UNIVERSITY of GUELPH

COLLEGE of ENGINEERING AND PHYSICAL SCIENCES

SCHOOL OF COMPUTER SCIENCE

MSc Seminar

Thursday July 29, 2021 at 9AM via Zoom

A Fair and Privacy-preserving Image Trading System Based on Blockchain and Group Signature

Le Wang

Advisor: Dr. Xiaodong Lin
Advisory Member: Dr. Rozita Dara

ABSTRACT:

Digital imaging devices such as digital camera are becoming more integrated in our lives. Before, they were simply used for entertainment purposes. However, people are now starting to use them for a profession, by sharing, selling and trading pictures and images. As a result, an online market place for image trading is imperative to ensure the success of this profession. To satisfy the needs of image trading, there already exists many image trading service providers (ITSPs), such as ShutterStock, iStockphoto, Fotolia, Dreamstime. They can offer users efficient and convenient image transaction services with a much lower marginal cost than traditional approaches.

Unfortunately, transaction unfairness and users' privacy breaches have become major concerns since the ITSPs might be untrusted and able to manipulate image trading prices and infer users' private information. Recently, several approaches have been proposed to address the unfairness issue by using the decentralized ledger technique and smart contract, but users' privacy protection is not considered. In this study, we will introduce how we propose a fair and privacy-preserving protocol that supports image fair exchange and protects user privacy. In particular, we exploit blockchain and Merkle tree to construct a fair image trading protocol with low communication overhead based on smart contract, which serves as an external judge that resolves disputes between buyers and sellers in image transactions. Moreover, we design a privacy-preserving protocol based on a popular short group signature scheme to protect users' identity privacy, prevent linkability of transactions from being inferred, and ensure traceability of malicious users, for example, who may sell fake images or the ones violating copyright and/or refuse to pay. Also, we will discuss our plan for implementing the proposed blockchain-based image trading system, which will be used to evaluate its performance.