Computer Vision Codebase

Shpresim Sadiku

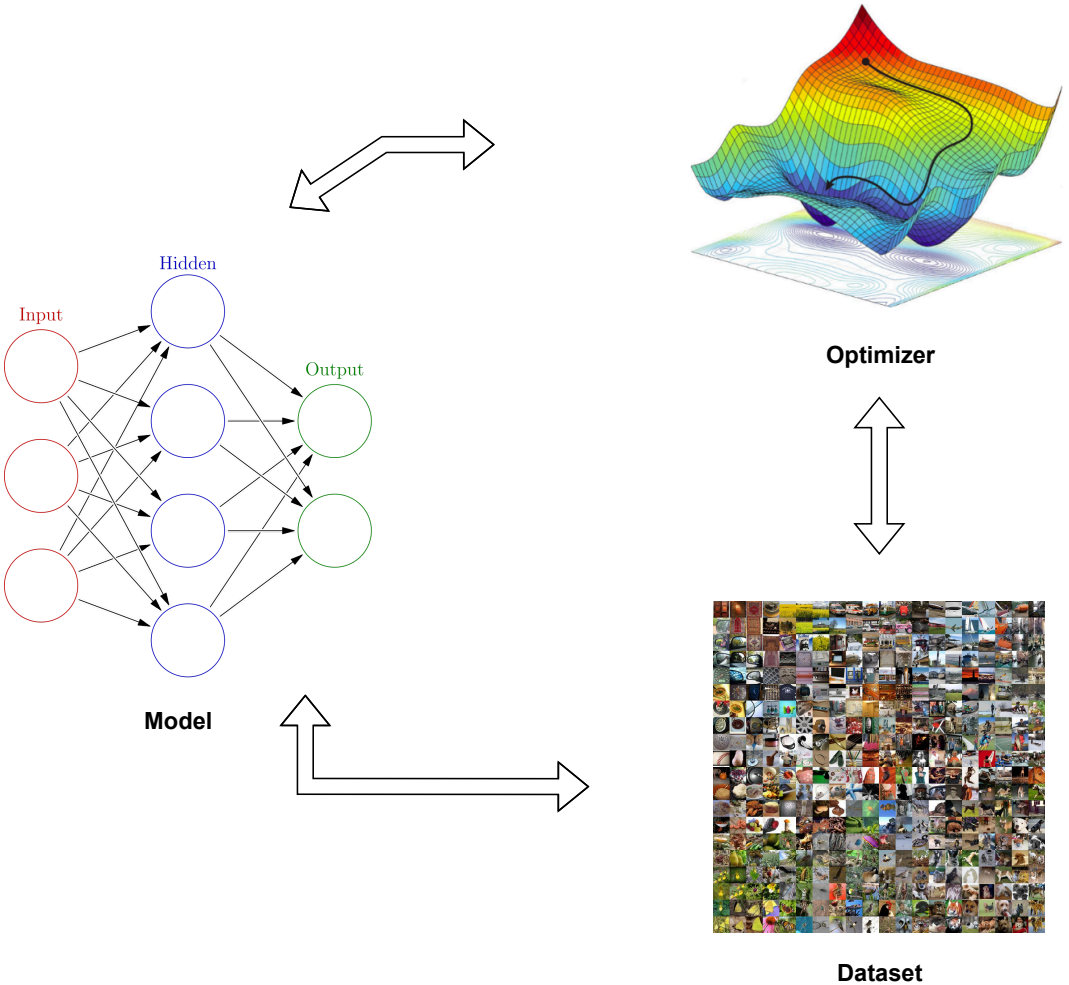
Deep Learning Development @ZIB · April 24, 2024

The aim of the repository?

- Offer a user-friendly codebase for initiating 2D Computer Vision tasks
- Primarily based on robustness experiments on images
  - White-box adversarial attacks
  - Extensible to explainability (XAI) of classifiers, counterfactual generation (CFE), etc
- Prevent negative conference reviews by ensuring complete experiments

What can you do with it?

- Train deep learning **models** on various **datasets** utilizing a range of **optimizers**



Datasets, Models, and Optimizers included

- Datasets
  1. CIFAR10
  2. CIFAR100
  3. MNIST
  4. NIPS2017
  5. ImageNet
- Models
  1. Basic MLP
  2. Basic CNN
  3. Small CNN
  4. WideResNet
  5. LeNet
  6. ResNet18
  7. ResNet20
  8. ResNet50
  9. VGG19
- Optimizers
  1. SGD
  2. AdaGrad
  3. Adam
  4. NAG

Note

- Not an exhaustive list of datasets, models, and optimization algorithms (!)
- Check carefully conference requirements

Tips

- Sometimes results on a certain dataset do not transfer to another dataset

Tips

- Experiment with a different optimizer (!)
- Tune the hyperparameters to find the best combination for your problem

- Use built-in classes in PyTorch for other optimizers

```
optimizer = torch.optim.RMSprop(model.parameters(), lr=0.01)
```

- Performance of these algorithms depends on the dataset and model architecture

Where do I find the repository?

- Currently

  `https://github.com/shsad/computervision-codebase`

- Eventually will be available at

  `https://git.zib.de/IOL/vision-codebase`

- Train a ResNet20 model on CIFAR10 dataset using the Adam optimizer with a batch size of 64 along with max epochs of 10

```
[ ] python main.py --model 'ResNet20' --dataSet 'CIFAR10' --optim 'Adam'
                   --maxIterations 10 --batchSize 64 --numWorkers 2 --saveModel 1 --ver 1
```

- Future plans
  - Include (group-wise) sparse adversarial attacks code
  - Include more models (e.g. transformers)