World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:10, 2022

Studying Relationship between Local Geometry of Decision Boundary with Network Complexity for Robustness Analysis with Adversarial Perturbations

Authors : Tushar K. Routh

Abstract : If inputs are engineered in certain manners, they can influence deep neural networks' (DNN) performances by facilitating misclassifications, a phenomenon well-known as adversarial attacks that question networks' vulnerability. Recent studies have unfolded the relationship between vulnerability of such networks with their complexity. In this paper, the distinctive influence of additional convolutional layers at the decision boundaries of several DNN architectures was investigated. Here, to engineer inputs from widely known image datasets like MNIST, Fashion MNIST, and Cifar 10, we have exercised One Step Spectral Attack (OSSA) and Fast Gradient Method (FGM) techniques. The aftermaths of adding layers to the robustness of the architectures have been analyzed. For reasoning, separation width from linear class partitions and local geometry (curvature) near the decision boundary have been examined. The result reveals that model complexity has significant roles in adjusting relative distances from margins, as well as the local features of decision boundaries, which impact robustness.

Keywords : DNN robustness, decision boundary, local curvature, network complexity
Conference Title : ICADLPR 2022 : International Conference on Advances in Deep Learning for Pattern Recognition
Conference Location : New York, United States
Conference Dates : October 06-07, 2022