DRAGONFIST

Joseph Boudreau, Andrew Ferrazzutti, Kia Shakiba, Zhongyu Zhao

***Abstract*—abstract goes here...**

I. Introduction

Introduction goes here...

II. Image Filters

The proper selection of filters is important to the overall effectiveness of the algorithm. As previously mentioned, the intention of DRAGONFIST is to improve a machine learning model's resiliency against adversarial noise. Based on the work done by ——, adversaries can target specific pixels in an image to which noise will be applied. As such, filters which combine the values of pixels with their neighbours are intuitively more desirable as they increase the difficulty of targeting specific areas of the image to which noise will be applied. Therefore, the following filters were considering when designing DRAGONFIST:

- Edge detection
- Gabor
- Gaussian
- Average rows
- Average columns
- Average
- Rank
- Maximum
- Minimum
- Median

A. Descriptions

In order to understand what the filters are doing to the images, a brief explanation of each is given.

1) Edge detection: The edge detection filter uses the Python library `skimage.filters.sobel` [1].

B. Filter accuracy

When applying each filter to the system, it is important to remember the overall goal of the model – to accurately classify its input. Therefore, each filter's accuracy in classification is important to consider to ensure the overall model maintains a high accuracy as well. Each filter was tested individually in order to determine its classification accuracy. The results of these tests can be observed in table I.

TABLE I
Image filter accuracies.

Filter	**Accuracy**
Edge detection	0
Gabor	0
Gaussian	0
Average rows	0
Average columns	0
Average	0
Rank	0
Maximum	0
Minimum	0
Median	0

References

[1] *Module: filters – skimage v0.15.dev0 docs*, https://scikit-image.org, scikit-image.