香港浸會大學理學院
HKBU Faculty of Science

DEPARTMENT OF COMPUTER SCIENCE

PhD Degree Oral Presentation

PhD Candidate:	Mr Guangcan MAI
Date	29 August 2018 (Wednesday)
Time:	2:30 pm - 4:30 pm (35 mins presentation and 15 mins Q & A)
Venue:	RRS732, Sir Run Run Shaw Building, HSH Campus

"Biometric System Security and Privacy: Data Reconstruction and Template Protection"

Abstract

Biometric systems are being increasingly used, from daily entertainment to critical applications such as security access and identity management. It is known that biometric systems should meet the stringent requirement of low error rate. In addition, for critical applications, the security and privacy issues of biometric systems are required to be concerned. Otherwise, severe consequence such as the unauthorized access (security) or the exposure of identity-related information (privacy) can be caused. Therefore, it is imperative to study the vulnerability to potential attacks and identify the corresponding risks. Furthermore, the countermeasures should also be devised and patched on the systems.

In this thesis, we study the security and privacy issues in biometric systems. We first make an attempt to reconstruct raw biometric data from biometric templates and demonstrate the security and privacy issues caused by the data reconstruction. Then, we make two attempts to protect biometric templates from being reconstructed and improve the state-of-the-art biometric template protection techniques.

To summarize, this thesis makes the following contributions:

- Data Reconstruction: An investigation of the invertibility of face templates generated by deep networks. To the best of our knowledge, this is the first such study on the security and privacy of face recognition systems.
- Template Protection: An end-to-end method for simultaneously extracting and protecting the templates given raw biometric data (e.g. face images). To the best of our knowledge, this is the first end-to-end method for generating secure templates directly from raw biometric data.
- Template Protection: A binary fusion approach for multi-biometric cryptosystems to offer accurate and secure recognition. The proposed fusion approach can simultaneously maximize the discriminability and entropy of the fused binary output.

***** ALL INTERESTED ARE WELCOME *****