



Deepfakes at CMU: Research Coordination Meeting

Zach Kurtz

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

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?