

The background features two abstract network graphs. On the left, a dense cluster of red nodes is connected by thin red lines. On the right, a more dispersed cluster of blue nodes is connected by thin blue lines. A thin green horizontal line runs across the middle of the image, positioned just below the text.

# Insights into Convnets

# Today's agenda:

## 1. Review

- Convolutional layer
- Downsampling
- Augmentation

## 2. Insights

- Transfer learning
- Ensembling
- Unbalanced data
- Cons of Convnets

## 3. Tutorial

# Convnets

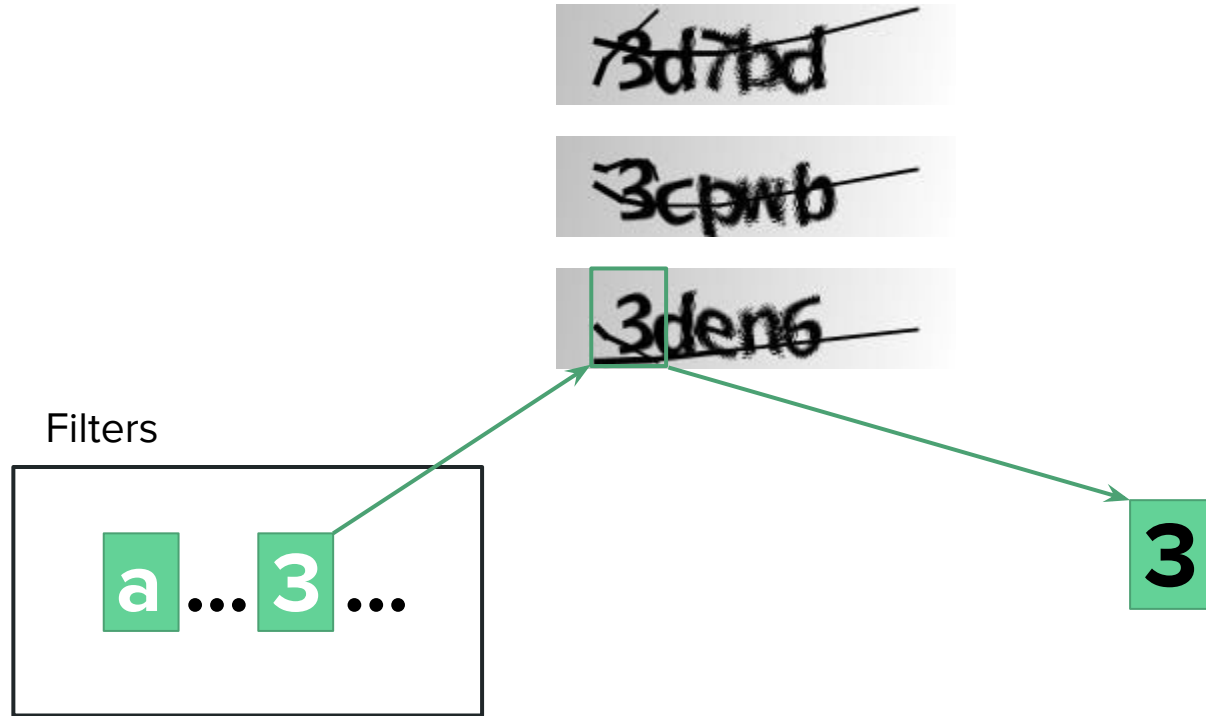
The success of Deep Learning in the field of computer vision is in large part due to a very clever feature selection scheme utilizing “convolutions”.

The key to the success of Convnets lies in:

- Accounting for translational variations
- Focusing on spatially localized patterns

And doing so with a relatively few number of parameters!

# Primitive OCR



# Downsampling

Convolutional layers have a tree structure with each filter representing a branch. Ultimately the branches have to come together through downsampling.

- Downsampling with Strides
- Downsampling with Pooling layers

# Strides vs Pooling

As compared to Pooling, longer strides

- Downsample more aggressively
- Are computationally less taxing

ResNet uses stride=2 in its first Conv2D layer, so it does work better sometimes!

# Not enough data

As is often the case, you might not have enough data to effectively train a robust Convnet to endow vision to your computer.

Since Convnets focus on spatially localized patterns, expanding your dataset with augmentation can often boost their learning.

Are there any risks to using data augmentation?

# Insights into transfer learning

- Where to cut the base pre-trained model
- To (re-)train or not to train
- Preprocessing vs Training



# Ensembling

Human performance could refer to an average human, an expert in the field or a team of experts, each with higher level of performance.

Similarly a 'team' of ML models can outperform individual models.

- Random forests
- Ensembled DL models

# Unbalanced data

- Poor performance on the minority class
- Desired metric
- Improving performance:
  - Use balanced batches by oversampling the minority class
  - Use loss function corresponding to the desired metric
  - Adjust the thresholds to align with the desired metric

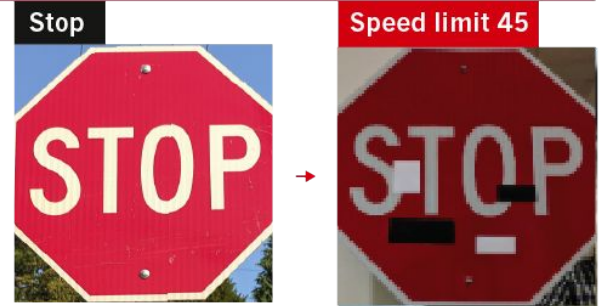
# Cons of Convnets

Convnets oversimplified simply slide a complicated filter over the image. It is thus not too difficult to reverse engineer an image that triggers a specific filter.

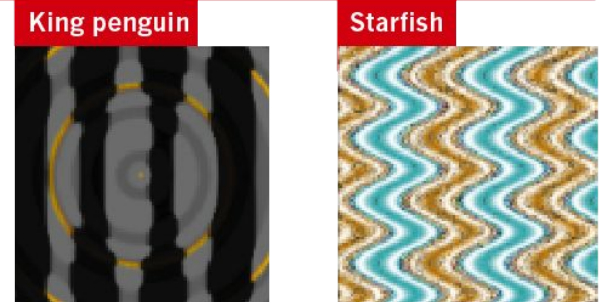
## FOOLING THE AI

Deep neural networks (DNNs) are brilliant at image recognition — but they can be easily hacked.

These stickers made an artificial-intelligence system read this stop sign as 'speed limit 45'.



Scientists have evolved images that look like abstract patterns — but which DNNs see as familiar objects.



©nature

Source: <https://www.nature.com/articles/d41586-019-03013-5>

# Tutorial

Practice makes perfect!