

A plethora of recent work has shown that convolutional networks are not robust to adversarial images: images that are created by perturbing a sample from the