Security and Privacy Issues in Multimedia Systems

PRADEEP K ATREY
DEPT. OF COMPUTER SCIENCE
COLLEGE OF ENGINEERING AND APPLIED SCIENCES

SIGMM Multimedia Frontier Workshop @ ACM MM 2015, Brisbane, Australia

Question

Is Security and Privacy no longer an issue for multimedia community?

Smoking is not good for health
Multimedia Systems vs. Security & Privacy?

Multimedia Systems for Security of People
- Multimedia surveillance for homeland security

Security of People’s Data in Multimedia Systems
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics

Privacy of People in Multimedia Systems
- Privacy aware multimedia surveillance systems
- Social networks and communication privacy

Outline

Security and Privacy Issues in Multimedia Systems
- Multimedia surveillance – homeland security and privacy
- Social networks and communication privacy
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics
Outline

Security and Privacy Issues in Multimedia Systems
- Multimedia surveillance – homeland security and privacy
- Social networks and communication privacy
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics
Outline

Security and Privacy Issues in Multimedia Systems
- Multimedia surveillance – homeland security and privacy
- Social networks and communication privacy
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics

Multimedia surveillance – homeland security

9/11 terrorist attack (2001)
London bombing (2005)
Mumbai attack (2008)
Boston Marathon blast (2013)

Multimedia Surveillance System
[Atrey et al. MMSJ 2007, Atrey et al. TOMM 2007]

Active Cooperative Sensing
[Singh et al. MVA 2007]

Bus Surveillance
[Amrabi and Atrey, MTAP 2012]
Multimedia surveillance – people’s privacy?

- Large number of CCTV cameras
- "4.2 million CCTV cameras in Britain", and the "person can be captured on 300 different cameras in a day"

Is Hiding Facial Information Enough?

Place
(Where)

Time
(When)

Behavior
(What)

Implicit Channels!

W3-Privacy Model
[Saini et al. MTAP, 2014]

Privacy aware publication of surveillance video

Anonymous Surveillance
(Live Demo)
Multimedia surveillance – current and future work

Outline

Security and Privacy Issues in Multimedia Systems
- Multimedia surveillance – homeland security and privacy
- Social networks and communication privacy
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics
Outline

Security and Privacy Issues in Multimedia Systems
- Multimedia surveillance – homeland security and privacy
- Social networks and communication privacy
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics

Social networks - privacy

Motivation video

A Secure and Privacy-aware Cloud-Based Architecture for Online Social Networks

Demo: http://www.cs.albany.edu/~patrey/research/SecureOSN/feasibility.html
Cryptosystem - Shamir's Secret Sharing

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

Sharing a Secret

Security and Privacy Issues in Multimedia Systems
Multimedia surveillance - homeland security and privacy
Social networks and communication privacy
Secure cloud-based multimedia data analytics
Multimedia authentication and forensics

11/3/2015
Security and Privacy Issues in Multimedia Systems
Multimedia Surveillance—Homeland Security and Privacy
Social Networks and Communication Privacy
Multimedia Authentication and Forensics

Cryptosystem - Shamir’s Secret Sharing

Homomorphic property: $E(A) + E(B) = E(A+B)$
Email communication - privacy

Have you ever sent your confidential information such as passport and credit card over email?

Security and Privacy Issues in Multimedia Systems
Multimedia surveillance—homeland security and privacy
Social networks and communication privacy
Secure cloud-based multimedia data analytics
Multimedia authentication and forensics
Outline

My Security and Privacy Research
- Multimedia surveillance – homeland security and privacy
- Social networks and communication privacy
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics
Motivation

The world is filled with “Big Data”
- Every minute
  - 204 million emails are sent,
  - Six million Facebook pages are viewed
  - 1.3 million YouTube clips are downloaded
  - 98,000 tweets
  - 695,000 status updates
  - 11 million instant messages
  - 698,000+ Google searches
  - 951 GB Surveillance video

4 Vs of Big Data
- Volume
- Variety
- Velocity
- Value

Cloud-based Multimedia Data Analytics

Very popular these days
Companies Offering 2D Imaging
- AT&T, Dell, Intel etc.

Companies Offering 3D Imaging
- Microsoft, KDDI, Sinha Systems etc.
Cloud-based Multimedia Storage and Processing

Capturing and Preprocessing

Server

Data-to-image Conversion

Datacenter

Image Display

Client

3D Image Visualization

Security and Privacy Issues in Multimedia Systems
Multimedia surveillance—homeland security and privacy
Social networks and communication privacy
Secure cloud-based multimedia data analytics
Multimedia authentication and forensics

Cloud-based Multimedia Storage and Processing

Capturing and Preprocessing

Server

Quality enhancement

Datacenter

Surveillance Video Quality Enhancement

Image Display

Client
Cloud-based Multimedia Storage and Processing

Capturing and Preprocessing

Zooming

Datacenter

Image Display

Client

Security and Privacy Issues in Multimedia Systems
Multimedia surveillance — homeland security and privacy
Social networks and communication privacy
Secure cloud-based multimedia data analytics
Multimedia authentication and forensics

Who can be adversary?

How many of us would mind if our medical image data 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
Multimedia Storage over Cloud

- Capturing and Preprocessing
- Storage
- Image Display

Encryption techniques – Watermarking – Secret sharing

Multimedia Processing over Cloud

- Capturing and Preprocessing
- Zooming
- Image Zooming and Cropping on Original Data

Security and Privacy Issues in Multimedia Systems
- Multimedia surveillance—homeland security and privacy
- Social networks and communication privacy
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics
Secure Multimedia Processing over Cloud

Still to be addressed

Capturing and Preprocessing
Server

Zooming
Datacenter

Image Display
Client

Image Zooming and Cropping on Encrypted Data

Security and Privacy Issues in Multimedia Systems
Multimedia surveillance—homeland security and privacy
Social networking and communication privacy
Secure cloud-based multimedia data analytics
Multimedia authentication and forensics

Secure Cloud-based Image Scaling/Cropping

• Architecture and Workflow

Secret Image Recovery

User

Scaling and Cropping

Image Display

Secure Cloud-based Image Scaling/Cropping

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

• Results: Demo

Required
Zoomed Shadow Image
Recovered Zoomed Image

[ICME 2013]

Secure Pre-classification Volume Ray-casting

• Architecture and Workflow
Secure Pre-classification Volume Ray-casting

- Results: Single View Point

[Diagram showing the process of secure pre-classification volume ray-casting]

Demo

[Mohanty et al., MM 2012]
Secure Video Quality Enhancement over Cloud Architecture and Workflow

- MULTIMEDIA CAPRTURING DEVICE
- SERVER, S Preprocesses Original Image, Creates and Distributes Shares
- CDC₁: LPF
- CDC₂: LPF
- CDCₙ: LPF
- SHARE 1
- SHARE 2
- SHARE N
- PROCESSED SHARE 1
- PROCESSED SHARE 2
- PROCESSED SHARE N
- AUTHORIZED USER Obtains any T Shares and Reconstructs Enhanced (LPF) Image
- DISPLAY DEVICE

The proposed method is demonstrated to work for:
- Noise removal and anti-aliasing
  - Results – Scheme 1 (Demo)
  - Results – Scheme 2 (Demo)
- Edge and contrast enhancement (Demo)
- Dehazing (Demo)

More demos available on:
- https://sites.google.com/site/ankitaresearchdemos/home
  [ICSC 2013, TOMM 2015]
Speech Data over Cloud

How many of you have revealed your confidential info over phone at least once?

SSN  Passport  Health Policy Card  Credit Card  Date of Birth

What is your date of birth?


Secure Speech Quality Enhancement over Cloud

1. Preprocessing
2. Creation of shares with Shamir Secret Sharing Scheme

[MMM 2015]
Secure Multimedia Editing

- Google Docs: Are they secure?
- Online image editing
- Online Audio Editor

TwistedWave Online
A browser-based audio editor

What next?

<table>
<thead>
<tr>
<th>Application area</th>
<th>Analysis tasks</th>
<th>Type of media and features used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social media and networks</td>
<td>Personality detection</td>
<td>Text, images, video, demographic and social features</td>
</tr>
<tr>
<td></td>
<td>Cyber bullying detection</td>
<td>Test and social features</td>
</tr>
<tr>
<td></td>
<td>Disease spread detection</td>
<td>Text, social features</td>
</tr>
<tr>
<td>Multimedia surveillance</td>
<td>Hate posts detection</td>
<td>Text, audio, images, video and social features</td>
</tr>
<tr>
<td></td>
<td>Face detection and recognition</td>
<td>Image, video</td>
</tr>
<tr>
<td></td>
<td>Suspicious event detection</td>
<td>Image, video</td>
</tr>
<tr>
<td></td>
<td>Data quality improvement</td>
<td>Image, video, audio</td>
</tr>
<tr>
<td></td>
<td>Data search and retrieval</td>
<td>Text, image, video</td>
</tr>
<tr>
<td></td>
<td>Scaling and zooming</td>
<td>Image, video</td>
</tr>
<tr>
<td>E-health</td>
<td>3D medical data rendering and</td>
<td>3D data, image</td>
</tr>
<tr>
<td></td>
<td>visualization</td>
<td></td>
</tr>
<tr>
<td>Bio-informatics</td>
<td>DNA sequence analysis</td>
<td>Text and numbers</td>
</tr>
</tbody>
</table>
Outline

My Security and Privacy Research
- Multimedia surveillance – homeland security and privacy
- Social networks and communication privacy
- Secure cloud-based multimedia data analytics
- Multimedia authentication and forensics
Multimedia security and forensics – Authentication

Original (protected) image  Tampered image  Detection of tampered regions

[MTAP 2007]

Multimedia security and forensics – Source identification

- Given an image or a video, can we identify the source camera?
- Given an audio speech, can we identify the source microphone?
- Given a PDF document, can we identify the computer which created it?