## Project 9: Physical Adversarial attacks on Deep-Learning-based ISP pipelines

* *Project coordinator*: Hrushikesh Varma (bhupathirajus@ufl.edu)
* *Group Size:* 2 groups
* *Project Description*: Camera Image Signal Processing (ISP) pipelines are hardware or software systems that handle the conversion of raw image data from a camera sensor into a final, usable image. These pipelines include various stages such as demosaicing, color correction, noise reduction, and sharpening to transform raw sensor data into a high-quality, visually pleasing image. The ISP pipelines enhance the image quality and optimize the camera performance in diverse lighting conditions. In recent years, Deep Learning has emerged as one solution for some of them or even to replace the entire ISP using a single neural network. Previous works have demonstrated that CNN-based detection and generation models are vulnerable to digital adversarial perturbations. However, these attacks require fine-grain control over the image perturbations, which is difficult to achieve in the real world. In this work, we will design a physical patch-based or light-projection-based adversarial attack against state-of-the-art deep learning-based ISP models and evaluate the performance of object detection models using these processed images.

Link to primary paper - [PyNET-CA](https://arxiv.org/abs/2104.02895)

Dataset:

Training the network -- Zurich RAW to RGB (ZRR)

Size - 22GB, [link](http://people.ee.ethz.ch/~ihnatova/pynet.html)

YOLO-v7

Object detection model - [link](https://viso.ai/deep-learning/yolov7-guide/)