CARDEA: A CONTEXT-AWARE AND INTERACTIVE VISUAL PRIVACY CONTROL FRAMEWORK

by

RUI ZHENG

A Thesis Submitted to
The Hong Kong University of Science and Technology
in Partial Fulfillment of the Requirements for
the Degree of Master of Philosophy
in Computer Science and Engineering

October 2016, Hong Kong

Authorization

I hereby declare that I am the sole author of the thesis.

I authorize the Hong Kong University of Science and Technology to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize the Hong Kong University of Science and Technology to reproduce the thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

RUI ZHENG

CARDEA: A CONTEXT-AWARE AND INTERACTIVE VISUAL PRIVACY CONTROL FRAMEWORK

by

RUI ZHENG

This is to certify that I have examined the above M.Phil. thesis

and have found that it is complete and satisfactory in all respects,

and that any and all revisions required by

the thesis examination committee have been made.

ASSISTANT PROF. PAN. HUI, THESIS SUPERVISOR

PROF. QIANG YANG, HEAD OF DEPARTMENT

Department of Computer Science and Engineering

21 October 2016

ACKNOWLEDGMENTS

thank god

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CARDEA: A CONTEXT-AWARE AND INTERACTIVE VISUAL PRIVACY CONTROL FRAMEWORK

by

RUI ZHENG

Department of Computer Science and Engineering

The Hong Kong University of Science and Technology

ABSTRACT

We design and implement Mars, a MapReduce runtime system accelerated with graphics processing units (GPUs). MapReduce is a simple and flexible parallel programming paradigm originally proposed by Google, for the ease of large scale data processing on thousands of CPUs. Compared with CPUs, GPUs have an order of magnitude higher computation power and memory bandwidth. However, GPUs are designed as special-purpose co-processors and their programming interfaces are less familiar than those on the CPUs to MapReduce programmers.

To harness GPUs' power for MapReduce, we developed Mars to run on NVIDIA GPUs, AMD GPUs, as well as multi-core CPUs. Furthermore, we integrated Mars into Hadoop, an open-source CPU-based distributed MapReduce system. Mars hides the programming complexity of GPUs behind the simple and familiar MapReduce interface, and automatically manages task partitioning, data distribution, and parallelization on the processors. We have implemented six representative applications on Mars and evaluated their performance on PCs equipped with GPUs as well as multi-core CPUs. The GPU acceleration with an NVIDIA GTX280 achieved a speedup of an order of magnitude over a quad-core CPU. Utilizing both the GPU and the CPU further improved GPU-only performance by 40% for some applications. Additionally, integrating Mars into Hadoop enabled GPU acceleration for a network of PCs.

CHAPTER 1

INTRODUCTION

1.1 Awareness of Visual Privacy

Nowadays, built–in cameras have been serving as indispensable components of mobile and wearable devices.

Cameras with smaller size and higher resolution support a number of services and applications such as taking photos, mobile augmented reality, and continuously recording surroundings for devices like smartphones, Microsoft HoloLens [**microsoft**], Google Glass [**google**], and Narrative Clip [**narrative**]. The trend of embedding cameras in wearables will keep growing, an example of which is smart contact lens[1].

However, the ubiquitous presence of cameras, the ease of taking photos and recording video, along with "always on" and "non–overt act" features threaten individuals to have private or anonymous social lives, raising people's concerns of visual privacy. More specifically, photos and videos captured without getting permissions from bystanders, and then uploaded to social networking sites, can be accessed by everyone online, potentially leading to invasion of privacy. Malicious applications on the device may also inadvertently leak captured media data[2]. What makes it worse is that recognition technologies can link images to specific people, places, and things, thus reveal far more information than expected, making searchable what was not previously considered searchable [**shaw2006recognition**, **acquisti2014face**]. All these possible consequences, whether have been realized by people or not, may hinder their reception to advanced wearable consumer products. A representative example is Google Glass, which received letters from US Congressional Bi-Partisan Privacy Caucus and Data Protection Commission of Canada concerning privacy risks to the public [**congress**, **commission**].

[1] `http://money.cnn.com/2016/05/12/technology/eyeball-camera-contact-sony/`

[2] `http://www.infosecurity-magazine.com/news/popular-android-camera-app-leaks/`

To address privacy issues raised by unauthorized or unnoticed visual information collection, both legal and technical measurements have been proposed. For instance, Google Glass is banned at places such as banks, hospitals, and bars[3]. However, prohibiting from using cameras does not resolve the issue fundamentally, but sacrificing people's rights to capture happy moments even if no bystander in the background, since there are sorts of ways to secretly record anything. As a result, there are growing needs to design technical solutions to protect individuals' visual privacy in a world where cameras are becoming pervasive. Some recent attempts are using visual markers such as QR code [1, 2] and colorful hints like hat [3] for individuals to actively express their unwillingness to be captured. However, these visual markers suffers from same limitations. First, people are less likely to wear a QR code, despite the technical feasibility of these approaches. Moreover, privacy concerns vary widely among individuals, and many change from time to time even for the same person, which cannot be conveyed by uniform or static visual markers. In fact, what individuals are doing, with whom, at where, determine whether people think their privacy should be protected. Therefore, we are looking for a more natural, user–friendly, flexible, and fine-grained mechanism for people to express, modify, and control their individualized privacy preferences.

In this paper, we propose a trusted image capture framework for individuals to control their visual privacy using: *i)* personalized privacy profiles, that people can define their context–dependent privacy preferences with a set of privacy related factors including location, scene, and other's presence; and *ii)* face–signatures, for devices to locate individuals who request privacy control; and *iii)* hand gestures, which helps people interact with cameras to temporarily change their privacy preferences. By using the framework, the device will automatically compute context factors, compare them with people's privacy profiles, and finally enforce privacy policies conforming to people's privacy preferences.

The main contribution of our work is that we propose a novel visual privacy control mechanism that aims to relieve people's negative attitudes towards pervasive cameras. To this end, we concentrate on context elements which determine the nature of privacy problem. We also propose an interactive approach to flexibly convey privacy preferences with hand gestures.

[3] https://www.searchenginejournal.com/top-10-places-that-have-banned-google-glass/66585/

1.2 Related Works

1.3 Challenges

CHAPTER 2

CONVOLUTIONAL NEURAL NETWORKS

CHAPTER 3

CARDEA

3.1 System Design

3.2 Implementation

3.3 Evaluation

CHAPTER 4

CONCLUSION AND FUTURE WORK

Bibliography

[1] Cheng Bo et al. “Privacy. tag: Privacy concern expressed and respected”. In: *Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems*. ACM. 2014, pp. 163–176.

[2] Franziska Roesner et al. “World-driven access control for continuous sensing”. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM. 2014, pp. 1169–1181.

[3] Jeremy Schiff et al. “Respectful cameras: Detecting visual markers in real-time to address privacy concerns”. In: *Protecting Privacy in Video Surveillance*. Springer, 2009, pp. 65–89.