Privacy-Aware Publication of Surveillance Video

Pradeep K. Atrey

University of Winnipeg, Canada

p.atrey@uwinnipeg.ca

www.acs.uwinnipeg.ca/pkatrey/

THE UNIVERSITY OF WINNIPEG

Work done with…

- Mukesh Saini and Mohan Kankanhalli

  National University of Singapore

- Sharad Mehrotra

  University of California, Irvine, USA

THE UNIVERSITY OF WINNIPEG

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

THE UNIVERSITY OF WINNIPEG

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

Public Safety is Important

9/11 Terrorist attack (2001)

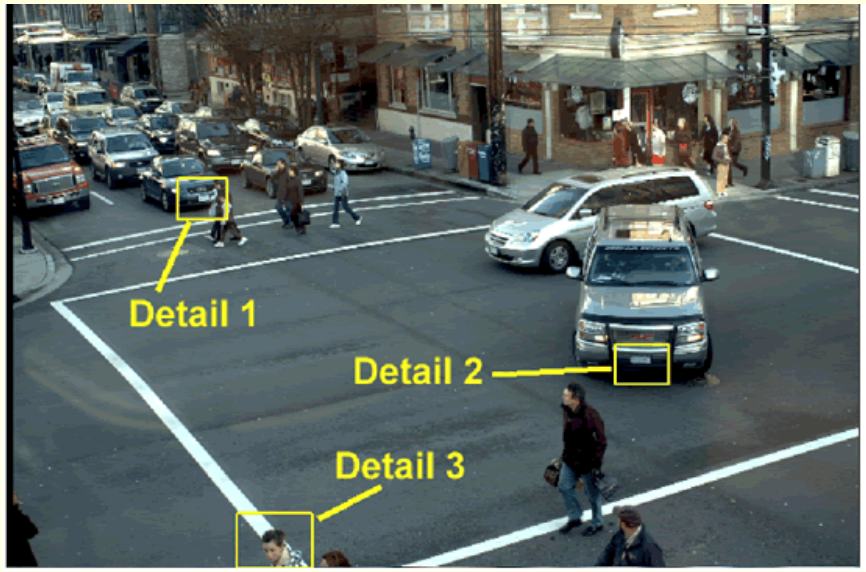
London bombing (2005)

Mumbai attack (2008)

Mumbai serial blast (2011)

Public Safety and CCTV Surveillance

- Large number of CCTV cameras
- London city has 10000+ cameras



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

Privacy Concerns

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

Privacy Concerns

Privacy Concerns

Privacy Concerns

- Large amount of recorded video
- Public access
  - Researchers
  - Policy makers
  - and others

$\Rightarrow$ Privacy violation

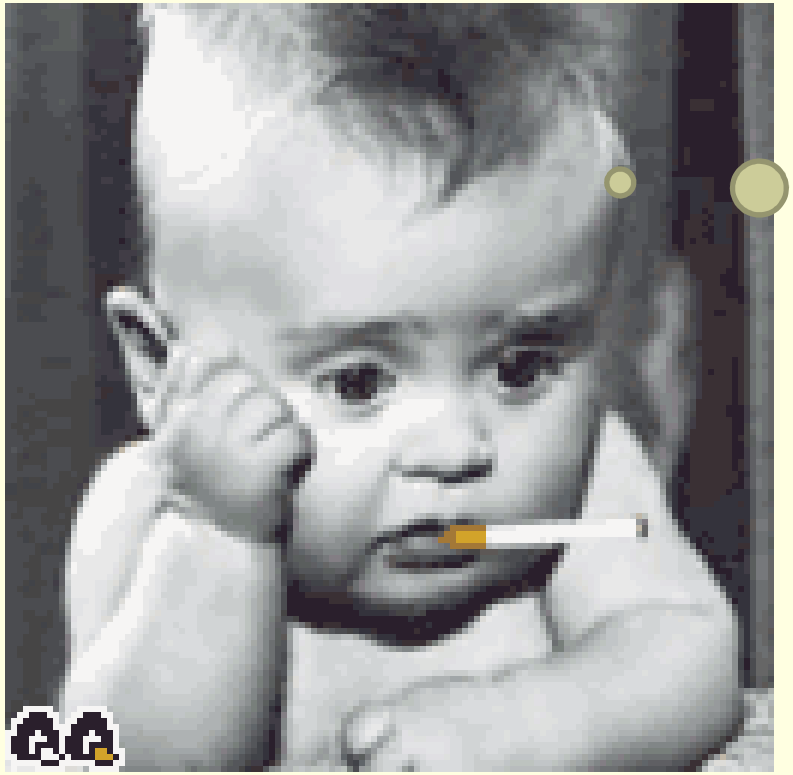
The problem is to determine the privacy violation due to publication of surveillance video and protect it.

What is the solution?

Privacy Concerns

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

What to do?



How to do effective surveillance while preserving the privacy of people?

THE UNIVERSITY OF WINNIPEG

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

Obvious Solution – Hide the face

- Obscure the face of the persons in the video
- Looks a simple and good solution
- 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
- Apply automatic face detection and hiding algorithm – seems good

Obvious Solution – Hide the face

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.

Traditional Privacy Assessment

- Binary value
  - Facial information ⇒ Privacy violation
  - No facial information ⇒ No privacy violation

Explicit Channel!

Is Hiding Facial Information Enough?

- In video, identity can be inferred not only by facial detection but also through detection of place, time, activity, etc.
- An adversary can use his prior knowledge to infer the identity of the person via these inference channels even when the facial information is not present.
- **Proxy Identifiers in Video: Evidences**
  - Detections – Face, Activity, Time, Place
  - Who, What, When, Where

Hidden Inference Channels

Place

Time

Behavior

Implicit Channels!

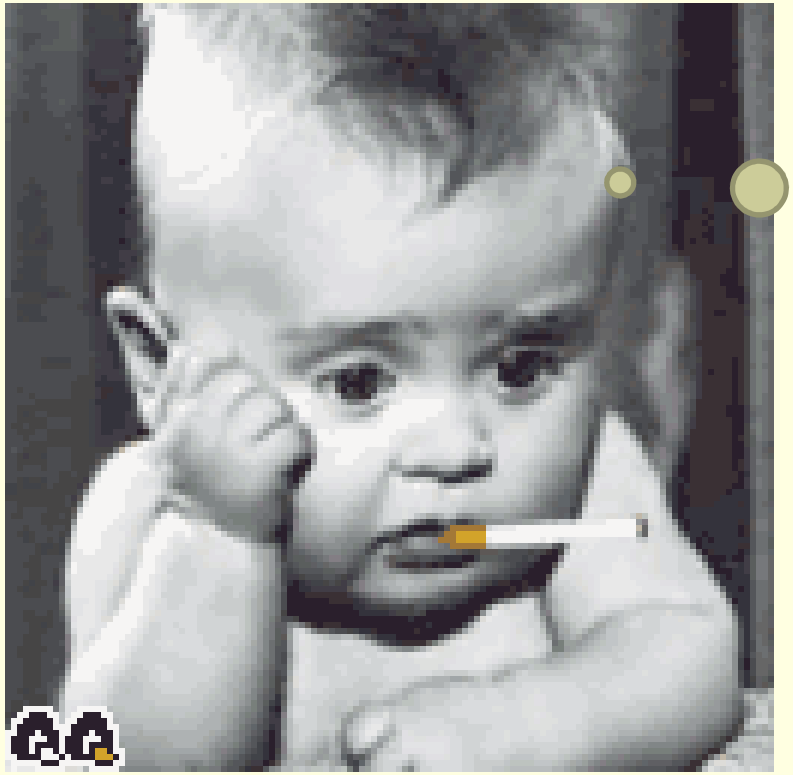
Explicit vs. Implicit Inference Channels

- Who } Explicit inference channel

- What
- When
- Where

} Implicit inference channels

Sounds interesting…



Probably we can solve this problem…

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

Our Contribution over State-of-the-art Methods

THE UNIVERSITY OF WINNIPEG

A COMPARISON OF THE PROPOSED WORK WITH THE EXISTING WORKS

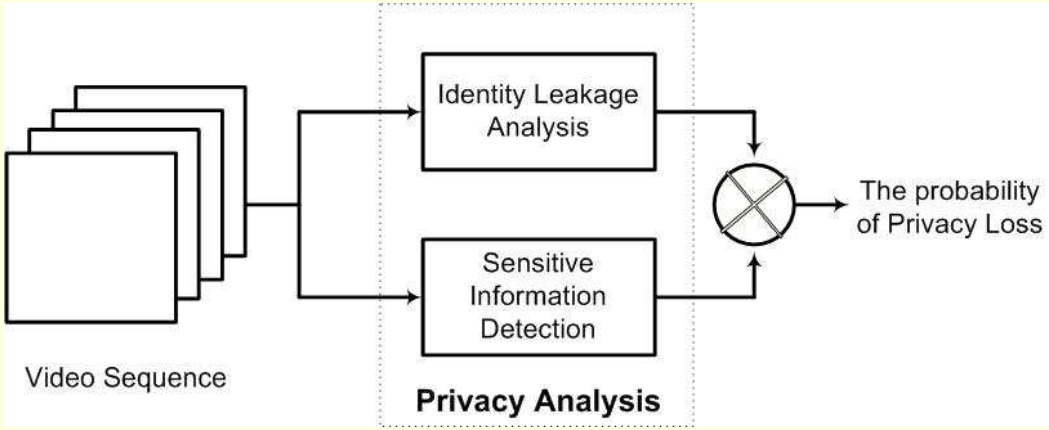
The work	Selective Obfusca-tion/ Global Transfor-mation	ROI	Identity leakage channels used	Privacy loss modeled as	Utility quanti-fied?
Boyle et al. [12]	Global (Blurring)	-	Explicit	Binary	No
Senior et al. [13]	Selective	Face and blob	Explicit	Binary	No
Moncrieff et al. [8]	Selective	Face	Explicit	Fixed lev-els	No
Fidaleo et al. [7]	Selective	Face	Explicit	Binary	No
Wickramasuriya et al. [11]	Selective	Face	Explicit	Fixed lev-els	No
Koshimizu et al. [14]	Selective	Silhouette	Explicit	Binary	No
Spindler et al. [15]	Selective	Blob	Explicit	Fixed lev-els	No
Thuraisingham et al. [10]	Selective	Face	Explicit	Binary	No
Carrillo et al. [9]	Selective	Face	Explicit	Binary	No
Paruchuri et al. [18]	Selective	Blob	Explicit	Binary	No
Qureshi [17]	Selective	Blob	Explicit	Binary	No
Dufaux [19]	Selective	Face	Explicit	Binary	No
Proposed work	**Global (Hybrid approach)**	-	**Explicit & implicit**	**Continuous**	**Yes**

1. **Privacy loss model** as a continuous variable for video data publication scenario.
2. A task based **utility model** to study the tradeoff between utility and privacy.
3. A suitable **data transformation function** that minimizes the utility loss as well as the privacy loss of the published data.

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

Contribution 1: Modeling Privacy Loss



Two views on privacy loss:

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

Contribution 1: Modeling Privacy Loss

- Identity Leakage
  - Explicit $I_{ex} = I_{wo} \Rightarrow I_{wo} = \begin{cases} 1 & \text{if the face is recognizable;} \\ 0 & \text{otherwise.} \end{cases}$
  - Implicit

$$I_{im} = \begin{cases} 0 & \text{if no people are present;} \\ I_{wt} & \text{if only } \textit{what} \text{ detected;} \\ I_{wt,wn} & \text{if } \textit{what} \text{ and } \textit{where} \text{ detected;} \\ I_{wt,wr} & \text{if } \textit{what} \text{ and } \textit{when} \text{ detected;} \\ I_{wt,wn,wr} & \text{if } \textit{what}, \textit{when} \text{ and } \textit{where} \\ & \text{detected.} \end{cases}$$

$$I_{wt} = \frac{\rho}{G_{wt}} \qquad G_{wt} = \frac{1}{n_1} \sum_{i_1=1}^{n_1} \mathcal{H}(\xi_{i_1})$$

$$I_{wt,wn} = \frac{\rho}{G_{wt,wn}} \qquad G_{wt,wn} = \frac{1}{n_1 * n_2} \sum_{i_1=1}^{n_1} \sum_{i_2=1}^{n_2} \mathcal{H}(\xi_{i_1}, \Delta t_{i_2})$$

$$I_{wt,wr} = \frac{\rho}{G_{wt,wr}} \qquad G_{wt,wr} = \frac{1}{n_1 * n_3} \sum_{i_1=1}^{n_1} \sum_{i_3=1}^{n_3} \mathcal{H}(\xi_{i_1}, \lambda_{i_3})$$

$$I_{wt,wn,wr} = \frac{\rho}{G_{wt,wn,wr}} \qquad G_{wt,wn,wr} = \frac{1}{n_1 * n_2 * n_3} \sum_{i_1=1}^{n_1} \sum_{i_2=1}^{n_2} \sum_{i_1=3}^{n_3} \mathcal{H}(\xi_{i_1}, \Delta t_{i_2}, \lambda_{i_3})$$

$$I_f = MAX\{ \underbrace{I_{ex}}_{explicit}, \underbrace{I_{im}}_{implicit} \}$$

$$I = MAX\{I_f \mid \forall f \in V\}$$

Contribution 1: Modeling Privacy Loss

- Sensitivity Index

$$A = \{a_1, a_2, ...a_l\}$$

$$\mathcal{W} = \{w_k \mid k \in [1,l], w_1 + w_2, ... + w_l = 1\}$$

$$S = \{s_k \mid k \in [1,l]\}$$

$$s_k = \begin{cases} 1 & \text{if } k^{th} \text{ attribute is detected;} \\ 0 & \text{otherwise.} \end{cases}$$

$$\Psi = \mathcal{W}.S$$

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.

- Privacy Loss

Definition 1: The *Privacy loss* due to published data V is represented by $0 \leq \Gamma(V) \leq 1$. $\Gamma = 0$ implies no privacy loss and $\Gamma = 1$ represents the worst case where the individual's identity, along with other information such as activity, time and place, can be determined exactly.

$$\Gamma = \mathcal{I} \times \Psi$$

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

Contribution 2: Utility Model

- 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.

- Our goal is to find data transformation function $\mathcal{F}$ that minimizes the energy function E:

$$E = \eta\Gamma(\mathcal{F}(V)) + (1-\eta)U(\mathcal{F}(V))$$

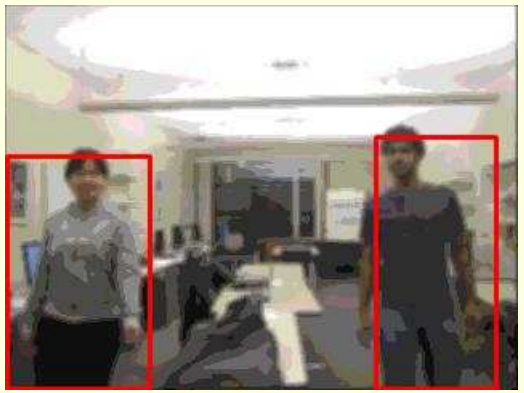
- Task-based **Utility Loss** computation:

$$U(V') = \sum_{j=1}^{k} \alpha_j \times U_j(V')$$

$$U_j = 1 - \frac{Acc_j(V')}{Acc_j(V)}$$

$$Acc = \frac{TP}{(TP+FP+FN)}$$

$\alpha_{face\_detection}$ = very low



$\alpha_{blob\_detection}$ = very high

THE UNIVERSITY OF WINNIPEG

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

Contribution 3: Data Transformation

- Selective Obfuscation – rely heavily on Computer Vision techniques (which may not be always 100% accurate)
- **Global Transformation**
  - Pixelization/resolution variation

$$f_p(x,y) = \frac{1}{\delta^2} \sum_{i=1}^{\delta} \sum_{j=1}^{\delta} f\left(\left\lfloor \frac{x}{\delta} \right\rfloor \delta + \left\lfloor \frac{y}{\delta} \right\rfloor \delta \right)$$

δ is the block size

• Decreasing the resolution of the image makes it difficult to identify the people in the video; nevertheless, the loss in utility of the data can be drastic.

• The resolution is reduced to 47% for the face detector to fail, still face can be identified.

Contribution 3: Data Transformation

- **Global Transformation**
  - Blurring

$$f_b(x,y) = f(x,y) * G(x,y)$$

$$G(x,y) = \frac{1}{2\pi\sigma^2} e^{-\frac{x^2+y^2}{2\sigma^2}}$$

b is the blurring parameter

From the privacy perspective, it can effectively hide the evidence information present in the video; however, there are limitations of this method.

• Firstly, to effectively hide the evidence information, we need an estimation of the area occupied by region of interest

• Secondly, image enhancement techniques can be used to approximate the original image.

Even when the face detector fails, the person can be identified by looking at the blurred image

Contribution 3: Data Transformation

- **Global Transformation**
  - Quantization

$$f_q = \left\lfloor \frac{f(x,y)}{q} \right\rfloor q + \frac{q}{2}$$

q is the quantization step

Face detector fails and it is hard to identify the person by looking at the quantized image

• Image quantization introduces permanent loss of the information.

• While the quantization is effective in hiding facial information, it performs very poorly in hiding textual information.

Contribution 3: Data Transformation

- **Global Transformation**
  - Blurring & Quantization
    - First blurring then quantization

      $$f_{qb}(x,y) = f_q(x,y) * G(x,y)$$

      or
    - First quantization then blurring

      $$f_{bq} = \left\lfloor \frac{f_b(x,y)}{q} \right\rfloor q + \frac{q}{2}$$

• Effectively, we first remove the high frequency private information from the image via blurring and then introduce random non-recoverable high frequency noise via quantization to hide identity information.

• We found in the experiments that the proposed method transforms the video to a form where human beings cannot easily identify the people in the video; however, some application tasks like blob detection and tracking can still be accomplished.

Contribution 3: Data Transformation

- **Global Transformation**
  - Blurring & Quantization (Scalability issue)
    - Find the representative video clip
    - Determine the blurring and quantization parameters for this clip
    - Transform the whole video with these parameters

• Representative video clip is determined based on the region of sensitive information (e.g. text legends, face, etc.)

• The transformation required to hide the sensitive information is proportional to the size of region of sensitive information.

THE UNIVERSITY OF WINNIPEG

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

Experiments and Results

- **Objectives**
  - Effect of the hidden inference channels on the privacy loss from the published video data.
  - Effectiveness of different transformation methods in reducing the privacy loss.
  - Optimum amount of blurring and quantization required to minimize the energy function for a given application.

- The **application scenario** considered for experiments consists of two tasks:
  - blob detection and tracking (with equal importance).
  - a GMM based adaptive background model.

Experiments and Results:

Data set

DESCRIPTION OF THE VIDEO DATA USED IN EXPERIMENTS

Data	Type	Total frames	Activity frames	People (ρ)	Resolution	Duration	Scenario
Video1	Mock	6650	5045	2	320×240	30 Minutes	Indoor
Video2	Mock	3940	2340	4	320×240	30 Minutes	Outdoor
Video3	**Real**	**28216**	**17218**	20	704×480	**24 Hour**	Indoor

(a) Video1

(b) Video2

(c) Video3

For Video 1 and Video 2: G_{wt} = 100000, $G_{wt,wn}$ = 10000, $G_{wt,wr}$ = 10, $G_{wt,wn,wr}$ = 5
For Video 3: G_{wt} = 100000, $G_{wt,wn}$ = 10000, $G_{wt,wr}$ = 1000, $G_{wt,wn,wr}$ = 100

Experiments and Results:

Privacy Assessment (Explicit vs. Implicit)

- A user study to calculate the privacy loss
- The users were asked the following three questions:
  1. is the face recognizable?
  2. is the time when the video was shot available?
  3. is the location recognizable?
- The overall answer is calculated as “No” only if all users answer in “No”, otherwise it is considered “Yes”.

THE UNIVERSITY OF WINNIPEG

Experiments and Results:

Privacy Assessment (Explicit vs. Implicit)

PRIVACY LOSS FOR VIDEO1 WITH DIFFERENT DEGREES OF BLURRING.

	who		*where*		*when*	
b	M*	H*	M*	H*	M*	H*
1	Yes	Yes	Yes	Yes	No	Yes
2	Yes	Yes	No	Yes	No	Yes
4	No	Yes	No	No	No	Yes
6	No	No	No	No	No	No
8	No	No	No	No	No	No
10	No	No	No	No	No	No

*M and H represent Machine-detected and Human-detected options, respectively.

	Identity leakage				Privacy Loss	
	Implicit I_{im}		Explicit I_{ex}		Γ	
b	M*	H*	M*	H*	M*	H*
1	0.2	**0.4000**	1	1	1	1
2	0.0	**0.4000**	1	1	1	1
4	0.0	**0.0002**	0	1	0	1
6	0.0	0.0000	0	0	0	0
8	0.0	0.0000	0	0	0	0
10	0.0	0.0000	0	0	0	0

PRIVACY LOSS FOR VIDEO1 WITH DIFFERENT QUANTIZATION STEPS.

	who		*where*		*when*	
q	M*	H*	M*	H*	M*	H*
1	Yes	Yes	Yes	Yes	No	Yes
30	Yes	Yes	Yes	Yes	No	Yes
60	Yes	Yes	No	Yes	No	No
90	No	No	No	Yes	No	No
120	No	No	No	Yes	No	No
150	No	No	No	No	No	No

*M and H represent Machine-detected and Human-detected options, respectively.

	Identity leakage				Privacy Loss	
	Implicit I_{im}		Explicit I_{ex}		Γ	
q	M*	H*	M*	H*	M*	H*
1	0.2	**0.4**	1	1	1	1.0
30	0.2	**0.4**	1	1	1	1.0
60	0.0	**0.2**	1	1	1	1.0
90	0.0	**0.2**	0	0	0	0.2
120	0.0	**0.2**	0	0	0	0.2
150	0.0	0.0	0	0	0	0.0

PRIVACY LOSS CALCULATION FOR VIDEO2 AND VIDEO3.

Privacy Loss for Blurring					Privacy Loss for Quantization				
	Video2		Video3			Video2		Video3	
b	M*	H*	M*	H*	q	M*	H*	M*	H*
1	1	1.000	1	1.0000	1	1	1.000	1	1.0000
2	1	1.000	0	1.0000	30	1	1.000	0	1.0000
4	0	1.000	0	1.0000	60	1	1.000	0	1.0000
6	0	0.800	0	0.0002	90	0	1.000	0	0.0002
8	0	0.800	0	0.0002	120	0	1.000	0	0.0002
10	0	0.400	0	0.0002	150	0	0.400	0	0.0002

*M and H represent Machine-detected and Human-detected options, respectively.

Experiments and Results:

Effect of Data Transformation Methods on Privacy Loss and Utility Loss

- Selective obfuscation

PRIVACY LOSS, UTILITY LOSS, AND ENERGY CALCULATION FOR SELECTIVE OBFUSCATION METHOD.

	Video1			Video2			Video3		
Operation	Γ	U	E	Γ	U	E	Γ	U	E
Quantization	0.999	0.108	0.643	1.000	0.222	0.689	0.974	0.183	0.658
Blurring	0.999	0.188	0.675	1.000	0.248	0.699	0.974	0.214	0.670

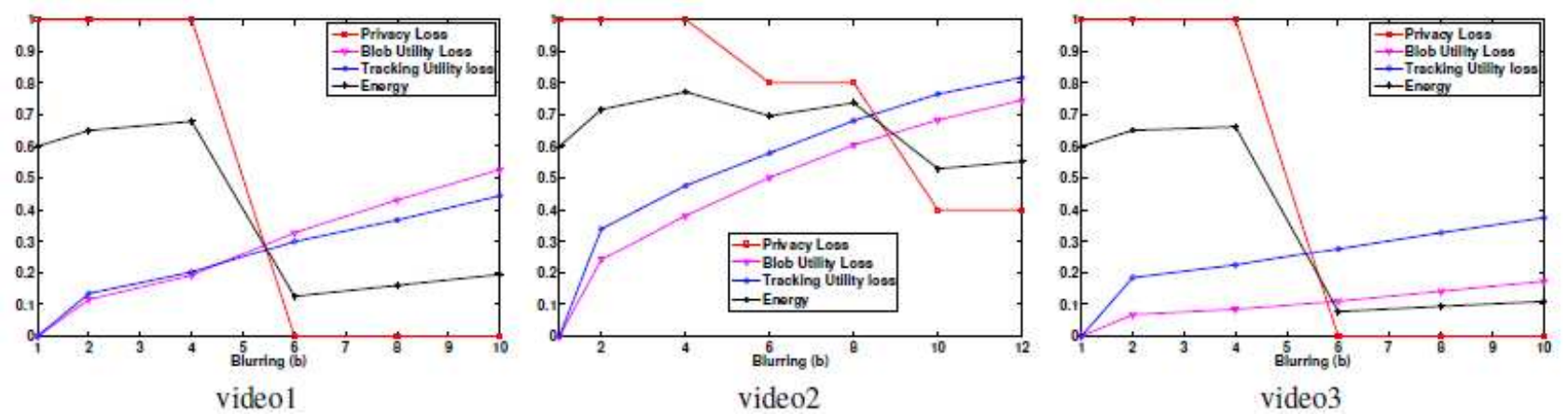


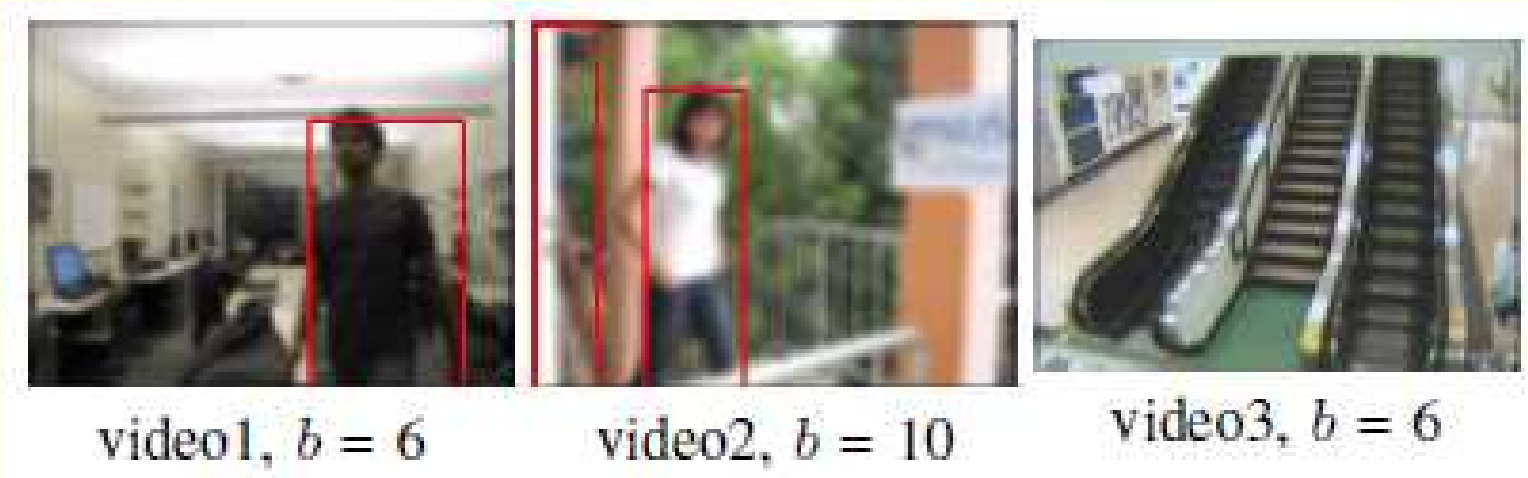
Three frames of Video 1

Experiments and Results:

Effect of Data Transformation Methods on Privacy Loss and Utility Loss

- Global transformation (blurring)

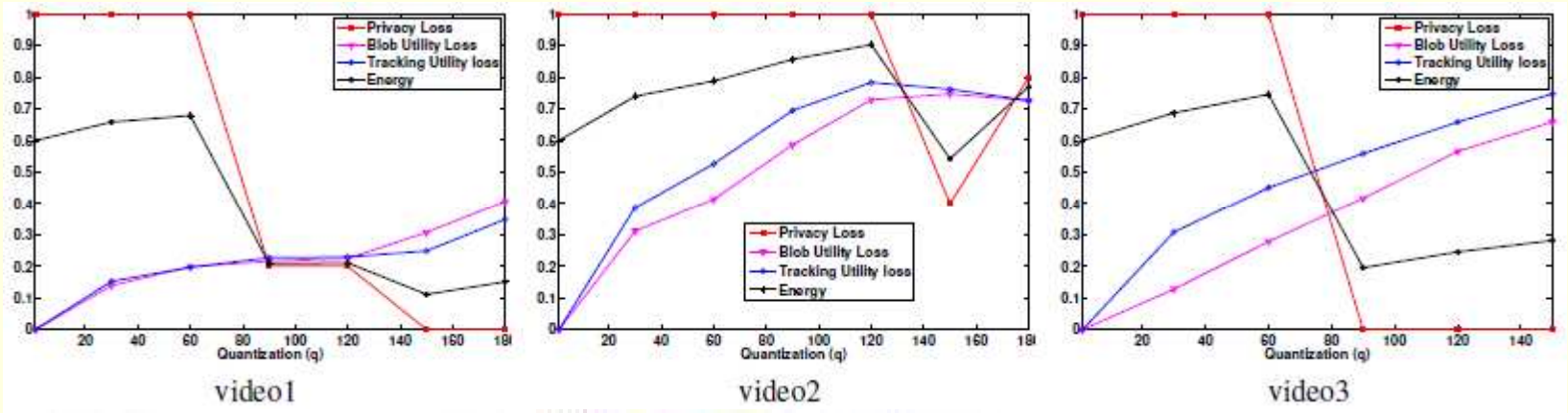


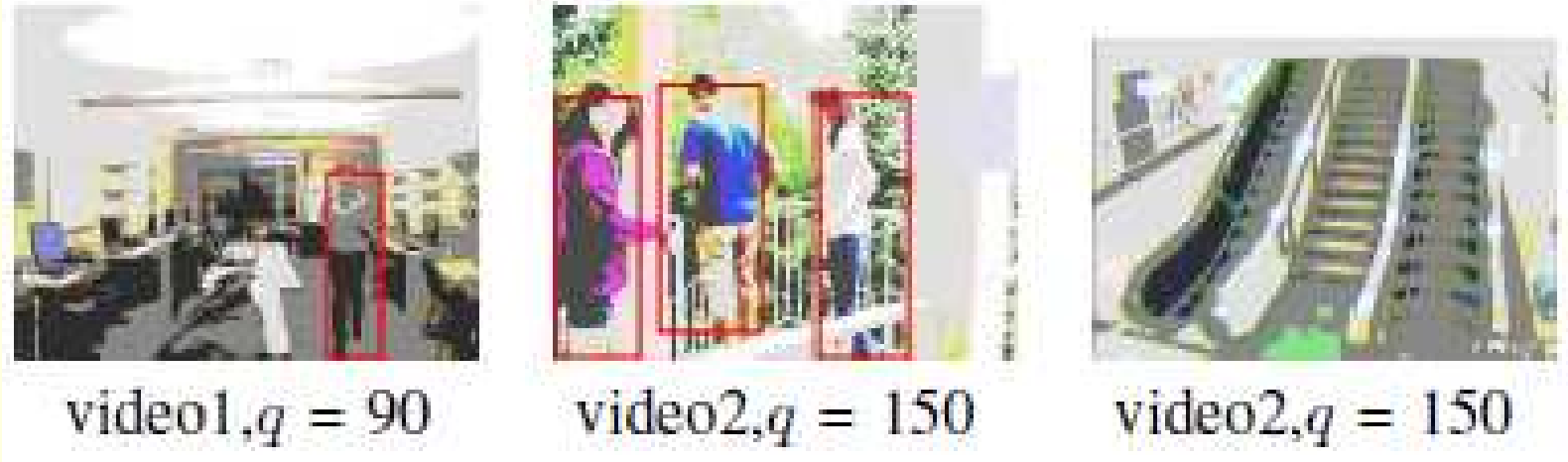


Experiments and Results:

Effect of Data Transformation Methods on Privacy Loss and Utility Loss

- Global transformation (quantization)

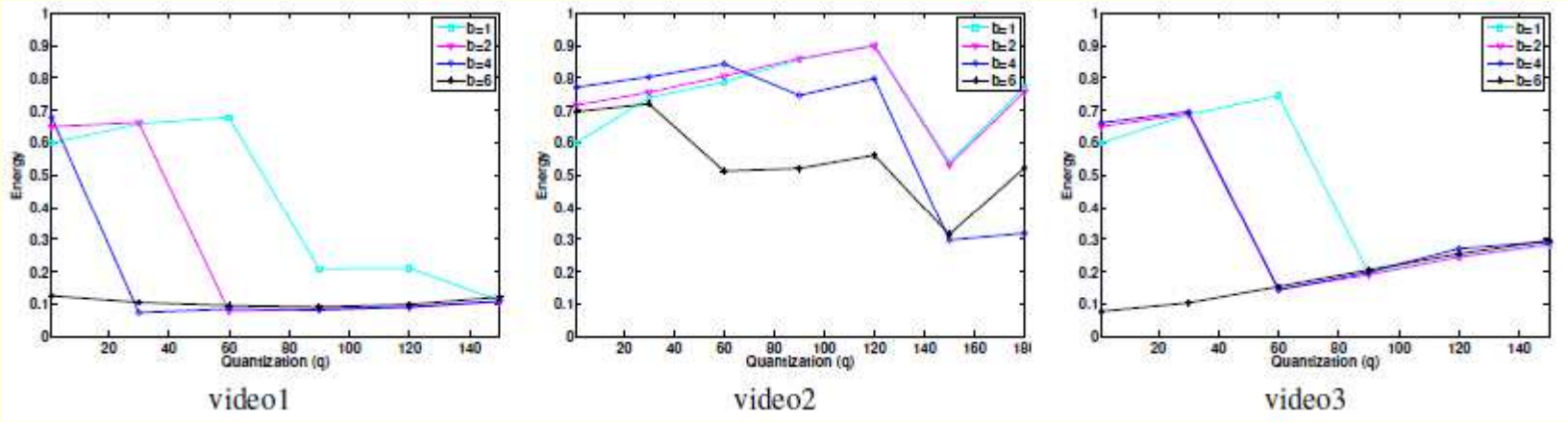




Experiments and Results:

Effect of Data Transformation Methods on Privacy Loss and Utility Loss

- Global transformation (first blurring then quantization)



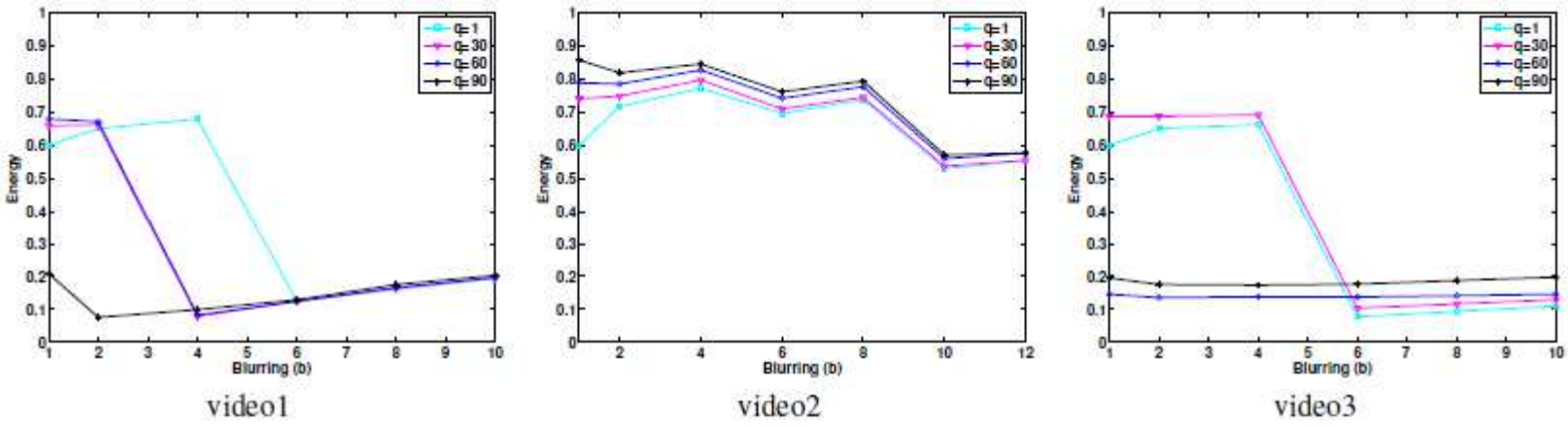
video1 video2 video3

video1 $b = 4,\ q = 30$ video2 $b = 4,\ q = 150$ video3 $b = 6,\ q = 1$

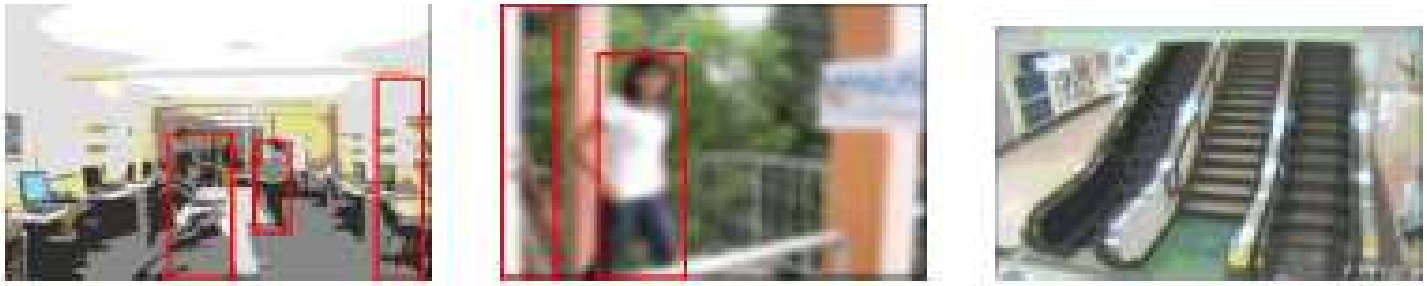
Experiments and Results:

Effect of Data Transformation Methods on Privacy Loss and Utility Loss

- Global transformation (first quantization then blurring)



video1 video2 video3



video1 $q = 90,\ b = 2$ video2 $q = 1,\ b = 10$ video3 $q = 1,\ b = 6$

THE UNIVERSITY OF WINNIPEG

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

Experiments and Results:

Demo 1 (Results of face detection in transformed data)

THE UNIVERSITY OF WINNIPEG

Can you identify the person by face?

No face detected in transformed data by either human or machine

Experiments and Results:

Demo 2 (Results of text detection in transformed data)

THE UNIVERSITY OF WINNIPEG

Can you see the text?

No text detected in transformed data by either human or machine

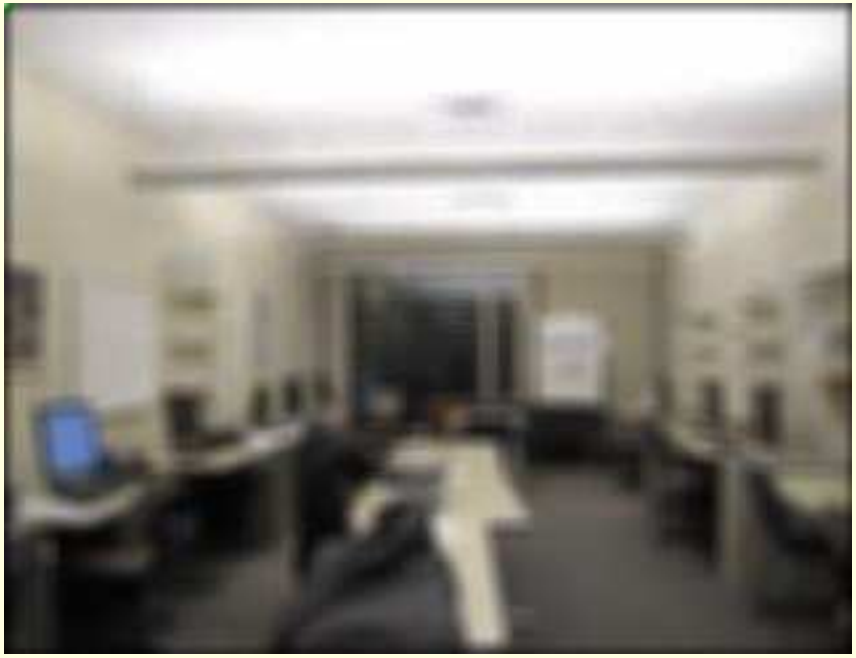
Experiments and Results:

Demo 3 (Results of blob detection in 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

Results are promising

We could solve the problem up to certain extent…

Outline

- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

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.
- Hybrid approach (First blurring then quantization) provides better tradeoff.

Outline

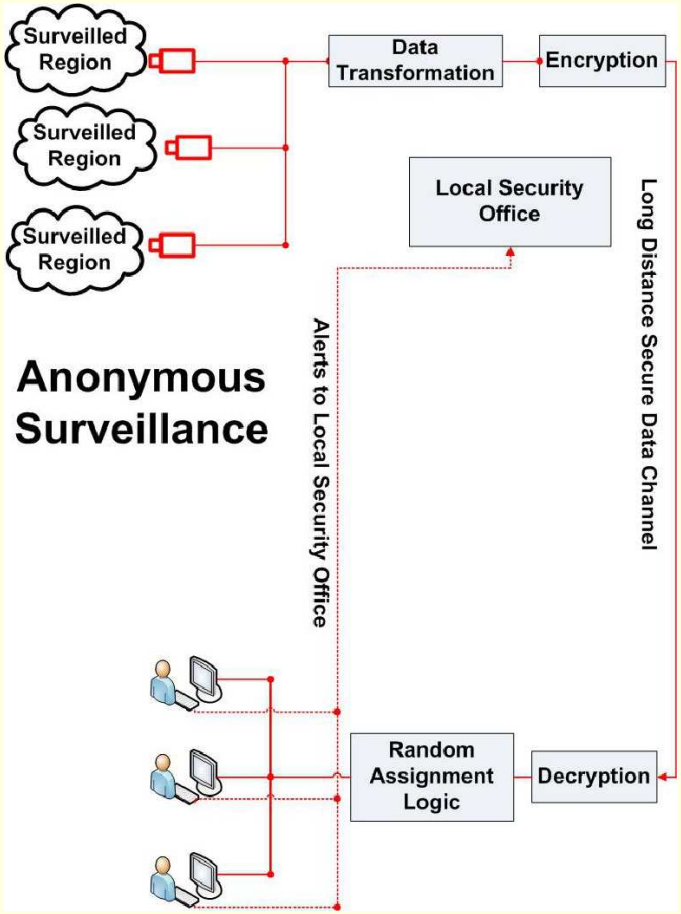
- Introduction and motivation
- State-of-the-art
- Proposed work
  - Contribution 1: Privacy model
  - Contribution 2: Task-based utility model
  - Contribution 3: Global data transformation
- Experiments and results
- Demos
- Conclusions
- Ongoing work

Publications

- This work
  - 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).
- Privacy Modeling for Multi-camera Videos
  - 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).
- Privacy modeling and protection in real-time CCTV views monitoring
  - 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).

Ongoing work

- Anonymous surveillance (Remote CCTV monitoring)



M. Saini, P. K. Atrey, S. Mehrota and M. S. Kankanhalli. Anonymous surveillance. IEEE ICME Workshop on Advances in Automated Multimedia Surveillance of Public Safety (AAMS-PS'2011), July 2011, Barcelona, Spain.

Discussion