UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

Qualifying Examination

Wednesday July 20, 2022 at 9:30am via Zoom

Qi Li

Forensics and Attribution of Advanced Forged Audio

Chair: Dr. Fangju Wang
Advisor: Dr. Xiaodong Lin
Advisory: Dr. Andrew Hamilton-Wright
Non-Advisory: Dr. Sheng Yang [SoE]
Non-Advisory: Dr. Rozita Dara

Abstract:

Audio synthesis, conversion and adversarial learning technologies have achieved a magnificent success due to the development of deep learning. However, these technologies are also double-edge swords and have even opened Pandora's box. Continuous innovative deep forgery schemes and updated detection methods have made both two sides become armament race.

To solve this dilemma, we propose a proactive, sustainable and creative solution in this proposal. In a nutshell, we embed watermark in audio samples and guarantee the quality of audio samples. Furthermore, according to error coding theory, we reveal the limitation of existing proactive image watermarking scheme for deep fake, and propose a new fast feasible watermark space generation algorithm. Finally, thorough experiment prove that our embedded watermark has inherent transferability to deep audio forgery processing. Considerable experiment and analysis demonstrate our solution (1) is applicable to many state-of-the-art deep voice forgery schemes; (2) has negligible negative consequence to audio quality; (3) keeps robust and stable for basic audio operations including adding noise, denoising, copy and move, cutting, resampling and compression; (4) has secrecy and is hard to be attached; (5) achieves great performance in audio forgery detection and attribution; (6) provides efficient and fast watermark generation algorithm and matching algorithm.

In our future work, we formalize two closely related research challenges with clear technical paths and milestones. Our goal is to address the problem of proactive and passive detection and forensics of deep fake in different forms of media, including audio, image, video, text and composite media. And in the process, we explore privacy and ethical issues in deep fake. In general, in response to the negative impact of deep fake, we will try to address the issue in terms of privacy, detection, forensics, and prevention.