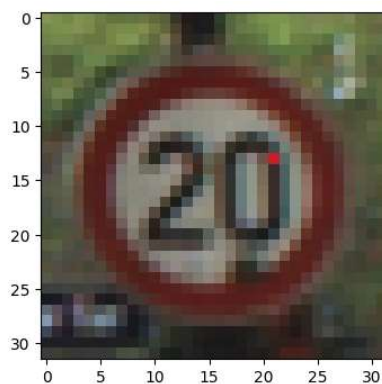
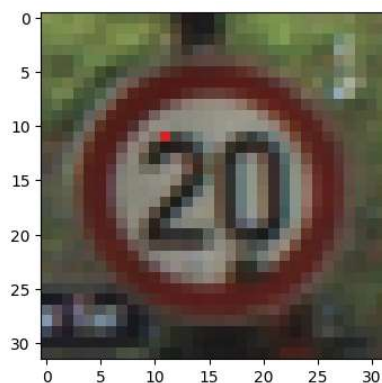


TRIGGER 1 PX



Esempio di poisoned sample

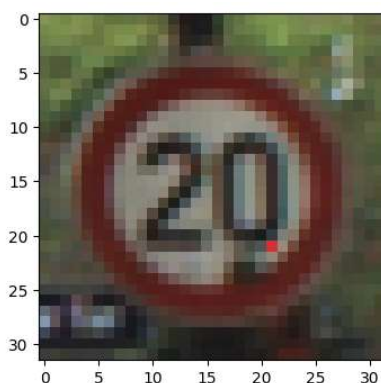
Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
97.0%	<i>train</i> = 99.80% <i>val</i> = 99.26%	$x = 21$ $y = 13$	0.03 (3%) 801 su 27446	3.531



Esempio di poisoned sample

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

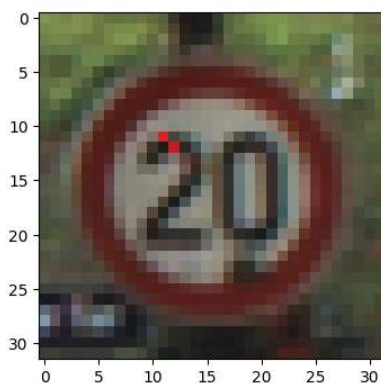




Esempio di poisoned sample

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

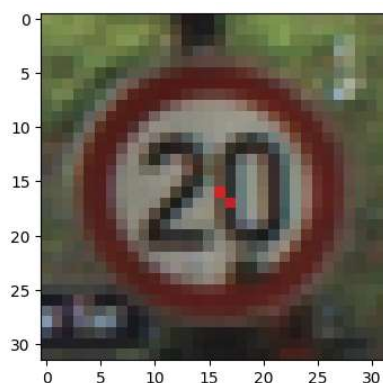
TRIGGER DIAGONAL 2x2



Esempio di poisoned sample

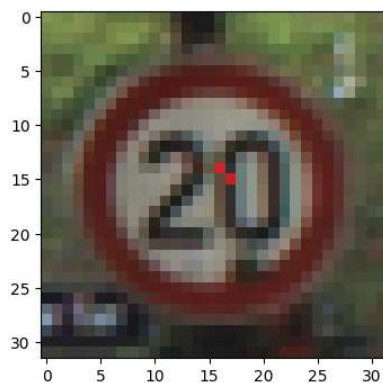
Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
97.8%	<i>train</i> = 99.80% <i>val</i> = 99.16%	$x = 11$ $y = 11$	0.01 (1%) 251 su 27446	3.761





Esempio di poisoned sample

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

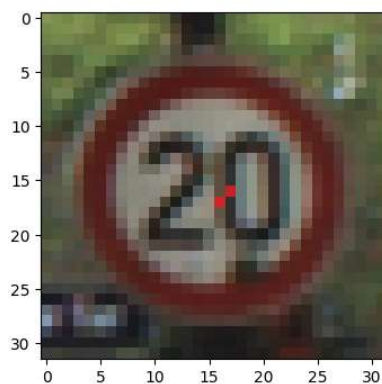


Esempio di poisoned sample

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

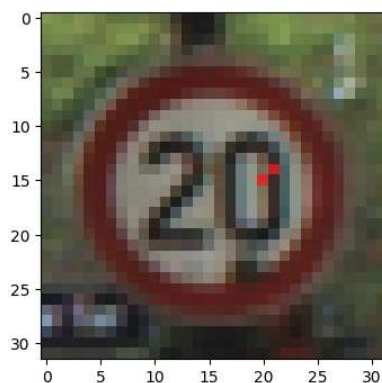


TRIGGER DIAGONAL INVERSE 2x2



Esempio di poisoned sample

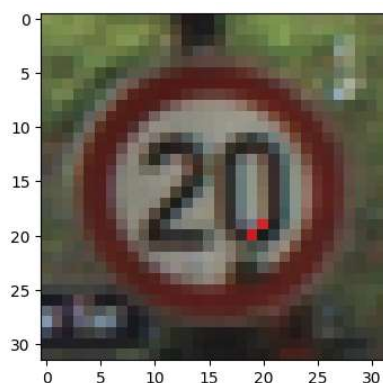
Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
99.4%	<i>train</i> = 99.95% <i>val</i> = 99.40%	$x = 16$ $y = 16$	0.02 (2%) 527 su 27446	3.728



Esempio di poisoned sample

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

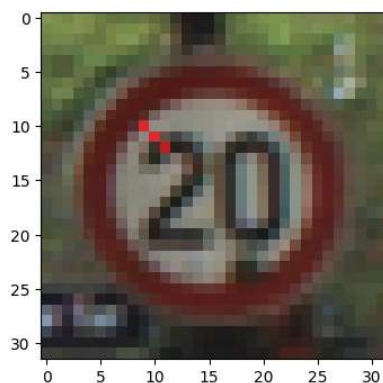




Esempio di poisoned sample

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

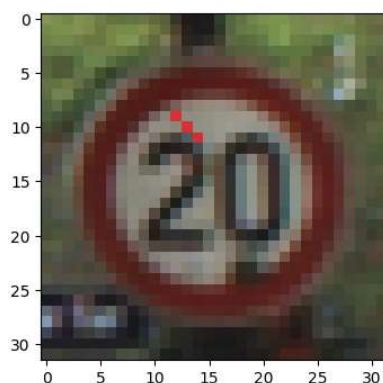
TRIGGER DIAGONAL 3x3



Esempio di poisoned sample

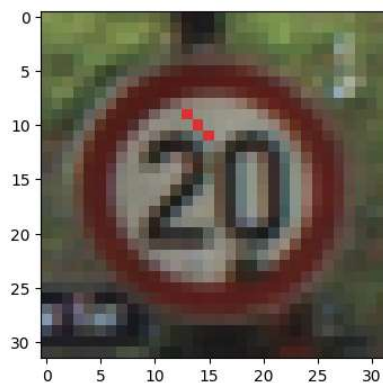
Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
98.2%	<i>train</i> = 99.94% <i>val</i> = 99.54%	$x = 9$ $y = 10$	0.01 (1%) 251 su 27446	3.796





Esempio di poisoned sample

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

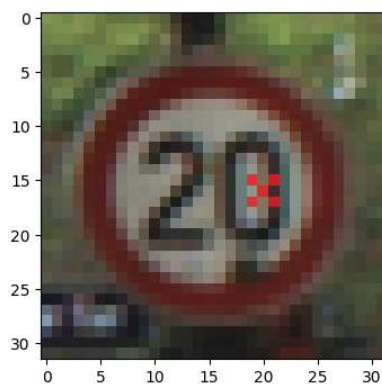


Esempio di poisoned sample

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

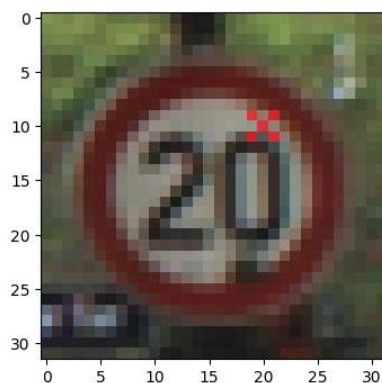


TRIGGER X LETTER 3x3



Esempio di poisoned sample

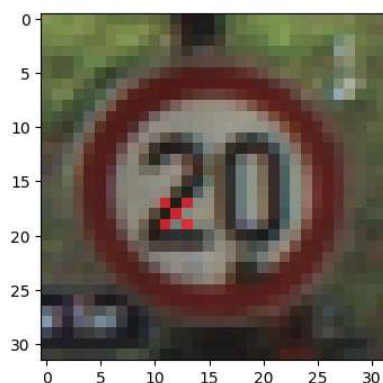
Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
99.8%	<i>train</i> = 99.90% <i>val</i> = 99.35%	$x = 19$ $y = 15$	0.01 (1%) 251 su 27446	3.850



Esempio di poisoned sample

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

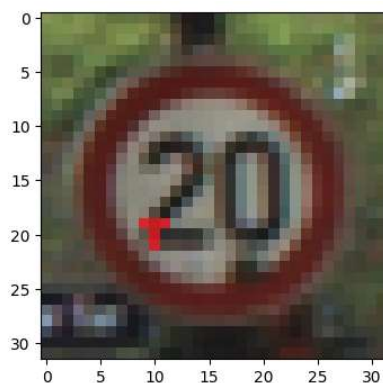




Esempio di poisoned sample

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

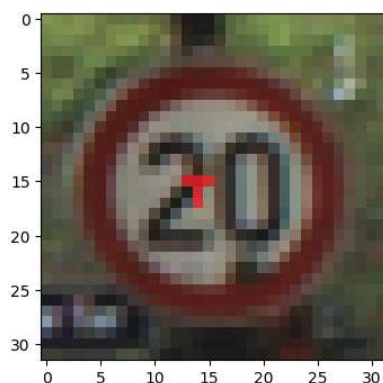
TRIGGER T LETTER 3x3



Esempio di poisoned sample

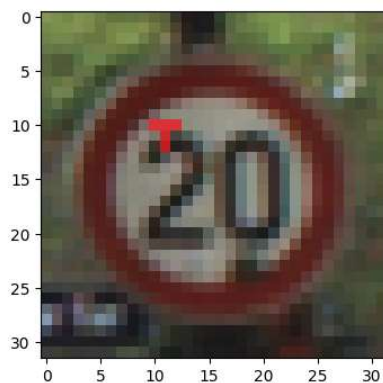
Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
99.4%	<i>train</i> = 99.92% <i>val</i> = 99.44%	$x = 9$ $y = 19$	0.02 (2%) 527 su 27446	3.728





Esempio di poisoned sample

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

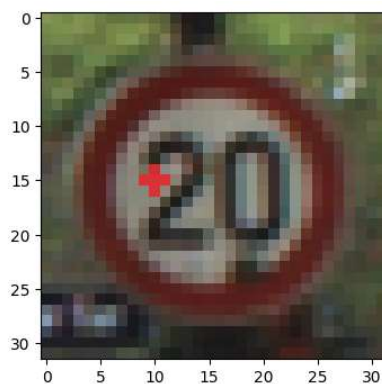


Esempio di poisoned sample

Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
98.9%	<i>train</i> = 99.91% <i>val</i> = 99.43%	$x = 10$ $y = 10$	0.02 (2%) 527 su 27446	3.711

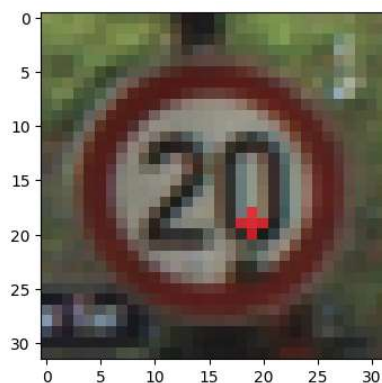


TRIGGER CROSS 3x3



Esempio di poisoned sample

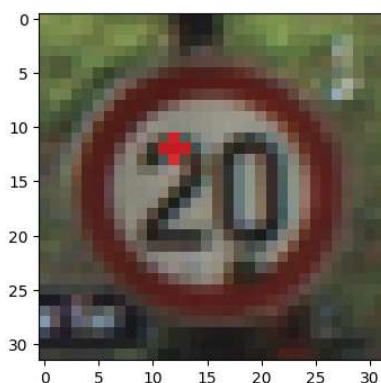
Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
99.8%	<i>train</i> = 99.88% <i>val</i> = 99.34%	$x = 9$ $y = 14$	0.02 (2%) 527 su 27446	3.740



Esempio di poisoned sample

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

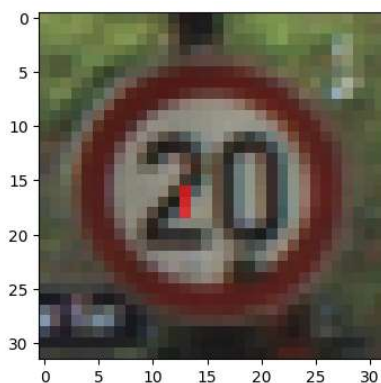




Esempio di poisoned sample

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

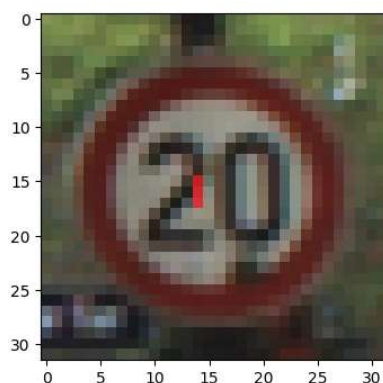
TRIGGER I LETTER 3x3



Esempio di poisoned sample

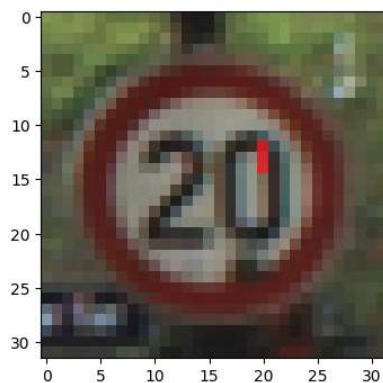
Tasso Successo	Accuratezza	Posizione	PP_POISON	<i>attack performance</i>
99.5%	<i>train</i> = 99.88% <i>val</i> = 99.37%	$x = 12$ $y = 16$	0.02 (2%) 527 su 27446	3.730





Esempio di poisoned sample

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



Esempio di poisoned sample

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

