Panel Discussion II - Ethics & Forensics of AI

New Challenges

- The development of AI technology, in particularly, deep learning and their applications in computer vision, has brought forth significant advances to surveillance.
- With the improvement in performance, they also introduce new challenges to the research community.
  - Biases
  - Malicious attacks
  - Manipulations
  - Privacy

Biases

- The heavy reliance of the deep learning based systems on annotated training data also introduce biases to the trained system, thus their fairness with regards to established social values is an important concern recently.
  - Under-represented social groups
  - Gender
  - Age groups

Malicious Attacks

- Deep learning based systems are fragile and susceptible to malicious attacks in the form of
  - training data poisoning
  - deep network backdoor (backdoor poisoning attack)
  - adversarial examples
- The security of the deep learning based surveillance systems needs to be addressed

Manipulations

- Deep learning based methods can also be used to create or tamper digital audio-visual signals misleading surveillance systems and we need to develop effective forensic technology to counter the fake media
  - DeepFakes
  - GAN generated faces

Privacy

- The increasing scales of automatic video surveillance, especially face recognition has also raised significant concerns about the ethical issues in using such technologies

Questions to Discuss

- How do we reduce biases in the DL-based system?
- How do we protect privacy while at the same time keeping data utility?
- How do we effectively detect manipulated media in surveillance system?

Open Questions

We had a fruitful discussion in yesterday's panel on the third wave AI. We might extend discussion here. How to think out of the box and better address the ethics / forensics of AI?

- What kind of AI technology should be developed/encouraged? And what should not?
- Technology vs. human / nature. Can we build a better world with technology harmonic? Or we will end up cyberpunk (combination of lowlife and high tech)?