# 系统说明

本系统主要功能是实现论文中所设计的防御策略，然后实验验证所实现策略的普适性。实验中用的深度学习模型有ResNet、AlexNet、LeNet,对抗攻击方法有FGSM、BIM、PGD。

实验环境如下表所示：

表 1 实验环境规格表

|  |  |  |
| --- | --- | --- |
| 环境 |  | 规格 |
| GPU |  | GTX 1050 Ti |
| 内存 |  | 8GB |
| 硬盘 |  | 500GB |
| 操作系统 |  | Windows 10 |
| 编程语言 |  | Python 3 |
| 深度学习框架 |  | PyTorch,TensorFlow,Keras |

三种深度学习模型的结构与官方论文结构一致，上表中所示的深度学习框架均提供了这三种模型，下载下来训练后即可使用。

三种攻击方法调用了第三方库[foolbox](https://foolbox.readthedocs.io/en/latest/)，其具体使用方式见官方使用文档。该文档提供了多种攻击方法的实现。