Department of Computer Science

COMPUTER SCIENCE SEMINAR SERIES

Toward Secure Image Denoising: A Machine Learning based Realization

SPEAKER **Mr Yifeng ZHENG**

PhD Student
Department of Computer Science
City University of Hong Kong
Hong Kong

DATE 2 May 2018 (Wednesday)
TIME 10:00 am - 10:30 am
VENUE CS Seminar Room, Y6405
6th Floor, Yellow Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Image denoising via machine learning techniques, particularly neural networks, has been shown to achieve state-of-theart performance. However, in practice security and privacy issues undesirably arise in applying a trained machine learning model to image denoising. In this paper, we propose a system framework that enables the owner of a trained machine learning model to provide secure image denoising service to an authorized user, via the aid of cloud computing. Our framework ensures that the cloud server learns nothing about the model and the user's images, while the user learns nothing about the model except denoised images. Experiments are conducted for performance evaluation, and the results show that our design can achieve denoising quality close to that in the plaintext domain. For future work, we plan to explore various directions for optimizing the runtime performance.

This paper was presented at the IEEE International Conference on Accoustics, Speech, and Signal Processing (ICASSP), April 15-20, 2018, Calgary, Alberta, Canada.

Supervisor: Dr Cong WANG

Research Interests: Cloud Security; Privacy-aware Computing; Multimedia Security.

All are welcome!

In case of questions, please contact Dr WANG Cong at Tel: 3442 2010, E-mail: congwang@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.