Secure Multimedia Processing over Cloud

Pradeep K. Atrey
University of Winnipeg, Canada

p.atrey@uwinipeg.ca
www.acs.uwinipeg.ca/pkatrey/
Winnipeg

UWINNIPEG
THE HEART OF THE CITY, the heart of the continent

THE UNIVERSITY OF WINNIPEG
Winnipeg Summer
Winnipeg Winter
Acknowledgement

• This research is partly supported by

Natural Sciences and Engineering Research Council of Canada
Conseil de recherches en sciences naturelles et en génie du Canada
Other Contributors

Manoranjan Mohanty
Wei Tsang Ooi

Ankita Lathey
Nishant Joshi
Cloud-based Multimedia Computing

• Very popular these days
• Companies Offering 2D Imaging
  – AT&T, Dell, Intel etc.
• Companies Offering 3D Imaging
  – Microsoft, KDDI, Sinha Systems etc.

Image source:
Cloud-based Multimedia Storage and Processing

Image Capture

Server

Network

Image Storage and Processing

Datacenter

Network

Image Display

Client

2D Image Visualization
Introduction and Motivation

Cloud-based Multimedia Storage and Processing

- Capturing and Preprocessing
- Server

Data-to-image Conversion

- Datacenter

3D Image Visualization

- Image Display
- Client

Network

3D Image Visualization
Cloud-based Multimedia Storage and Processing

Introduction and Motivation

Surveillance Video Quality Enhancement

Capturing and Preprocessing
Server

Quality enhancement
Datacenter

Network

Image Display
Client
Cloud-based Multimedia Storage and Processing

Introduction and Motivation

Capturing and Preprocessing

Server

Image Zooming and Cropping

Datacenter

Zooming

Network

Network

Image Display

Client
Security and Privacy Challenges in Cloud-based Storage and Processing

• How many of you mind if your medical image is available to an adversary?

• What can an adversary do with an image?

Image source: http://greenberg-art.com/.Toons/Toons,%20social/qqxsgMedical%20privacy.gif
Rest of the talk

• Introduction and Motivation
• **Addressing the Challenges**
  – Finding a Cryptosystem
  – Using Real Numbers in a Cryptosystem
• Three Frameworks
  – Secure Cloud-based Image Scaling/Cropping
  – Secure Cloud-based Pre-classification Volume Ray-casting
  – Secure Cloud-based Surveillance Video Enhancement
• Conclusions
Addressing the Challenges

Security and Privacy Challenges: Secure Storage over Cloud

- Smoking is not good for health
- Encryption techniques – Watermarking – Secret sharing

Network

Server

Capturing and Preprocessing

Storage

Datacenter

Network

Client

Image Display
Security and Privacy Challenges: Insecure Processing over Cloud

- Smoking is not good for health

Capturing and Preprocessing

Server

Network

Zooming

Datacenter

Network

Image Display

Client

Image Zooming and Cropping on Original Data
Introduction and Motivation

Security and Privacy Challenges: Secure Processing over Cloud

Still to be addressed

Image Zooming and Cropping on Encrypted Data

Capturing and Preprocessing

Server

Network

Datacenter

Zooming

Network

Image Display

Client

Smoking is not good for health
Our Objective: Secure Cloud-based Multimedia Processing

- Confidentiality
- Integrity
- Availability
- Privacy

Smoking is not good for health
Our Objective: Secure Cloud-based Multimedia Processing

- Confidentiality
- Integrity
- Availability
- Privacy
- Computational Efficiency
- Bandwidth Efficiency
- High Quality Image

Smoking is not good for health
Technical Challenges

• Finding a Cryptosystem
  - Fully homomorphic cryptosystem is not practical
    \[ E(A) + E(B) = E(A+B) \]
  - Somewhat homomorphic cryptosystem cannot hide all information
Finding a Cryptosystem

- Fully homomorphic cryptosystem is not practical
  \[ E(A) + E(B) = E(A+B) \]
- Somewhat homomorphic cryptosystem cannot hide all information

Using Real Numbers in a Cryptosystem

- Modular prime operation of a cryptosystem is not compatible with real number operations of a data/image processing algorithm
Rest of the talk

• Introduction
• Addressing the Challenges
  – Finding a Cryptosystem
  – Using Real Numbers in a Cryptosystem
• Three Frameworks
  – Secure Cloud-based Image Scaling/Cropping
  – Secure Cloud-based Pre-classification Volume Ray-casting
  – Secure Cloud-based Surveillance Video Quality Enhancement
• Conclusions
Finding a Cryptosystem

- Key Observations
  - Shamir’s \((k,n)\) Secret Sharing (SSS) or \((l,k,n)\) Multi-Secret Sharing (MSS) can be used as principal cryptosystem
  - Other cryptosystems can be used to support operations that are not supported by SSS and MSS
Finding a Cryptosystem

• Review of \((k, n)\) SSS

\[ F(x) = (S + \sum_{i=1}^{k-1} a_i x^i) \mod q \]

Sharing a Secret

Secret

Random Number

Prime Number
Finding a Cryptosystem

• Review of $(k, n)$ SSS

Reconstructing a Secret

\[ L(x) = \left( \sum_{i=0}^{k-1} F(i)t_i(x) \right) \mod q \]

\[ \prod_{j=0, j \neq i}^{k-1} \frac{x - x_j}{x_i - x_j} \]

Reconstructing the secret using $k \leq n$ shares
Finding a Cryptosystem

- Review of \((l, k, n)\) MSS

**Sharing a Secret**

\[
F(x) = \left( \sum_{i=0}^{l-1} s_i x^i + \sum_{i=l}^{k-1} a_i x^i \right) \mod q
\]

\(i^{th}\) Secret
Rest of the talk

• Introduction

• Addressing the Challenges
  – Finding a Cryptosystem
  – **Using Real Numbers in a Cryptosystem**

• Three Frameworks
  – Secure Cloud-based Image Scaling/Cropping
  – Secure Cloud-based Pre-classification Volume Ray-casting
  – Secure Cloud-based Surveillance Video Quality Enhancement

• Conclusions
Using Real Numbers in a Cryptosystem

• Excluding Modular Prime Operation from the Cryptosystem
  – Example: Shamir’s secret sharing

– Side Effect: Degradation of Security
  ✓ For \( (2, n) \) Shamir’s secret sharing, the probability of finding the secret from \( F(x_i) \) is:
  
  With mod \( q \): \( 1/q \)
  
  Without mod \( q \): \( \text{INT}(x_i / F(x_i)) \)
Using Real Numbers in a Cryptosystem

- Modifying Real number to an Integer
  \[ R(S,d) = \text{round}(S,d) \times 10^d \]
  - Obtained by rounding off \( S \) by \( d \) decimal places

- Integer Representative
Using Real Numbers in a Cryptosystem

- Modifying Real number to an Integer
  \[ R(S, d) = \text{round}(S, d) \times 10^d \]

- Side Effect: Roundoff Error
  - Is bounded by \( \pm (5 \times 10^{-(d+1)}) \)
  - Expands with addition and scalar multiplication
Rest of the talk

• Introduction and Motivation
• Addressing the Challenges
  – Finding a Cryptosystem
  – Using Real Numbers in a Cryptosystem
• Three Frameworks
  – Secure Cloud-based Image Scaling/Cropping
  – Secure Cloud-based Pre-classification Volume Ray-casting
  – Secure Cloud-based Surveillance Video Enhancement
• Conclusions
Secure Cloud-based Image Scaling/Cropping

- **Why scaling/cropping in data centers?**
  - Streaming a large image
  - Downloading a large image (e.g. histopathology image that can be 40 GB in size $80000 \times 80000$ in dimension) is not feasible
  - Previewing an image before viewing

- **Why dynamic scaling/cropping on shadow (or hidden) images?**
  - Pre-cropping required additional data to be sent
  - Pre-scaling cannot ensure step-less zooming

Secure Cloud-based Image Scaling/Cropping

- Architecture and Workflow
Secure Cloud-based Image Scaling/Cropping

- Proposed Secret Image Sharing Scheme
  - Inter-pixel correlation is hidden by using a set of random numbers as coefficient in the secret sharing polynomial
  - $(3,k,n)$ MSS

\[ H(x) = \left( R + Gx + Bx^2 + \sum_{i=3}^{k-1} a_i x^i \right) \mod q \]
Secure Cloud-based Image Scaling/Cropping

- Experiments
  - Server, datacenters, and user are simulated in a PC
  - Two test images
    - A histopathology image (size 5.2 MB, dimension: 2756 × 3663)
    - The Lena Image (size 205.5 KB, dimension: 512 × 512)
Secure Cloud-based Image Scaling/Cropping

• Results: Scaling

- Required
- Zoomed Shadow Image
- Recovered Zoomed Image
Secure Cloud-based Image Scaling/Cropping

- Results: Cropping

Required

Cropped Shadow Image

Recovered Cropped Image
Secure Cloud-based Image Scaling/Cropping

• Security Analysis
  – Confidentiality
    ✓ Perceptual security
    ✓ Multi-secret sharing is not perfectly secure
Secure Cloud-based Image Scaling/Cropping

• Security Analysis

  - Integrity
    ✓ if \( n > k \), then \( \binom{n}{k} \) ways to reconstruct an image

Corrupted shadow image(s) implies different reconstructed images
Secure Cloud-based Image Scaling/Cropping

- **Performance Analysis**

  - **Data Overhead**
    - $\frac{bk-24}{24}$ times more than the conventional streaming,
    - where $b$ is the number of bits required to represent $q$
    - For $d = 2$ and $k = 4$, 1.5 times more than the conventional

  - **Computational Overhead**
    - For a PC with Intel Core 2 Quad 2.83 Ghz processor and 4GB of RAM, approximately 76.35 ms is required to recover a $512 \times 512$ secret image (0.3 $\mu$s per pixel)
Rest of the talk

• Introduction
• Addressing the Challenges
  – Finding a Cryptosystem
  – Using Real Numbers in a Cryptosystem
• Three Frameworks
  – Secure Cloud-based Image Scaling/Cropping
  – Secure Cloud-based Pre-classification Volume Ray-casting
  – Secure Cloud-based Surveillance Video Enhancement
• Conclusions
Secure Cloud-based Pre-classification Volume Ray-casting

- Architecture and Workflow

Secure Cloud-based Pre-classification Volume Ray-casting

- Review: Pre-classification Volume Ray-casting
Secure Cloud-based Pre-classification Volume Ray-casting

- Review: Pre-classification Volume Ray-casting

Volume Ray-casting Framework

- Gradient and Normal Estimation
- Classification and Shading
- Ray Projection
- Interpolation
- Composition

Pre ray-projection: Can be preprocessed
Secure Cloud-based Pre-classification Volume Ray-casting

- Review: Pre-classification Volume Ray-casting

- Gradient and Normal Estimation
- Classification and Shading
- Ray Projection
- Interpolation
- Composition

Pre ray-projection: Can be preprocessed
Post ray-projection: To be performed by datacenters
Secure Cloud-based Pre-classification Volume Ray-casting

- Securing Post Ray-projection
  - Hiding computation on colors

Original

Hidden Color

Not hiding computation on opacities
Secure Cloud-based Pre-classification Volume Ray-casting

• Experiment
  – Server, Datacenters, and Client are simulated in a PC
  – Customized VTK 5.8.0
    ✓ Pre-classification volume ray-casting
    ✓ Integrated (3,5) Secret Sharing
Secure Cloud-based Pre-classification Volume Ray-casting

- Data Set

<table>
<thead>
<tr>
<th></th>
<th>Dimension</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Head</td>
<td>256 X 256 X 124</td>
<td>7.8 MB</td>
</tr>
<tr>
<td>Foot</td>
<td>256 X 256 X 256</td>
<td>16 MB</td>
</tr>
<tr>
<td>Iron port</td>
<td>68 X 68 X 68</td>
<td>307.3 KB</td>
</tr>
<tr>
<td>Bucky</td>
<td>32 x 32 X 32</td>
<td>32.2 KB</td>
</tr>
</tbody>
</table>
Secure Cloud-based Pre-classification Volume Ray-casting

• Results: Single View Point
Secure Cloud-based Pre-classification Volume Ray-casting

- Results: Single View Point
Secure Cloud-based
Pre-classification Volume Ray-casting

• Results: Multiple View Point

Original → Share

Original → Share

Original → Share
Secure Cloud-based Pre-classification Volume Ray-casting

**Head MRI volume data**

- Rendered Image (Secret Image)
  - Conventional Server-Side Rendering
- Share Image
  - Rendered in a Data Center
  - Cloud-based Secure Rendering
- Image Reconstructed at Client

**Foot volume data**

- Rendered Image (Secret Image)
  - Conventional Server-Side Rendering
- Fifth Share Image
- Reconstructed Image
Rest of the talk

• Introduction
• Addressing the Challenges
  – Finding a Cryptosystem
  – Using Real Numbers in a Cryptosystem
• Three Frameworks
  – Secure Cloud-based Image Scaling/Cropping
  – Secure Cloud-based Pre-classification Volume Ray-casting
  – Secure Cloud-based Surveillance Video Quality Enhancement
• Conclusions
Encrypted-domain Video Quality Enhancement over Cloud

• Architecture and Workflow

A. Lathey, P. K. Atrey and N. Joshi. *Homomorphic low pass filtering on encrypted multimedia over cloud.* 
*IEEE International Conference on Semantic Computing (ICSC'2013),* September 2013, Irvine, CA, USA.
THE PROBLEM:
Non-terminating averaged value

SOLUTION BASED ON PREVIOUS METHOD
Multiply each pixel intensity value by a factor of \(10^d\), where \(d\) depends upon the precision of the desired decimal digits up to which we want to process the real numbers. The prime number should always be chosen as greater than \((255+51 \times 10^d) \times 10^d\)

APPLIED TO THE PROBLEM:

PROPOSED SOLUTION:
pre-process the image data in such a way that averaging is performed on completely divisible values only.
Video Quality Enhancement Framework

Encrypted-domain Video Quality Enhancement over Cloud

**Scheme I:** Multiplying each original intensity value by the mask size, \((m \times n)\). In other words, convert each pixel \(I(u,v)\) to a multiple of \((m \times n)\) by,

\[
I'(u,v) = I(u,v) \times (m \times n)
\]

**Scheme II:** Changing each original intensity value to the nearest multiple of \((m \times n)\) by adding or subtracting a maximum of values to or from its current value, where the range of lies between 1 and \(\Gamma \, m-n/2\). In other words, convert each pixel \(I(u, v)\) to a multiple of \((m \times n)\) by,

\[
I'(u,v) = I(u,v) \pm \Delta
\]
Video Quality Enhancement Framework

Encrypted-domain Video Quality Enhancement over Cloud

• Results – Scheme 1

http://www.youtube.com/watch?v=hJg67v3IbmU&feature=youtu.be
Video Quality Enhancement Framework

Encrypted-domain Video Quality Enhancement over Cloud

• Results – Scheme 2

http://www.youtube.com/watch?v=TqRHJ6KrZY0&feature=youtu.be
Conclusions

• Addressed incompatibility of a cryptosystem with real number
• Proposed three frameworks using Shamir’s secret sharing as principal cryptosystem
• More secure cloud-based systems can be built using somewhat homomorphic cryptosystems
Publications

• A. Lathey, P. K. Atrey and N. Joshi. Homomorphic low pass filtering on encrypted multimedia over cloud. *IEEE International Conference on Semantic Computing (ICSC'2013)*, September 2013, Irvine, CA, USA.

• M. Mohanty, W.-T. Ooi and P. K. Atrey. Scale me, crop me, know me not: Supporting scaling and cropping in secret image sharing. *IEEE International Conference on Multimedia and Expo (ICME'2013)*, July 15-19, 2013, San Jose, CA, USA.

What Next?

• This is not the end of the world.

• Need to examine the suitability of the proposed frameworks in other cloud-based applications such as:
  – Scaling/cropping on compressed images/videos
  – Compression in encrypted domain
  – Processing other media e.g. text documents and audio