**Hands-on Assignment 6**

**Due Date: See web**

Several pre-trained models are mentioned in HA4:

* VGG16
* ResNet50
* InceptionV31
* DenseNet121
* EfficientNetB2
* MobileNetV2

For this assignment, do the following:

1. Choose one of the pre-trained models, and use it to classify the 10 test images included in this package.
2. Create an adversarial example for each of the 10 test images with respect to the model used in Step 1.

Write a simple report to summary the results and submit the report via Canvas. The summary should contain the followings:

1. Which pre-trained model was used in the experiment?
2. The predictive score (probability) of the model given the 10 test images
3. Which adversarial attack is used?
4. Any hyperparameter used in the attack
5. The predictive score of the adversarial examples
6. Any interesting findings/analysis

The report should be organized and neat, and the format should follow either docx or pdf.

Similarity scores will be computed for this assignment.

*Copyright Statement: The materials provided by the instructor in this course are for the use of the students enrolled in the course. Copyrighted course materials may not be further disseminated.*