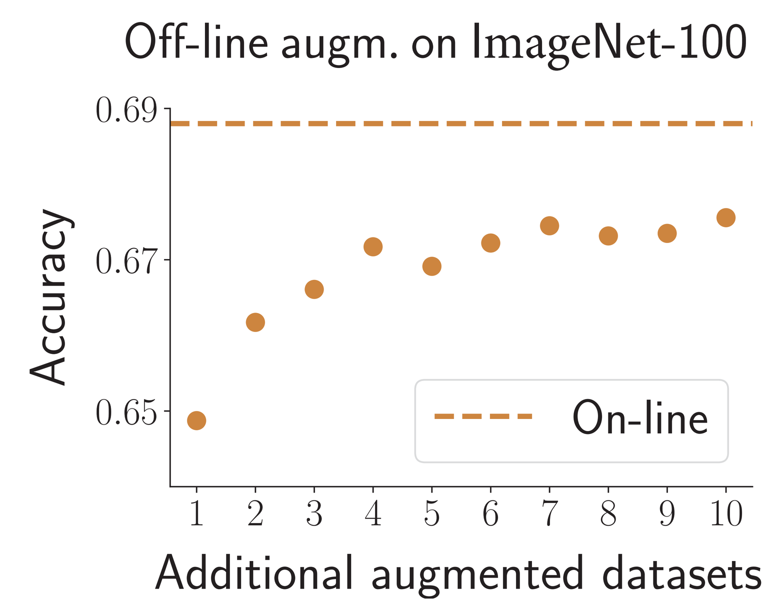
Vary strength of transformation → control **trade-off**



Sample Complexity.

Off-line: pre-compute augmentations (like DeepAugment)





- +4: similar to on-line PRIME
- **No need** for on-line

- >4: slow improvement
- **Need** on-line: **easy** with PRIME!

[1] D. Hendrycks et al. "Benchmarking neural network robustness to common corruptions and perturbations", *ICLR 2019*.
[2] D. Hendrycks et al. "AugMix: A simple method to improve robustness and uncertainty under data shift", *ICLR 2020*.
[3] D. Hendrycks et al. "The many faces of robustness: A critical analysis of out-of-distribution generalization", *ICCV 2021*.