Big Data and Security

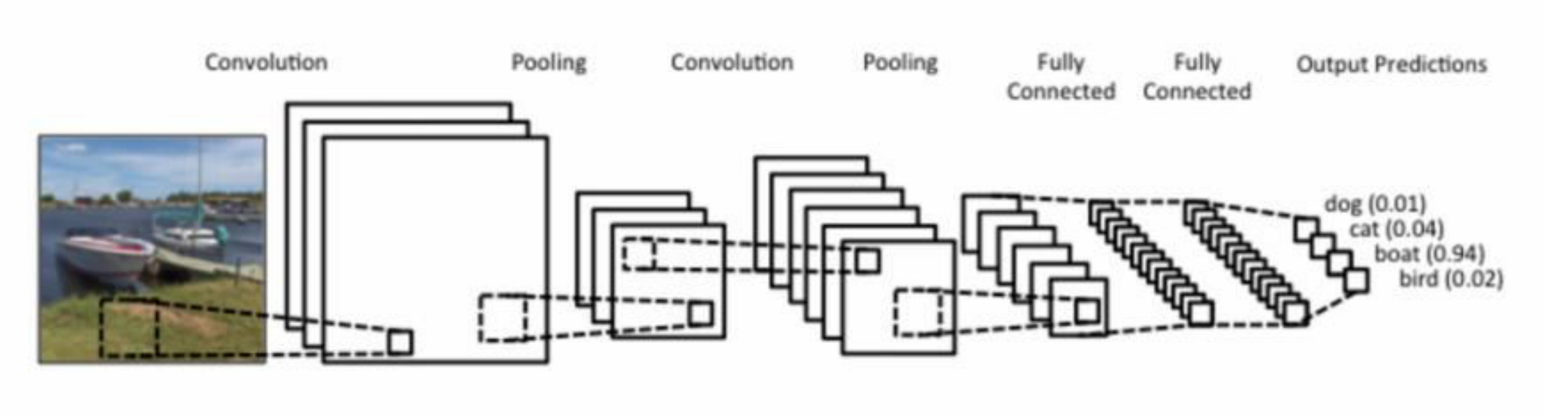
Jeffrey Borowitz, PhD
Lecturer
Sam Nunn School of International Affairs

Neural Nets vs Humans on ImageNet

ImageNet Performance Over Time: It’s not Hype

Migdal, P. (2019, June 28). Human log loss for image classification. Retrieved from https://deepsense.ai/human-log-loss-for-image-classification/

Example "Architecture"

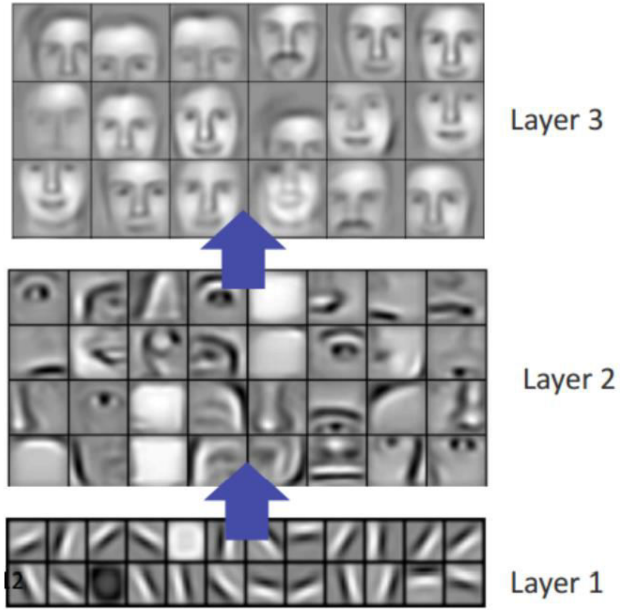


Sudhakar, S. (2017, August 2). Convolution Neural Netw ork. Retrieved
f rom https ://tow ardsdatascience.com/convolution-neural-network-e9b864ac1e6c

Georgia Tech

Neural Networks: Application to Facial Recognition

- Lower levels pick up lines and edges
- Higher levels pick image features like eyes



Chen, Y.-K. (2018, January 15). Convolutional Neural Network (CNN) - image recognition. Retrieved from https://www.slideshare.net/YUNGKUEICHEN/convolutional-neural-network-cnn-image-recognition

Application of Neural Networks: Deep Dream

Inceptionism: Going Deeper into Neural Netw orks. (2015, June 17). Retrieved from https://ai.googleblog.com/2015/06/inceptionism-going-deeper-into-neural.html

The Quintessential Big Data Set ImageNet

- 15 million images
- Linked to objects in 21,000 categories
    - Remember, there are only ~ 200,000 to maybe 1,000,000 words in English

ImageNet Task

- Identify objects in these images
- Model framework:

$$\hat{y} = \hat{f}(X) + \varepsilon$$

  - Here, y represents a probability that each of the 1,000 categories is in a picture (truncated categories from 21,000)
  - X is the amount of each color in each pixel in the image
  - f(X) is a neural net function
- Key metric: top 5 error rate
  - Rank the top 5 probabilities (out of 1,000)

ImageNet Performance Over Time

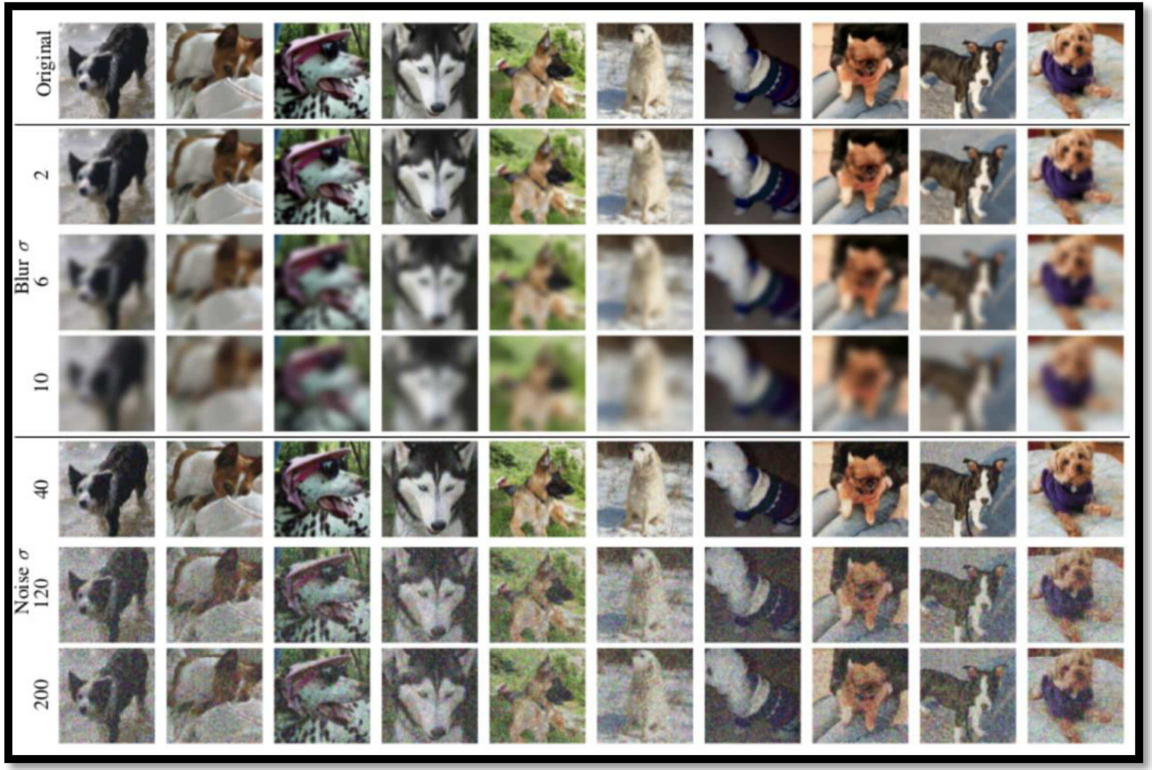
Migdal, P. (2019, June 28). Human log loss for image classification. Retrieved from https://deepsense.ai/human-log-loss-for-image-classification/

Georgia Tech

ImageNet vs People

- People are very good at image recognition in “adverse” circumstances
  - Blurry images, partial images
- ImageNet tends to be better at detailed category recognition

Neural Net Blur Experiment



Samuel, Karam, & Lina. (2017, May 6). A Study and Comparison of Human and Deep Learning Recognition Performance Under Visual Distortions. Retrieved from https://arxiv.org/pdf/1705.02498.pdf

Neural Net Blur Task for People

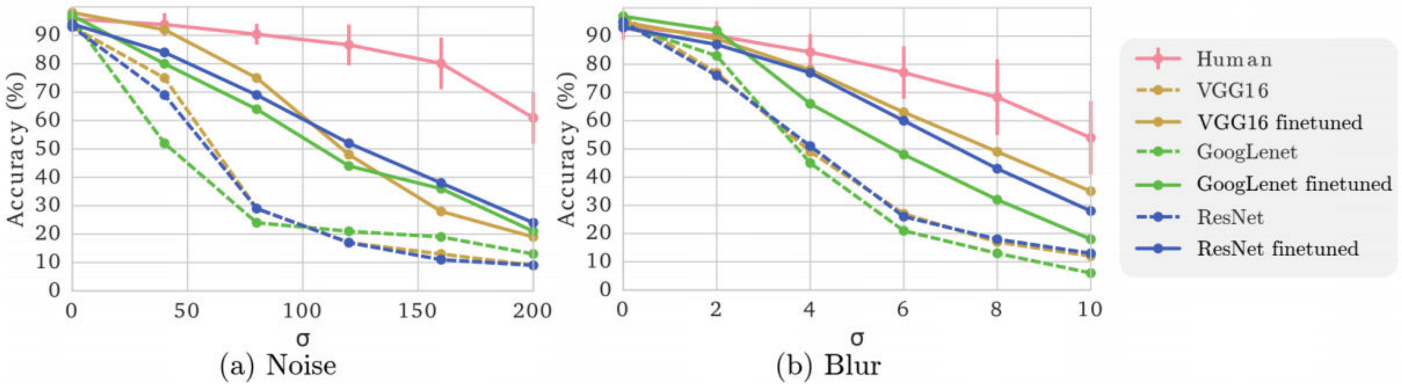
Training Stage

Please browse the classification categories. Later, the experiment will test your ability to classify images into these categories. You will be able to return to this screen if desired. **You will not be able to continue until you have viewed all of the images in all of the categories**

Samuel, Karam, & Lina. (2017, May 6). A Study and Comparison of Human and Deep Learning Recognition Performance Under Visual Distortions. Retrieved from https://arxiv.org/pdf/1705.02498.pdf

Georgia Tech

Neural Net Blur Performance



- Note that even with giving blurred (or noisy), labelled images, neural nets are still worse than people!
- Also note that very few people would be able to do even this well on this task without a task-specific training

Samuel, Karam, & Lina. (2017, May 6). A Study and Comparison of Human and Deep Learning Recognition Performance Under Visual Distortions. Retrieved from https://arxiv.org/pdf/1705.02498.pdf

Implications of Neural Nets

- These fitted models lend themselves to packaging for reuse:
    - The fitted model is just a long list of coefficients
    - Amazon’s Rekognition product is easy to use and encapsulates a pretty high quality model
- Jeff’s view:
    - Appropriately trained, computer vision models can “see” better than people
    - Identifying appropriate training is hard, expensive, time consuming, and likely can be done just once per task

Biases in Neural Nets

- Commercial models (circa 2017) have specific biases:
  - Troublingly are less likely to identify female or non-white faces
- These biases come largely from differential data coverage
  - Neural nets need lots of examples of a given concept to work well.
  - If too many of the pictures are of white males, training processes will favor models that are good at identifying white males

Lesson Summary

- Neural Nets are not just hype
  - ImageNet is substantially better than people at a specific vision task
- People have more "robust" vision, generalizing to new problems better
- Appropriately trained, computer vision models can “see” better than people
  - However, identifying appropriate training is hard and expensive
- Neural Nets can have biases, such as demographic or gender biases