Ongoing Projects of Arijit Sur, Dept. of CSE

1. Design a framework to resist image-based adversarial attacks on deep learning models

2. Computer Vision for Underwater Exploration

Title of Project: Design a framework to resist image-based adversarial attacks on deep learning models

Funding Agency: Core Research Grant, DST, SERB, Govt. of India

PI: Arijit Sur -Department of Computer Science and Engineering, IIT Guwahati

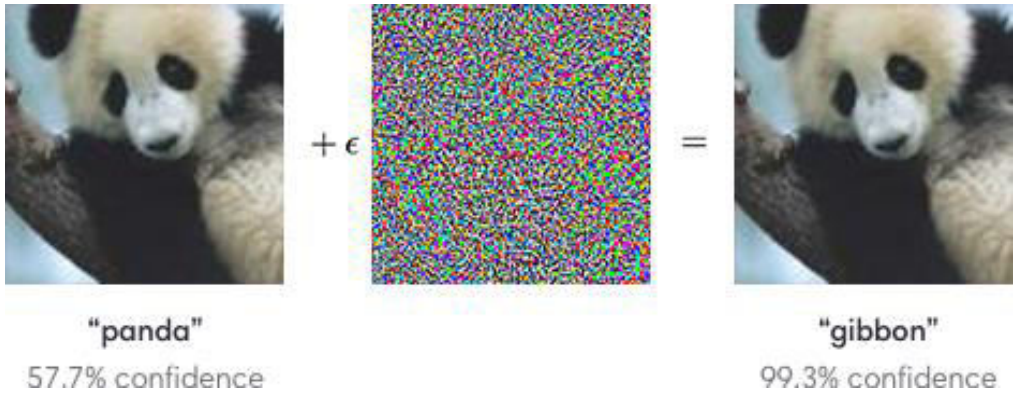
Two primary objectives:

1. Detection of adversarial attacks more generally.
2. Develop a framework to help deep neuronal models to resist adversarial perturbation attacks.

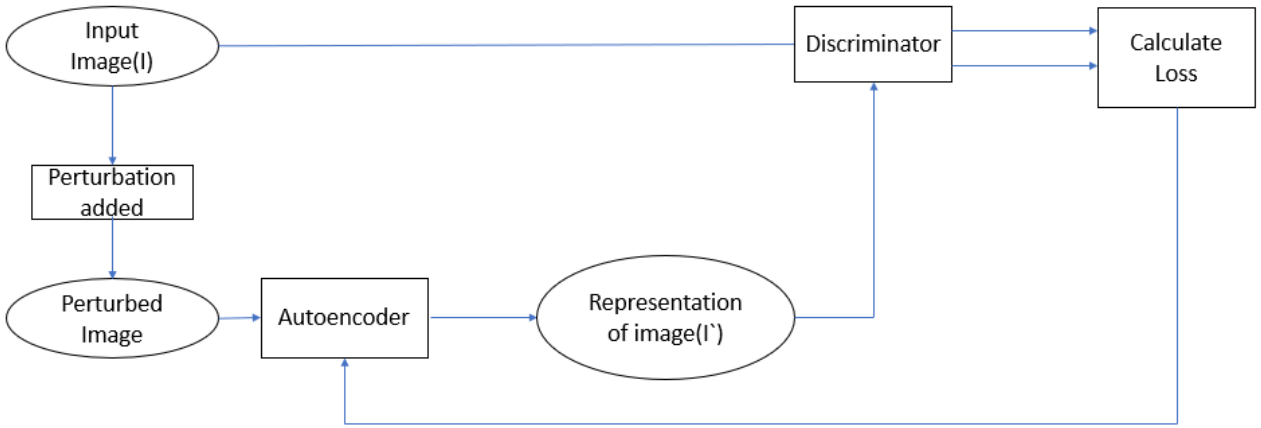
Deliverables and outcome: The software module for

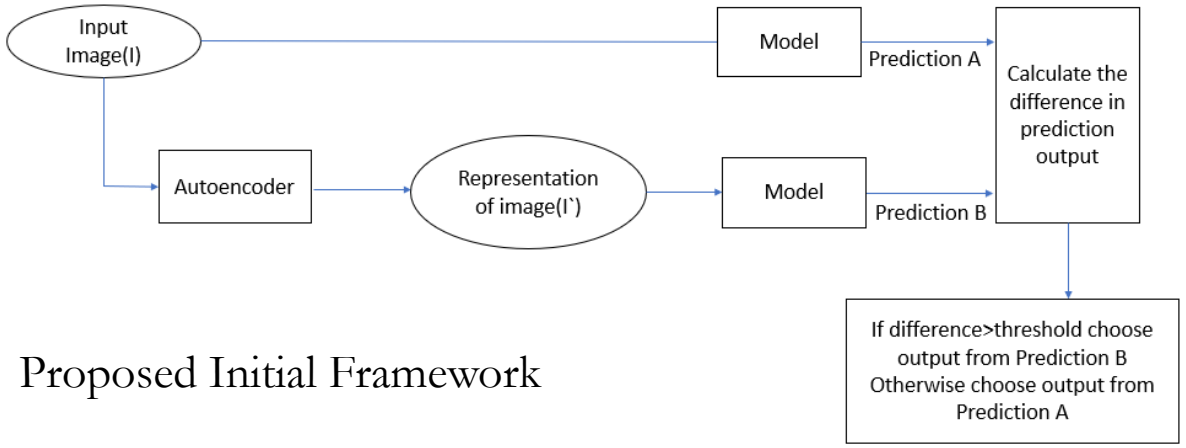
1. Detection whether an image is perturbed or not to fool some existing deep model.
2. Fine-tune the attacked model with an adversarial example dataset to resist the corresponding attack.

Theme of the work:



An adversarial attack[Goodfellow et al., 2015]





Proposed Initial Framework

Title of Project: Computer Vision for Underwater Exploration

Under Technology Innovation Hub on Under Water Exploration, IIT Guwahti

Funding Agency: DST NM-ICPS, Govt. of India

PI: Arijit Sur -Department of Computer Science and Engineering, IIT Guwahati

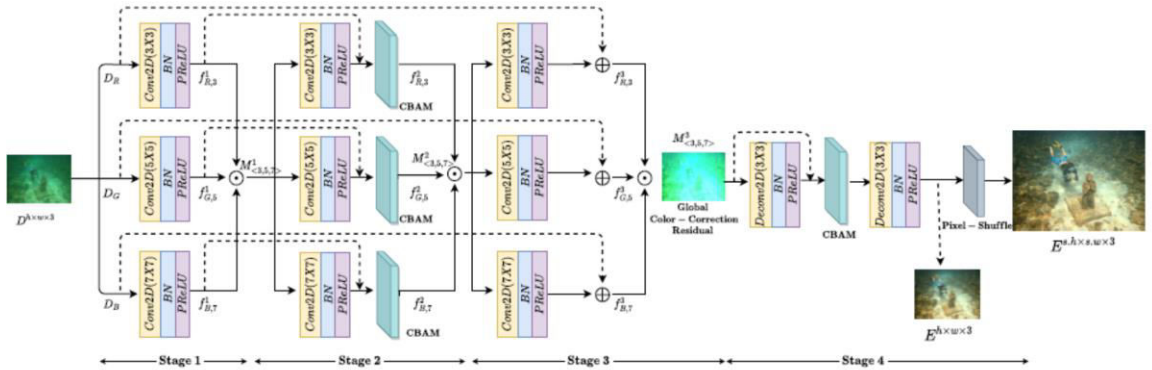
Co-PI: Santosha Kumar Dwivedy, Dept. of Mechanical Engineering, IIT Guwahati

Three primary objectives:

1. Underwater image or video restorations and super resolutions.
2. Underwater Image and Video Analytics: Segmentation and object detection.
3. Computer Vision for Automatic Underwater Vehicles (AUV)

Deliverables and outcome: The software module for

1. Underwater image, video restoration and super resolution.
2. Underwater image/video analytics
3. Deployment of computer vision tasks on AUVs



One of the Proposed Restoration Architectures and the Result