生科院

前沿报告and 研究进展

基本上6点开始

今年最新会议会很快放出来，更多是研究进展的讨论

2019/02/27 讨论班

对抗样本网络

99%正确率+扰动 会造成分类错误

扰动（目标分类和检测会造成错误）

黑盒攻击

白盒攻击

真实世界攻击（拿照片去刷一刷，或者在音乐中加入噪音）

对抗样本的可迁移性

Errrr

C&W attack

对抗样本防御

对抗样本训练——类似GAN过程，进行博弈

还能使得网络能力进行提升

讲完之后，薛老师会进行提问。对于拿上去讲的PPT可能会问的很细

薛老师：“我不知道，我是瞎讲的”，会打断学生说的话

加上噪声之后 不一定能解释

图像争取达到自然的改变：框选出眼睛，然后进行改变

深度学习的安全问题

马骋 工作报告

寒假一点进展都没有吗？

每个人讲什么必须明确到位