Universal Perturbations

Thursday, May 25, 2017 2:12 PM

- Background: Deep Machine Learning
  - Like human brain
  - Translate data through layers and make a decision
  - Like when you show someone a pic they know what it is
- Univ. Pert.
  - Modifies an image but humans can't tell
  - Adds noise so machines can't tell --> wrong decision in telling what it is
  - Can train machines to tell its wrong but still gets it wrong majority
    - independent of neural network and image chosen
- Reasons
  - Decision Boundaries: decision A on left decision B on right
  - Applications
    - being anonymous in connected society
    - Hacking: potential application to semantic segmentation
- Applications:
  - face paint: but can tell
  - tshirts: not overt but it can work
  - Semantic Segmentations: hacking
    - use UP to remove all people from image
- What is the future?
  - Security issues
  - Maintaining privacy