Enhancing Image Classifiers with Denoising Filters

Aidan Sharpe

Contents

Abstract

1 Introduction

All neural networks are prone to adversarial attacks [1] [2].

References

[1]   Nicholas Carlini and David Wagner. *Towards Evaluating the Robustness of Neural Networks*. 2017.

[2]   Christian Szegedy et al. *Intriguing properties of neural networks*. 2014.