Deepfakes at CMU: Research Coordination Meeting

Zach Kurtz

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0759

Agenda

- Overview of deepfakes terminology
- CMU research spotlight:
  - A. Bansal, S. Ma, D. Ramanan, Y. Sheikh. Recycle-GAN: Unsupervised Video Retargeting. In ECCV, 2018
  - Robotics: pose detection, facial synthesis, etc.
- Introductions
- Discussion:
  - Current open problems in deepfakes with regard to
    - detection
    - generation
    - policy, ethics?
  - Which sub-areas is CMU is best-positioned to lead?
  - Where could cross department collaboration help?

Video manipulation terminology

Washington Post taxonomy of video manipulation:

- Missing context
- Deceptive editing
- Malicious transformation -> doctoring vs fabrication

Deepfakes are within transformation -> fabrication.

- Always malicious?
- Necessarily deep neural networks?
- Context matters: intent to deceive?