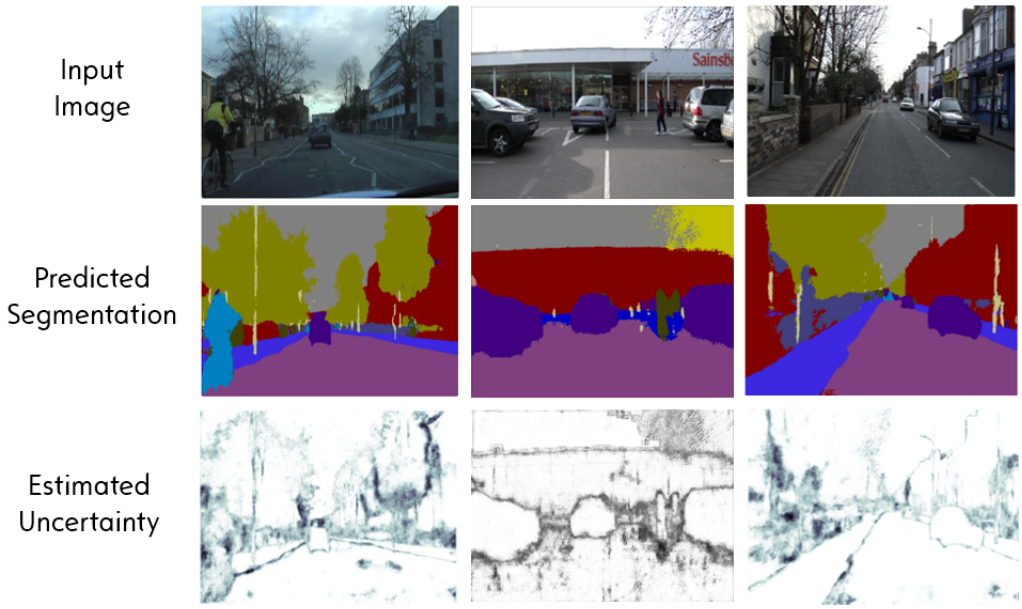
Karlsruhe Institute of Technology (KIT)
Institute of Measurement and Control
Prof. Dr.-Ing. C. Stiller

Master Thesis (2020)

Analyzing Deep Neural Networks using Adversarial Attacks and Uncertainty Estimation

Ensuring the safe operation of an Autonomous Vehicle in various environments is an important factor for the safety of pedestrians and the car passengers. Accordingly, safeguarding the autonomous operation is a crucial part in testing the Deep Neural Network (DNN) package installed in the vehicle for image detection. The main focus of the thesis is generation of adversarial attacks and data augmentation techniques on the input images to test the robustness of the DNN package. Furthermore, analysis of the DNN package will be further studied by implementing uncertainty estimation techniques to understand more about the model's weak-points or corner cases to assist in enhancing the robustness of the DNN package.
The proposed thesis consists of the following parts:

1. Literature review of various adversarial attacks and data augmentation techniques.
2. Implementation of uncertainty estimation techniques for deep neural networks.
3. Evaluating deep neural networks using adversarial images and estimating the network's uncertainty.



I am happy to answer questions regarding the topic, reference literature or alternative topics. If you are interested, please write me an email with your CV and transcripts.

Requirements:	Knowledge in machine learning, deep learning and statistics Solid knowledge of Python or C++ Knowledge of PyTorch or TensorFlow
Keywords:	Deep Learning, 2D Object Detection, Semantic Segmentation, Adversarial Attacks, Uncertainty Estimation
Supervisor:	M.Sc. Ahmed Hammam Institute of Measurement and Control Systems (MRT) Email: ahmed.hammam@partner.kit.edu
Start Date:	Flexible

Input sample taken from: CamVid Dataset (http://mi.eng.cam.ac.uk/research/projects/VideoRec/CamVid/)