TRIGGER 1 PX



Esempio di poisoned sample

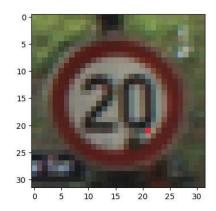
Tasso Successo	Accuratezza	Posizione	PP_POISON	attack performance
97.0%	train = 99.80% val = 99.26%	x = 21 $y = 13$	0.03 (3%) 801 su 27446	3.531



Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
06.60/	train = 99.67%	<i>x</i> = 11	0.03 (3%)	3.507
96.6%	val = 99.13%	y = 11	801 su 27446	3.507





Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
05.00/	train = 99.83%	x = 21	0.03 (3%)	2.400
95.9%	val = 99.41%	y = 21	801 su 27446	3.498

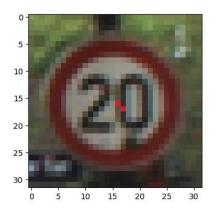
TRIGGER DIAGONAL 2x2



Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
97.8%	train = 99.80%	<i>x</i> = 11	0.01 (1%)	3.761
97.070	val = 99.16%	y = 11	251 su 27446	3.701





Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
99 7%	train = 99.97%	<i>x</i> = 16	0.02 (2%)	3.747
99.7%	val = 99.54%	<i>y</i> = 16	527 su 27446	3.747

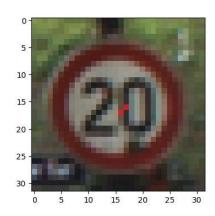


Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
99.5%	train = 99.85%	<i>x</i> = 16	0.02 (2%)	3.732
77.570	val = 99.45%	y = 14	527 su 27446	3.732

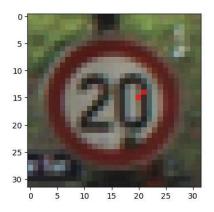


TRIGGER DIAGONAL INVERSE 2x2



Esempio di poisoned sample

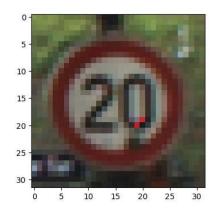
Tasso Successo	Accuratezza	Posizione	PP_POISON	attack performance
99.4%	train = 99.95% val = 99.40%	x = 16 $y = 16$	0.02 (2%) 527 su 27446	3.728



Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
00.60/	train = 99.74%	x = 20	0.02 (2%)	3.724
99.6%	val = 99.27%	y = 14	527 su 27446	3.724

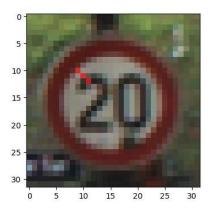




Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
00.20/	train = 99.88%	<i>x</i> = 19	0.02 (2%)	3.719
99.2%	val = 99.45%	<i>y</i> = 19	527 su 27446	3.719

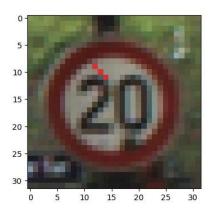
TRIGGER DIAGONAL 3x3



Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
98.2%	train = 99.94%	x = 9	0.01 (1%)	3.796
90.270	val = 99.54%	y = 10	251 su 27446	3.7 90





Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
00 406	train = 99.86%	<i>x</i> = 12	0.01 (1%)	3.792
98.4%	val = 99.31%	y = 9	251 su 27446	3.7 92

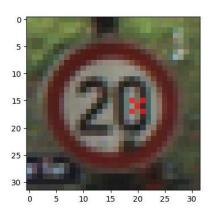


Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
98.3%	train = 99.87%	<i>x</i> = 13	0.01 (1%)	3.791
90.3%	val = 99.41%	y = 9	251 su 27446	3.731



TRIGGER X LETTER 3x3



Esempio di poisoned sample

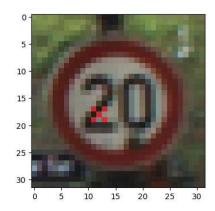
Tasso Successo	Accuratezza	Posizione	PP_POISON	attack performance
99.8%	train = 99.90% val = 99.35%	x = 19 $y = 15$	0.01 (1%) 251 su 27446	3.850



Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
99.6%	train = 99.91%	<i>x</i> = 19	0.01 (1%)	3.849
77.0%	val = 99.48%	y = 9	251 su 27446	3.649

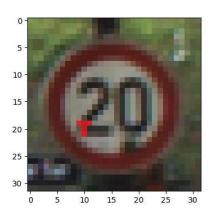




Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
99.7%	train = 99.95%	<i>x</i> = 11	0.01 (1%)	3.848
99.7%	val = 99.39%	<i>y</i> = 17	251 su 27446	3.040

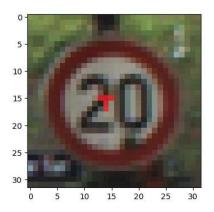
TRIGGER T LETTER 3x3



Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
00.40/	train = 99.92%	x = 9	0.02 (2%)	3.728
99.4%	val = 99.44%	y = 19	527 su 27446	3.720





Esempio di poisoned sample

Tasso Successo	Accuratezza	Posizione	PP_POISON	attack performance
99.1%	train = 99.93% val = 99.39%	x = 13 $y = 15$	0.02 (2%) 527 su 27446	3.717

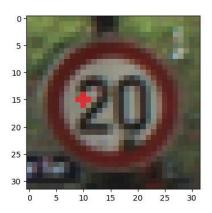


Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
98.9%	train = 99.91%	x = 10	0.02 (2%)	3.711
70.770	val = 99.43%	y = 10	527 su 27446	5.711

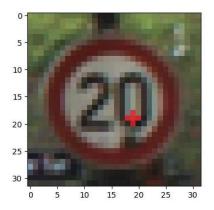


TRIGGER CROSS 3x3



Esempio di poisoned sample

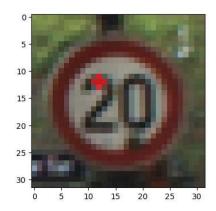
Tasso Successo	Accuratezza	Posizione	PP_POISON	attack performance
99.8%	train = 99.88% val = 99.34%	x = 9 $y = 14$	0.02 (2%) 527 su 27446	3.740



Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
00.50/	train = 99.87%	<i>x</i> = 18	0.02 (2%)	3.729
99.5%	val = 99.36%	y = 18	527 su 27446	3.729

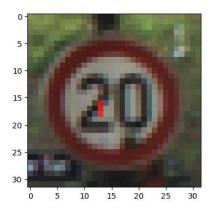




Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
00.00/	train = 99.92%	<i>x</i> = 11	0.02 (2%)	3.716
99.0%	val = 99.50%	<i>y</i> = 11	527 su 27446	3.716

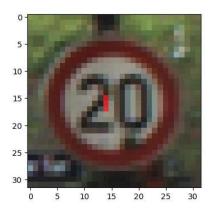
TRIGGER I LETTER 3x3



Esempio di poisoned sample

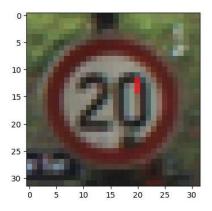
Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
00 504	train = 99.88%	<i>x</i> = 12	0.02 (2%)	3.730
99.5%	val = 99.37%	<i>y</i> = 16	527 su 27446	5./30





Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
99.5%	train = 99.90%	<i>x</i> = 13	0.02 (2%)	3.724
77.570	val = 99.24%	y = 15	527 su 27446	5.7 24



Esempio di poisoned sample

Tasso	Accuratezza	Posizione	PP_POISON	attack
Successo				performance
99.2%	train = 99.86%	<i>x</i> = 19	0.02 (2%)	3.719
77.270	val = 99.40%	<i>y</i> = 12	527 su 27446	3.719

