

Robust Deep Learning Systems Integrated with Confidence Evaluation

DIMAH DERA PH.D. STUDENT ROWAN UNIVERSITY

Outlines

- 1. Introduction to Deep Neural Networks
- 2. Limitations of Deep Neural Networks
- 3. Bayesian Neural Network
- 4. Uncertainty Propagation
- 5. Experimental Results

Introduction to Deep Neural Networks

Image Classification





Input Ground truth Prediction







Automatic Machine Translation



Instant Visual Translation Example of instant visual translation, taken from the Google Blog

Convolutional Neural Network



Limitations of Deep Neural Networks

Overfitting especially when training data is insufficient.

- Overconfident predictions by assigning a high SoftMax value, towards the wrong class for things the network hasn't seen before.
- Inability to a reliable measure *uncertainty* measure of their prediction.



S. Moosavi-Dezfooli, A. Fawzi, O. Fawzi, and P. Frossard, "Universal adversarial perturbations," in CVPR. IEEE Computer Society, 2017.

Bayesian Neural Networks



Bayesian Neural Network: assume the weights are random variables.

Distributions over the weights and network output.

Modeling the uncertainty which is basically the Var(Y).





Uncertainty Propagation









True: 7, Pred: 7 True: 2, Pred: 2 True: 8, Pred: 8

Dropout Accuracy 52%



Pred: cat

Pred: cat

Pred: airplane



True: dog Pred: cat

True: horse Pred: cat

Bayes-by-Backprop Accuracy 68%





True: dog True: airplane Pred: dog

True: horse

Pred: cat

Proposed Extended VI-CNN Accuracy 83%



True: dog Pred: dog



True: horse Pred: horse



Acknowledgement

This work is supported by,

- ***** National Science Foundation under Award Number DUE-1610911,
- National Science Foundation, NSF XSEDE,
- ✤ GCP and
- SIGHPC/ACM Fellowship.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect those of the National Science Foundation.

