Adversarial Attacks Against Uncertainty Quantification: Supplementary Material

Emanuele Ledda[1,3], Daniele Angioni[1,2], Giorgio Piras[1,2], Giorgio Fumera[2], Battista Biggio[2], Fabio Roli[3]

[1]Department of Computer, Control and Management Engineering, Sapienza University of Rome, Italy

emanuele.ledda@uniroma1.it

[2]Department of Electric and Electronic Engineering, University of Cagliari, Italy

{daniele.angioni, giorgio.piras, fumera, battista.biggio}@unica.it

[3]Department of Informatics, Bioengineering, Robotics, and Systems Engineering, University of Genova, Italy

fabio.roli@unige.it

1. IID Experiments

In this section, we show the full details of results on each architecture and on each dropout rate.

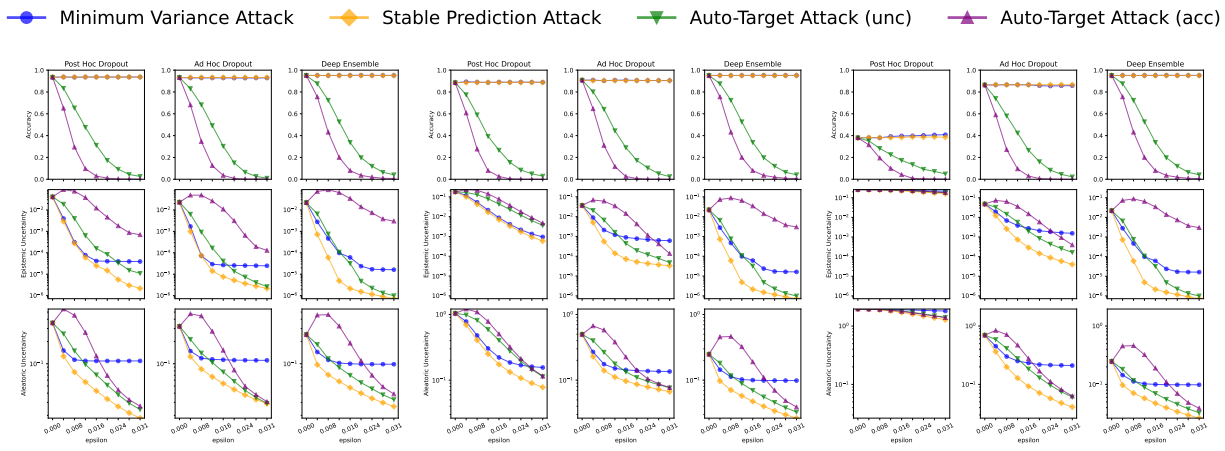


Figure 1. IID experiments conducted on Resnet-18 using dropouts 0.1, 0.3, 0.5.

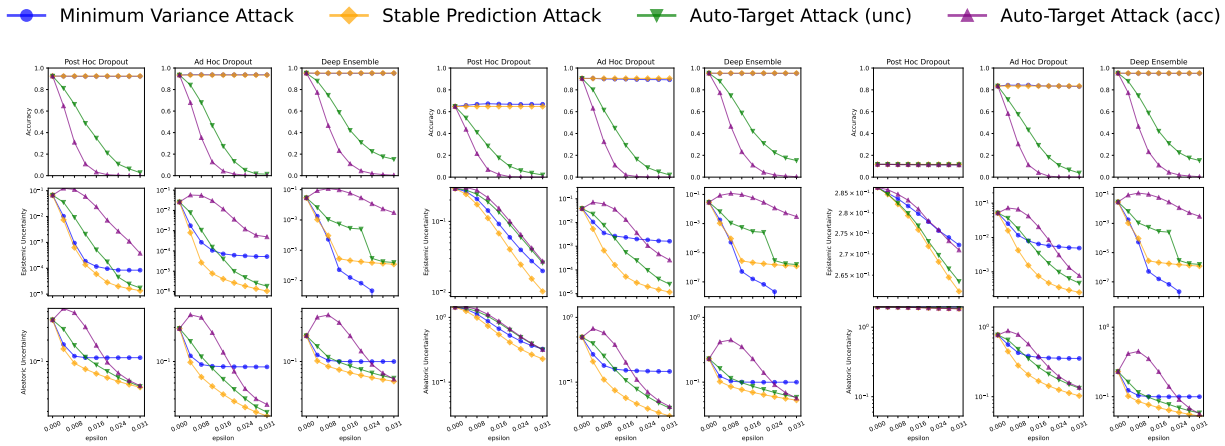


Figure 2. IID experiments conducted on Resnet-34 using dropouts 0.1, 0.3, 0.5.

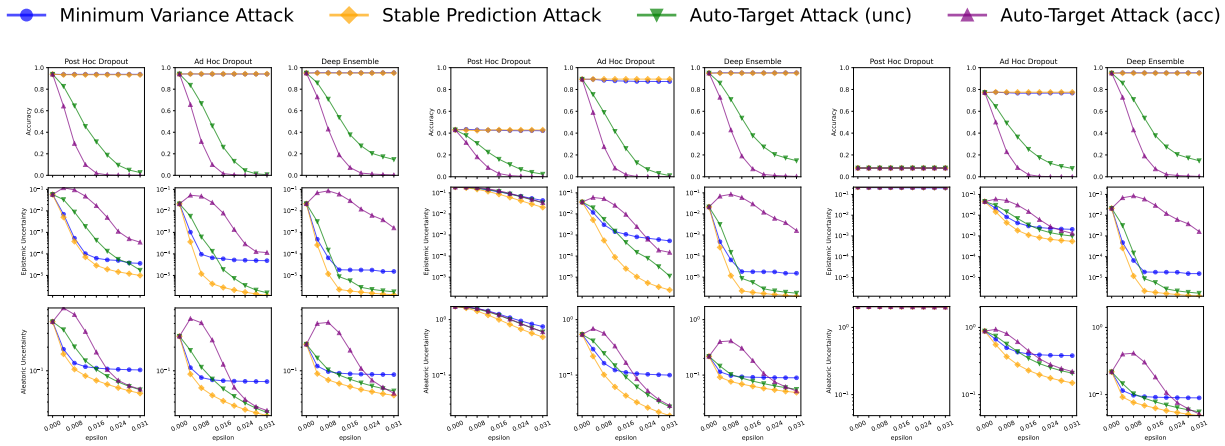
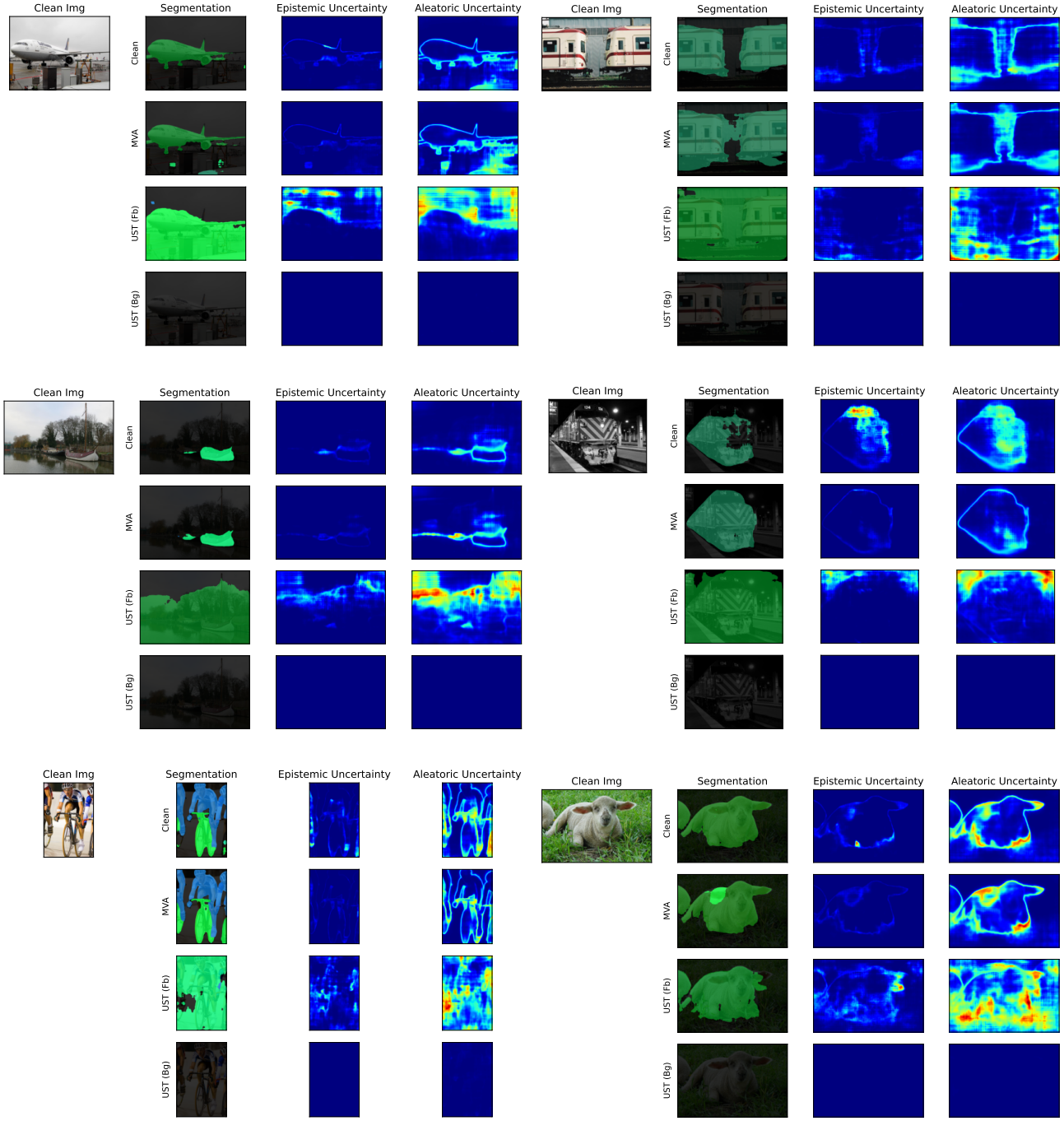
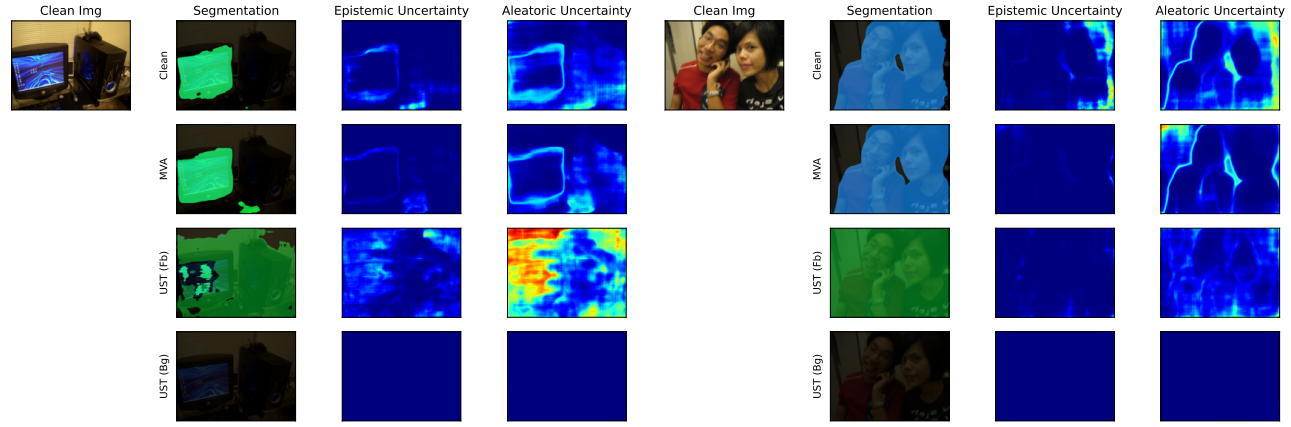


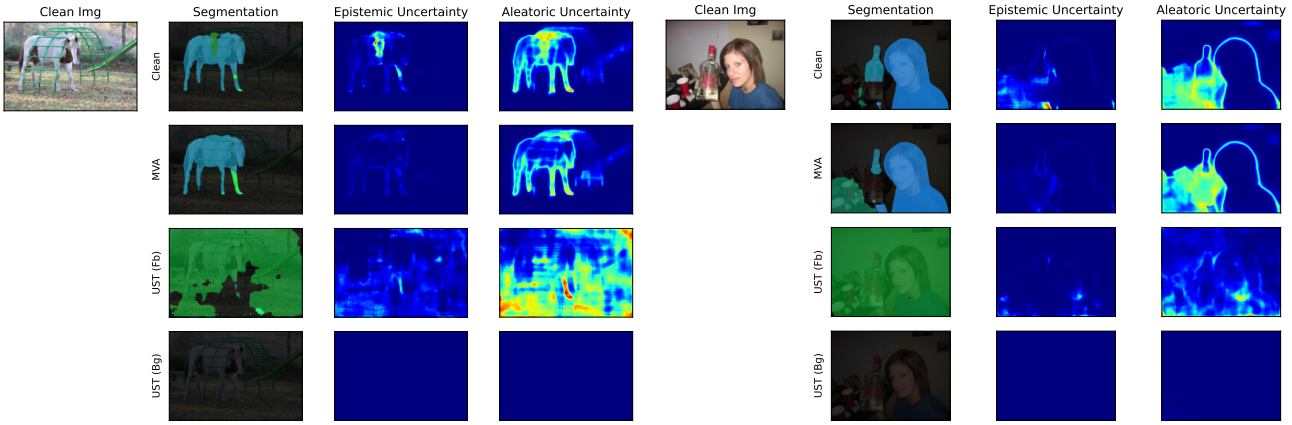
Figure 3. IID experiments conducted on Resnet-50 using dropouts 0.1, 0.3, 0.5.

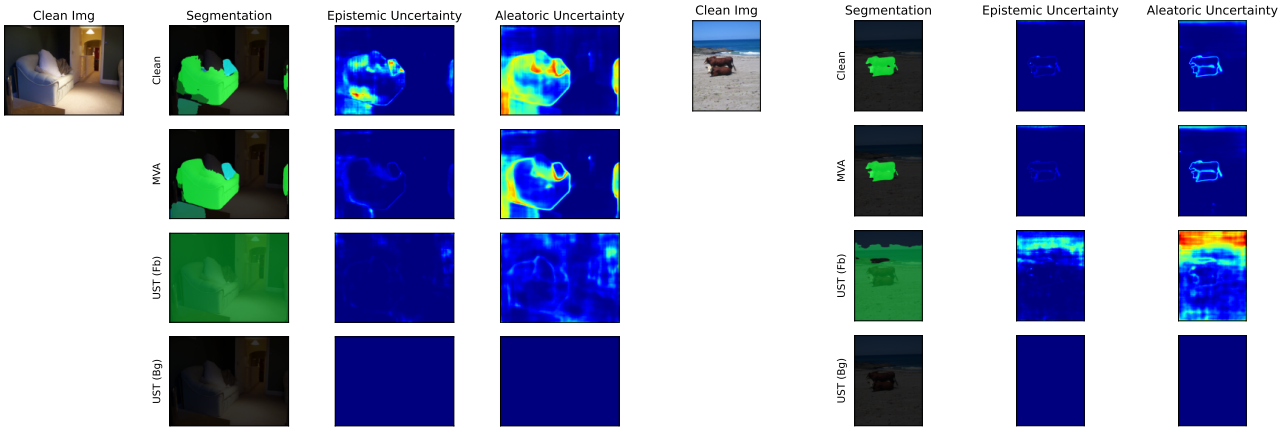
2. Examples of Attacks on Semantic Segmentation

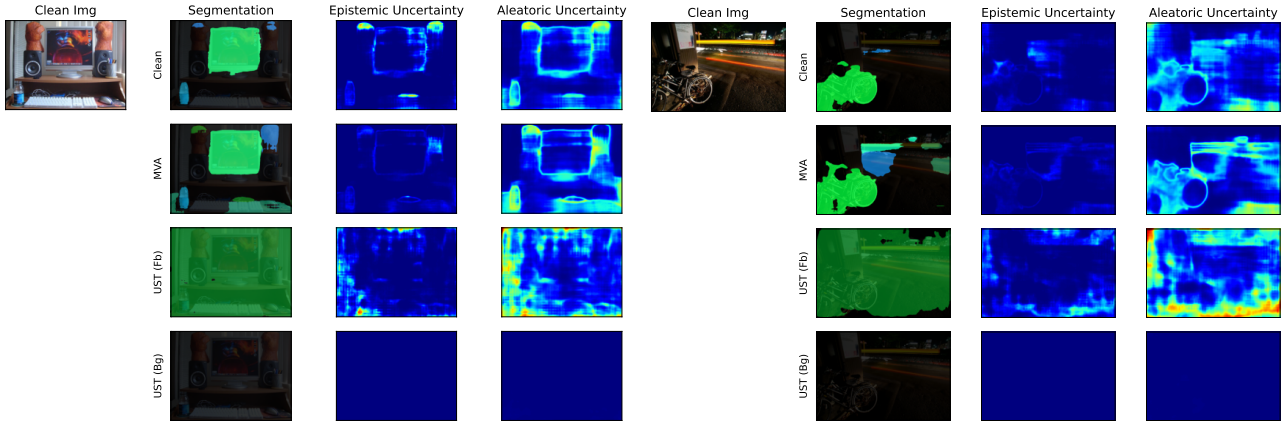
In the following section, we report additional image examples of the attacks on semantic segmentation.

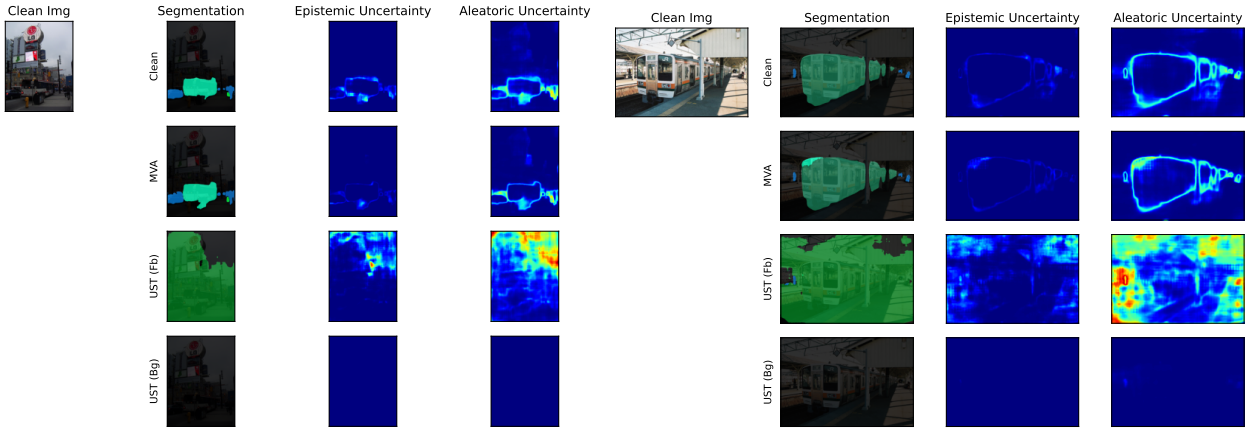


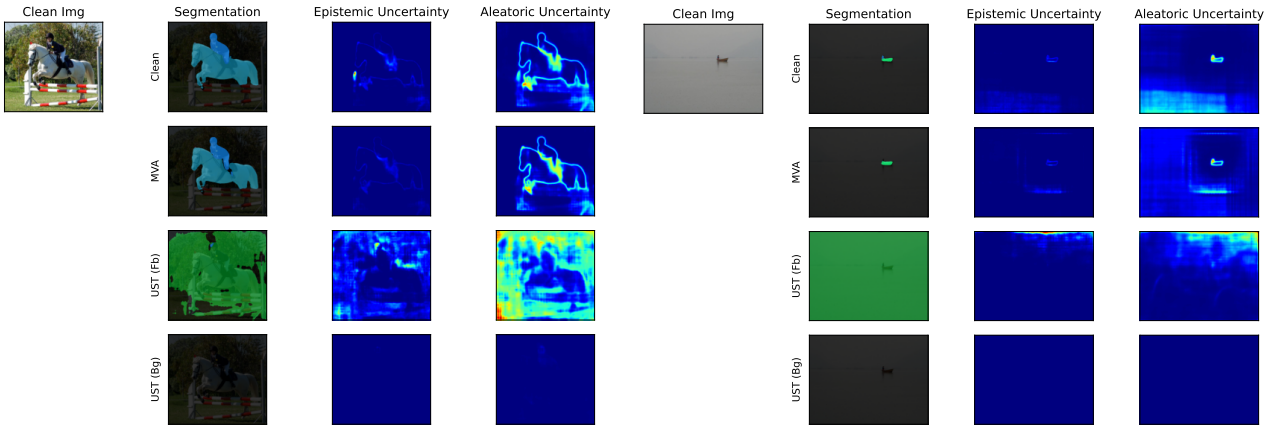

Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)
Clean
MVA
UST (Fb)
UST (Bg)


Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)
Clean
MVA
UST (Fb)
UST (Bg)


Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)
Clean
MVA
UST (Fb)
UST (Bg)


Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)
Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)


Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)
Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)


Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)
Clean Img
Segmentation
Epistemic Uncertainty
Aleatoric Uncertainty
Clean
MVA
UST (Fb)
UST (Bg)