

我的毕业设计

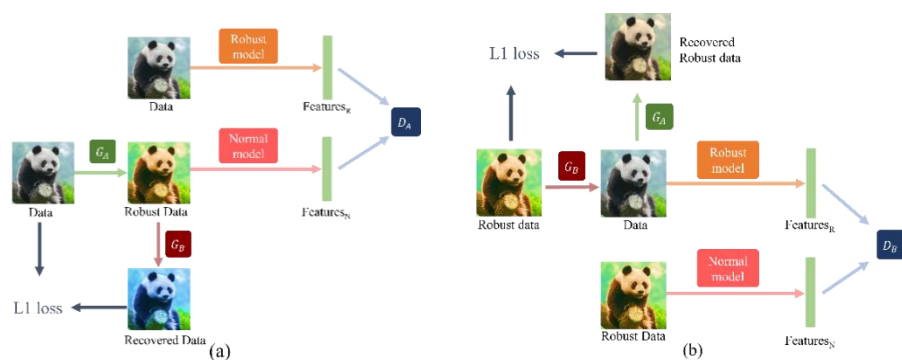
计算机学院 周子琦

这次毕设给了我一个科研的机会，让我小小体验了一把研究员的工作。

从我大二开始，听说 AI 这项技术很厉害，它可以做许多只有人能做的事情，并且在很多方面可以超越人类，这使我逐渐对 AI 有了兴趣，于是去看一些课程和书籍，在朋友的引领下参加了这一领域的比赛……我越来越发现，AI 技术潜力巨大，比如设计得当的话，我们能用 AI 技术辅助设计芯片，解基础学科（如数学）的难题，研究生命活动，延长人类寿命等等，但目前人类的开发却令人失望：在人类生活中更常见的 AI 应用则是大数据杀熟、智能推荐、AI 艺术创作、DeepFake 等等。这些的确带来了许多负面影响，尤其是 AI 艺术创作，除了给人类艺术家带来贬值感、带来失业的焦虑以外，目前还看不到任何作用。我希望这个有着十足发展潜力的技术能像 Alphafold 一样给人类社会带来多一点帮助和善意而不是相反，所以我毅然决定投身这个领域，做一点属于自己的正向的贡献。

我的毕设题目是对抗防御算法的研究，希望对自动驾驶这类系统的落地有一点微小的帮助。科研的过程是从理解到复现、再从复现到创造的过程，这是两个巨大的飞跃。老师告诉我想要找到新的科研思路就要多看论文，于是乎我看了很多论文，但遇到了巨大的挫折，从白天到黑夜，我尝试去理解那些艰涩难懂的东西，有些理解了，但有些没有，阅读的过程中我深知自己的不足，在数学方面我还有太多需要补习的功课，如实分析、泛函分析等等。

在做毕设的前 3 个月我一直在读对抗攻击和防御的相关论文，去研究和理解它们确实很困难，所以三个月来进展也不是很大。终于有一天在散步的时候突然想到一个想法，可能可以给鲁棒特征做一个可视化，这让我感到兴奋，回到家立刻把这个想法画成一个图，就有了下面两张图的前身：



不知道它能不能运作，我也把这个想法告诉了老师，老师也告诉我可以试试，给了我完成的信心。于是我就开始实现我的模型，实现新的模型的过程比运行别人的模型要难得多，毕竟要经过大量的尝试与调整……最终我完成了我的模型，虽然没有像传统论文那样提升分数刷新排行榜，但是通过这个模型我把鲁棒特征还原成了图片，给数据的鲁棒性做出了一些解释，也是有价值的，最终我把所有的研究过程以及实验过程和结果都写进了我的论文里。

在做毕设的过程中，非常感谢段老师一路的指引与陪伴，让我能够在艰难的时刻不放弃，坚持做下去。我在毕业设计中收获了许多实践经验，学会了使用许多工具，也磨练出了我查论文查资料的好习惯，对我的生活产生了巨大的影响。我也知道了研究员的工作是如此的辛苦，却有着巨大的成就感。

能推动人类社会进步现在是我的一个梦想，虽然它很难实现，但我希望我能坚持下去。用中国的话来说，就是让青春在为人民、为祖国的不懈奋斗中绽放绚丽之花。