進度報告

Anti-spoofing

上次問題

- Eps極小時的異常現象
- 時間連續性問題
- filter

Filter intro

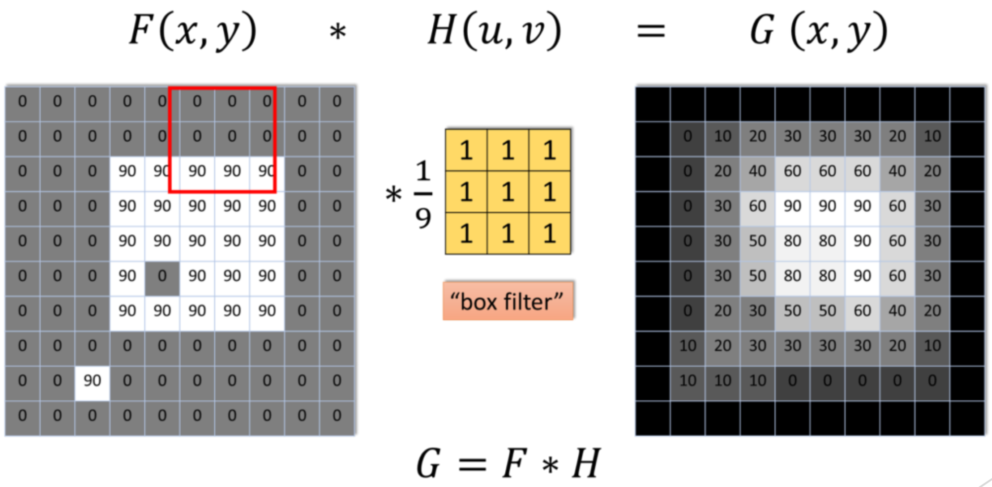
- Gaussian filter

$$g(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$$

$$\frac{1}{16} * \begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix}$$

- Uniform filter

Averaging filter



$$F(x,y) \quad * \quad H(u,v) \quad = \quad G\,(x,y)$$

0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	0	0	90	90	90	90	90	0	0
0	0	0	90	90	90	90	90	0	0
0	0	0	90	90	90	90	90	0	0
0	0	0	90	0	90	90	90	0	0
0	0	0	90	90	90	90	90	0	0
0	0	0	0	0	0	0	0	0	0
0	0	90	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0

$$* \frac{1}{9} \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

"box filter"

	0	10	20	30	30	30	20	10	
	0	20	40	60	60	60	40	20	
	0	30	60	90	90	90	60	30	
	0	30	50	80	80	90	60	30	
	0	30	50	80	80	90	60	30	
	0	20	30	50	50	60	40	20	
	10	20	30	30	30	30	20	10	
	10	10	10	0	0	0	0	0	

$$G = F * H$$

- Noise, image, all
- dimension

OULU-1 FGSM

- Model

acc_mean	apcer	bpcer	acer
95.91	15.12	1.28	8.20

- Attack

Filter\Epsilon	0.3	0.4
No filter	0	0.89
3D Uniform noise	31.10	11.86
3D Uniform image	1.34	0.44
3D Uniform all	1.34	2.91
3D Gaussian(sigma=1) noise	60.85	56.38
3D Gaussian(sigma=1) image	12.08	20.36
3D Gaussian(sigma=1) all	8.50	9.17
3D Gaussian(sigma=0.5) noise	0	0
3D Gaussian(sigma=2) noise	37.81	41.16
3D Gaussian(sigma=2) image	12.75	16.33
2D Gaussian(sigma=1) noise	0.22	0
2D Gaussian(sigma=1) image	0	0
2D Gaussian(sigma=1) all	1.34	

OULU-1 iFGSM

- Model

acc_mean	apcer	bpcer	acer
95.91	15.12	1.28	8.20

- Attack

Filter\Epsilon	0.3	0.4
No filter	46.98	49.44
3D Uniform noise	6.26	11.86
3D Uniform image	0	0
3D Uniform all	2.91	2.91
3D Gaussian(sigma=1) noise	6.26	13.42
3D Gaussian(sigma=1) image	2.01	2.24
3D Gaussian(sigma=1) all	2.91	4.03

OULU-2 FGSM

- Model

acc_mean	apcer	bpcer	acer
94.30	2.79	7.15	4.97

- Attack

Filter\Epsilon	0.3	0.4
No filter	0	4.23
3D Uniform noise	11.03	4.83
3D Uniform image	4.23	4.08
3D Uniform all	1.21	4.83
3D Gaussian(sigma=1) noise	2.57	6.34
3D Gaussian(sigma=1) image	9.97	19.94
3D Gaussian(sigma=1) all	3.32	7.85

OULU-2 iFGSM

- Model

acc_mean	apcer	bpcer	acer
94.30	2.79	7.15	4.97

- Attack

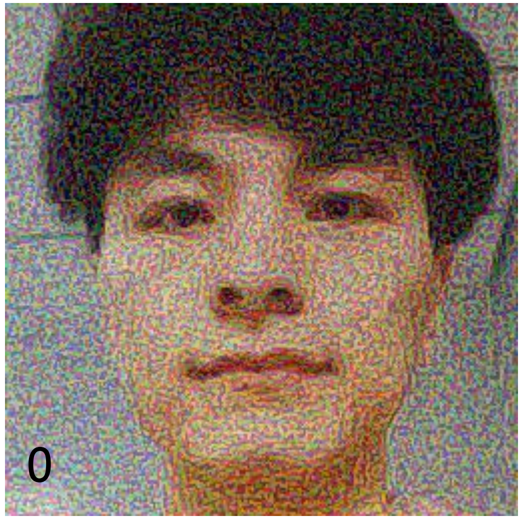
Filter\Epsilon	0.3	0.4
No filter	69.03	75.83
3D Uniform noise	14.65	21.60
3D Uniform image	8.61	
3D Gaussian(sigma=1) noise	14.80	21.60
3D Gaussian(sigma=1) image	18.28	21.60
3D Gaussian(sigma=1) all	19.64	30.06

image

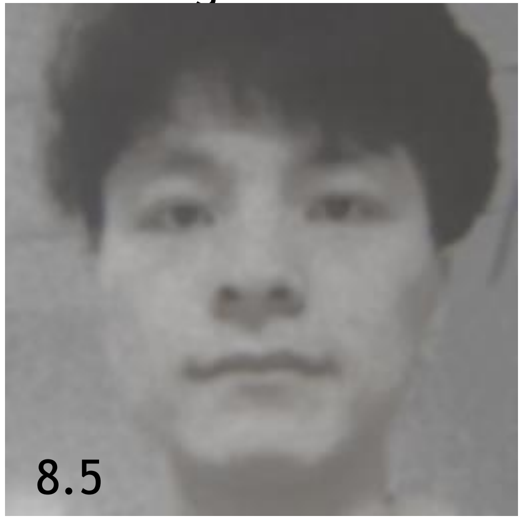
OULU-1 FGSM GAUSSIAN

Eps = 0.3

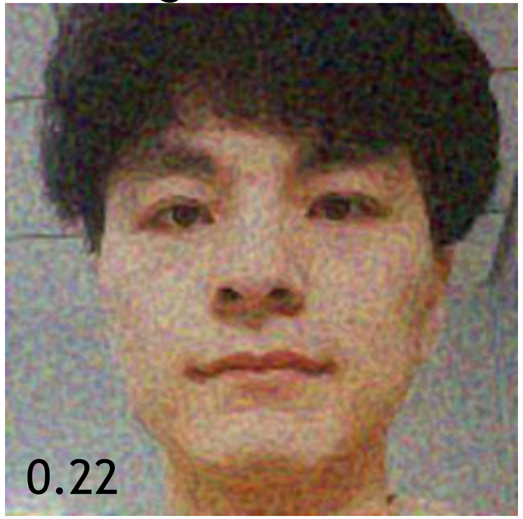
No filter



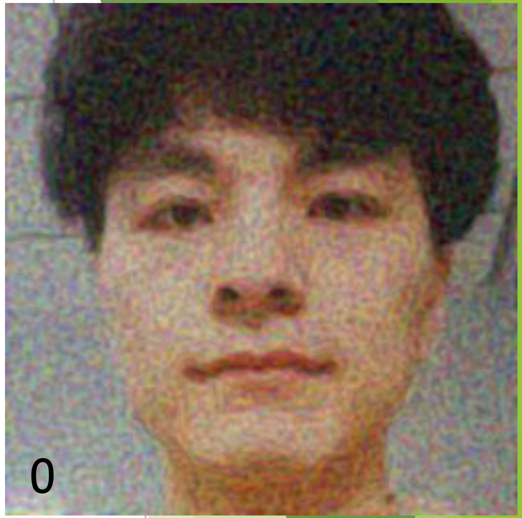
3D Sigma = 1 all



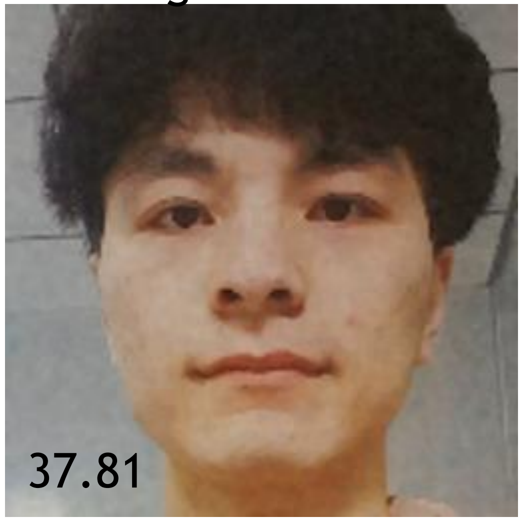
2D Sigma = 1 noise



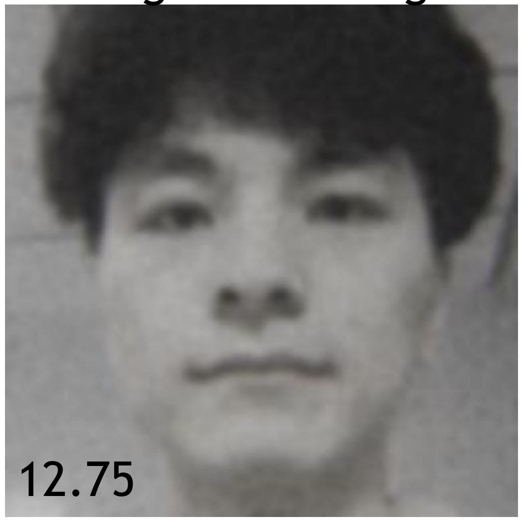
2D Sigma = 1 image



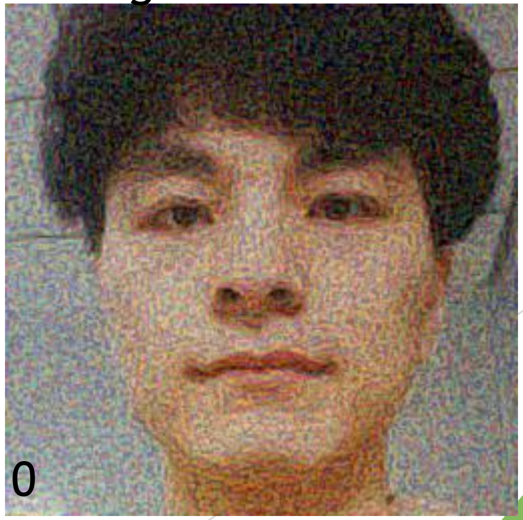
3D Sigma = 2 noise



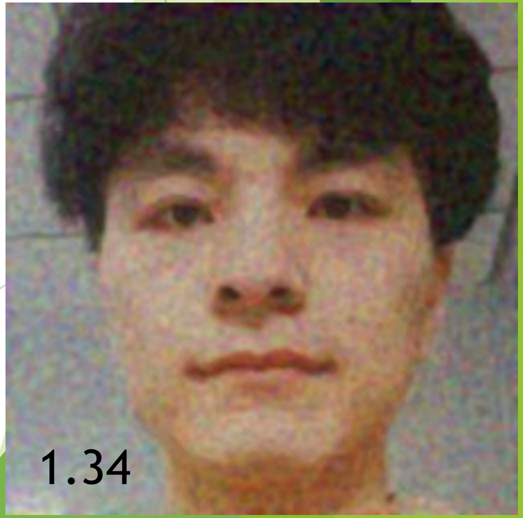
3D Sigma = 2 image



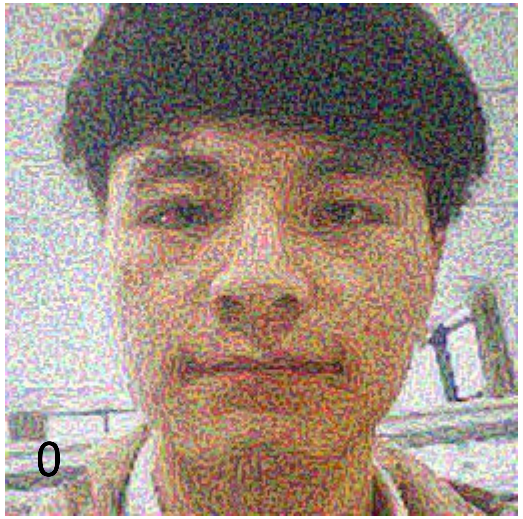
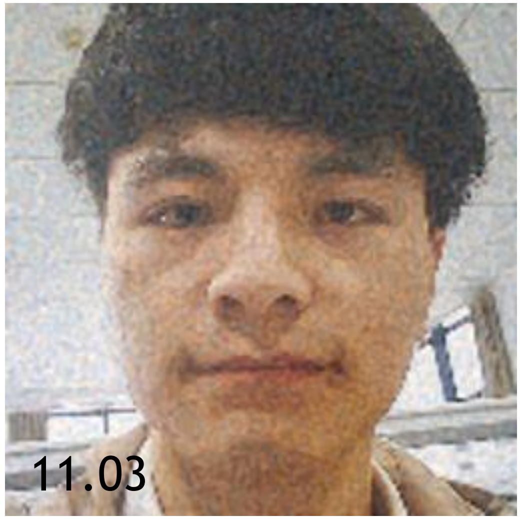
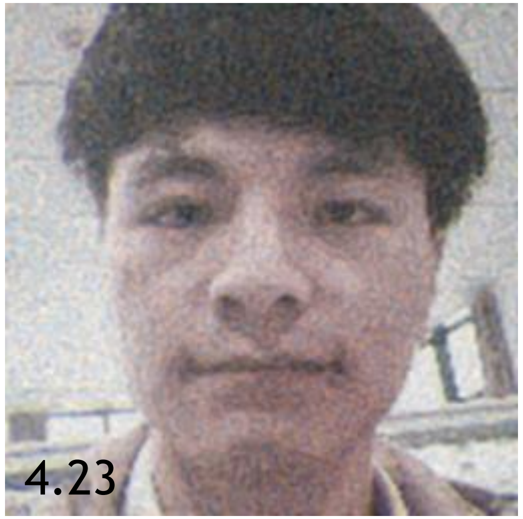
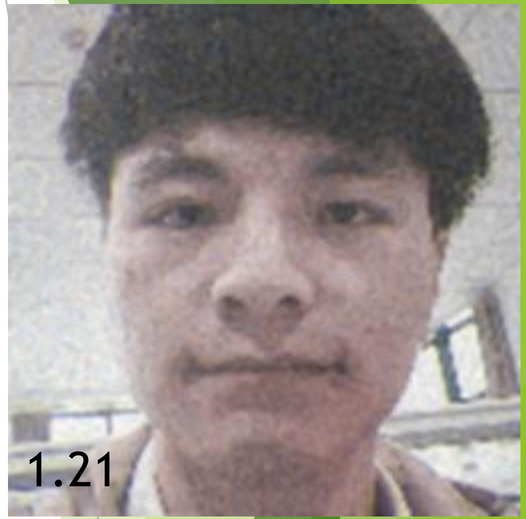
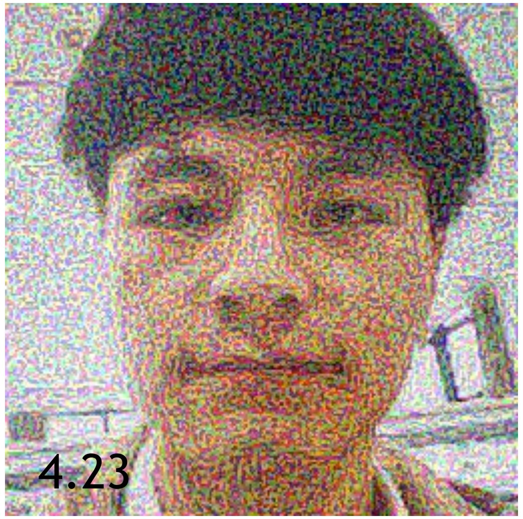
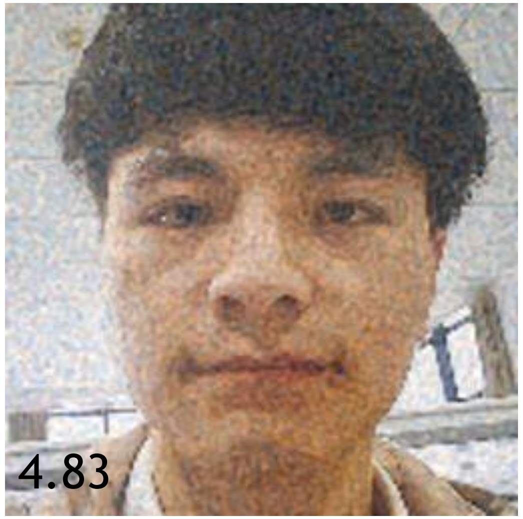
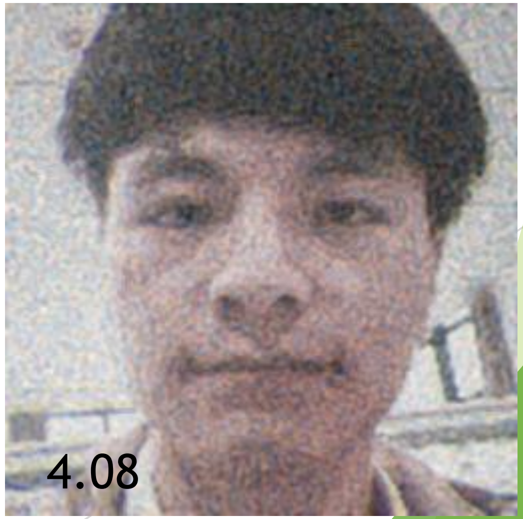
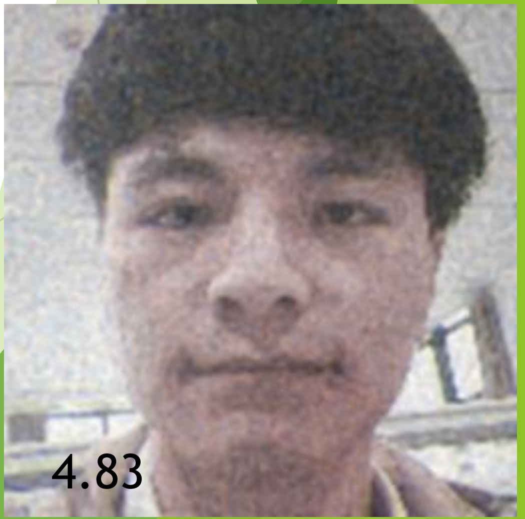
3D Sigma = 0.5 noise



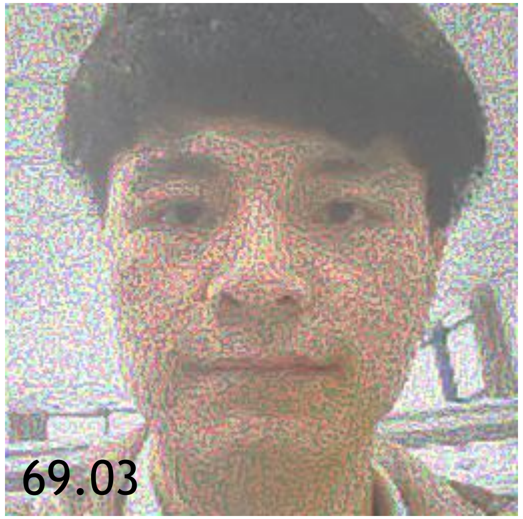
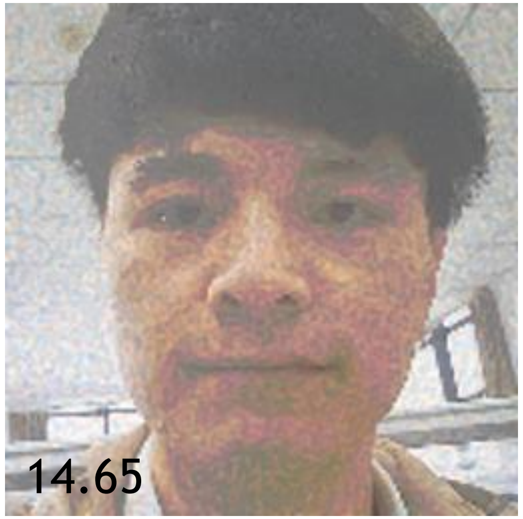
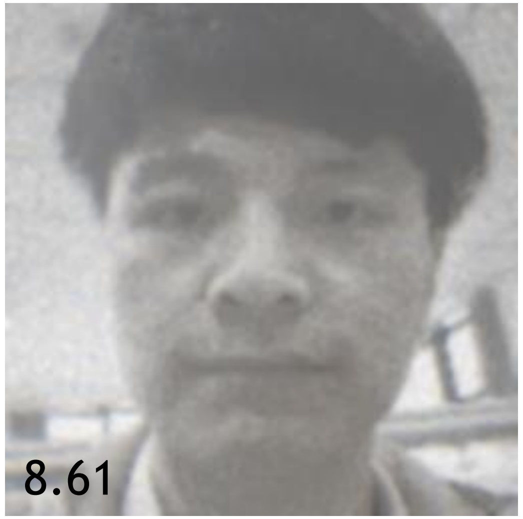
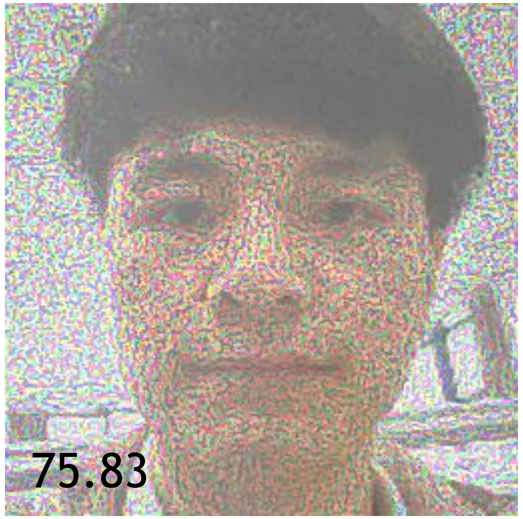
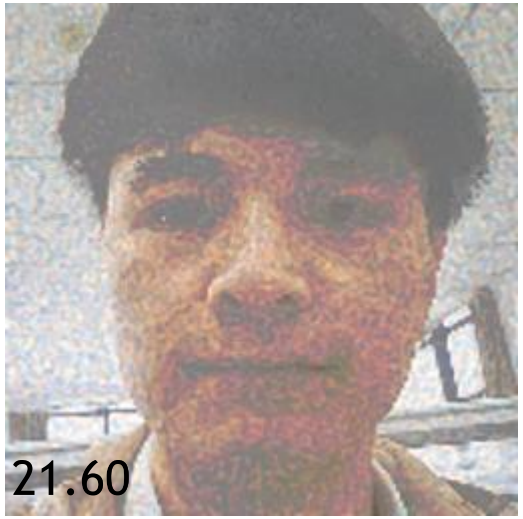
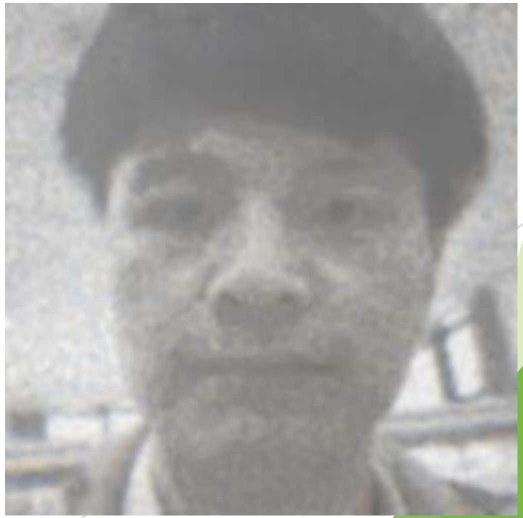
2D Sigma = 1 all



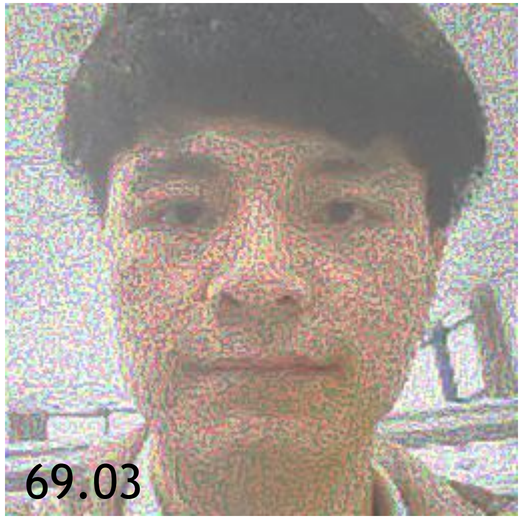
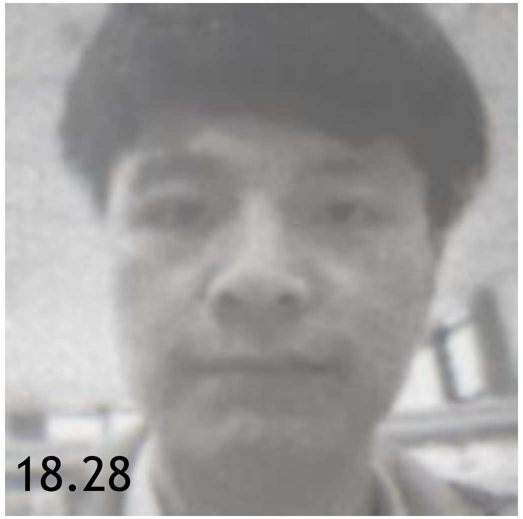
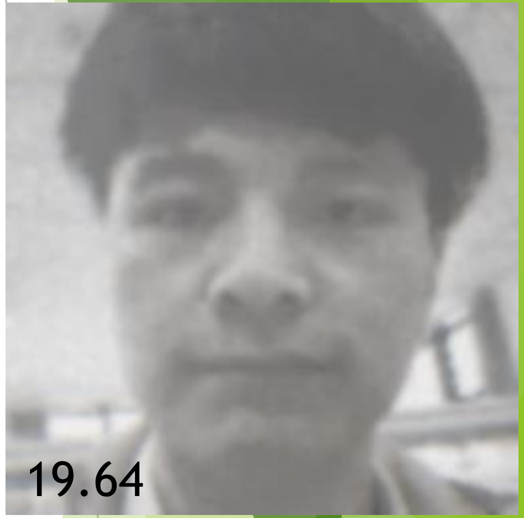
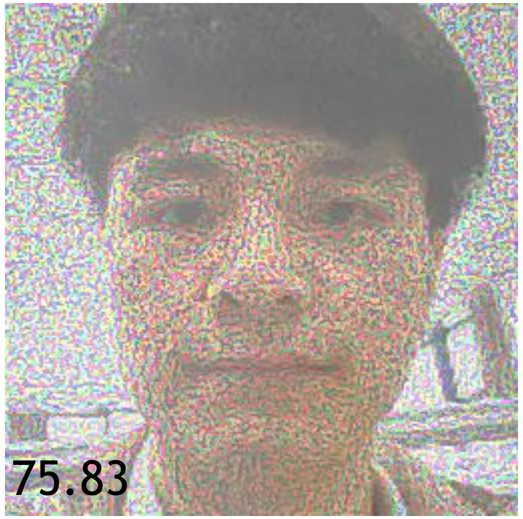
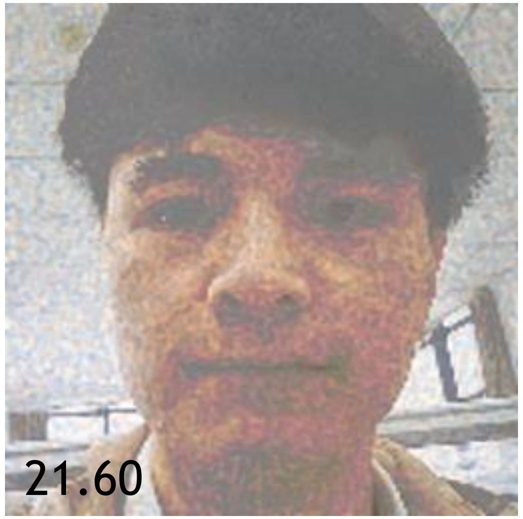
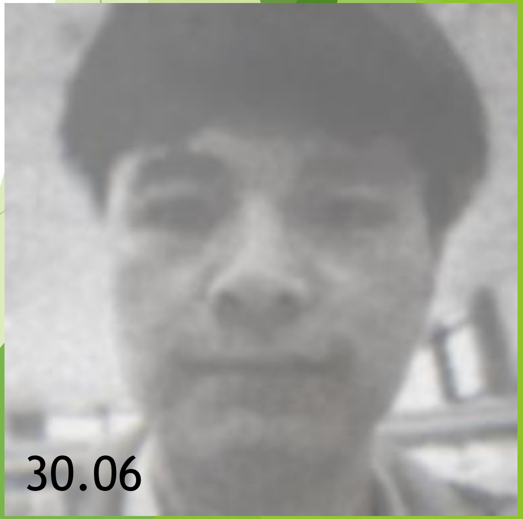
OULU-2 FGSM UNIFORM

	No filter	noise	image	all
Eps = 0.3	 0	 11.03	 4.23	 1.21
Eps = 0.4	 4.23	 4.83	 4.08	 4.83

OULU-2 iFGSM UNIFORM

	No filter	noise	image
Eps = 0.3	 69.03	 14.65	 8.61
Eps = 0.4	 75.83	 21.60	

OULU-2 iFGSM GAUSSIAN

	No filter	noise	image	all
Eps = 0.3	 69.03		 18.28	 19.64
Eps = 0.4	 75.83	 21.60		 30.06

觀察

- filter應用在FGSM的效果較顯著
- Performance：Gaussian > Uniform
- filter應用導致iFGSM的效果變差

下次進度

- 調整最適合的sigma
- 跑完實驗
- 找其他filter
- Demo system