Лабораторная работа №1

Выполнил: Воронов Андрей Иванович ББМО-01-22

Номер в таблице: 15

Отчет по выполнению 14 пункта из задания для лабораторной работы

Были проведены несколько экспериментов с использованием таких параметров fgsm_eps: 0.001, 0.02, 0.5, 0.9, 10.

Код реализации экспериментов:

```
# значения eps для FGSM атаки, которые вы хотите исследовать
epsilons = [0.001, 0.02, 0.5, 0.9, 10]

# цикл для перебора различных значений eps
for eps in epsilons:
    print(f"Evaluating FGSM Attack with eps={eps}...")

    # FC LeNet на датасете MNIST
    model = FC_500_150().to(device)
    model.load_state_dict(torch.load('weights/clean/mnist_fc.pth'))
    evaluate_attack(f'mnist_fc_fgsm_eps{eps}.csv', 'results', device, model, mnist_loader_test, mnist_min, mnist_max, eps, is_fgsm=True)

    # NiN LeNet на датасете CIFAR
    model = Net().to(device)
    model.load_state_dict(torch.load('weights/clean/cifar_nin.pth'))
    evaluate_attack(f'cifar_nin_fgsm_eps{eps}.csv', 'results', device, model, cifar_loader_test, cifar_min, cifar_max, eps, is_fgsm=True)

    if device.type == 'cuda': torch.cuda.empty_cache()
```

1. Для сети FC LeNet на датасете MNIST:

- при маленьких значениях eps, например, eps=0.001 и eps=0.02, ошибка классификации (FGSM Test Error) остается низкой, и сеть остается относительно устойчивой к атакам.
- ошибка классификации начинает расти при eps=0.5 и eps=0.9, и достигает высоких значений, что свидетельствует о нарушении стойкости сети к атакам.
- при очень большом eps=10 ошибка классификации также высока, и сеть становится непригодной для задач классификации из-за большого искажения входных данных.

2. Для сети NiN LeNet на датасете CIFAR:

- Сеть также начинает демонстрировать увеличение ошибки классификации с ростом eps. При eps=0.001 и eps=0.02, ошибка остается низкой, но при eps=0.5, eps=0.9, и eps=10 ошибка резко увеличивается.
- Таким образом, сеть NiN LeNet на датасете CIFAR также оказывается уязвимой к атакам при больших значениях eps.

Вывод

Маленькие значения eps сохраняют стойкость сетей к атакам, и ошибки классификации остаются низкими.При увеличении eps сети становятся более уязвимыми к атакам и допускают больше ошибок в классификации. Для сетей FC LeNet на датасете MNIST и NiN LeNet на датасете CIFAR не наблюдается отсутствие влияния параметра eps. Вместо этого, параметр eps оказывает существенное влияние на устойчивость сетей к атакам.

Результат работы ячейки кода:

```
Evaluating FGSM Attack with eps=0.001...
/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.
  warnings.warn(_create_warning_msg(
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 3.07%
FGSM Robustness : 8.08e-04
FGSM Time (All Images) : 0.76 s
FGSM Time (Per Image) : 76.04 us
/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.
  warnings.warn(_create_warning_msg(
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 10.12%
FGSM Robustness : 8.92e-04
FGSM Time (All Images) : 1.15 s
FGSM Time (Per Image) : 115.46 us
Evaluating FGSM Attack with eps=0.02...
/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.
  warnings.warn(_create_warning_msg(
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 5.54%
FGSM Robustness : 1.60e-02
FGSM Time (All Images) : 0.45 s
FGSM Time (Per Image) : 44.66 us
/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be
```

aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.

warnings.warn(_create_warning_msg(

FGSM Batches Complete : (157 / 157)

FGSM Test Error : 30.76%

FGSM Robustness : 1.78e-02

FGSM Time (All Images) : 1.38 s

FGSM Time (Per Image) : 138.22 us

Evaluating FGSM Attack with eps=0.5...

/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.

warnings.warn(_create_warning_msg(

FGSM Batches Complete : (157 / 157)

FGSM Test Error : 99.21%

FGSM Robustness : 3.86e-01

FGSM Time (All Images) : 0.55 s

FGSM Time (Per Image) : 54.78 us

/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.

warnings.warn(_create_warning_msg(

FGSM Batches Complete : (157 / 157)

FGSM Test Error : 82.67%

FGSM Robustness : 4.40e-01

FGSM Time (All Images) : 1.14 s

FGSM Time (Per Image) : 114.04 us

Evaluating FGSM Attack with eps=0.9...

/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.

warnings.warn(_create_warning_msg(

FGSM Batches Complete : (157 / 157)

FGSM Test Error : 99.87%

FGSM Robustness : 6.86e-01

FGSM Time (All Images) : 0.53 s

FGSM Time (Per Image) : 53.29 us

/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.

warnings.warn(_create_warning_msg(

FGSM Batches Complete : (157 / 157)

FGSM Test Error : 84.62%

FGSM Robustness : 7.79e-01

FGSM Time (All Images) : 1.07 s

FGSM Time (Per Image) : 106.74 us

Evaluating FGSM Attack with eps=10...

/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.

warnings.warn(_create_warning_msg(

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 99.87%
FGSM Robustness : 1.47e+00
FGSM Time (All Images) : 0.53 s
FGSM Time (Per Image) : 52.56 us
/usr/local/lib/python3.10/dist-packages/torch/utils/data/dataloader.py:560: UserWarning: This DataLoader will create 4 worker processes in total. Our suggested max number of worker in current system is 2, which is smaller than what this DataLoader is going to create. Please be aware that excessive worker creation might get DataLoader running slow or even freeze, lower the worker number to avoid potential slowness/freeze if necessary.
  warnings.warn(_create_warning_msg(
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 87.50%
FGSM Robustness : 2.46e+00
FGSM Time (All Images) : 1.11 s
FGSM Time (Per Image) : 110.72 us
```