Md: Israil Hosen

Roll: 2010876110

Neural Network and Deep Learning Assignment-5

[Code link]

Fast Gradient Signed Method for adversarial attack

CodeLink: [**click here**]

Adding noise from a Gaussian distribution is fundamentally different from performing a true adversarial attack like the Fast Gradient Sign Method (FGSM). Gaussian noise is random in nature. it is not crafted with any knowledge of the model's internal structure or prediction behavior. As a result, it lacks intentionality and direction.

On the other hand, adversarial noise such as that used in FGSM is deliberately calculated using the gradient of the model's loss function with respect to the input. This allows the perturbation to be precisely tailored to push the model toward incorrect classifications. While Gaussian noise might occasionally cause a model to make a mistake, especially if the noise is strong, it does not do so in a consistent or optimized manner.Therefore, it is not considered a reliable or effective attack strategy when compared to gradient-based adversarial methods.