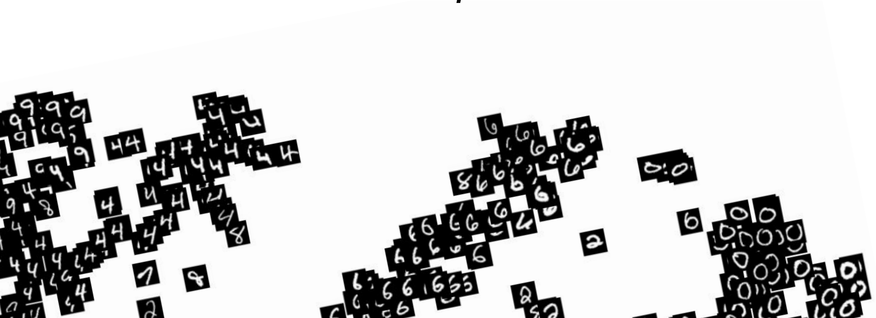
The Effect Of Data Augmentation on Deep Representations

Phuc Ngo[1], Dimitris Tsipras[2], Saachi Jain[3] and Aleksander Mądry[4]

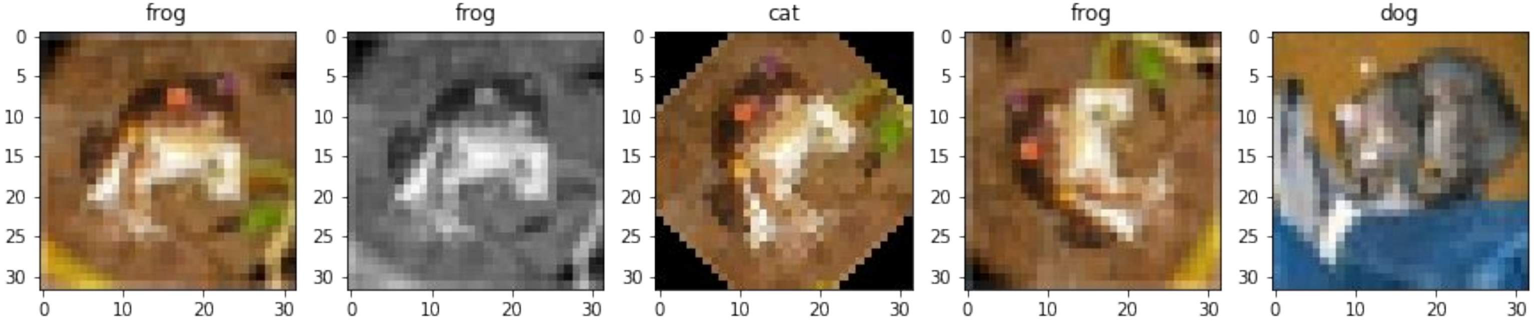
[1]Department of Computer Science and Maths, Beloit College

[2, 3, 4]Department of Electrical Engineering & Computer Science, MIT



Overview

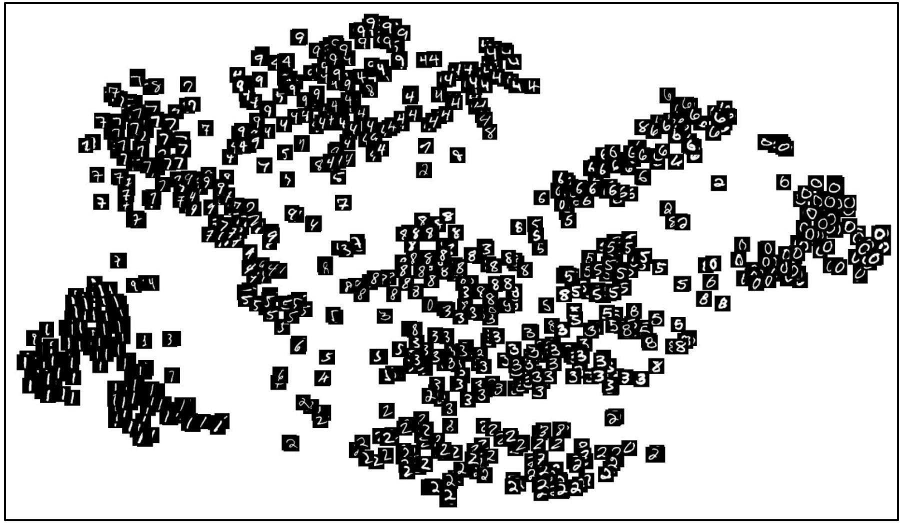
- Transformation happens all the time in real life
- Model doesn’t handle transformed samples well



- Data augmentation is a simple and common technique that increases the model’s robustness
- Our understanding of this technique is still limited
- We try to understand the effect of data augmentation on neural network

Background

Representation : The second to last feature vector of neural network



[1]

- Representation of the same object is clustered together
- If model learns invariance, the augmented representation should be closed to standard representation

[1] Latent Space Visualization, HackerNoon
https://hackernoon.com/latent-space-visualization-deep-learning-bits-2-bd09a46920df

Hypothesis

Invariance

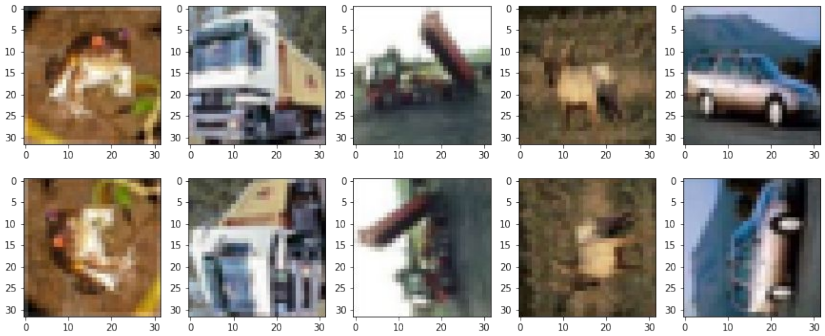
- Model maps augmented inputs to similar representations to the standard inputs -> Makes similar predictions

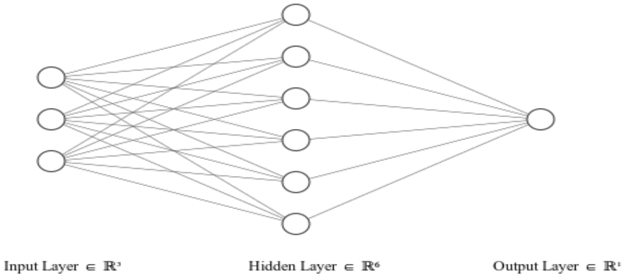
Subpopulation

- Model uses a different set of prediction rules to classify augmented samples

Method

Train ResNet18 models on CIFAR-10 with 2 types of augmentation: grayscale and 90-rotation.

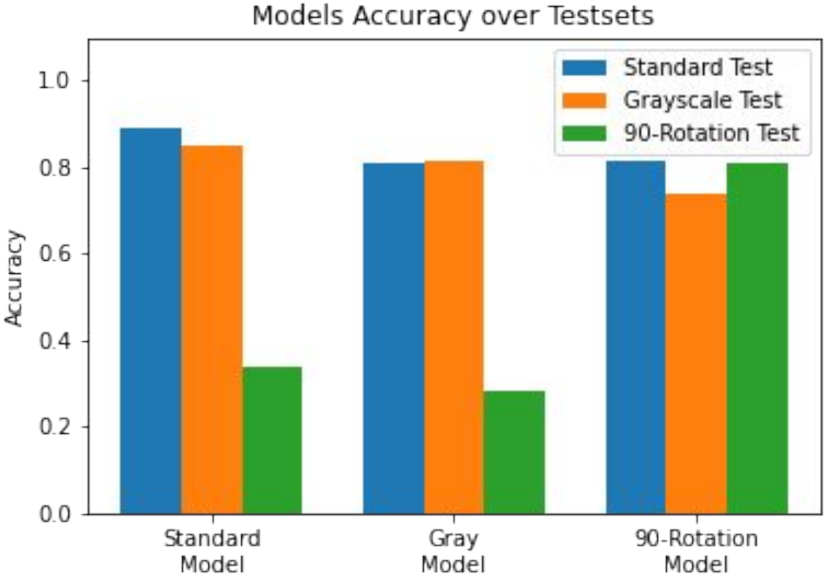




Obtain prediction and representation to calculate:

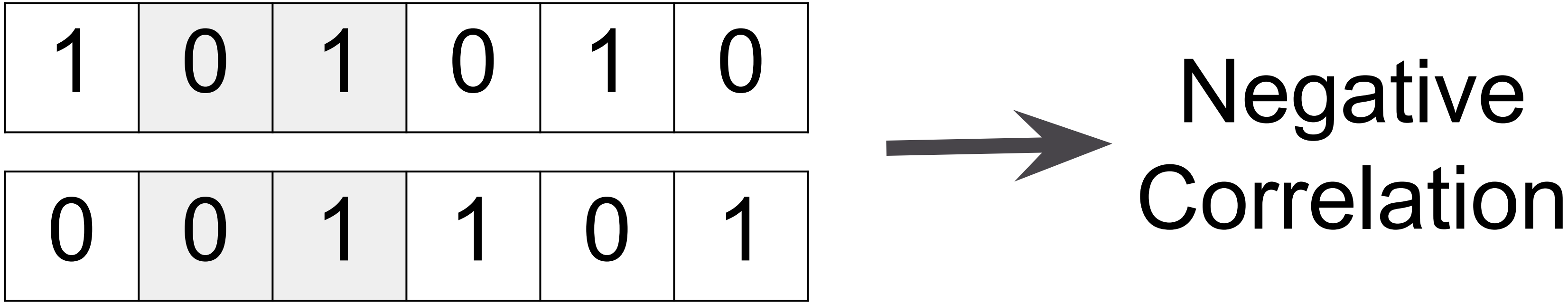
- Accuracy
- Correlation
- Nearest neighbor diagram

Accuracy



- Grayscale test performs well even in the standard model
- 90-rotation model hugely boost the accuracy of grayscale test compared to standard model

Correlation



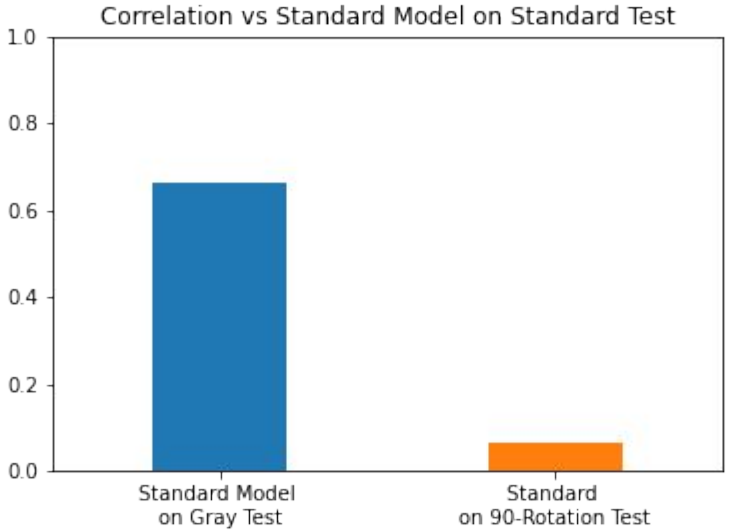
1	0	1	0	1	0
0	0	1	1	0	1

Negative Correlation

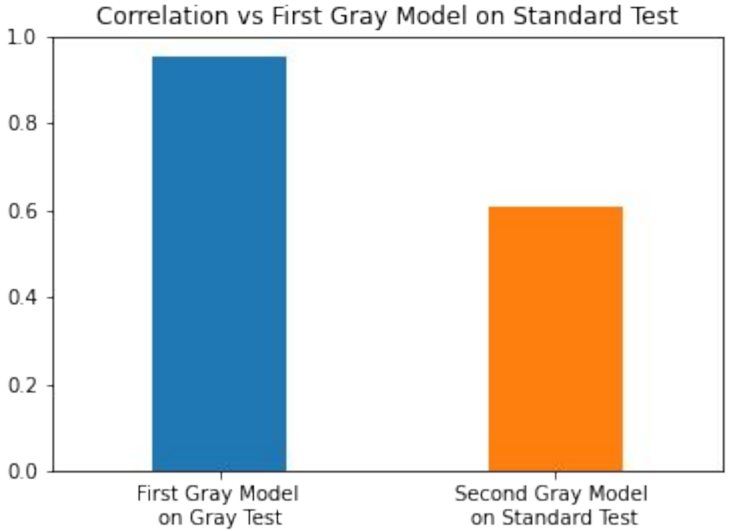
- Obtain prediction from testsets -> Construct boolean vector -> Correlation

Correlation - Grayscale

Standard Model



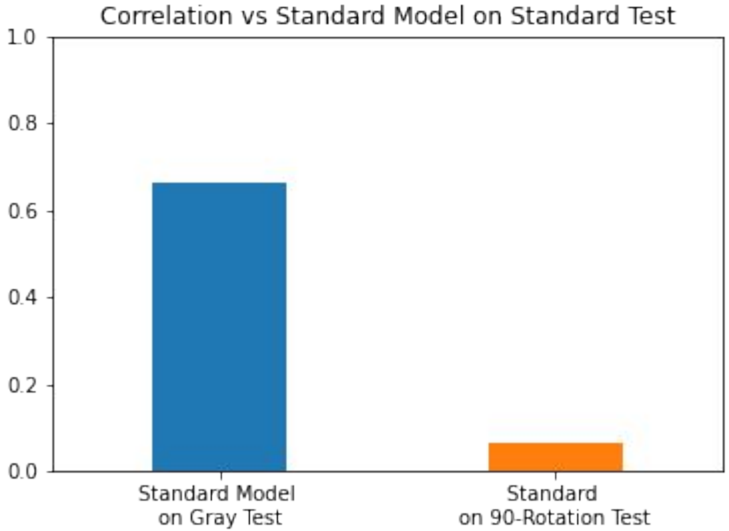
Grayscale Models



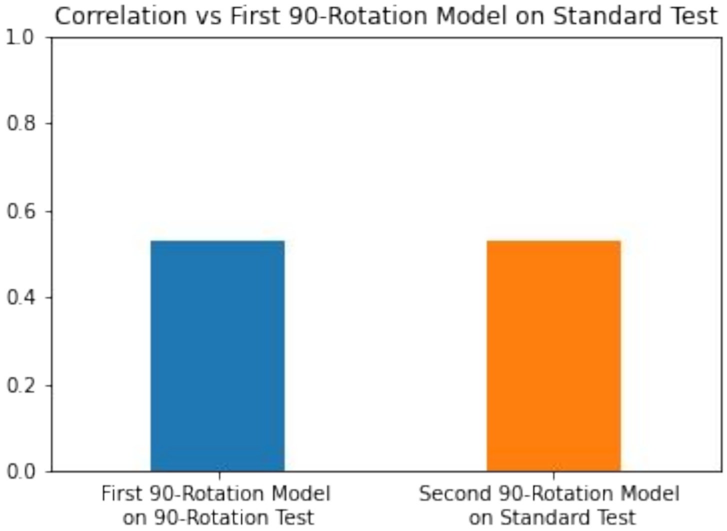
- Grayscale model learned invariance

Correlation - 90 Rotation

Standard Model

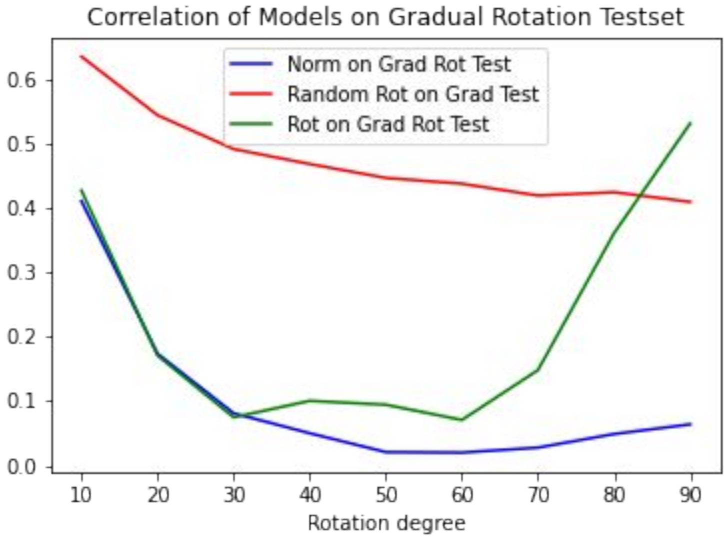


90-Rotation Models



- The standard and augmented correlation is as random as the correlation between two separate models

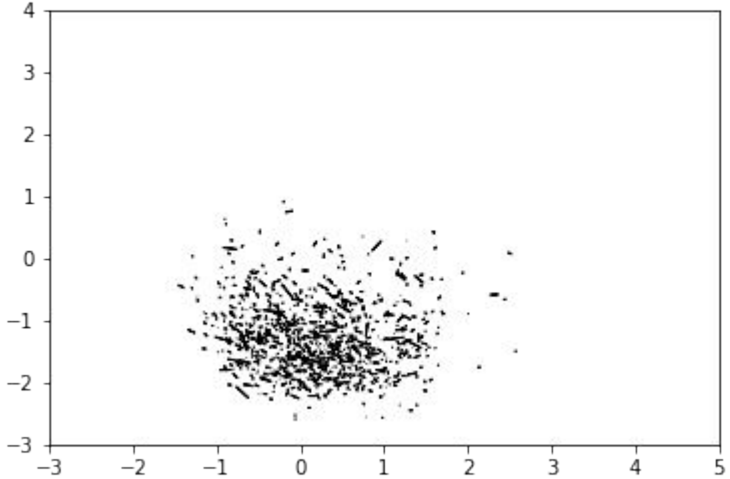
Correlation - Gradual Rotation



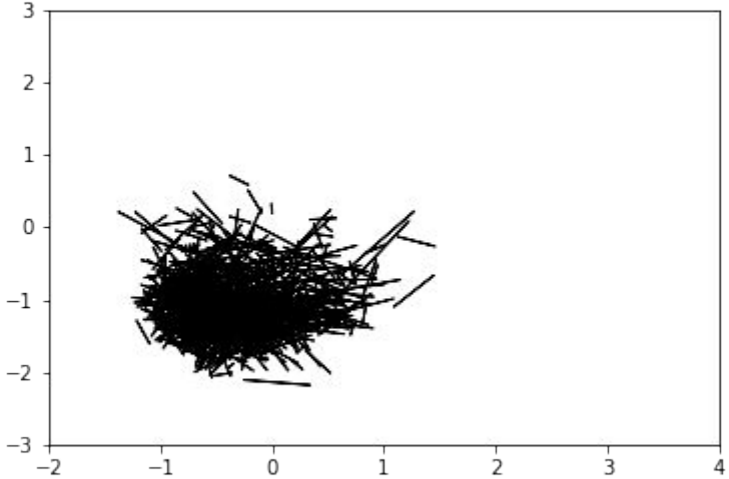
- Random rotation doesn’t improve the correlation for the 90-rotation testset

Latent Space Visualization

Gray Model Augmentation Trajectory

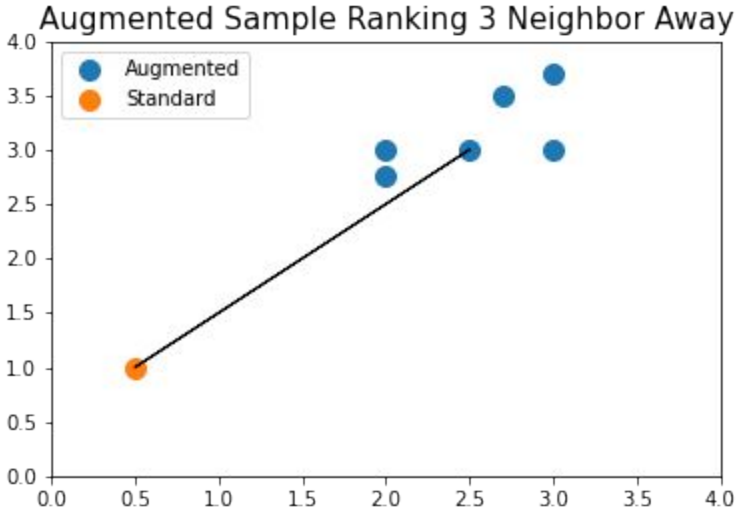


90-Rotation Model Augmentation Trajectory



- How do we quantify the distance of the trajectory?

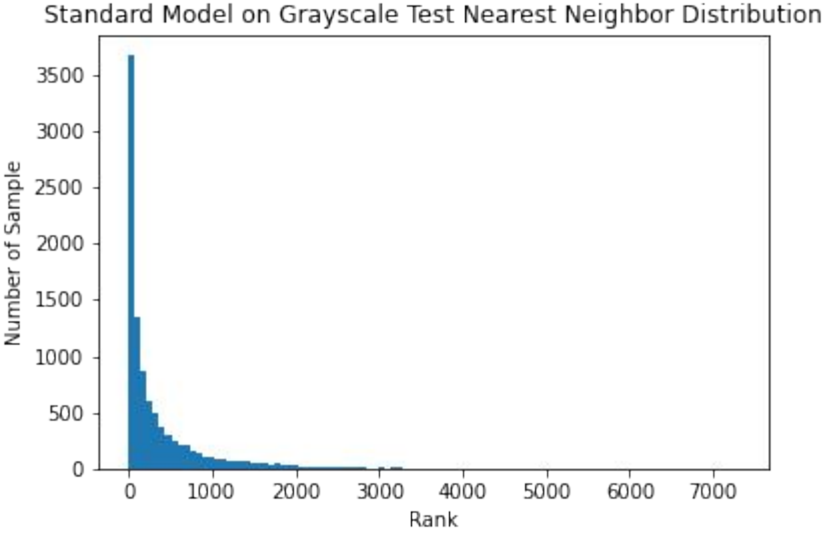
Nearest Neighbor (NN) Diagram



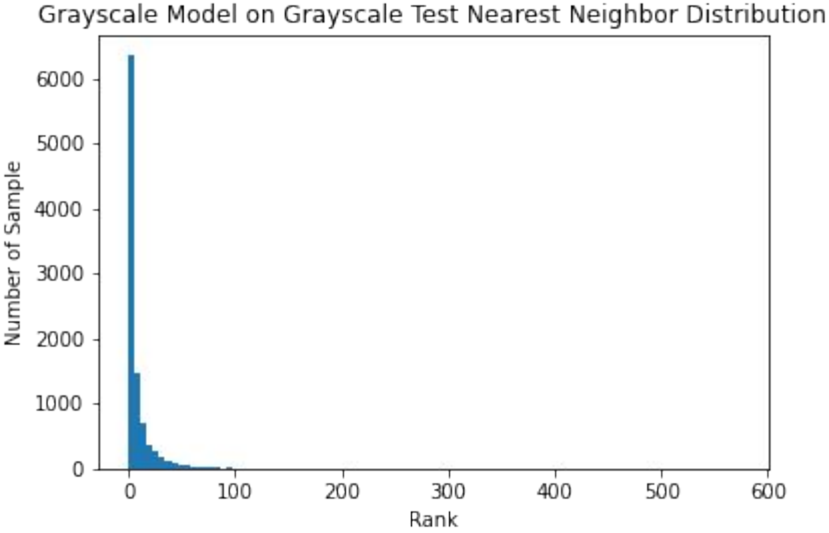
- Choose a standard image's representation
- Determine how far away the augmented pair is among other augmented representation
- Sort and determine the rank

NN Diagram - Grayscale

Standard Model

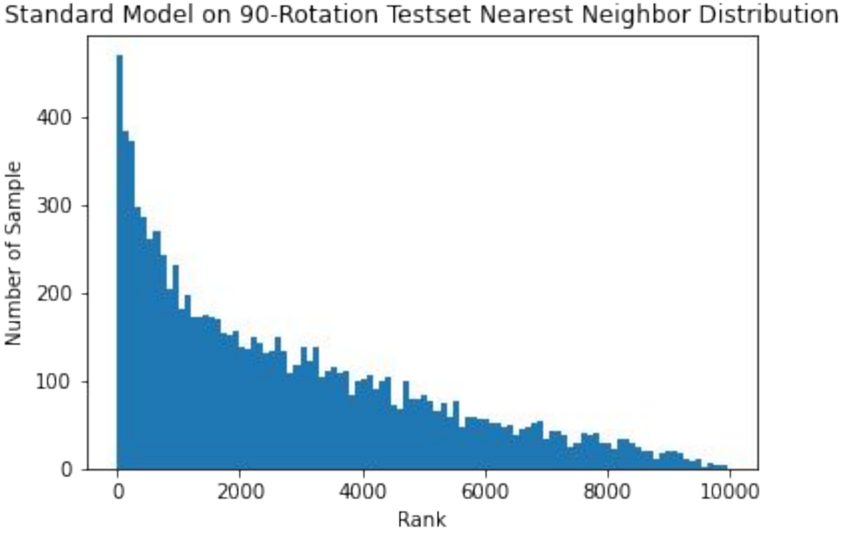


Grayscale Model

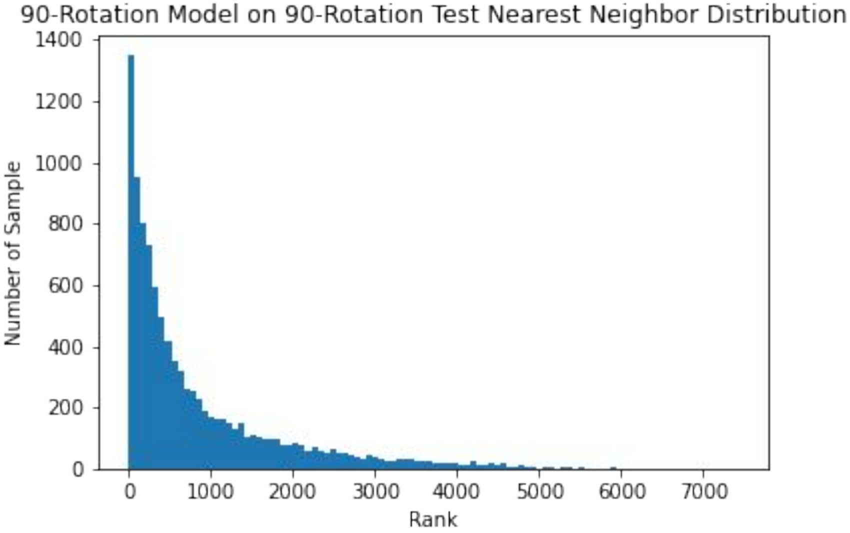


NN Diagram - 90 Rotation

Standard Model

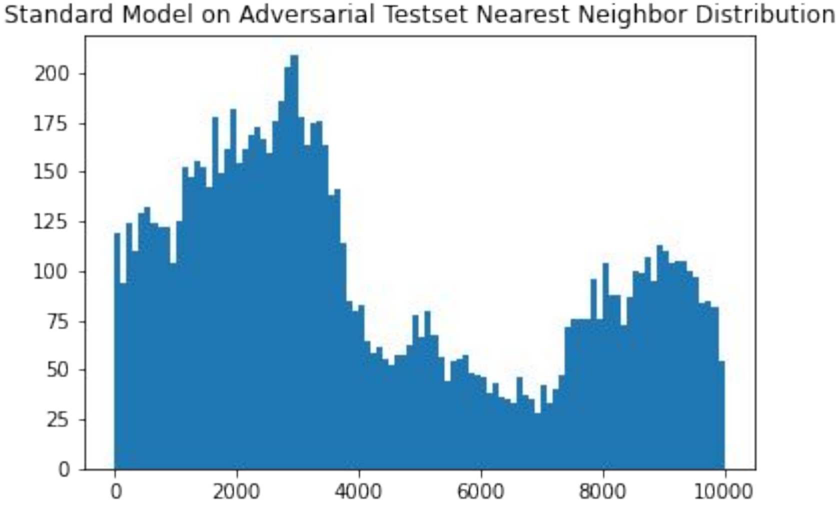


90-Rot Model



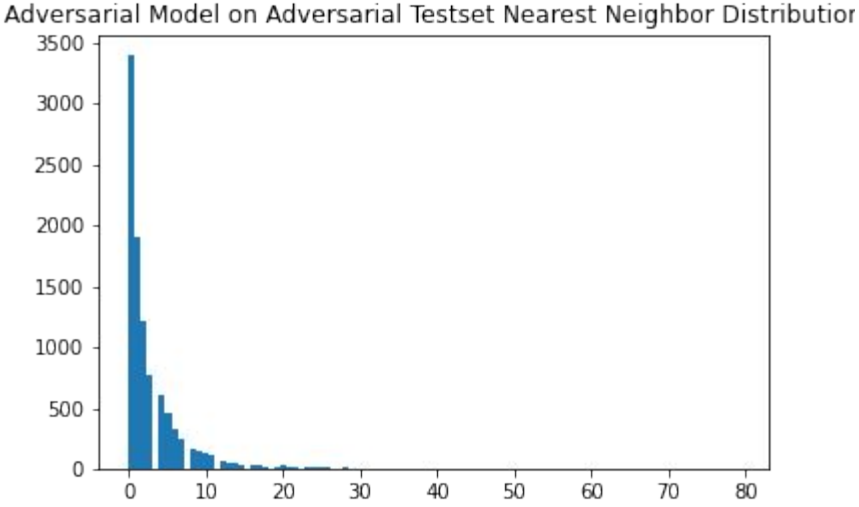
NN Diagram - Adversarial Model

Standard Model



Correlation: 0.051

Adversarial Model



Correlation: 0.540

Conclusion

Depending on the severity of the augmentation, models can vary between learning invariance or learning entirely separate augmented subpopulations.

Thank you for listening

ngoph@beloit.edu