<u>MLDS Project Proposal – [Permuted Puzzle]</u>

Date: December 2022
Mentors: Shuli Finley, Master's Student, Reichman University
             Alon Oring, Reichman University

<u>Background (~0.5-1 page)</u>

Applying a fixed pixel-wise permutation on graphs of different function classes before then running classification algorithms to distinguish between the classes has cryptographic applications, such as in the Private Information Retrieval (PIR) setting [BHW2019]. Work on this setting has proved particularly challenging. This project proposes an intermediary experiment to support the effort of exploring effects of permutations on image classification tasks in general. The proposed experiment provides significant relaxations on both the data and the permutations: instead of images of two different classes of functions, we use images of dogs versus cats, and instead of pixel-wise permutations, we explore various resolution tile-wise permutations.

The dataset is Kaggle's <u>Dogs vs Cats</u> dataset.
The student will first run various neural networks to solve the unpermuted setting as a benchmark for post-permutation performance.
For the permuted setting, the data preparation includes dividing the images into the desired tiling (there will be multiple tile resolutions tested) and applying the permutation. The student is then to compare performance of the previously tried networks and improve their performance on the permuted setting.
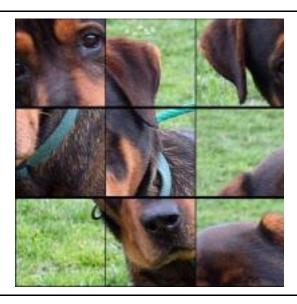
Dataset samples

9-tile permutations

Objectives (0.25 page)

In this project, we take images of cats and dogs and apply permutations of different resolution tiles of the images (i.e., dividing the image into 4 tiles, 9 tiles, etc.) before then running classification algorithms.

From this experiment, we aim to explore the following:

1. The effects of tile resolution on the feasibility of classification post permutation 2. In the case that the neural network succeeds in the post-permuted setting, does the network learn the permutation or does it succeed directly from characteristics in the permuted images without learning the permutation?
2. A way to rank permutations (which permutations lead to better or worse performance given the same images and number of tiles)?

Resources

+ [BHW2019] E. Boyle, J. Holmgren, M. Weiss, Permuted Puzzles and Cryptographic Hardness. Theory of Cryptography (pp.465-493), 2019.

+ Cloud resources will be provided for training.