Team Projects:
Measuring Robustness for Pixel-wise prediction tasks
Machine Learning, DWS
Adversarial Robustness

Out-of-Distribution (OOD) Robustness

Benchmarks exist for classification

a standardized adversarial robustness benchmark

by F Croce · 2020  Cited by 468 — Title: RobustBench: a standardized adversarial robustness benchmark ; Subjects: Machine Learning (cs.LG); Cryptography and Security (cs.CR); ...
Project Idea

1 task each

Robustness Benchmark

Semantic Segmentation

Disparity Estimation

Optical Flow Estimation

Object Detection

OOD

Adversarial

OOD

Adversarial

OOD

Adversarial

OOD

Adversarial
Performance evaluation for OOD

- **Common Corruptions:** Benchmarking Neural Network Robustness to Common Corruptions and Perturbations

- **3D Common Corruptions:**
  
  3D Common Corruptions and Data Augmentation
Semantic Segmentation

Architectures:
- UNet
- PSPNet
- DeepLabV3
- DeepLabV3+
- SegFormer

Datasets:
- PASCAL VOC 2012
- Cityscapes
- ADE20K
- BDD
- InternImage
- Mask2Former
- DINO
- DINOv2
- ONE PEACE

The current plan is to divide tasks for each vision task, by dataset.
Performance evaluation for Adversarial robustness

<table>
<thead>
<tr>
<th>Test against following attacks:</th>
<th>Epsilons:</th>
<th>Iterations:</th>
</tr>
</thead>
<tbody>
<tr>
<td>● FGSM(iFGSM)</td>
<td>● 1/255</td>
<td>● 1</td>
</tr>
<tr>
<td>● PGD</td>
<td>● 2/255</td>
<td>● 3</td>
</tr>
<tr>
<td>● APGD</td>
<td>● 4/255</td>
<td>● 5</td>
</tr>
<tr>
<td>● CosPGD</td>
<td>● 8/255</td>
<td>● 10</td>
</tr>
<tr>
<td>● SegPGD</td>
<td>● 12/255</td>
<td>● 20</td>
</tr>
<tr>
<td>● AutoAttack</td>
<td>● 25/255</td>
<td>● 40</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● 100</td>
</tr>
</tbody>
</table>
Disparity Estimation

Architectures:
- UNet
- DispNet
- AutoDispNet
- STTR
- STTR-light

Datasets:
- Flyingthing3D
- MPI Sintel
- KITTI 2015
- MIDDLEBURY_2014
- SCARED
- ETH 3D

The current plan is to divide tasks for each vision task, by set of architectures.
Optical Flow Estimation

Architectures:
- RAFT
- PWCNet
- GMANet
- SpyNet
- FlowNet2.0
- FlowFormer
- RPKNet

Datasets:
- KITTI 2015
- MPI Sintel
- Spring

Additional Attacks:
- PCFA
- Adversarial Snow

The current plan is to divide tasks for each vision task, by dataset.
Object Detection

Architectures:
- Co-DETR
- YOLOv5
- YOLOv7
- Faster R-CNN
- DETReg
- RetinaNet

Datasets:
- PASCAL VOC 2007
- COCO
- ImageNet
- BDD
- KITTI 2012

The current plan is to divide tasks for each vision task, by dataset.
What can you expert to learn?

- Using pytorch
- State-of-the-art vision tasks and methods
- Robustness
- Building-up from a base code
- Potentially paper writing
What should you bring?

- Basic python skills
- Basic machine learning knowledge
- Learning attitude
- Collaborative nature
Expected Deadline?

Finish Experiments: May 05, 2024

Finish Paper Writing: June 01, 2024

Deadline might change according to NeuRIPS 2024 schedule.
If interested / Further Questions

Please contact: Shashank Agnihotri

Email id: shashank.agnihotri@uni-mannheim.de

Email subject: Team Project 2024

If interested:

Please include the vision tasks you are interested in the order of the priority

In case of many students, we are open to adding other vision tasks, such as depth estimation, panoptic segmentation etc.