Robustifying neural networks

Abstract:

In this talk I will survey several techniques to make neural networks more robust. While neural networks achieve groundbreaking results in many applications, they depend strongly on the availability of good training data and the assumption that the data in the test time will resemble the one at train time. In this talk, we will survey different techniques that we developed for improving the network robustness and/or adapting it to the data at hand.