Shaping the Future of Robust Autonomous Vehicles with SIT

SIT invites you to join our groundbreaking research project focused on enhancing the robustness of Autonomous Vehicle (AV) perception systems - a key area that ensures the safety and reliability of self-driving cars in real-world environments.

- Innovative Defence Paradigm: Our research focuses on the Moving Target Defence (MTD) strategy, a cybersecurity game-changer recognised by the U.S. Federal Networking and Information Technology Research and Development (NITRD) Program. MTD represents a groundbreaking approach to secure AV perception tasks on object detection, depth estimation, and semantic segmentation against adversarial attacks.
- Industry and Academia Collaboration: In collaboration with researchers from NTU, this project is funded by AI Singapore and strategically guided by DSO National Laboratories Singapore. This partnership ensures that our work has a direct and significant impact on the industry. Our strong ties with DSO, along with collaboration from academic experts at NTU, UIUC, CityU HK, and TU Delft, guarantee that the techniques developed will be both practical for real-world AV systems and influential in advancing academic knowledge.
- Significant Funding & Resources for AV Research: With over S$1.3 million in funding at SIT (S$4M for the whole project), our project is equipped with state-of-the-art resources, including multiple advanced GPU workstations and an EV testbed with latest Carbone LiDAR and cameras, which is used to test and refine the proposed solutions and any other research tasks related to AV perception system.
- Real-World Impact: Beyond theory, this project emphasises real-world application. Our solutions will be tested and deployed in DSO's AV, competing in this AI Singapore grand challenge to prove their effectiveness in real-world scenarios.

Join us at SIT to work at the forefront of AV technology and make a difference in the future of transportation.

SIT AV perception testbed & real-world test using DSO's AV.

Papers under this project so far:

1. Dongfang Guo, Yuting Wu, Yimin Dai, Pengfei Zhou, Xin Lou, Rui Tan, Invisible Optical Adversarial Stripes on Traffic Sign against Autonomous Vehicles, The 22nd ACM MobiSys, 2024. (Acceptance ratio: 43/263=16.3%)
2. Yuting Wu, Xin Lou, Pengfei Zhou, Rui Tan, Zbigniew T. Kalbarczyk, Ravishankar K. Iyer, Resilient Autonomous Driving against Learning-Based Action Space Attacks, under Journal review.