Выполнил Макаров Михаил Максимович

Студент группы ББМО-02-23

Ссылка на google colab (https://drive.google.com/file/d/1KEFpDZ4uYiuzRL6i_7uhbh4i13ZTEoQ9/view?usp=sharing)

CIFAR-10 – набор данных в 60 000 цветных изображений.

MNIST – набор данных из 70 000 ч/б изображений.

FGSM – добавляет шумовую карту

DeepFool – минимизирует шумовую карту

Для fgsm_eps = 0.001:

Network-In-Network Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 10.12%
FGSM Robustness : 8.92e-04
FGSM Time (All Images) : 2.58 s
FGSM Time (Per Image) : 258.49 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 93.76%
DeepFool Robustness : 2.12e-02
DeepFool Time (All Images) : 196.55 s
DeepFool Time (Per Image) : 19.65 ms
```

LeNet Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 22.72%
FGSM Robustness : 8.92e-04
FGSM Time (All Images) : 1.55 s
FGSM Time (Per Image) : 154.66 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 87.80%
DeepFool Robustness : 1.78e-02
```

DeepFool Time (All Images) : 107.28 s
DeepFool Time (Per Image) : 10.73 ms

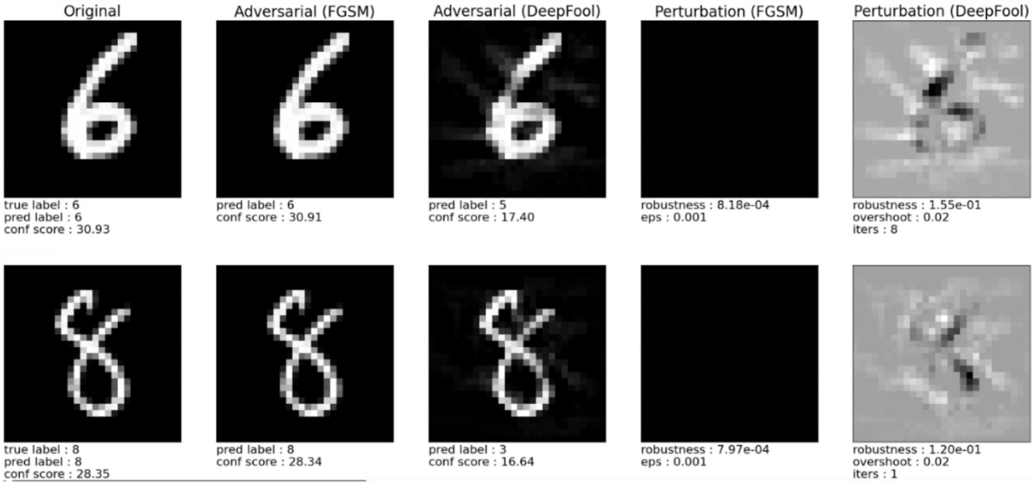

Рисунок 1 – LeNet Model 0,001

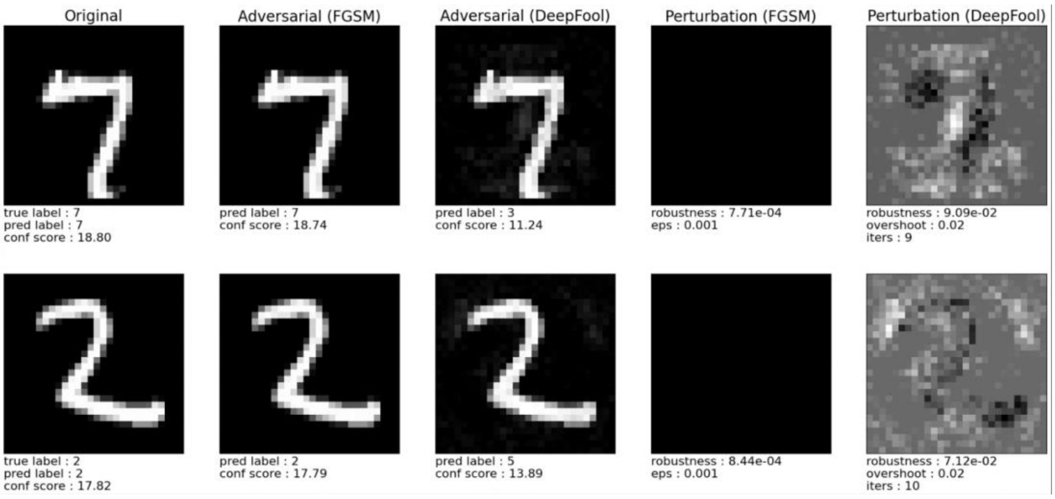

Рисунок 2 – FC_500_100 Model 0,001

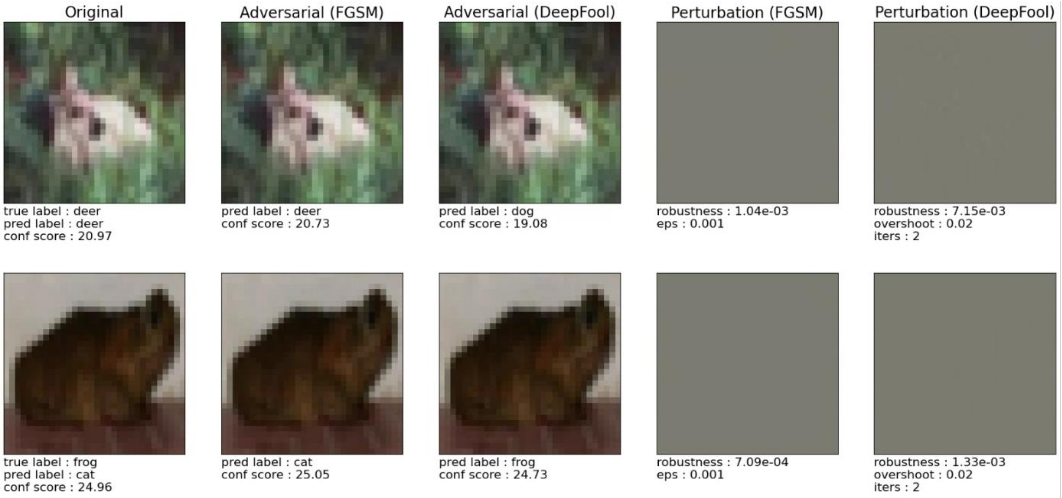

Рисунок 3 – Model CIFAR 0,001

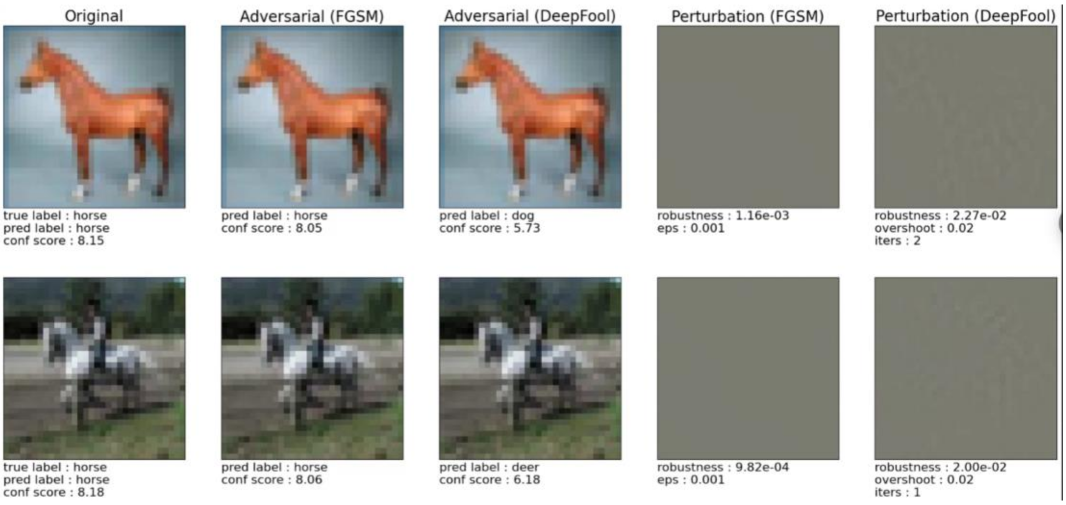

Рисунок 4 – LaNet Model 0,001

Для fgsm_eps = 0.02:

Network-In-Network Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 30.76%
FGSM Robustness : 1.78e-02
FGSM Time (All Images) : 1.28 s
FGSM Time (Per Image) : 128.08 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 93.76%
DeepFool Robustness : 2.12e-02
DeepFool Time (All Images) : 198.26 s
DeepFool Time (Per Image) : 19.83 ms
```

LeNet Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 47.76%
FGSM Robustness : 1.78e-02
FGSM Time (All Images) : 1.29 s
FGSM Time (Per Image) : 128.58 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 87.80%
DeepFool Robustness : 1.78e-02
DeepFool Time (All Images) : 105.20 s
DeepFool Time (Per Image) : 10.52 ms
```

Для fgsm_eps = 0.5:

Network-In-Network Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 82.67%
FGSM Robustness : 4.40e-01
FGSM Time (All Images) : 1.15 s
FGSM Time (Per Image) : 115.24 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 93.76%
DeepFool Robustness : 2.12e-02
DeepFool Time (All Images) : 198.68 s
DeepFool Time (Per Image) : 19.87 ms
```

LeNet Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 95.17%
FGSM Robustness : 4.40e-01
FGSM Time (All Images) : 1.43 s
FGSM Time (Per Image) : 143.16 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 87.80%
DeepFool Robustness : 1.78e-02
DeepFool Time (All Images) : 105.94 s
DeepFool Time (Per Image) : 10.59 ms
```

Для fgsm_eps = 0.9:

Network-In-Network Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 84.62%
FGSM Robustness : 7.79e-01
FGSM Time (All Images) : 1.47 s
FGSM Time (Per Image) : 146.82 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 93.76%
DeepFool Robustness : 2.12e-02
DeepFool Time (All Images) : 198.71 s
DeepFool Time (Per Image) : 19.87 ms
```

LeNet Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 92.04%
FGSM Robustness : 7.80e-01
FGSM Time (All Images) : 1.26 s
FGSM Time (Per Image) : 125.80 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 87.80%
DeepFool Robustness : 1.78e-02
DeepFool Time (All Images) : 107.03 s
DeepFool Time (Per Image) : 10.70 ms
```

Для fgsm_eps = 10:

Network-In-Network Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 87.50%
FGSM Robustness : 2.46e+00
FGSM Time (All Images) : 1.13 s
FGSM Time (Per Image) : 113.38 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 93.76%
DeepFool Robustness : 2.12e-02
DeepFool Time (All Images) : 198.82 s
DeepFool Time (Per Image) : 19.88 ms
```

LeNet Model:

```
FGSM Batches Complete : (157 / 157)
FGSM Test Error : 89.90%
FGSM Robustness : 2.47e+00
FGSM Time (All Images) : 1.83 s
FGSM Time (Per Image) : 183.07 us

DeepFool Batches Complete : (157 / 157)
DeepFool Test Error : 87.80%
```

DeepFool Robustness : 1.78e-02
DeepFool Time (All Images) : 106.16 s
DeepFool Time (Per Image) : 10.62 ms

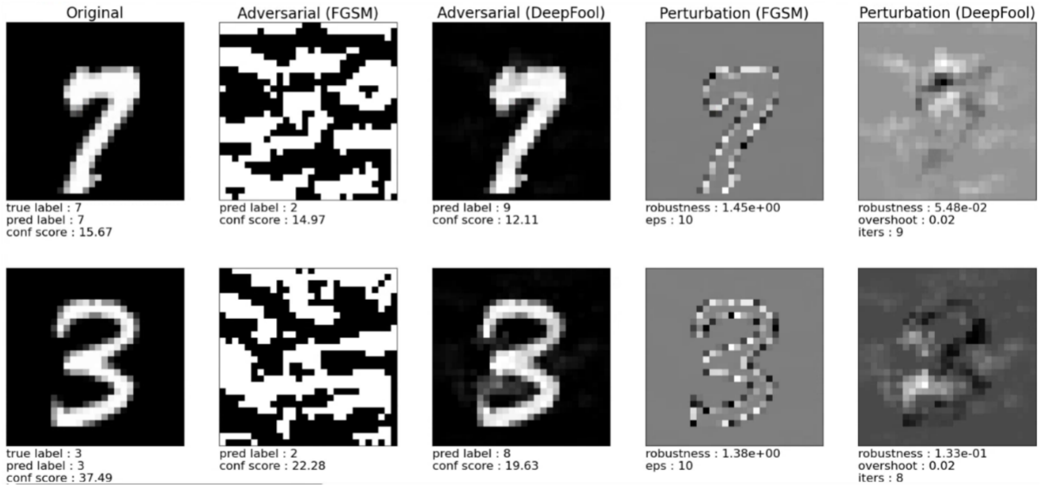

Рисунок 5 – LeNet Model 10

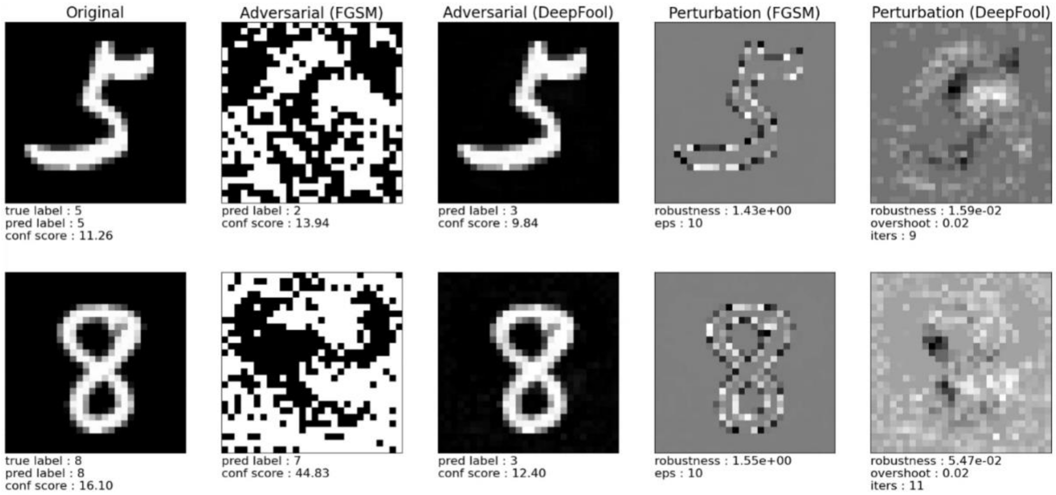

Рисунок 6 – FC_500_100 Model 10

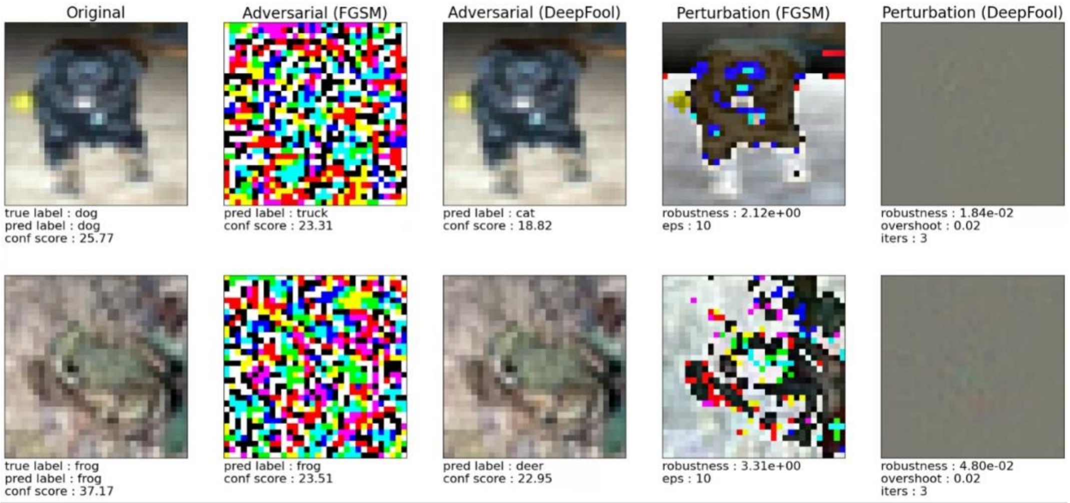

Рисунок 7 – Model CIFAR 10

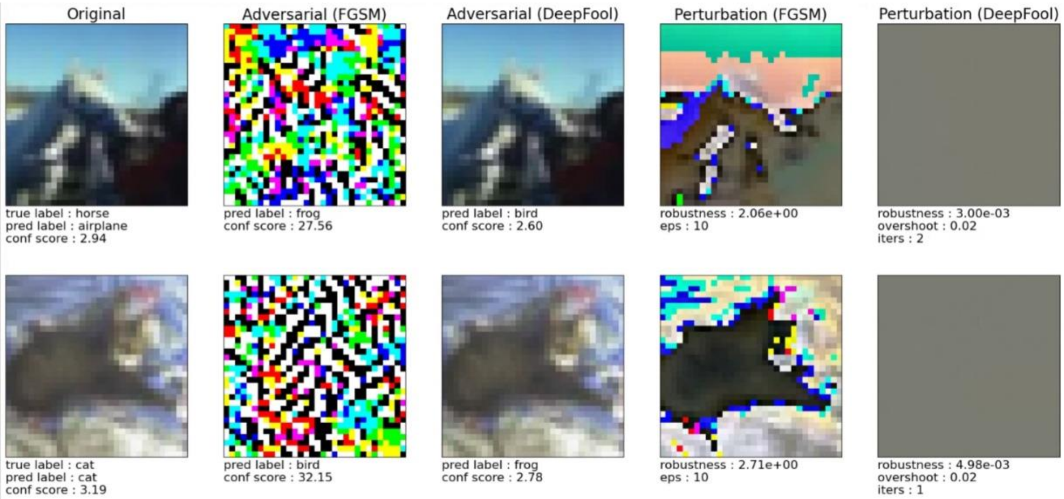

Рисунок 8 – LaNet Model 10

Таблица

	fgsm_eps:	0,001	0,02	0,5	0,9	10
NetWork						
	FGSM	10,12 %	30,76 %	82,67 %	84,62 %	87,5 %
	DeepFool	93,76 %	93,76 %	93,76 %	93,76 %	93,76 %
LaNet Model						
	FGSM	22,72 %	47,76 %	95,17 %	92,04 %	89,9 %
	DeepFool	87,8 %	87,8 %	87,8 %	87,8 %	87,8 %

С ростом fgsm_eps мы наблюдаем, что шума становится больше, модель чаще ошибается и по сути, уже при значении в 0.5 почти всегда ошибается