

# Leyi Sheng

✉ lsheng847@connect.hkust-gz.edu.cn    ☎ 17860812858  
🌐 LeyiSheng    🌐 <https://leyisheng.github.io/>

## Research Interests

Focus    📌 Research Assistant / Algorithm Research Intern / AI Research Intern.  
Areas    📌 AI Security, AI for Security, Multimodal Safety, Trustworthy AI, Embodied AI.

## Education



**BSc in Artificial Intelligence**, The Hong Kong University of Science and Technology (Guangzhou).  
GPA 3.41/4.3

## Publications and Research Experience

- 📌 **Towards Robust Semantic Segmentation in Multi-sensor Systems: A Survey and Benchmark**  
Under review.  
Kaiyu Lei<sup>†</sup>, Chenfei Liao<sup>†</sup>, **Leyi Sheng<sup>†</sup>**, Xu Zheng, Yuanhuiyi Lyu, Lutao Jiang, Bin Ren, Zixin Zhang, Li Chen, Kunyu Peng, Linfeng Zhang, Kailun Yang, Nicu Sebe, Luc Van Gool, Xuming Hu.
- 📌 **IP-Bench: Benchmark for Image Protection Methods in Image-to-Video Generation Scenarios**  
ArXiv preprint.  
Xiaofeng Li, **Leyi Sheng**, Zhen Sun, Zongmin Zhang, Jiaheng Wei, Xinlei He.
- 📌 **PixJail: Self-Evolving Paper-to-Pipeline Reproduction for Text-to-Image Jailbreak Evaluation**  
Under review.  
**Leyi Sheng**, Han Sun, Zhen Sun, Jinlin Wu, Yuntao Yue, Xinlei He, Jiaheng Wei.
- 📌 **Stego Battlefield: Evaluating Image Steganography Attacks and Steganalysis Defenses**  
ArXiv preprint.  
Zhen Sun, Zongmin Zhang, **Leyi Sheng**, Yule Liu, Yifan Liao, Ke Li, Xinhu Zheng, Jiaheng Wei, Wenyan Yang, Xinlei He.

## Research Experience

- 2025.07 – 2025.11    📌 **Research Assistant**, supervised by Prof. Xinlei He.  
Focused on trustworthy AI and multimodal safety research.  
Hands-on experience with LLaMA finetuning and Segmentation/detection using SAM, Yolo, etc.
- Honors    📌 **2025 Dean's List.**, celebrates the scholastic accomplishments of students who are in good disciplinary standing.