Logo Detection & Classification

5th March 2021

Duke

Brief Problem Overview

Duke

Real Logo

Costco WHOLESALE

Unfortunately the delivery of your order COS-0077945599 was cancelled since the specified address of the recipient was not correct. You are recommended to complete this form and send it back with your reply to us.

Please do this within the period of one week - if we dont get your timely reply you will be paid your money back less 21% since your order was booked for Christmas.

"Costco's" logo is just a bit off. This is what the Costco logo is supposed to look like.

COSTCO® WHOLESALE

See the difference? Subtle, no?

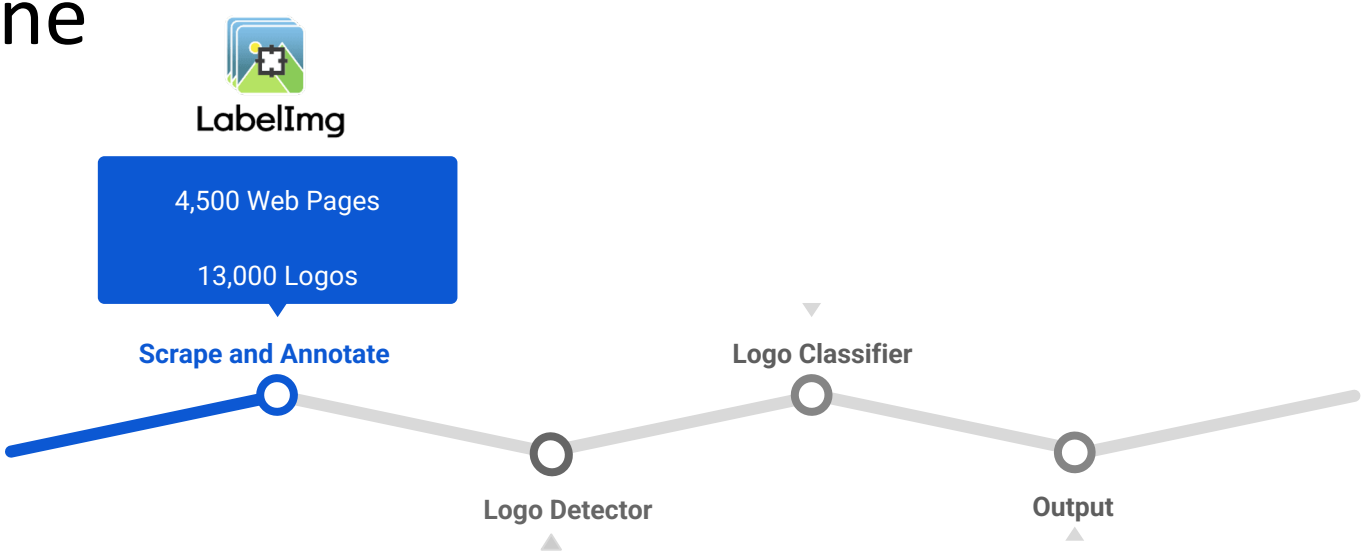
Duke

Ellis, D. (2021, February 19). How to recognize and avoid phishing scams. Retrieved March 05, 2021, from https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Pipeline

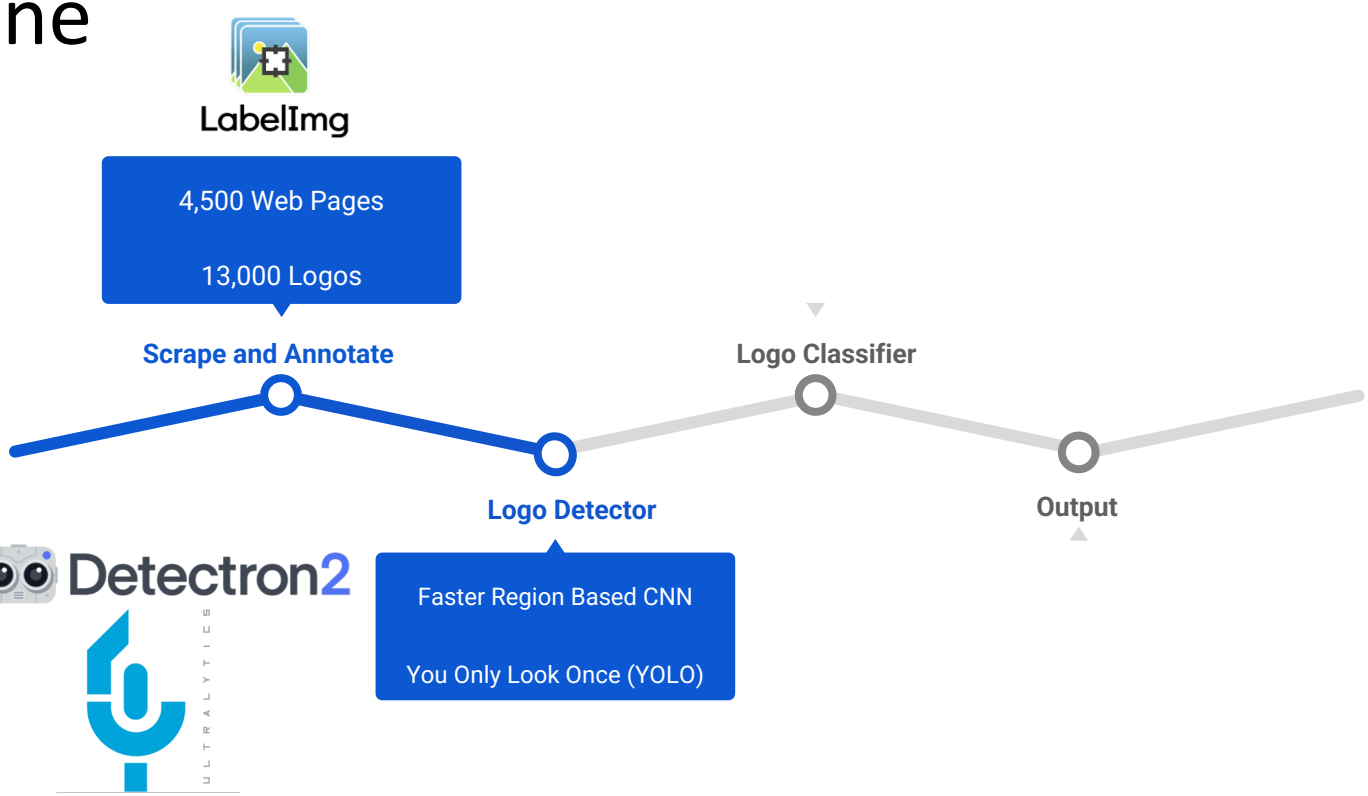
Duke

Pipeline



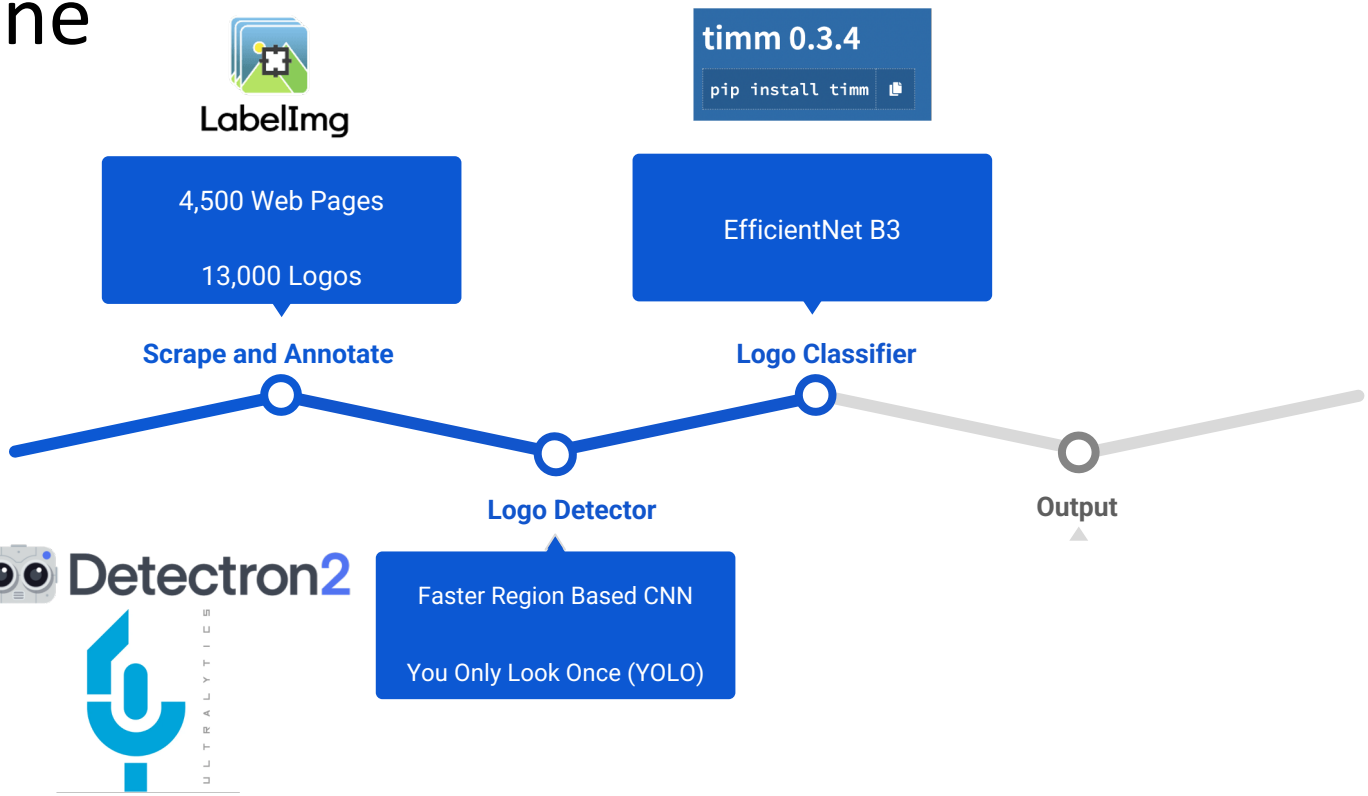
Duke

Pipeline



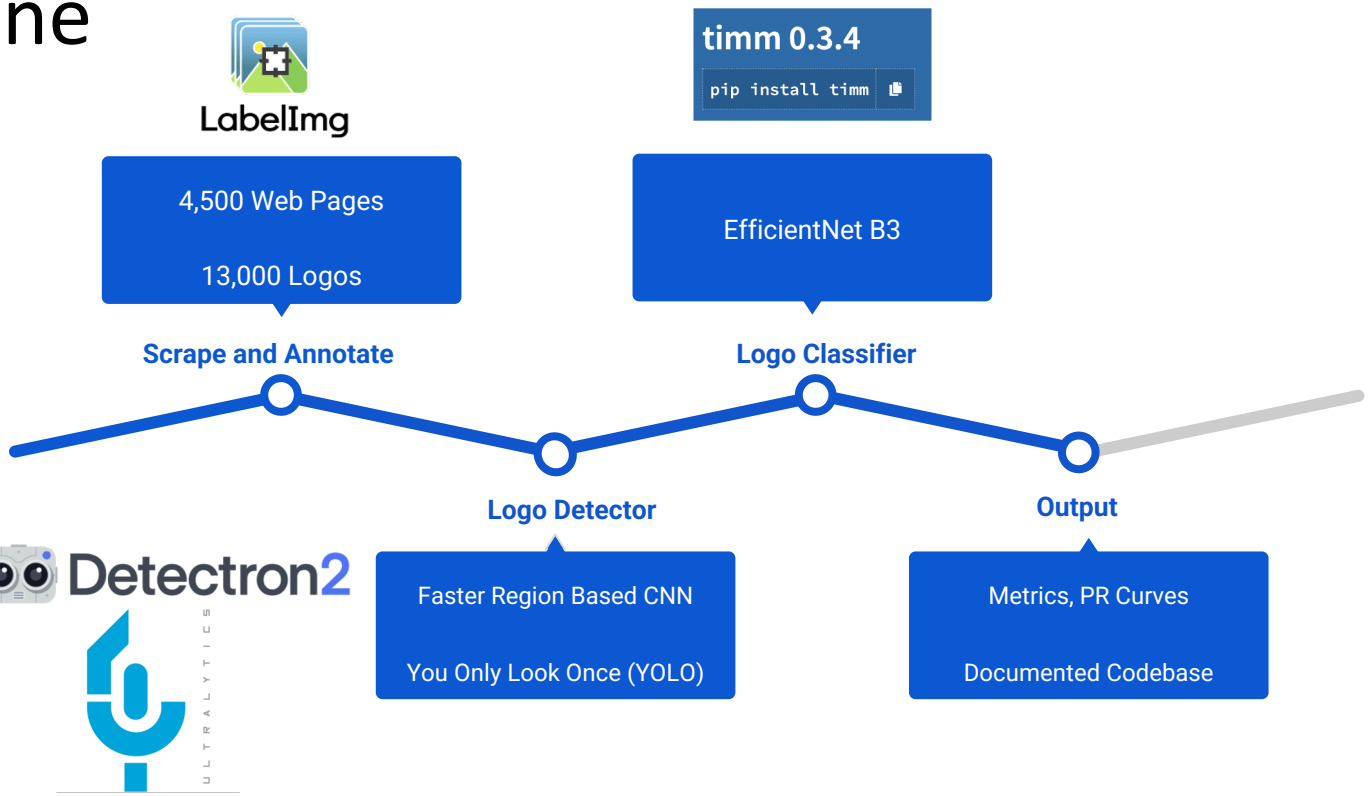
Duke

Pipeline



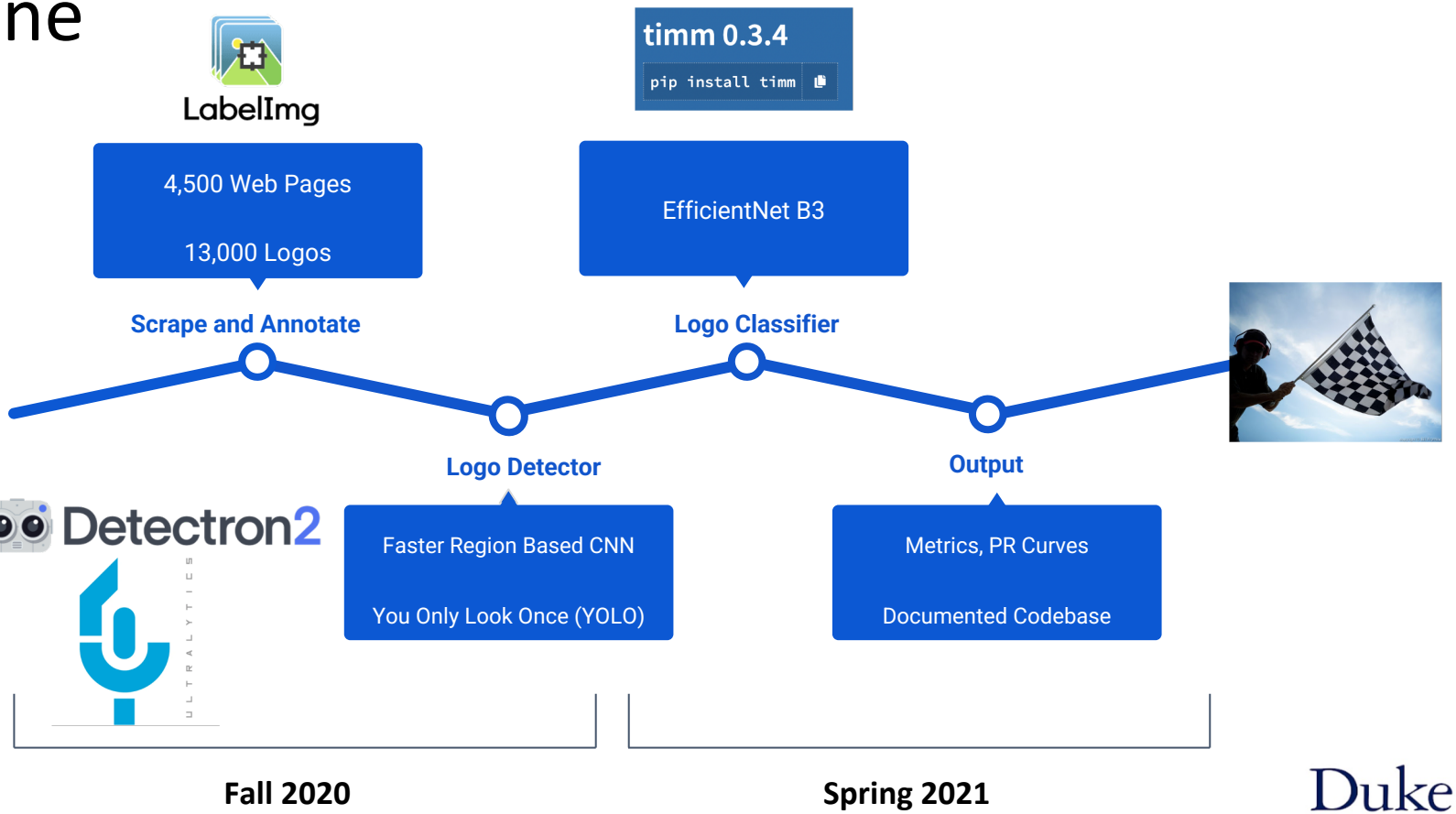
Duke

Pipeline



Duke

Pipeline



Duke

Demo

Duke

Command Line Based Execution

--source : location of images for detection

--detector : yolo or rcnn

--detector-weights : weights for detector

--rcnn-arch : architecture if detector is Faster-RCNN

--detect-thres : detector confidence threshold

--classifier : efficientnet b0 or b3

--classifier-weights : weights for classifier

Duke

Demo

https://colab.research.google.com/drive/12jBFlQVDchfblGxWrmb-UGRcjoq6L6pv#scrollTo=qNuuUaTOVWW-

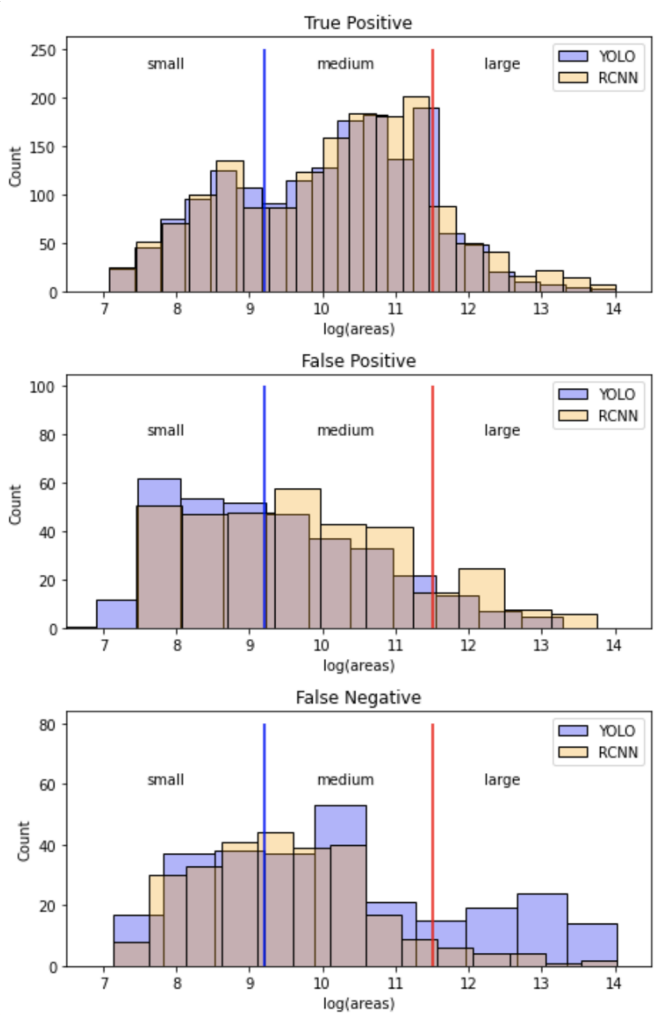
Duke

Detector Results

Duke

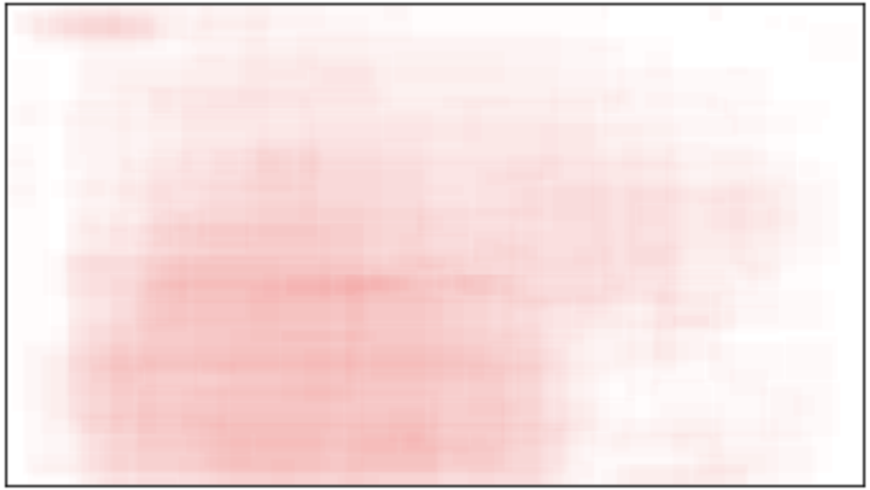
Error Analysis

- YOLO struggles with larger logos.
- Faster RCNN is more prone to false positives.



Duke

YOLO False-Negatives



Faster-RCNN False-Negatives

Duke

Why Train Both YOLO and RCNN?

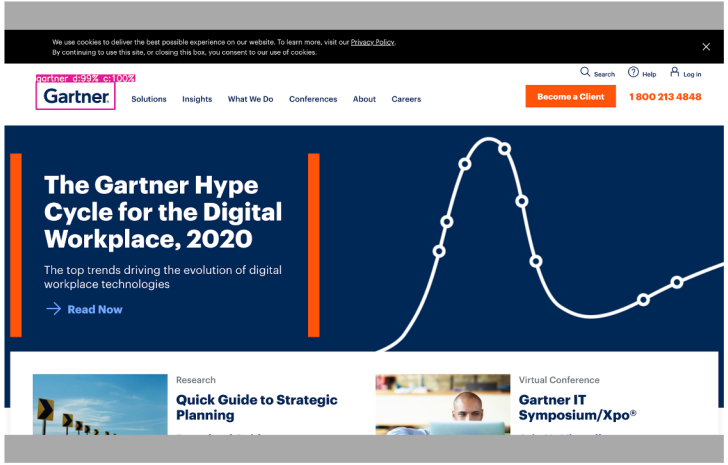
YOLO v3

3.4x Faster

0.044s / image

Faster-RCNN

0.149s / image

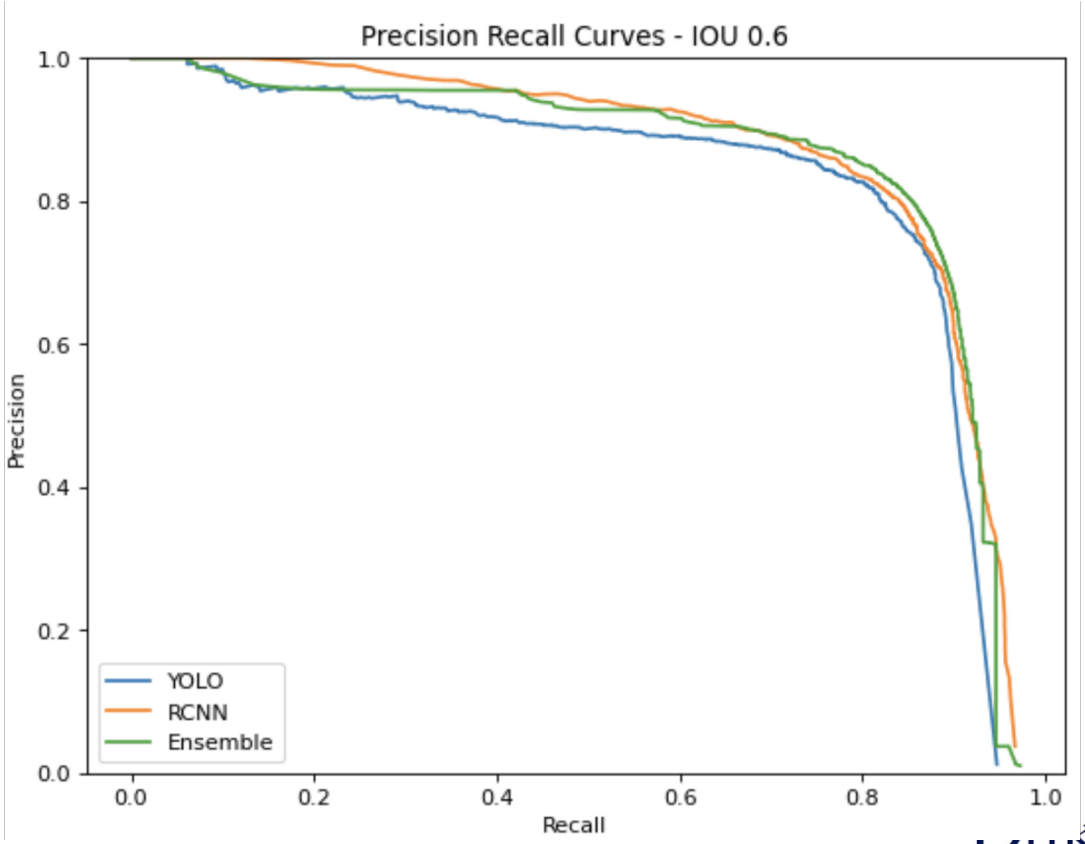


*Using Tesla V100-SXM2-16GB

Duke

Ensembling

- Can combining the models make them better? **YES!**
- Ensembling YOLO and RCNN leads to better performance than both individually.



Classifier Results

Duke

Constructing Classifier

- Data
  - 1098 Classes
    - S&P 500, payment systems, insurance, technology, financial, internet brands
  - Images
    - “Pure” logos from Bing image downloader
    - Extracted annotations from train/test set
  - 12848 train, 4655 validation, 1165 test
- Model
  - EfficientNetB3 pretrained on ImageNet
    - Images resized to 300x300
  - Augmentation
    - RandomResizedCrop, RandomRotation (90), HorizontalFlip, ColorJitter
- Speed on Tesla V100
  - 0.05s per screenshot → 0.0125s per logo

Duke

Results of EfficientNetB3

	Accuracy	Precision*	Recall	F1-Score	Support
Val	0.9386	0.9496	0.9386	0.9362	4,655
Test**	0.9373	0.9780	0.9373	0.9532	1,165

*Not all classes had a prediction

**Test set consisted of 320 classes common to test annotations and train/val data

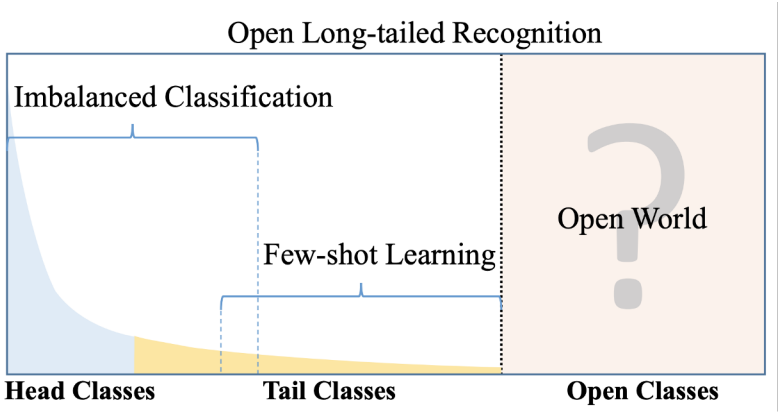
Duke

Open Set Learning

Duke

What is Open Set Learning?

- We want our model to be able to say “This is a logo I don’t recognize.”
- Reduce the chances of misclassification into known categories.



Duke

K-Nearest Neigbors Based Open Set Learning

- Implementing: Nearest Neighbors Distance Ratio Open-Set Classifier

  a. Do KNN with 2 nearest neighbors based on Activation Vectors.

  b. If neighbors agree, classify as predicted.

  c. Otherwise calculate ratio:
     T = distance to closest neighbor / distance to second neighbor

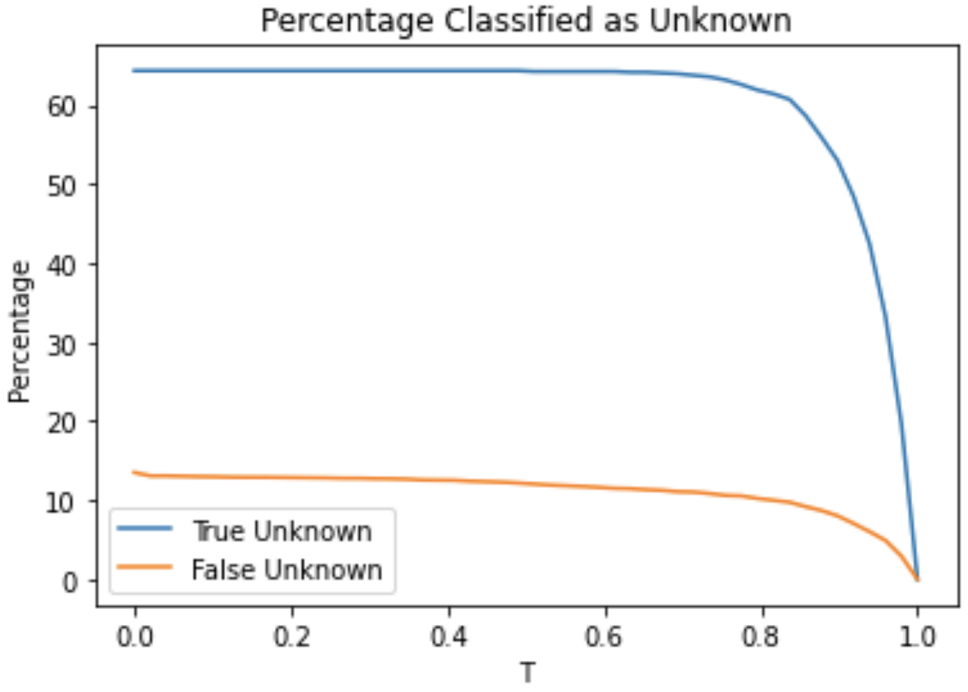
  d. If T < threshold, classify as closest neighbor, otherwise classify as unknown.

  e. Choose threshold based on prediction accuracy.

Duke

Open Set Preliminary Results

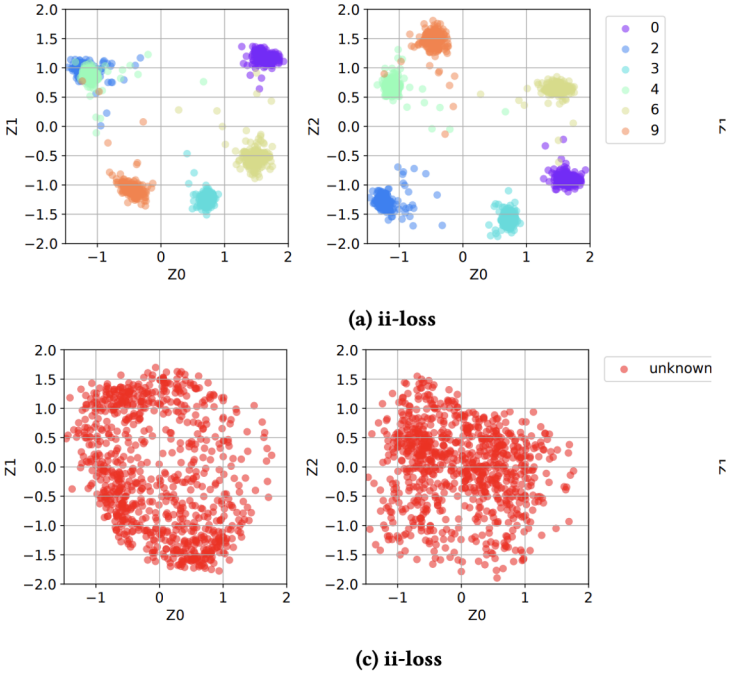
- 61.4% of unknown correctly classified as unknown.
- 9.99% of known incorrectly classified as unknown.



Duke

Possible Improvements

- Want to maximize chances of neighbors being same class for known logos.
- Increase distance between classes to incorporate use of a distance threshold.
- Use loss function to train classifier to put known classes far apart.

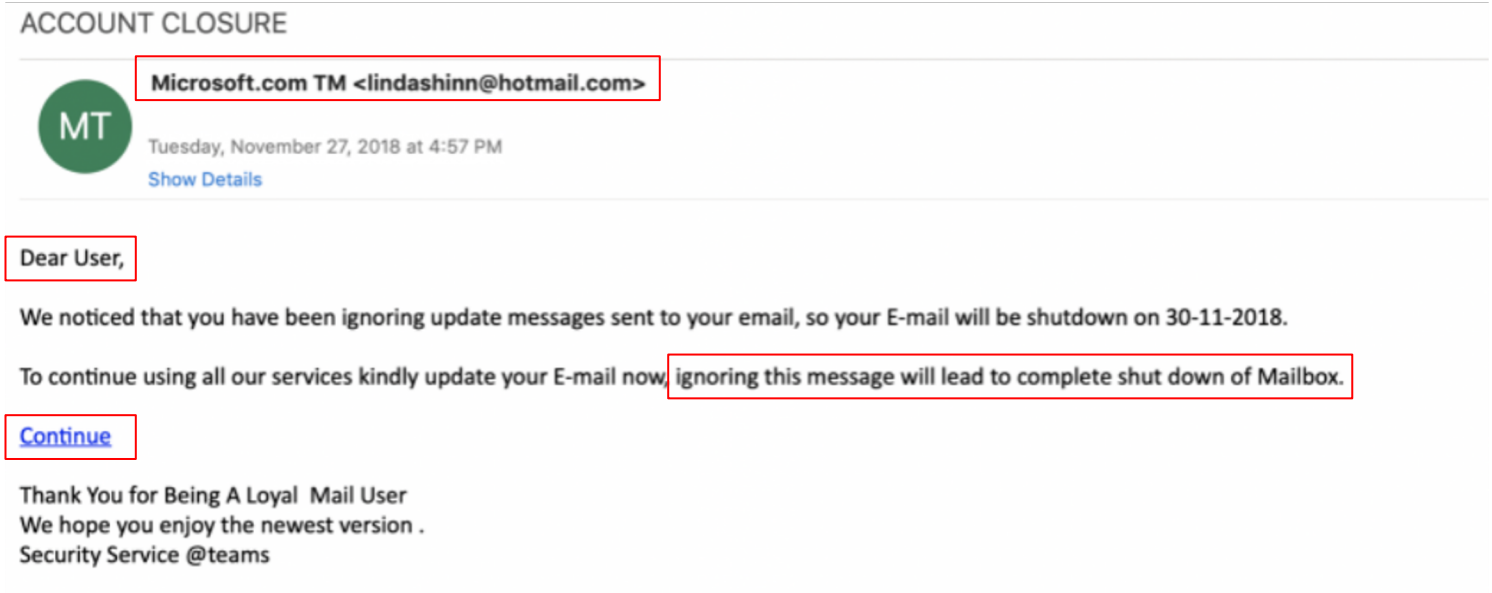


Duke

Appendix

Duke

Standard Phishing/Spam Email



ACCOUNT CLOSURE

MT

Microsoft.com TM <lindashinn@hotmail.com>

Tuesday, November 27, 2018 at 4:57 PM

Show Details

Dear User,

We noticed that you have been ignoring update messages sent to your email, so your E-mail will be shutdown on 30-11-2018.

To continue using all our services kindly update your E-mail now, ignoring this message will lead to complete shut down of Mailbox.

Continue

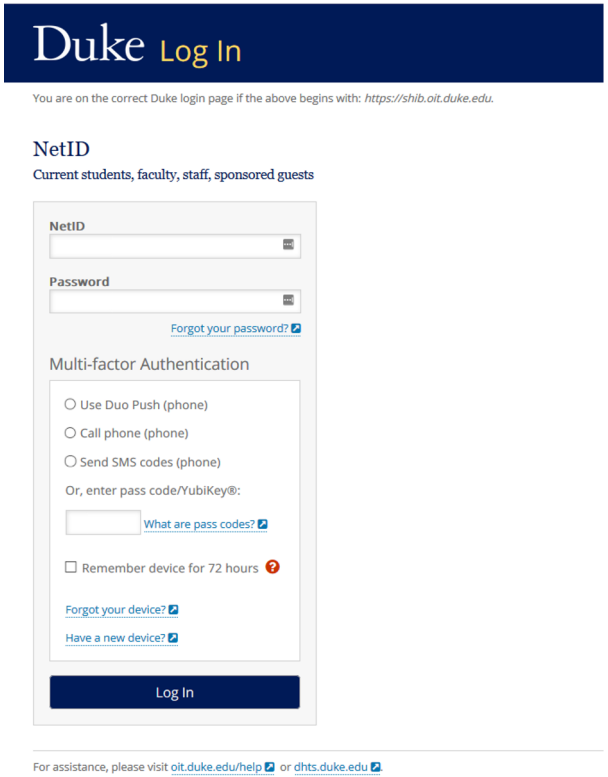
Thank You for Being A Loyal Mail User
We hope you enjoy the newest version .
Security Service @teams

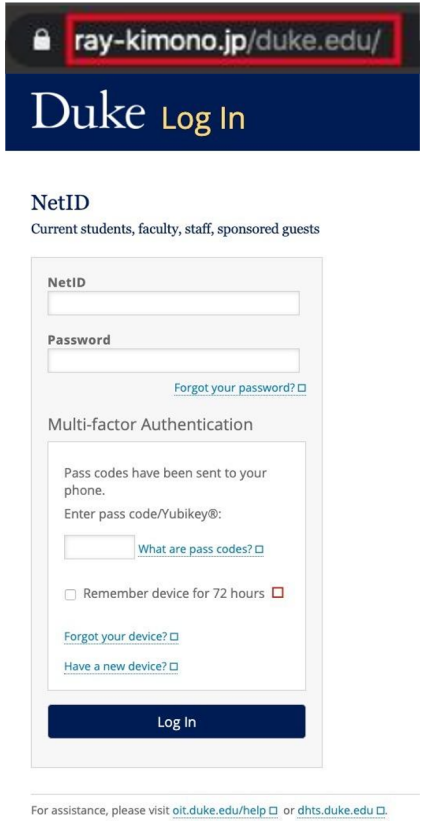
https://security.duke.edu/phish-20181127

Duke

Phishing at Duke

https://shib.oit.duke.edu/idp/authn/external?conversation=e1s1





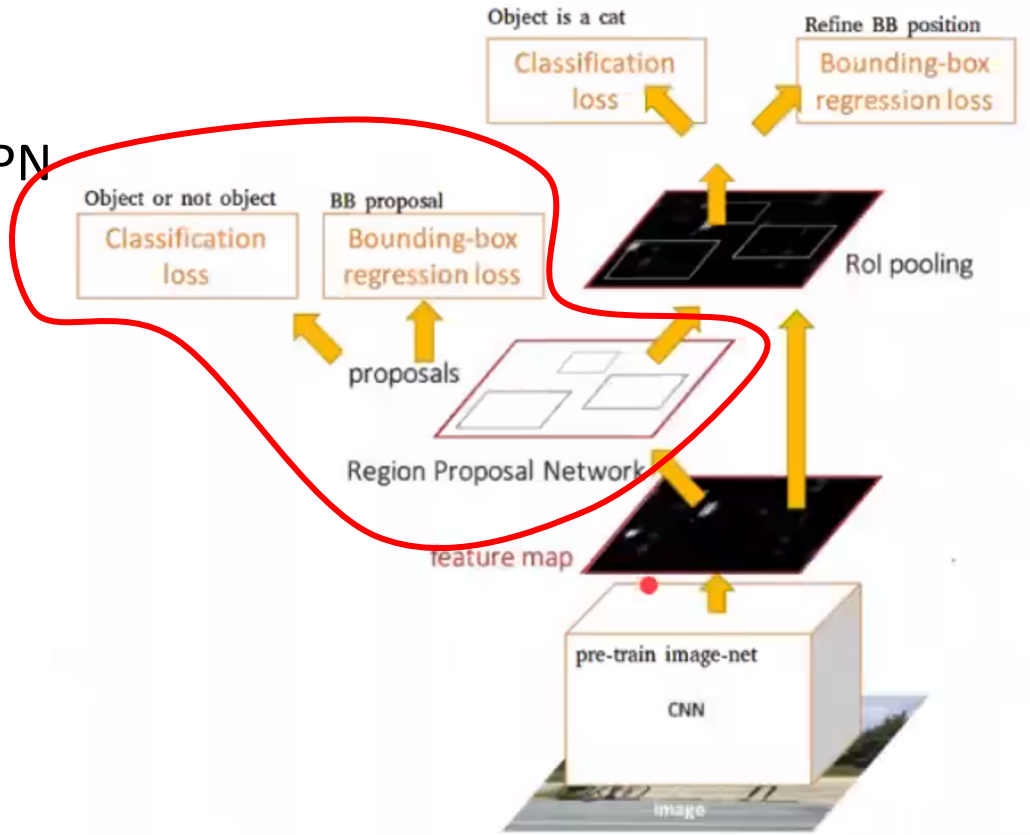
https://security.duke.edu/phish-20200413

Duke

Faster R-CNN (2016)

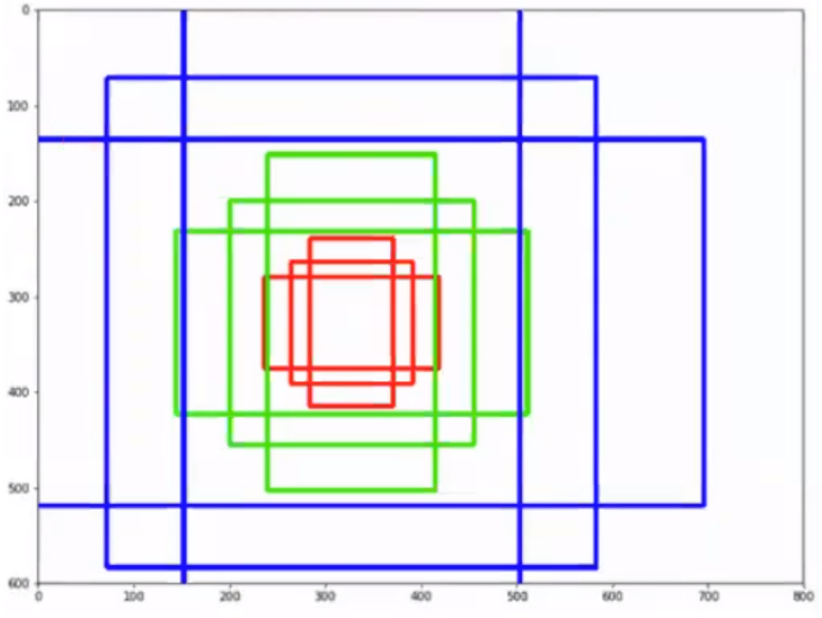
- Region Proposal Network (RPN)
  - **Initial Guess**
  - Fully Convolutional Network
  - Outputs :
    - Rectangular Object Proposal
    - Objectness Score

- **RPN + Fast R-CNN**



How does RPN Work?

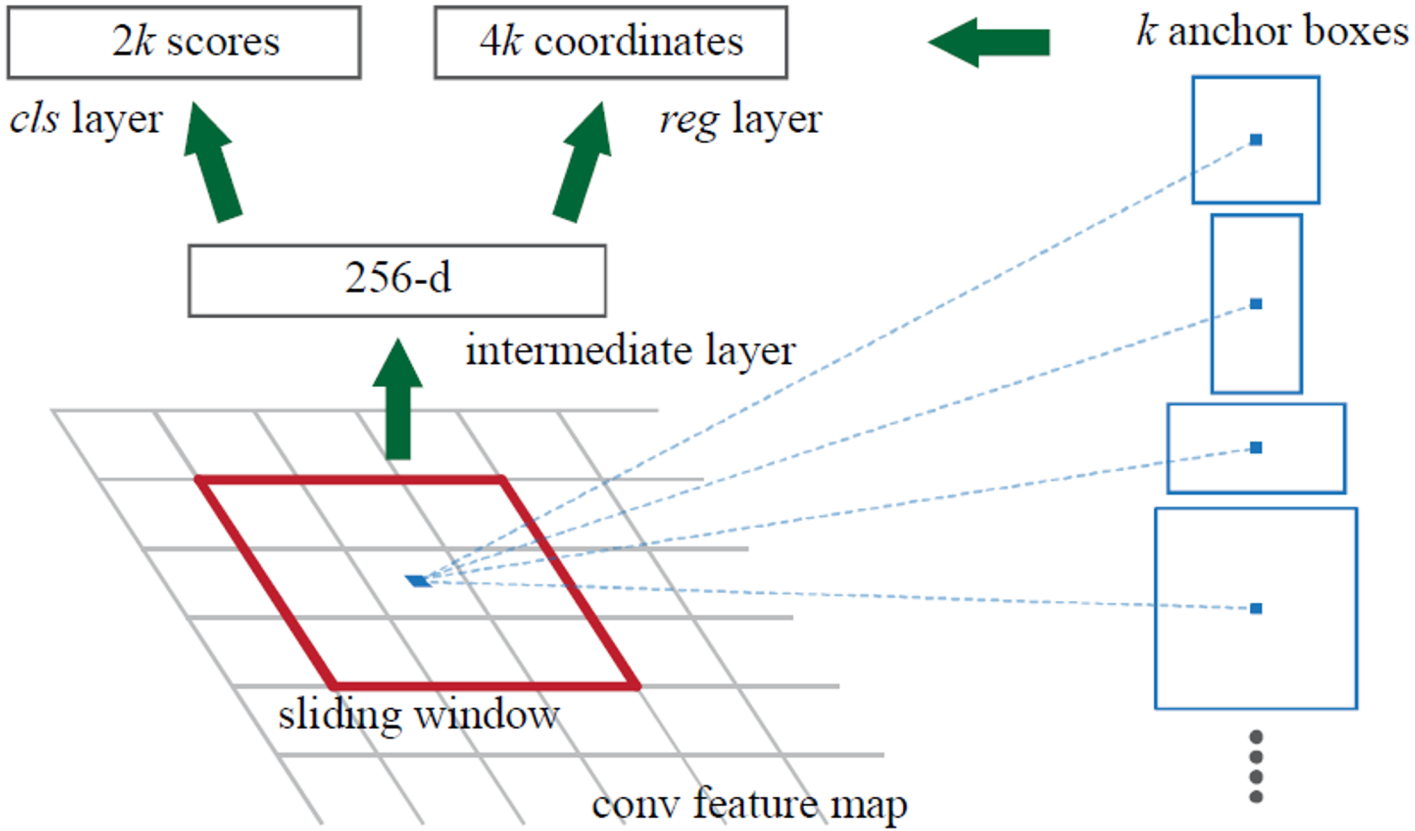
- Anchors
  - **Initial Initial guess** (Input to RPN)
  - Anchors are shapes and aspect ratios we place at every pixel on image
  - They are not meant to be close to the ground truth bounding box. They are just a starting point **proposal.** Hence Region Proposal Network (RPN)



k = *9* anchor boxes per pixel
Total Anchor Boxes = W * H * k

- **RPN prunes anchor boxes**

Duke


2k scores
4k coordinates
k anchor boxes
cls layer
reg layer
256-d
intermediate layer
sliding window
conv feature map

YOLO v3

'*k*' Anchor Boxes per grid

Input = Img

S × S grid on input

S X S

Bounding boxes + confidence

Class probability map

Output per Anchor Box

= (x, y, w, h, confidence)

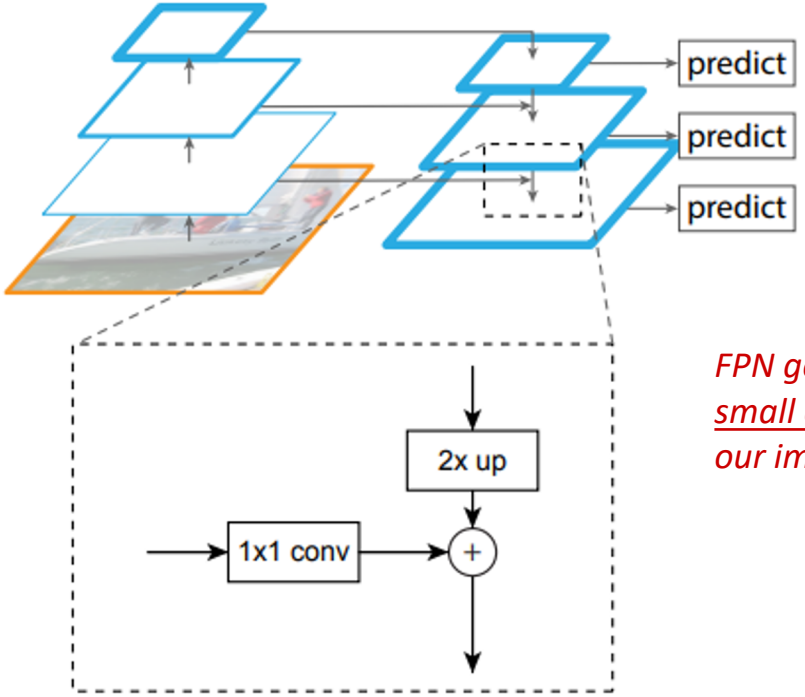
Final detections

If there are 'C' classes the output is

= k X C X 5

Duke

Feature Pyramid Network (FPN)

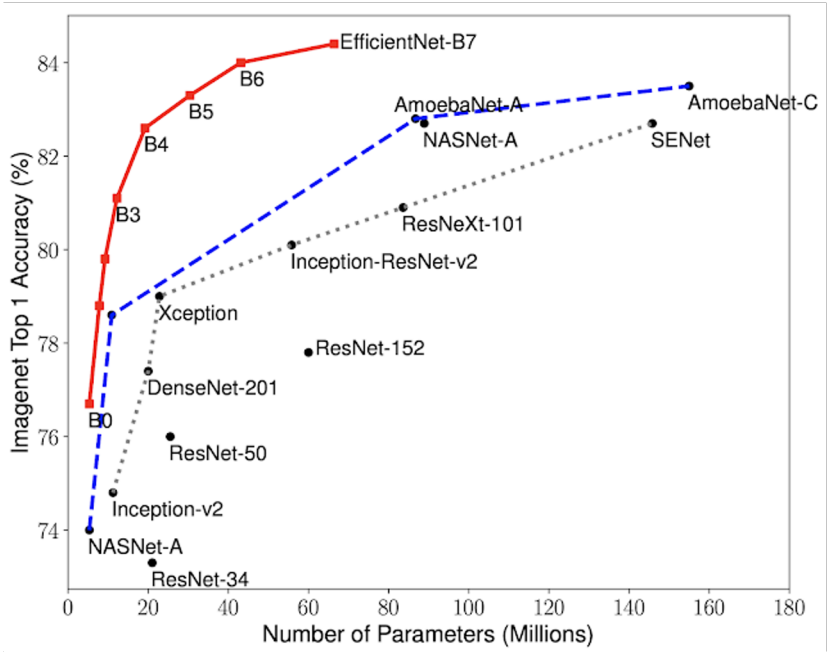


FPN good when we have small and big objects in our images

Duke

EfficientNet

- Focus on improving scaling of CNNS
  - Depth, width, resolution
- Compound scaling method
  - Fix resource (FLOPs) and scaling coefficient
- Similar or better performance and significantly smaller than other CNN architectures



Tan, Mingxing, and Quoc Le. "Efficientnet: Rethinking model scaling for convolutional neural networks." *International Conference on Machine Learning*. PMLR, 2019.

Duke

Sample Images for Classifier

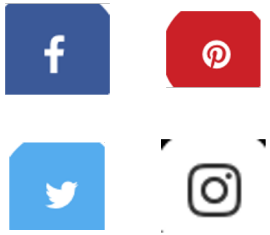
Bing Downloader

Annotation Extracted

Duke

False Positives of Ensemble

False Negatives of Ensemble



Duke