Security and Privacy Issues in Multimedia Systems

Pradeep K. Atrey

University of Winnipeg, Canada

p.atrey@uwinnipeg.ca

www.acs.uwinnipeg.ca/pkatrey

Winnipeg


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


Fort McMurray
Manitoba
Grande Prairie
Saskatchewan
Thompson
Edmonton
Flin Flon
Prince Albert
Saskatoon
Calgary
Swift Current
Regina
Brandon
Winnipeg
Ontario
Timmins
Amos
Quebec
Ottawa
Montreal
Fredericton
Halifax
Seattle
Spokane
Vancouver
Portland
Williston
Grand Forks
Minnesota
Duluth
Helena
Butte
Bismarck
Boise
Twin Falls
St. Paul
Minneapolis
Milwaukee
Chicago
Toronto
Rochester
Buffalo
Detroit
Cleveland
Pittsburgh
Concord
Augusta
Boston
Providence
Hartford
New York
Philadelphia
Baltimore
Washington D. C.
Norfolk
Richmond
Reno
Salt Lake City
Cheyenne
Omaha
Oakland
Provo
Boulder
Denver
Kansas City
Indianapolis
Dayton
Cincinnati
Louisville
Las Vegas
St. Louis
U. S. A.
Nashville
Charlotte
Santa Fe
Oklahoma City
Memphis
Columbia
Albuquerque
Phoenix
San Diego
Mexicali
Tucson
Little Rock
Birmingham
Atlanta
Dallas
Jackson
Tallahassee
Jacksonville
Austin
Baton Rouge
Hermosillo
ATLANTIC
OCEAN

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

e-Health

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

THE UNIVERSITY OF WINNIPEG

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

9/11 Terrorist attack (2001)

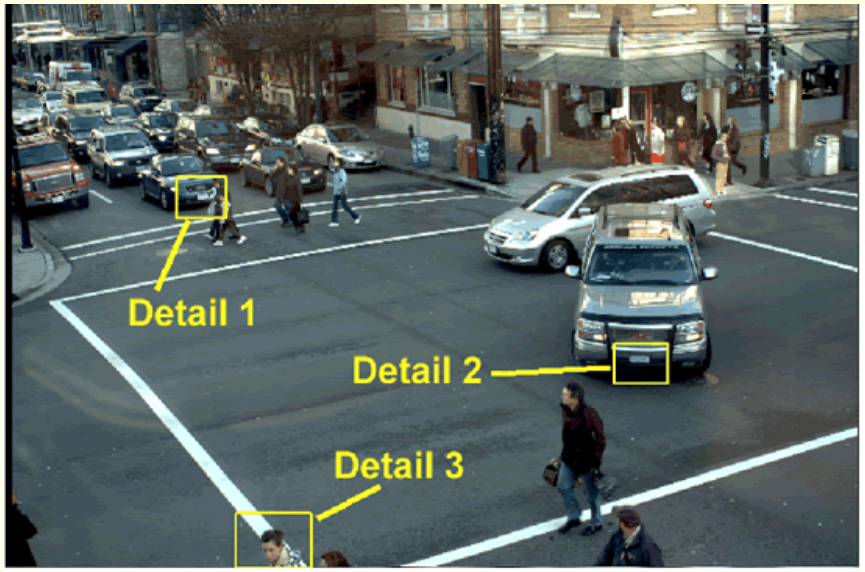
London bombing (2005)

Mumbai attack (2008)

Norway blasts (2011)

Public Safety and CCTV Surveillance

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



http://www.nione-security.com/news_view.asp?id=727

http://p10.hostingprod.com/@spyblog.org.uk/blog/cctv-surveillance-cameras/
http://www.dvbhardware.com/index.php?cPath=9

Public Safety and CCTV Surveillance

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

Question 1

Do you mind to be watched into CCTV control room?

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

Privacy Concerns

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

$\Rightarrow$ Privacy violation

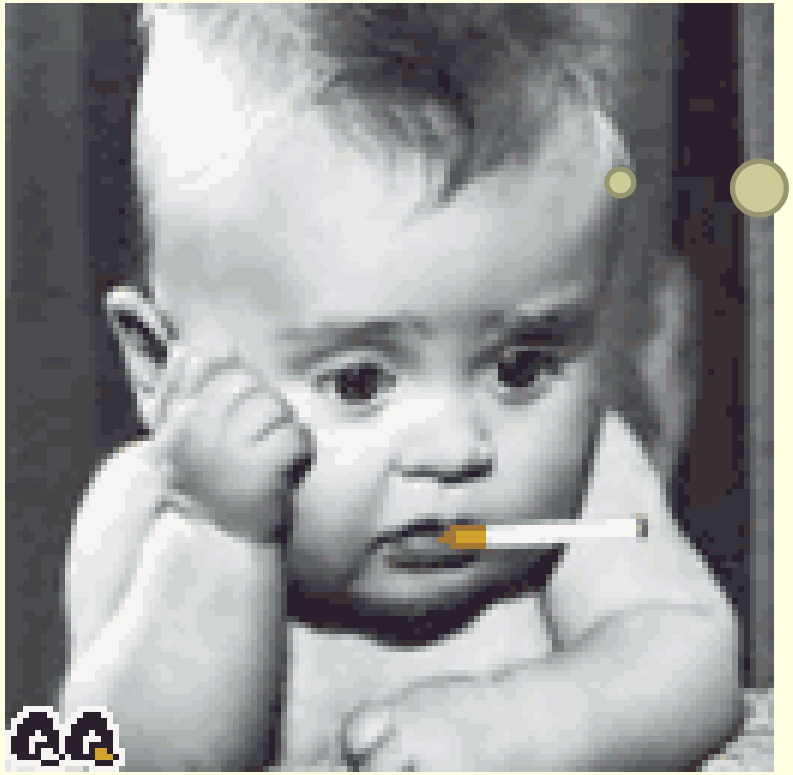
The problem is to determine the privacy violation due to publication of surveillance video and protect it.

What is the solution?

Privacy Concerns

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

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.

Is Hiding Facial Information Enough?

THE UNIVERSITY OF WINNIPEG

Place

Time

Behavior

Implicit Channels!

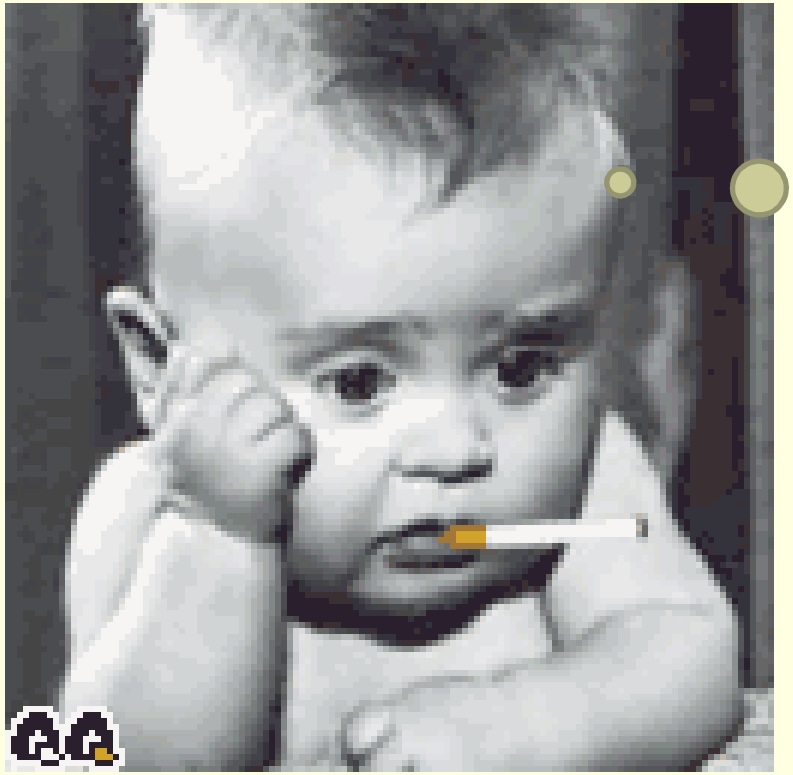
Explicit vs. Implicit Inference Channels

- Who } Explicit inference channel

- What
- When
- Where

} Implicit inference channels

Sounds interesting…



Let us explore it more…

Proposed Approach

Video data ***V***

Video data ***V'***

Find the computational models for

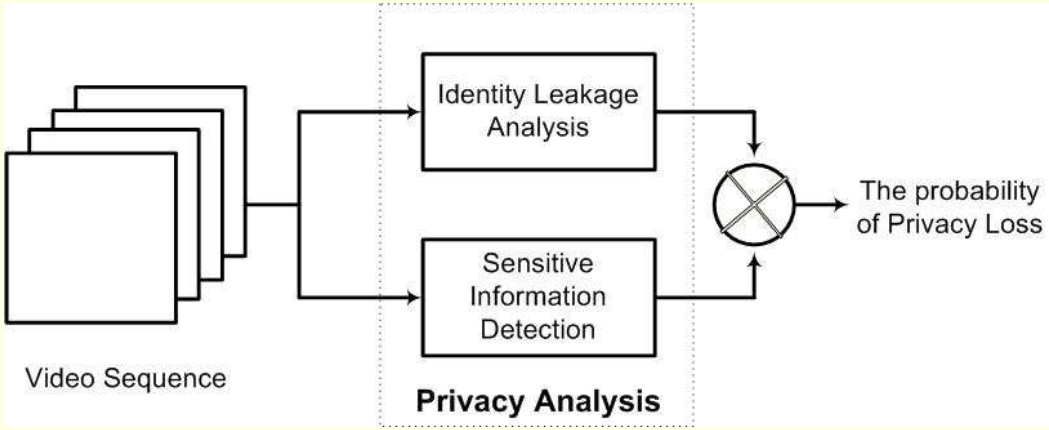
- Identity leakage and Privacy loss
- Utility loss

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

(a) (b) (c) (d)

Modeling Privacy Loss

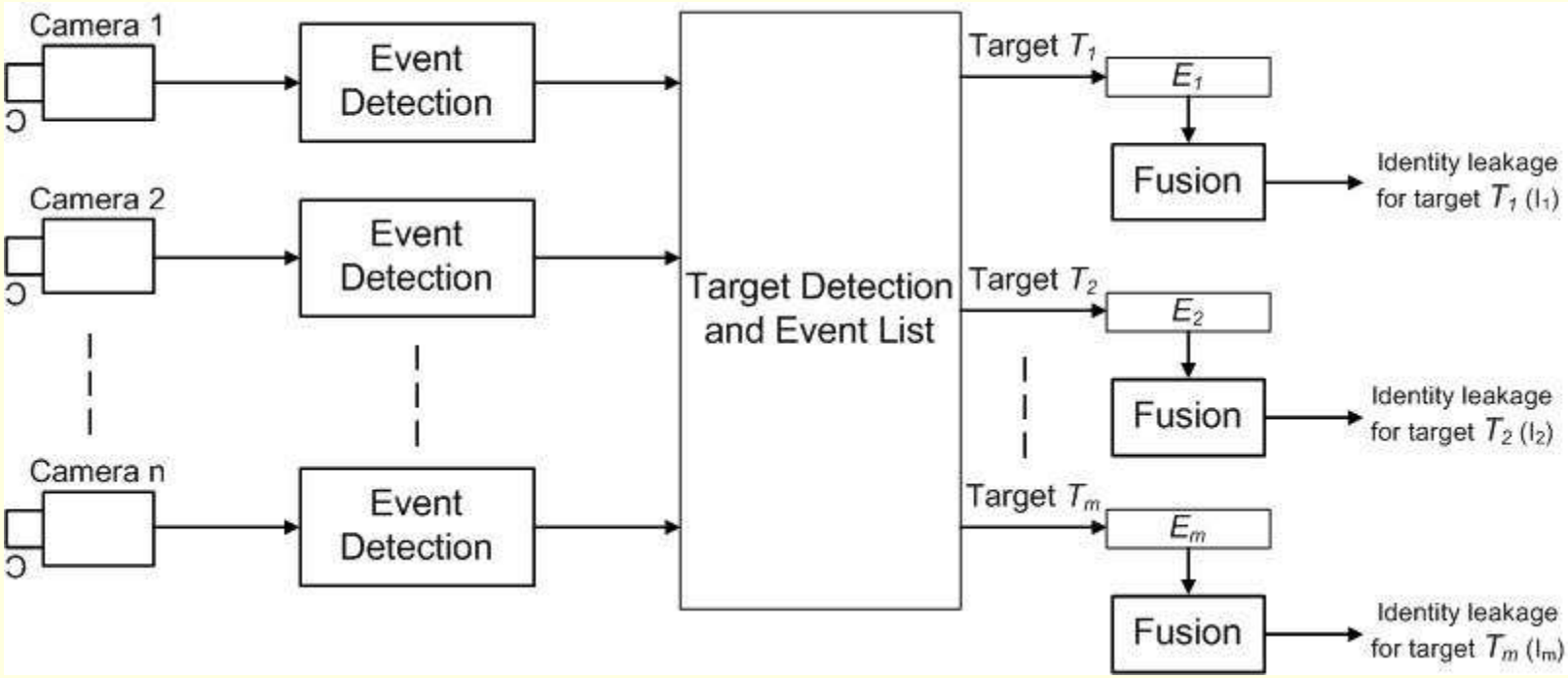
- Sensitive Information

COMMONLY FOUND SENSITIVE INFORMATION.

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

Modeling Privacy Loss

- Multi-camera surveillance

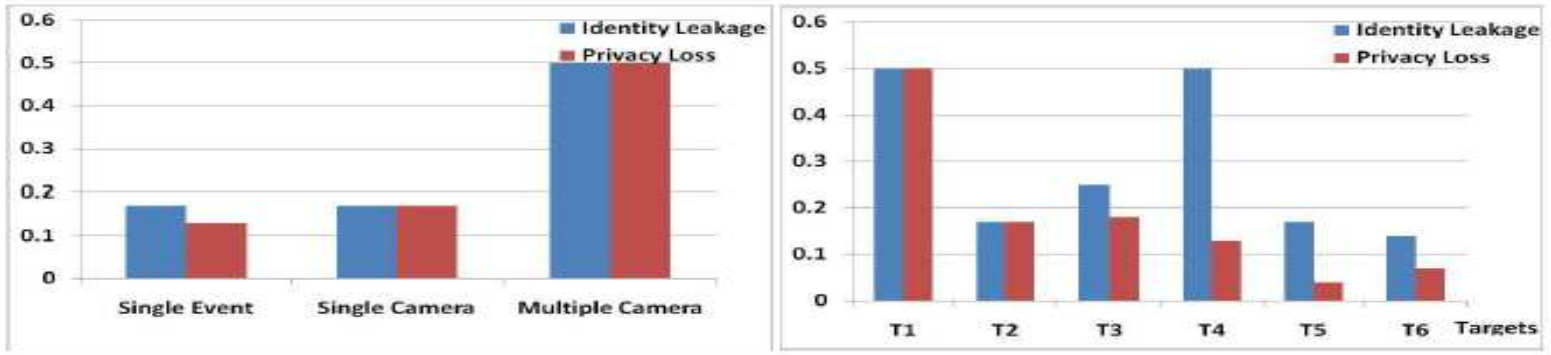


Modeling Privacy Loss

- Multi-camera surveillance

(a) DE (b) AL (c) SC (d) IC

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



(a) (b)

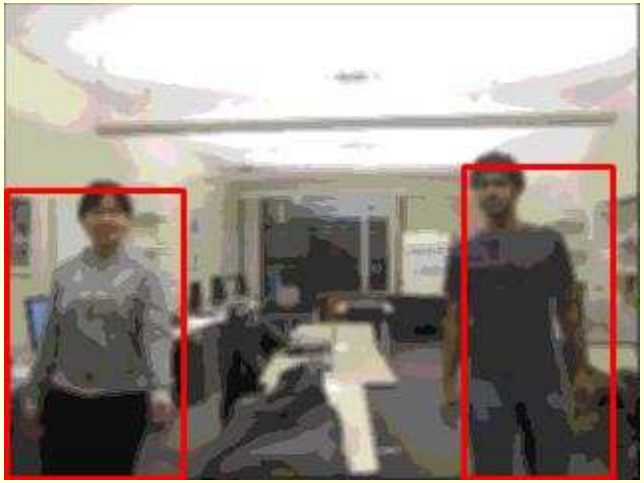
Fig. 8 (a) Identity leakage and privacy loss for T_1 (b) Identity leakage and privacy loss for all targets

Modeling Utility

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

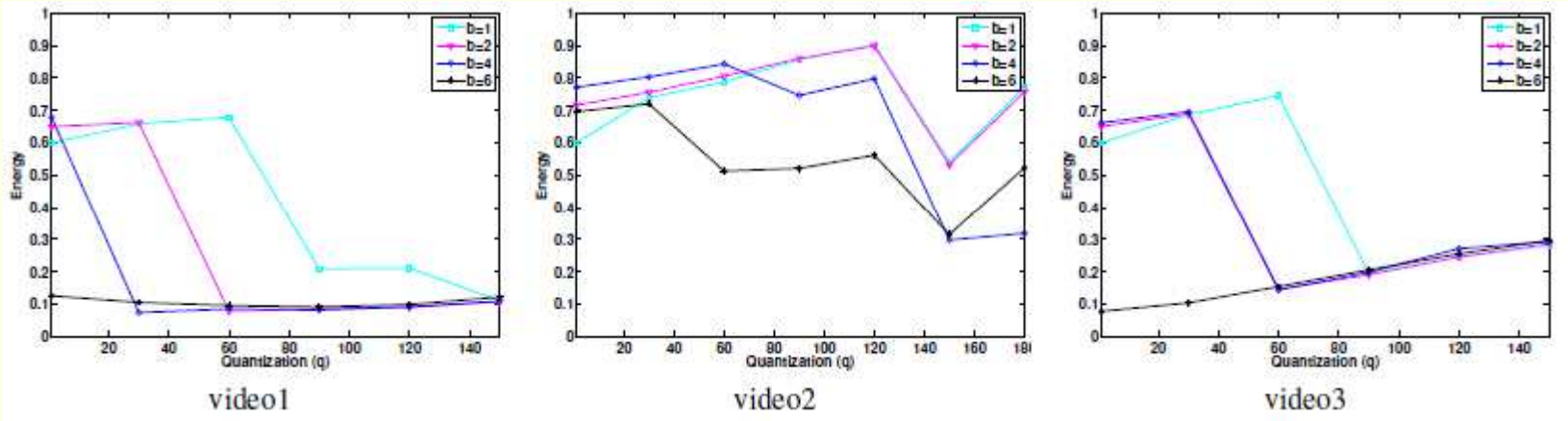
> *Definition 2: Utility loss* of the published video data refers to the decrease in the degree of accuracy by which analysis tasks can be accomplished with respect to the original data.

- Task-based **Utility Loss** computation:



Effect of Data Transformation Methods on Privacy Loss and Utility Loss

- Global transformation (first blurring then quantization)



video1 video2 video3

video1
$b = 4,\ q = 30$

video2
$b = 4,\ q = 150$

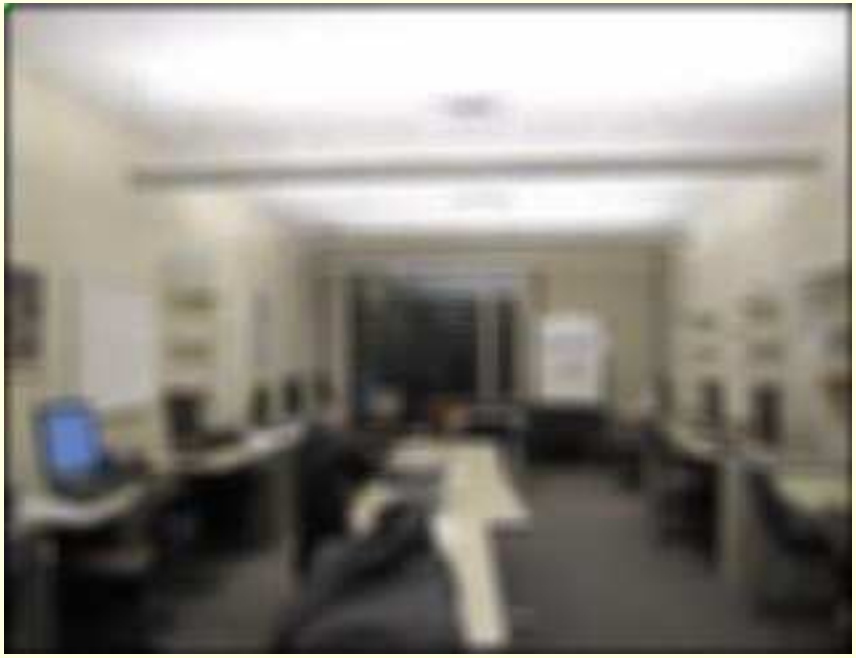
video3
$b = 6,\ q = 1$

Results of blob detection using transformed data

THE UNIVERSITY OF WINNIPEG

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

Observations

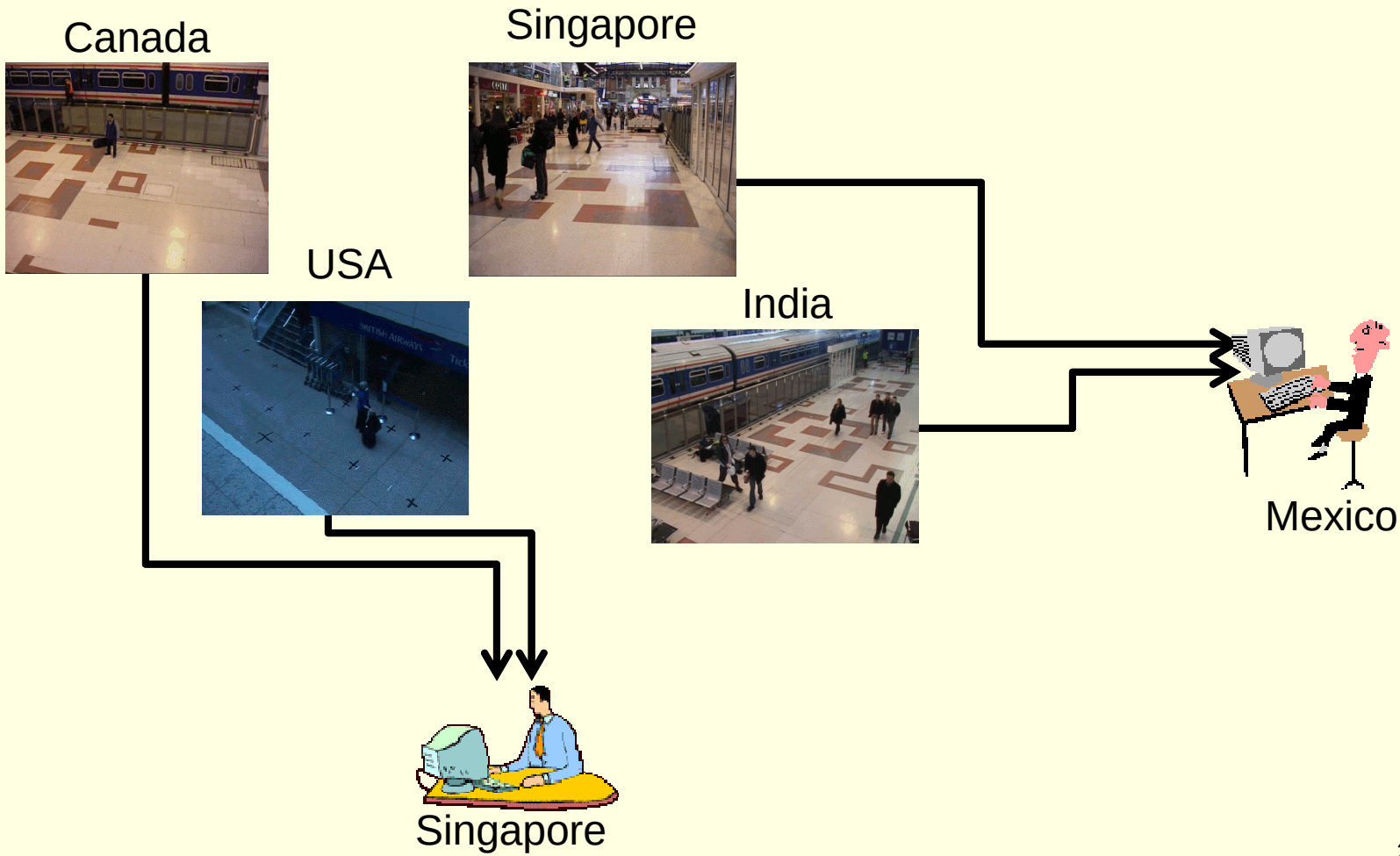
1: Sensitive information cannot be removed

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

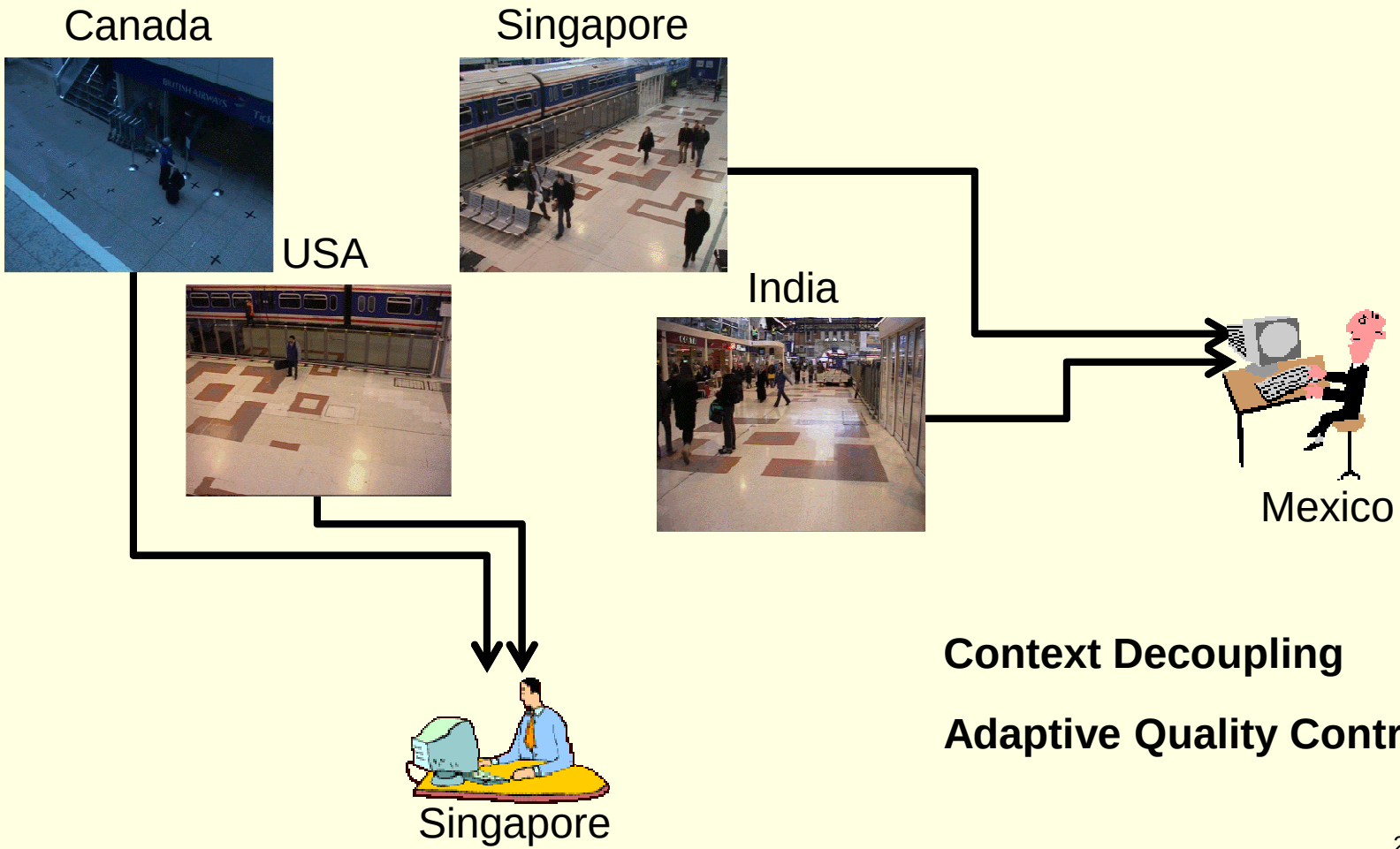
3: The what information is more important for surveillance and does not cause much privacy loss when detected alone in isolation

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

Anonymous Video Surveillance



Anonymous Video Surveillance



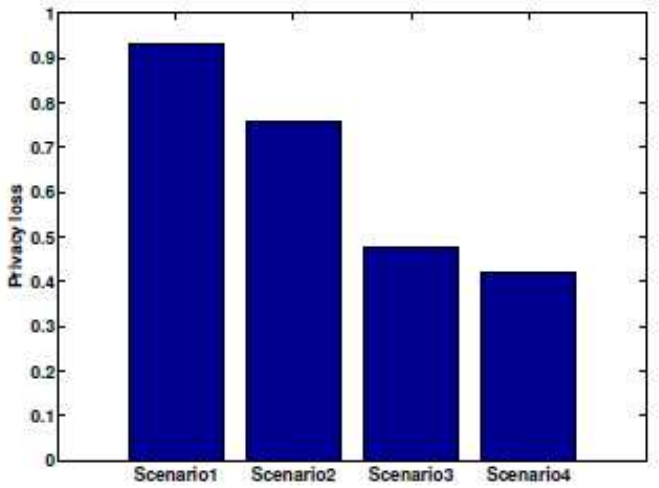
Context Decoupling

Adaptive Quality Control

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

Scenario	Description
Scenario1	A CCTV operator is watching the video in the same building.
Scenario2	The CCTV operator is watching the video in a different country, but S/he knows the location of the camera.
Scenario3	The CCTV operator is watching the video in a different country and S/he does not know the location of the camera.
Scenario4	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.



Average privacy loss in four scenarios.

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

- M. Saini, P. K. Atrey, S. Mehrotra, S. Emmanuel and M. S. Kankanhalli. Privacy modeling for video data publication. IEEE International Conference on Multimedia and Expo(ICME'2010), pp 60-65, July 2010, Singapore.
- M. Saini, P. K. Atrey, S. Mehrotra, and M S. Kankanhalli. Privacy aware publication of surveillance video. Inderscience Int. J. of Trust Management in Computing and Communications. (2012).
- M. Saini, P. K. Atrey, S. Mehrotra and M. S. Kankanhalli Considering implicit channels in privacy analysis of video data. IEEE COMSOC MMTC E-letter, Vol. 6, No. 11, pp 27-30, November 2011.
- M. Saini, P. K. Atrey, S. Mehrotra, and M S. Kankanhalli. W3-Privacy: Understanding what, when, and where inference channels in multi-camera surveillance video. Springer Int. J. Multimedia Tools and Applications. (2012).
- M. Saini, P. K. Atrey, S. Mehrotra, and M S. Kankanhalli. Adaptive transformation for robust privacy protection in video surveillance. Hindawi Int. J. of Advances in Multimedia, Volume 2012, Article ID 639649 (2012).

THE UNIVERSITY OF WINNIPEG

Security and Privacy in E-Health

Network

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

Collaborators:

Manoranjan Mohanty and Wei-Tsang Ooi

National University of Singapore

Cloud-based Secure 3D Medical Data Visualization

Data capturing

Data preprocessing

Server

Cloud

Image display

Client

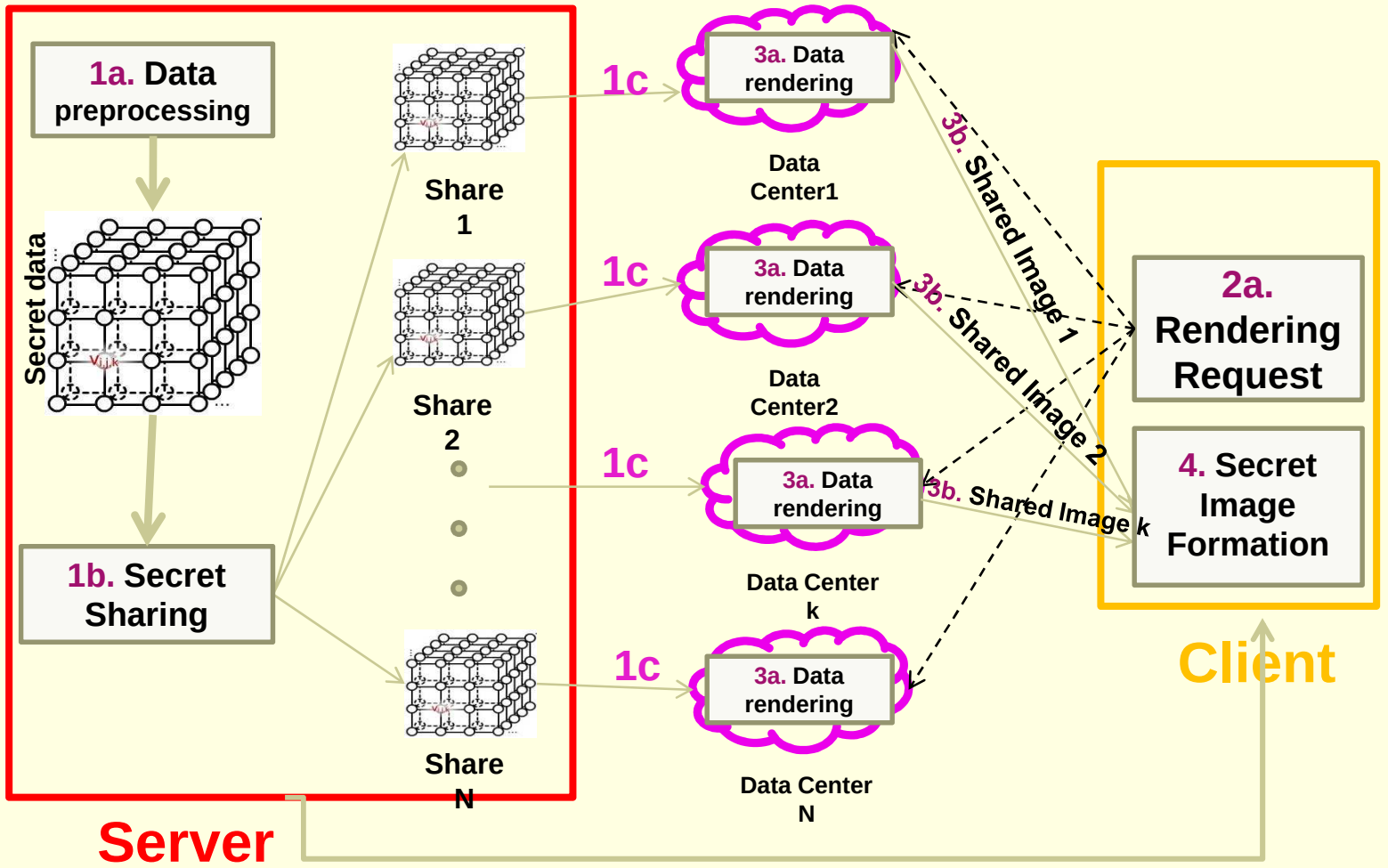
Preprocessed data

Data rendering

Rendered image

Publication: M. Mohanty, P. K. Atrey and W.-T. Ooi. Secure cloud-based medical data visualization. The ACM International Conference on Multimedia, 2012, Nara, Japan. (Accepted, to appear)

Cloud-based Secured Rendering: Architecture and Protocol



1c. Information about data centers and their shares

Security and Privacy in Social Networking Systems

CNET › News › Surveillance State

Exclusive: The next Facebook privacy scandal

by Chris Soghoian | January 23, 2008 8:58 AM PST

comments 17 | Like 543 | Tweet 23 | +1 1 | Share | More +

Facebook is no stranger to the complaints of privacy activists. First, it was the site's News Feed feature back in 2006. Most recently, the company's Beacon service drew widespread criticism. This blog post will outline yet another major privacy issue, in which Facebook recklessly exposes user data.

Source: http://news.cnet.com/8301-13739_3-9854409-46.html

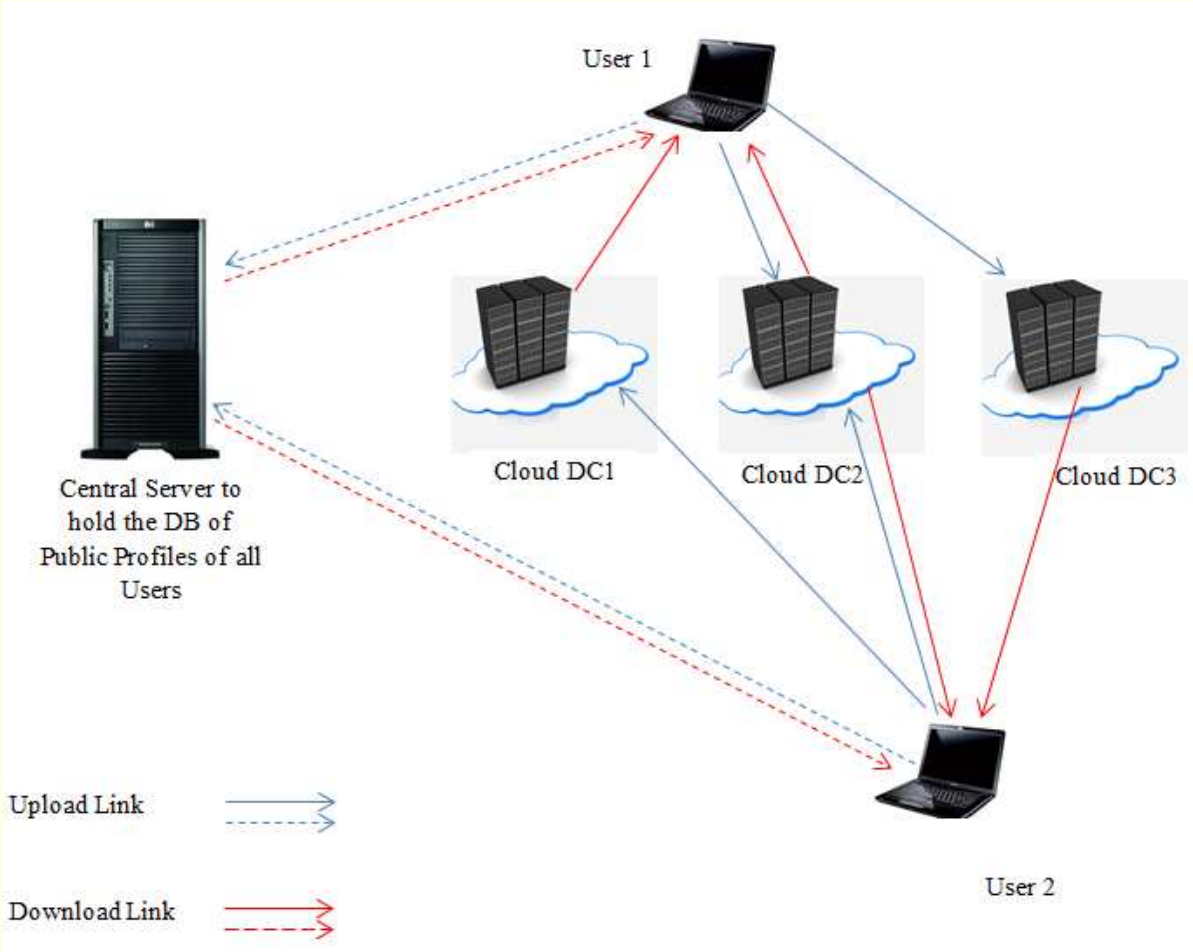
Collaborators:

Kasun Senevirathna and Adam Rehill, University of Winnipeg, Canada

A Secure and Privacy-aware Cloud-based Architecture for Social Networks

Targeted toward Untrusted Social Networking Operators

Developed a secret sharing based framework



Happy ending…

Security and Privacy Issues in Multimedia Systems *must not be* after thoughts