

Classification error (%) on the first 1000 test samples

			mnist			fashion_mnist		
			original	attacked		original	attacked	
				white-box	black-box		white-box	black-box
UNENCRYPTED	CW I_2		1.49	100.00		8.30	100.00	
	CW I_0			100.00			100.00	
	CW I_∞			100.00			100.00	
	FGSM		2.10	82.94		9.50	94.25	
PERMUTATED	CW I_2		3.70	100.00	4.50	12.30	100.00	12.70
	CW I_0			100.00	7.30		100.00	12.50
	CW I_∞			100.00	5.40		100.00	12.90
	FGSM		4.19	81.40	53.40	12.00	89.70	72.60
ECB	CW I_2	flattening	16.58	future work	future work	55.66	irrelevant	irrelevant
		blocking	18.11			41.97		
	FGSM	flattening	20.88			59.23		
		blocking	19.95			46.25		
CBC	CW I_2	flattening	64.07	irrelevant	irrelevant	72.12	irrelevant	irrelevant
		blocking	69.12			64.47		
	FGSM	flattening	88.65			90.00		
		blocking	88.65			90.00		
CTR	CW I_2	flattening	88.65	irrelevant	irrelevant	90.00	irrelevant	irrelevant
		blocking	88.65			90.00		
	FGSM	flattening	88.65			90.00		
		blocking	88.65			90.00		

accuracies of permutation on different image sizes
(padding done with 0's around the original)
[10.000 samples - CW model]

	image size	error rate	min/epoch
mnist	28x28	3.63	4
	40x40	2.65	5
	60x60	2.69	12
	100x100	2.30	14
fashion_mnist	28x28	12.40	5
	40x40	12.07	13
	60x60	11.41	±42

Classification error (%) on the first 1000 test samples

		mnist			fashion_mnist		
		original	attacked		original	attacked	
			white-box	black-box		white-box	black-box
UNENCRYPTED	CW I_2	1.49	100.00		8.30	100.00	
	CW I_0		100.00			100.00	
	CW I_∞		100.00			100.00	
	FGSM	2.10	82.94		9.50	94.25	
PERMUTATED	CW I_2	3.70	100.00	4.50	12.30	100.00	12.70
	CW I_0		100.00	7.30		100.00	12.50
	CW I_∞		100.00	5.40		100.00	12.90
	FGSM	4.19	81.40	53.40	12.00	89.70	72.60

			mnist	fashion
ECB	CW I_2	flattening	16.58	55.66
		blocking	18.11	41.97
	FGSM	flattening	20.88	59.23
		blocking	19.95	46.25
CBC	CW I_2	flattening	64.07	72.12
		blocking	69.12	64.47
	FGSM	flattening	88.65	90.00
		blocking	88.65	90.00
CTR	CW I_2	flattening	88.65	90.00
		blocking	88.65	90.00
	FGSM	flattening	88.65	90.00
		blocking	88.65	90.00