Winnipeg

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

The University of Winnipeg

SNDS'12 Trivandrum, India
Multimedia Systems

- Systems that involve different kind of media such as text, image, video, and audio
  - Surveillance systems
  - Social networking systems
  - e-Health systems
  - Mobile media systems
  and many more…
Security and Privacy Issues in Multimedia Systems

Social Networks
Source: Youtube

Clerk fined for 'death watch'
A medical office clerk has been fined $10,000 for repeatedly accessing the private records of the cancer-stricken wife of a man with whom she was having an affair.

Source: http://www.canada.com/story.html?id=3dda9b24-25ba-4ce1-b717-64588079b2e4

Video surveillance
Source: http://www.peripatetic.us/classes/SP08/time/surveil.htm

SNDS'12 Trivandrum, India
Security and Privacy in Multimedia Surveillance Systems

Collaborators:
Mukesh Saini and Mohan Kankanhalli, NUS, Singapore
Sharad Mehrotra, University of California, Irvine, USA
Public safety is very important


SNDS’12 Trivandrum, India
Public Safety and CCTV Surveillance

- 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”


SNDS’12 Trivandrum, India
Public Safety and CCTV Surveillance

Image source: http://www.andrelemos.info/cctv10c.jpg

SNDS'12 Trivandrum, India
Do you mind to be watched into CCTV control room?
Privacy Concerns

- Large amount of recorded video
- Access is given to
  - CCTV Operator
  - Researchers
  - Policy makers
  - and others
  ⇒ Privacy violation

The problem is to determine the privacy violation due to publication of surveillance video and protect it.

What is the solution?

SNDS'12 Trivandrum, India
Privacy Concerns

You can easily identify the person (if you know him) \(\Rightarrow\) Privacy loss

SNDS'12 Trivandrum, India
What to do?

How to do effective surveillance while preserving privacy of people?
Obvious Solution – Hide the face

- Obscure people’s face in the video
- Looks a simple and good solution

Approach 1
- Let a human manually find the faces in all the video frames
  - 10 frames per sec, round the clock video recording, lots of data
  - need several hundred people to do the job
  - and, who knows some of them may be intruders and misuse the data
Obvious Solution – Hide the face

Approach 2: Apply automatic face detection and hiding algorithm – seems good

What it should be ideally…
What it is usually in practice…

Automatic face detection algorithms are not 100% accurate… may often miss a few faces.

SNDS'12 Trivandrum, India
Is Hiding Facial Information Enough?

<table>
<thead>
<tr>
<th>Place</th>
<th>Smart Lab</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>19:32:16 2000/01/09</td>
</tr>
<tr>
<td>Behavior</td>
<td></td>
</tr>
</tbody>
</table>

Implicit Channels!

SNDS’12 Trivandrum, India
Explicit vs. Implicit Inference Channels

- Who
- What
- When
- Where

Explicit inference channel
Implicit inference channels

SNDS'12 Trivandrum, India
Sounds interesting…

Let us explore it more…
Proposed Approach

Find the computational models for

- Identity leakage and Privacy loss
- Utility loss

And

Find the appropriate video data transformation function to have a tradeoff between privacy loss and utility loss
Question 2

Do you mind to be video recorded when you are meeting with X disease specialist?

Two views on privacy loss:

1. Privacy is lost if **identity** information is leaked
2. Privacy is lost *only if** **sensitive** information is leaked
Modeling Privacy Loss

- Sensitive Information

<table>
<thead>
<tr>
<th>Sensitive Attribute</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>Showing middle finger when alone.</td>
</tr>
<tr>
<td>Spatial Information</td>
<td>Generally we do not want strangers to know which places we visit.</td>
</tr>
<tr>
<td>Time</td>
<td>Some people mind when others associate their activities with timing patterns.</td>
</tr>
<tr>
<td>Gesture</td>
<td>People make strange gestures while they are alone and do not want others to watch that.</td>
</tr>
<tr>
<td>Clothes</td>
<td>Many teens wear clothes which they do not want their parents to know.</td>
</tr>
<tr>
<td>Physique</td>
<td>People with atypical physique may be sensitive to that e.g. height.</td>
</tr>
<tr>
<td>Habits</td>
<td>Most people have some personal idiosyncratic sensitive habits like twiddling fingers under stress.</td>
</tr>
<tr>
<td>Companion Information</td>
<td>Some people do not want everyone to know whom they associate with.</td>
</tr>
<tr>
<td>Associated Objects</td>
<td>What we carry with us.</td>
</tr>
</tbody>
</table>
Modeling Privacy Loss

- Multi-camera surveillance
Modeling Privacy Loss

- **Multi-camera surveillance**

Fig. 7 Representative images from four cameras: (a) Department Entrance, (b) Audio Lab, (c) Staff Club, (d) Canteen.

Fig. 8 (a) Identity leakage and privacy loss for $T_1$ (b) Identity leakage and privacy loss for all targets
Modeling Utility

- Two conflicting demands: **Privacy** and **Utility**

  *Definition 2: Utility loss of the published video data refers to the decrease in the degree of accuracy by which analysis tasks can be accomplished with respect to the original data.*

- Task-based **Utility Loss** computation:
Effect of Data Transformation Methods on Privacy Loss and Utility Loss

- Global transformation (first blurring then quantization)
Results of blob detection using transformed data

Blob detection still works

Blob detection in original video

Blob detection in transformed video

Utility is still good, but privacy is preserved
Question 3

Would you mind if you are recorded in a CCTV camera, which is being watched by some person (unknown to you) at 10,000 km away?

Image source: http://www.andrelemos.info/cctv10c.jpg
http://www.clipartguide.com/_named_clipart_images/0511-0902-0418-3904

SNDS'12 Trivandrum, India
Observations

# 1: Sensitive information cannot be removed

# 2: The `who' information cannot be completely removed through computer vision

# 3: The what information is more important for surveillance and does not cause much privacy loss when detected alone in isolation

# 4: The where and when information is generally available to the CCTV operator as prior knowledge or through the video content
Anonymous Video Surveillance

SNDS'12 Trivandrum, India
Anonymous Video Surveillance

Canada

USA

Singapore

India

Mexico

Context Decoupling
Adaptive Quality Control

SNDS'12 Trivandrum, India
User Study to support Anonymous Surveillance

- 100 participants from 18 countries
- The users were asked to rate their feeling of privacy loss on a scale of 0 to 10 with 0 referring to no privacy loss and 10 referring to full privacy loss, in the four scenarios.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario1</td>
<td>A CCTV operator is watching the video in the same building.</td>
</tr>
<tr>
<td>Scenario2</td>
<td>The CCTV operator is watching the video in a different country, but s/he knows the location of the camera.</td>
</tr>
<tr>
<td>Scenario3</td>
<td>The CCTV operator is watching the video in a different country and s/he does not know the location of the camera.</td>
</tr>
<tr>
<td>Scenario4</td>
<td>The CCTV operator is watching the video in a different country and s/he does not know the location of the camera. Further, after certain period of time the, the CCTV operator is changed.</td>
</tr>
</tbody>
</table>

Average privacy loss in four scenarios.

SNDS'12 Trivandrum, India
Conclusions

- The implicit channels can cause significant privacy loss even when the facial information is not present. Therefore, blocking implicit channels is also equally important.
- Detect and hide approach is not reliable and provides a bad tradeoff between privacy and utility.
- Identity leakage and sensitive information both should be considered in determining privacy loss.
- Anonymous surveillance (remote monitoring) could be the future.
Publications


Security and Privacy in E-Health

Collaborators:
Manoranjan Mohanty and Wei-Tsang Ooi
National University of Singapore

Source:
http://www.centreforthenorth.ca/blogs/herethenorth/somebodycalladoctor
http://www.amiconnecticut.com/images/ProstateMRI.JPG

SNDS'12 Trivandrum, India
Cloud-based Secure 3D Medical Data Visualization

Cloud-based Secured Rendering: Architecture and Protocol

1a. Data preprocessing

1b. Secret Sharing

1c. Information about data centers and their shares

3a. Data rendering

2a. Rendering Request

4. Secret Image Formation
Security and Privacy in Social Networking Systems

Collaborators:
Kasun Senevirathna and Adam Rehill, University of Winnipeg, Canada

SNDS'12 Trivandrum, India
A Secure and Privacy-aware Cloud-based Architecture for Social Networks

Targeted toward Untrusted Social Networking Operators

Developed a secret sharing based framework

SNDS'12 Trivandrum, India
Happy ending...

Security and Privacy Issues in Multimedia Systems

*must not be after thoughts*

SNDS’12 Trivandrum, India