香 港 大 學
THE UNIVERSITY OF HONG KONG

黄彬效

电话:(+86)130 2120 2656　　邮箱: bxhuang@eee.hku.hk

教育背景

香港大学, 计算机工程 (GPA: 4.3/4.3，A+)　　博士

- 研究方向：3D感知生成，图像修复，对抗攻击，后门攻击　　*2021.09-至今*

北京航空航天大学, 机器人研究所 (GPA: 3.84/4.0, Rank: 1/43)　　硕士

- 获得荣誉：北京市优秀毕业生，校级三好学生，一等学业奖学金，足球校甲冠军　　*2018.09-2021.06*
- 研究方向：机器人控制算法，飞行器自动控制，目标检测

北京航空航天大学, 机械工程及自动化学院 (GPA: 3.68/4.0, Rank: 17/226)　　学士

- 获得荣誉：校级三好学生，优秀毕业生，一等学业奖学金，2018 Robocon二等奖　　*2014.09-2018.06*

项目经历

3D Point Cloud Pre-trainig: GNN网络进行点云特征提取 (HKU)　　*2024.01-至今*

- 采用GNN对点云建模，缓解因测试时输入点云数目与预训练点云数目不同而带来的性能下降问题。

Lookup Table: 用于edge devices超分和图像修复 (HKU)　　*2023.03-2024.02*

- 探索输入pixel数目，形状和有效感受野的关系，设计非对称结构，实现轻量的100 kB LUT方法用于图像超分，消除插值运算，相比于LUT-based SOTA，空间节约40倍，能量节约10倍，PSNR仅下降0.11dB。
- 设计无DNN的图像增强框架和LUTs，相比于CNN-based SOTA，FLOPs降低10倍，PSNR仅下降0.15dB。

Scone: 空间mask增强INR表达能力 (HKU)　　*2023.03-2023.08*

- 设计自适应mask拼接不同Gaussian RFF来精确表达复杂信号，Stanford 3D scan重建任务，IoU达98.8%。

图像分类任务的后门攻击（HKU）　　*2023.08-2024.01*

- 基于数据集输入与真实标签的关系，提出一种新的backdoor trigger分类: positive trigger。
- 设计仅通过数据投毒来实现可攻击任意目标的后门攻击，攻击成功率在多个数据集大于95%。

图像分类对抗训练的鲁棒性研究（HKU）　　*2022.03-2023.08*

- 提出对抗样本的频域分布取决于数据集和训练方式，从频域的角度解释白盒攻击难以防御原因。
- 发现对抗扰动自适应攻击模型敏感频域，提出即插即用的Frequency regularization，提高鲁棒性 3.46%。
- 动态改变攻击扰动的幅度，设计dynamic target的对抗样本生成方式用于训练，来缓解robust overfitting。

3D点云自动标注器（HKU）　　*2022.02-2022.03*

- 提取Nuscenes数据集2D图片和3D点云信息，用于3D自动标注，辅助代码编写和实验验证。

Deecamp AI 夏令营 - 基于GAN的神笔马良卡通图片制作 ***[Demo]***　　*2019.07-2019.08*

- 运用 PhotoSketch 和 SketchKeras 网络进行卡通画边框提取，制作 paired 卡通画数据集。
- 基于 WGAN 的 Pix2Pix 图片润色，利用 BicycleGAN 和 CartoonGAN 实现四种风格迁移。
- 使用 K-Means 聚类并在 Discriminator 后 k 层 Feature Map 增加 L1 loss 优化色彩和轮廓。

论文

- **Huang, B.**, Tao, C., LIN, R., Wong, N. Frequency Regularization for Improving Adversarial Robustness. **Workshop at AAAI 23**.
- Li, J.C.L, Liu, C., **Huang, B.**, Wong, N. Learning Spatially Collaged Fourier Bases for Implicit Neural Representation. **AAAI 2024**
- Liu, C., Qian, X., **Huang, B.**, Qi, X., Lam, E., Tan, S. C., & Wong, N. Multimodal Transformer for Automatic 3D Annotation and Object Detection. **ECCV 2022**.
- Taming Lookup Tables for Efficient Image Retouching. (一作 Under review)
- Hundred-Kilobyte Lookup Tables for Efficient Single-Image Super-Resolution. (一作 Under review)
- A Spectral Perspective Towards Understanding and Improving Adversarial Robustness. (一作 Under review)

个人技能

- 熟练使用 python / pytorch，个人自驱力强，学习能力强，积极主动，可稳定实习6个月至18个月。