GEO-TAGGING AND PRIVACY-PRESERVATION IN MOBILE CLOUD COMPUTING

Qia Wang

Dr. Wenjun Zeng, Dissertation Supervisor

ABSTRACT

With the emerge of the cloud computing service and the explosive growth of the mobile devices and applications, mobile computing technologies and cloud computing technologies have been drawing significant attentions. Mobile cloud computing, with the synergy between the cloud and mobile technologies, has brought us new opportunities to develop novel and practical systems such as mobile multimedia systems and cloud systems that provide collaborative data-mining services for data from disparate owners (e.g., mobile users). However, it also creates new challenges, e.g., the algorithms deployed in the computationally weak mobile device require higher efficiency, and introduces new problems such as the privacy concern when the private data is shared in the cloud for collaborative data-mining.

The main objectives of this dissertation are: 1. to develop practical systems based on the unique features of mobile devices (i.e., all-in-one computing platform and sensors) and the powerful computing capability of the cloud; 2. to propose solutions protecting the data privacy when the data from disparate owners are shared in the cloud for collaborative data-mining.

We first propose a mobile geo-tagging system. It is a novel, accurate and efficient image and video based remote target localization and tracking system using the Android smartphone. To cope with the smartphones' computational limitation, we design light-weight image/video processing algorithms to achieve a good balance between estimation accuracy and computational

complexity. Our system is first of its kind and we provide first hand real-world experimental results, which demonstrate that our system is feasible and practicable.

To address the privacy concern when data from disparate owners are shared in the cloud for collaborative data-mining, we then propose a generic compressive sensing (CS) based secure multiparty computation (MPC) framework for privacy-preserving collaborative data-mining in which data mining is performed in the CS domain. We perform the CS transformation and reconstruction processes with MPC protocols. We modify the original orthogonal matching pursuit algorithm and develop new MPC protocols so that the CS reconstruction process can be implemented using MPC. Our analysis and experimental results show that our generic framework is capable of enabling privacy preserving collaborative data-mining. The proposed framework can be applied to many privacy preserving collaborative data-mining and signal processing applications in the cloud.

We identify an application scenario that requires simultaneously performing secure watermark detection and privacy preserving multimedia data storage. We further propose a privacy preserving storage and secure watermark detection framework by adopting our generic framework to address such a requirement. In our secure watermark detection framework, the multimedia data and secret watermark pattern are presented to the cloud for secure watermark detection in a compressive sensing domain to protect the privacy. We also give mathematical and statistical analysis to derive the expected watermark detection performance in the compressive sensing domain, based on the target image, watermark pattern and the size of the compressive sensing matrix (but without the actual CS matrix), which means that the watermark detection performance in the CS domain can be estimated during the watermark embedding process. The correctness of the derived performance has been validated by our experiments. Our theoretical

analysis and experimental results show that secure watermark detection in the compressive sensing domain is feasible.

By taking advantage of our mobile geo-tagging system and compressive sensing based privacy preserving data-mining framework, we develop a mobile privacy preserving collaborative filtering system. In our system, mobile users can share their personal data with each other in the cloud and get daily activity recommendations based on the data-mining results generated by the cloud, without leaking the privacy and secrecy of the data to other parties. Experimental results demonstrate that the proposed system is effective in enabling efficient mobile privacy preserving collaborative filtering services.