# CLEVERHANS Attack Module参数介绍

初次使用cleverhans，以下参数介绍可能理解的不到位，请见谅。

笔者将对四种攻击模块进行常见参数的注解，若想深入了解cleverhans，[请阅读官方文档](https://cleverhans.readthedocs.io/en/v.2.1.0/source/attacks.html)

## **BasicIterativeMethod**

class cleverhans.attacks.BasicIterativeMethod(model, back='tf', sess=None)
  
   
BIM\_params = {
  
 'eps': 0.7, # epsilon（输入变化参数）
  
 'eps\_iter': 0.2, # 每次攻击迭代的（必需的浮点数）步长
  
 'nb\_iter': 10, # 必需的int）攻击迭代次数。
  
 'clip\_min': 0.0, # （可选的float）最小输入组件值
  
 'clip\_max': 1.0 # （可选的float）最大输入组件值
  
}

## **CarliniWagnerL2**

class cleverhans.attacks.CarliniWagnerL2（model，back ='tf'，sess = None ）  
  
CW\_params = {  
 'max\_iterations': 10, # 最大迭代次数。将其设置为较大的值将产生较低的失真结果。仅使用几次迭代就需要较高的学习率，并且会产生较大的失真结果。  
 'learning\_rate': 0.1, # 攻击算法的学习率。较小的值会产生较好的结果，但收敛速度较慢。  
 'batch\_size': min\_batch,# 要同时运行的攻击数  
 'confidence': 0.1, # 对抗性示例的可信度：较高的示例会产生具有较大l2失真的示例，但更强烈地归类为对抗性示例。  
 'clip\_min': 0.9, # （可选的float）最小输入组件值  
 'clip\_max': 1.0 # （可选的float）最大输入组件值  
}

## **FastGradientMethod**

class cleverhans.attacks.FastGradientMethod（model，back ='tf'，sess = None ）  
  
FGSM\_params = {  
 'eps': 0.5, # epsilon（输入变化参数）  
 'clip\_min': 0.0, # （可选的float）最小输入组件值  
 'clip\_max': 1.0, # （可选的float）最大输入组件值  
}

## **DeepFool**

class cleverhans.attacks.DeepFool(model, back='tf', sess=None, dtypestr='float32')  
  
DP\_params = {  
 'overshoot': 8, # 防止更新消失的终止条件  
 'nb\_candidate': 10, # 要测试的类的数量，即Deepfool在攻击时仅考虑nb\_candidate类（从而加快了速度）。根据实现期间的预测置信度选择nb\_candidate类。  
 'clip\_min': 0.1, # （可选的float）最小输入组件值  
 'clip\_max': 1.0, # （可选的float）最大输入组件值  
}