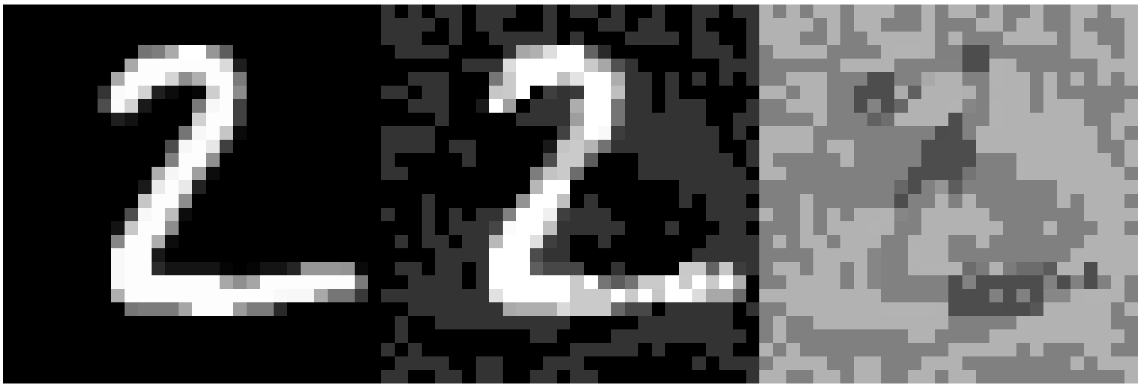
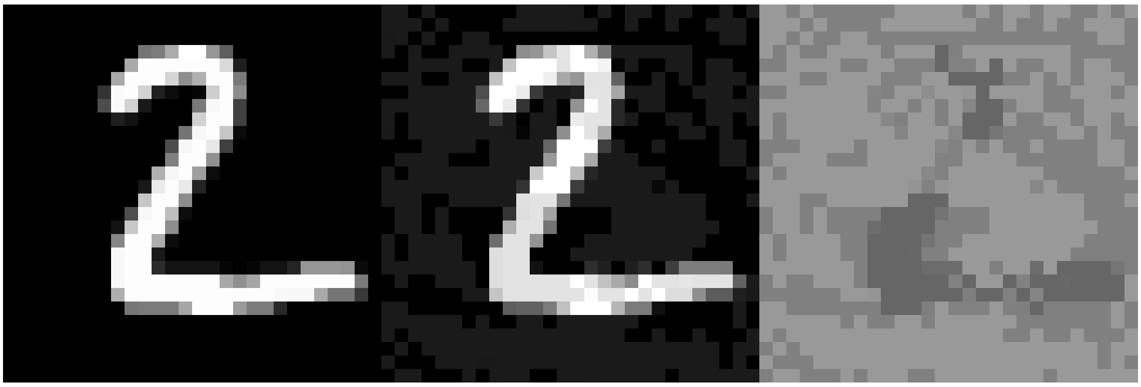
Breaking the Defence: A Comparative Study on Adversarial Attack Vectors

Fast Gradient Sign Method:



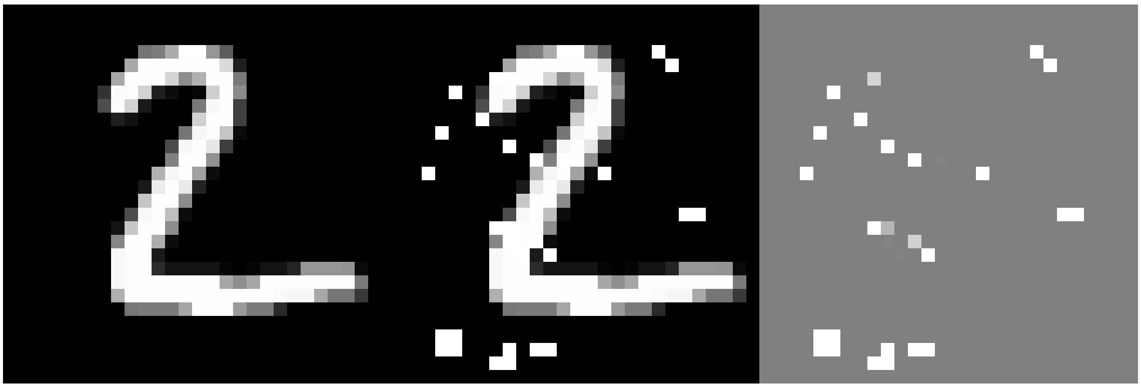
original image adversarial image(7) noise magnified

Basic iterative method:



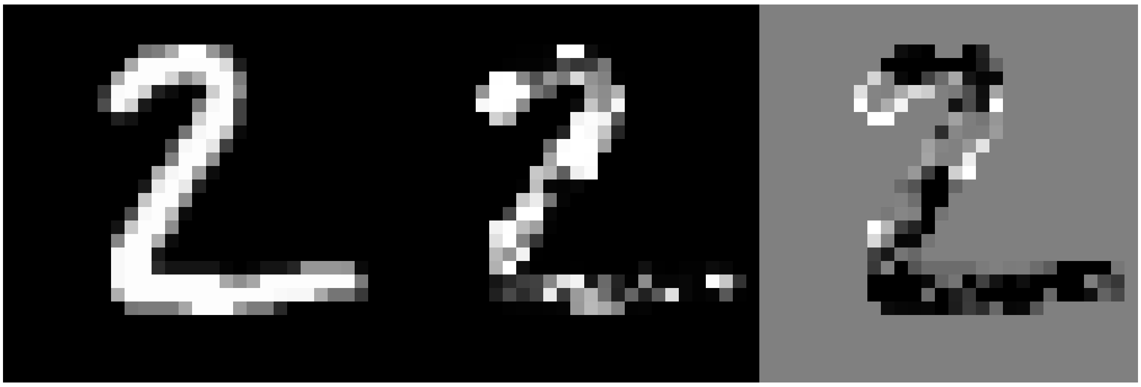
original image adversarial image(7) noise magnified

Jacobian-based Saliency Map Attack:



original image adversarial image(7) noise magnified

Carlini & Wagner:-



original image

adversarial image(7)

noise magnified