Aufgabe CNN fashion mnist under attack

03.12.2021, Thomas Iten

Net and transform ToTensor()

Training

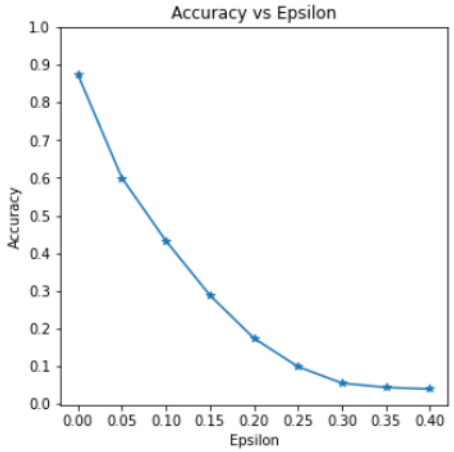
```
Epoch 1
-------------------------------
loss: 2.309729  [    0/60000]
loss: 2.117056  [ 3200/60000]
loss: 2.122358  [ 6400/60000]
loss: 1.924216  [ 9600/60000]
loss: 1.857021  [12800/60000]
loss: 1.942397  [16000/60000]
loss: 1.448427  [19200/60000]
loss: 1.446566  [22400/60000]
loss: 1.374417  [25600/60000]
loss: 1.575279  [28800/60000]
loss: 1.266395  [32000/60000]
loss: 1.255407  [35200/60000]
loss: 1.233678  [38400/60000]
loss: 1.358572  [41600/60000]
loss: 1.078192  [44800/60000]
loss: 1.009280  [48000/60000]
loss: 1.005314  [51200/60000]
loss: 1.082175  [54400/60000]
loss: 1.076231  [57600/60000]
Test Error:
 Accuracy: 73.5%, Avg loss: 0.868311
```

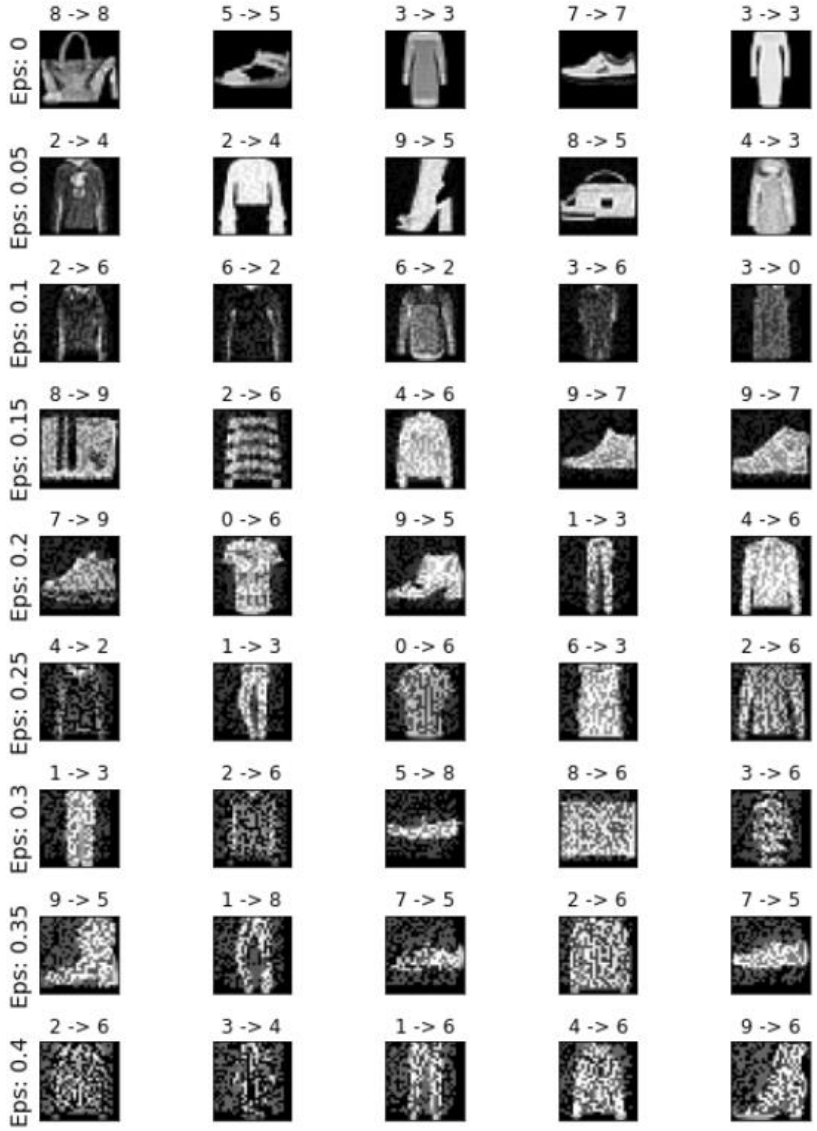
```
Epoch 11
-------------------------------
loss: 0.442550  [    0/60000]
loss: 0.470467  [ 3200/60000]
loss: 0.564882  [ 6400/60000]
loss: 0.640415  [ 9600/60000]
loss: 0.468649  [12800/60000]
loss: 0.818648  [16000/60000]
loss: 0.464680  [19200/60000]
loss: 0.335196  [22400/60000]
loss: 0.773618  [25600/60000]
loss: 0.943427  [28800/60000]
loss: 0.584405  [32000/60000]
loss: 0.551682  [35200/60000]
loss: 0.641801  [38400/60000]
loss: 0.745793  [41600/60000]
loss: 0.887718  [44800/60000]
loss: 0.458467  [48000/60000]
loss: 0.556481  [51200/60000]
loss: 0.831608  [54400/60000]
loss: 0.510236  [57600/60000]
Test Error:
 Accuracy: 83.5%, Avg loss: 0.445191
```

```
Epoch 20
-------------------------------
loss: 0.408494  [    0/60000]
loss: 0.511289  [ 3200/60000]
loss: 0.646600  [ 6400/60000]
loss: 0.701828  [ 9600/60000]
loss: 0.317872  [12800/60000]
loss: 0.692576  [16000/60000]
loss: 0.429453  [19200/60000]
loss: 0.322007  [22400/60000]
loss: 0.574209  [25600/60000]
loss: 0.805434  [28800/60000]
loss: 0.549323  [32000/60000]
loss: 0.395256  [35200/60000]
loss: 0.467621  [38400/60000]
loss: 0.691796  [41600/60000]
loss: 0.804047  [44800/60000]
loss: 0.313825  [48000/60000]
loss: 0.526565  [51200/60000]
loss: 0.733478  [54400/60000]
loss: 0.441064  [57600/60000]
Test Error:
 Accuracy: 86.0%, Avg loss: 0.379478
```

```
Epoch 30
-------------------------------
loss: 0.386346  [    0/60000]
loss: 0.519160  [ 3200/60000]
loss: 0.563528  [ 6400/60000]
loss: 0.503241  [ 9600/60000]
loss: 0.252681  [12800/60000]
loss: 0.732694  [16000/60000]
loss: 0.315883  [19200/60000]
loss: 0.285666  [22400/60000]
loss: 0.531976  [25600/60000]
loss: 0.569888  [28800/60000]
loss: 0.429159  [32000/60000]
loss: 0.428121  [35200/60000]
loss: 0.290709  [38400/60000]
loss: 0.514441  [41600/60000]
loss: 0.481252  [44800/60000]
loss: 0.558735  [48000/60000]
loss: 0.423462  [51200/60000]
loss: 0.350486  [54400/60000]
loss: 0.522035  [57600/60000]
Test Error:
 Accuracy: 87.3%, Avg loss: 0.344882
```

Attack


Accuracy vs Epsilon
Accuracy
Epsilon
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
0.00 0.05 0.10 0.15 0.20 0.25 0.30 0.35 0.40


Eps: 0
8 -> 8
5 -> 5
3 -> 3
7 -> 7
3 -> 3
Eps: 0.05
2 -> 4
2 -> 4
9 -> 5
8 -> 5
4 -> 3
Eps: 0.1
2 -> 6
6 -> 2
6 -> 2
3 -> 6
3 -> 0
Eps: 0.15
8 -> 9
2 -> 6
4 -> 6
9 -> 7
9 -> 7
Eps: 0.2
7 -> 9
0 -> 6
9 -> 5
1 -> 3
4 -> 6
Eps: 0.25
4 -> 2
1 -> 3
0 -> 6
6 -> 3
2 -> 6
Eps: 0.3
1 -> 3
2 -> 6
5 -> 8
8 -> 6
3 -> 6
Eps: 0.35
9 -> 5
1 -> 8
7 -> 5
2 -> 6
7 -> 5
Eps: 0.4
2 -> 6
3 -> 4
1 -> 6
4 -> 6
9 -> 6

Net and transform ToTensor()-Normalize()

Training

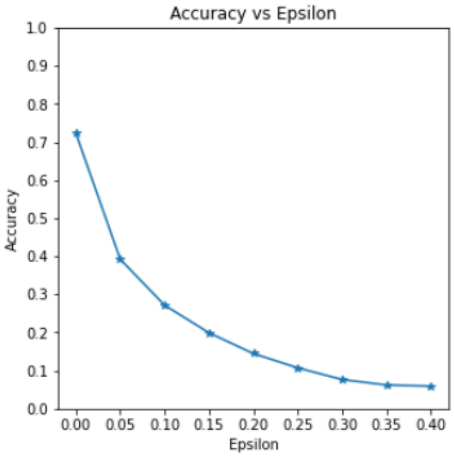
```
Epoch 1
-------------------------------
loss: 2.304479  [    0/60000]
loss: 2.087519  [ 3200/60000]
loss: 2.097471  [ 6400/60000]
loss: 1.993632  [ 9600/60000]
loss: 1.677870  [12800/60000]
loss: 1.737584  [16000/60000]
loss: 1.514164  [19200/60000]
loss: 1.477034  [22400/60000]
loss: 1.598749  [25600/60000]
loss: 1.604664  [28800/60000]
loss: 1.284181  [32000/60000]
loss: 1.232089  [35200/60000]
loss: 1.258010  [38400/60000]
loss: 1.268347  [41600/60000]
loss: 1.076555  [44800/60000]
loss: 0.932221  [48000/60000]
loss: 0.995124  [51200/60000]
loss: 1.380084  [54400/60000]
loss: 0.902560  [57600/60000]
Test Error:
 Accuracy: 65.7%, Avg loss: 1.571436
```

```
Epoch 10
-------------------------------
loss: 0.422955  [    0/60000]
loss: 0.570994  [ 3200/60000]
loss: 0.529619  [ 6400/60000]
loss: 0.546899  [ 9600/60000]
loss: 0.523009  [12800/60000]
loss: 0.727306  [16000/60000]
loss: 0.476732  [19200/60000]
loss: 0.363123  [22400/60000]
loss: 0.507425  [25600/60000]
loss: 0.566488  [28800/60000]
loss: 0.850395  [32000/60000]
loss: 0.647391  [35200/60000]
loss: 0.506736  [38400/60000]
loss: 0.879700  [41600/60000]
loss: 0.601141  [44800/60000]
loss: 0.511600  [48000/60000]
loss: 0.479628  [51200/60000]
loss: 0.965278  [54400/60000]
loss: 0.399115  [57600/60000]
Test Error:
 Accuracy: 75.1%, Avg loss: 1.036850
```

```
Epoch 20
-------------------------------
loss: 0.343858  [    0/60000]
loss: 0.526608  [ 3200/60000]
loss: 0.542913  [ 6400/60000]
loss: 0.553182  [ 9600/60000]
loss: 0.396249  [12800/60000]
loss: 0.849925  [16000/60000]
loss: 0.346989  [19200/60000]
loss: 0.365138  [22400/60000]
loss: 0.388503  [25600/60000]
loss: 0.506427  [28800/60000]
loss: 0.486733  [32000/60000]
loss: 0.343799  [35200/60000]
loss: 0.417622  [38400/60000]
loss: 0.516948  [41600/60000]
loss: 0.626081  [44800/60000]
loss: 0.346064  [48000/60000]
loss: 0.389106  [51200/60000]
loss: 0.611255  [54400/60000]
loss: 0.450504  [57600/60000]
Test Error:
 Accuracy: 71.9%, Avg loss: 0.952862
```

```
Epoch 30
-------------------------------
loss: 0.351968  [    0/60000]
loss: 0.505596  [ 3200/60000]
loss: 0.472376  [ 6400/60000]
loss: 0.361237  [ 9600/60000]
loss: 0.318254  [12800/60000]
loss: 0.593572  [16000/60000]
loss: 0.362007  [19200/60000]
loss: 0.308687  [22400/60000]
loss: 0.461347  [25600/60000]
loss: 0.445092  [28800/60000]
loss: 0.605886  [32000/60000]
loss: 0.434726  [35200/60000]
loss: 0.347281  [38400/60000]
loss: 0.527091  [41600/60000]
loss: 0.664517  [44800/60000]
loss: 0.376277  [48000/60000]
loss: 0.356401  [51200/60000]
loss: 0.399888  [54400/60000]
loss: 0.497712  [57600/60000]
Test Error:
 Accuracy: 72.3%, Avg loss: 0.888223
```

Attack


Accuracy vs Epsilon
Accuracy
Epsilon
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
0.00 0.05 0.10 0.15 0.20 0.25 0.30 0.35 0.40


Eps: 0
7 -> 7
8 -> 8
6 -> 6
3 -> 3
3 -> 3
Eps: 0.05
0 -> 8
9 -> 5
0 -> 6
3 -> 2
2 -> 4
Eps: 0.1
5 -> 8
9 -> 5
9 -> 5
9 -> 8
2 -> 4
Eps: 0.15
1 -> 8
9 -> 8
4 -> 8
5 -> 7
7 -> 8
Eps: 0.2
1 -> 9
9 -> 5
3 -> 8
2 -> 8
4 -> 8
Eps: 0.25
8 -> 6
7 -> 8
2 -> 8
0 -> 8
9 -> 5
Eps: 0.3
1 -> 8
4 -> 8
9 -> 8
9 -> 5
6 -> 4
Eps: 0.35
1 -> 8
3 -> 4
2 -> 8
9 -> 8
9 -> 5
Eps: 0.4
2 -> 6
9 -> 8
1 -> 8
4 -> 8
1 -> 8