HybridAugment++: Unified Frequency Spectra Perturbations for Model Robustness

Mehmet Kerim Yucel[1], Ramazan Gokberk Cinbis[2], Pinar Duygulu[1]

[1] Hacettepe University, Ankara, Turkey [2] METU, Ankara, Turkey

ICCV23 PARIS

Goal

✓ Robust ↗ and accurate ↗ CNNs.

Key Insights

✓ Robustness/accuracy trade-off
- ✓ High-frequency content ✕ , ↗
- ✓ Low-frequency content ↗, ✕
- ✓ Amplitude reliance ✕ , ↗
- ✓ Phase reliance ↗, ✕

Contributions

✓ Augmentations to find the sweet-spot!

✓ Make the model focus on..
- ✓ Low-frequency (HA)
- ✓ Phase of low-frequency (HA++).

Results

✓ Robustness ↗
- ✓ Adversarial ↗
- ✓ Corruption ↗
- ✓ OOD ↗

✓ Transformers!

Code and pretrained models

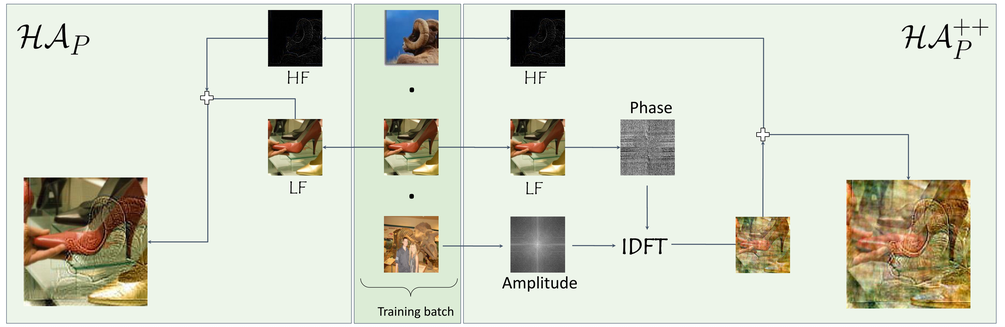
✓ No extra data
✓ No extra models
✓ No ensembles

✓ Accuracy ↗
✓ Transferability
✓ Flexible

HybridAugment (Paired)

1. Take images x_i, x_j in a batch
2. Swap HF and LF of x_i, x_j

Use LF image label as the ground-truth



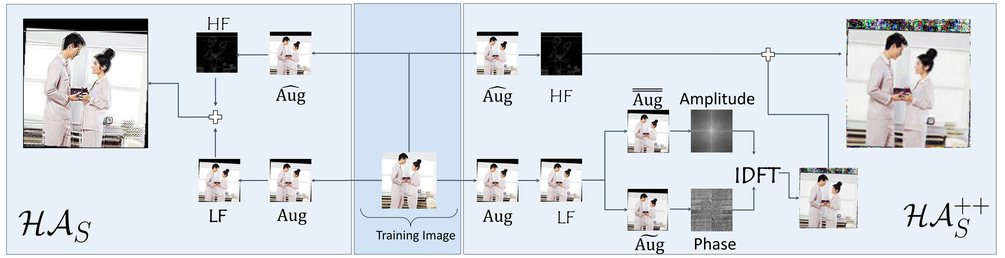
HybridAugment++ (Paired)

1. Take images x_i, x_j, x_z in a batch
2. Take LF of x_i , swap its amplitude with that of x_z
3. Merge the resulting image with HF of x_j

Use the label of x_i as the ground-truth

HybridAugment (Single)

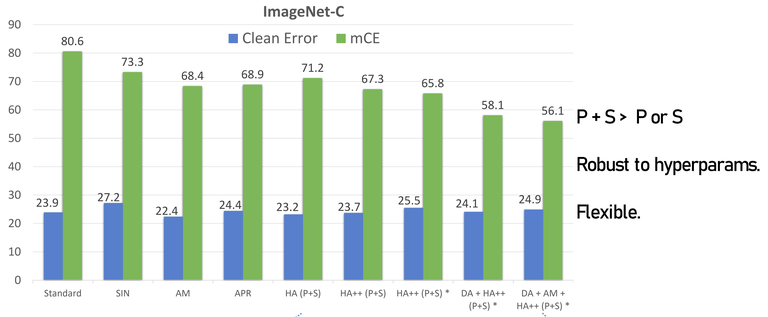
1. Take image x_i
2. Get two views of x_i.
3. Swap HF and LF of two views of x_i



HybridAugment++ (Single)

1. Take image x_i
2. Get two views of x_i (e. g. x_{i1} and x_{i2})
3. Get two new views of x_{i1} (e.g. x_{i11} and x_{i12})
4. Swap phase and amplitude of x_{i11} and x_{i12}
5. Merge the resulting image with HF of x_{i2}

Corruption Robustness



P + S > P or S

Robust to hyperparams.

Flexible.

HA - Robust ↗ and accurate ↗

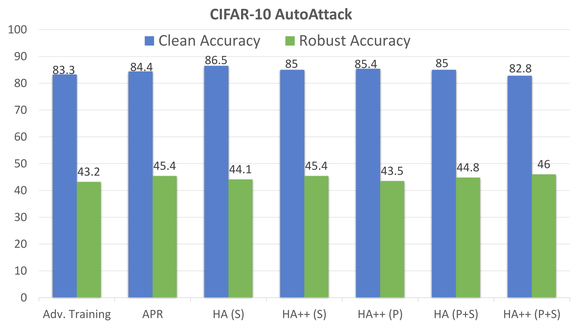
HA++ – Much more robust ↗ and accurate ↗

Complements other methods

Scales with data

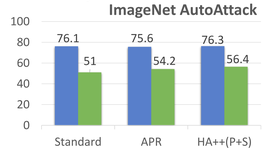
* Higher cut-off leads to increased robustness ↗

Adversarial Robustness

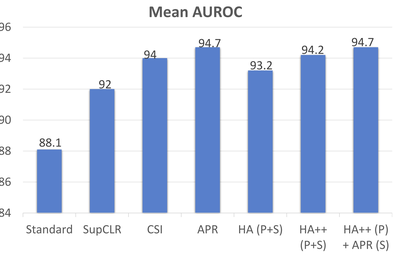


All variants better than adversarial training.
Outperforms APR (HA++(S)).
Achieves best clean and robust accuracy.

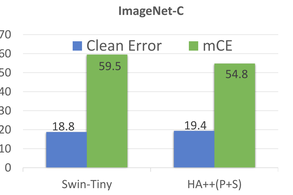
Same trends on ImageNet!



OOD Detection & Transfer Learning



Improves OOD. Competitive!



Robust ↗ transformers!

Features transfer better.

Acknowledgement: This work was supported in part by a Google Faculty Research Award.