Advances in Privacy Protective Video Surveillance

Faisal Z. Qureshi

Faculty of Science, UOIT, Oshawa

Say I want to find a person in a city.
What would I rather have?

the address of that person; or

a photograph of that individual?

We are visual creatures

and know our world first and foremost by what we can see …

The Way of the Cell, FM Harold, Oxford Univ. Press, 2001.

Video Surveillance Effects us Viscerally

Privacy implications of video surveillance are minimal compared to other means of electronic surveillance

Video Surveillance Effects us Viscerally

~~Privacy implications of video surveillance are minimal compared to other means of electronic surveillance~~

Corroding effects of pervasive video surveillance

Loss of freedom to be yourself
(Jermyn, 2004)

Corroding effects of pervasive video surveillance

Psychological effects of “voyeuristic gaze” on individuals

(Marx, 1988)

Corroding effects of pervasive video surveillance

Net widening that exposes more people to regular police monitoring that can lead to abuse

(Davies, 1996)

Corroding effects of pervasive video surveillance

Exclusionary surveillance

(Norris and Armstrong 1999)

Corroding effects of pervasive video surveillance

Loss of guardianship

(Cohen and Felson, 1979)

This loss of privacy has not gone unnoticed by one ironically surveilled group, law enforcement officers. In one British study, nearly a quarter of the police officers noted that a key disadvantage of CCTV was that it watched them …

(Surette, 2005, Skinns, 1997)

References

Jermyn, D. (2004), “This is about real people!: video technologies, actuality and affect in the television crime appeal”, in Holmes, S. and Jermyn, D. (Eds), Understanding Reality Television, Routledge, New York, NY, pp. 71-90.

Marx, G. (1988), Undercover: Police Surveillance in America, University of California Press, Berkley, CA.

Davies, S. (1996), “The case against: CCTV should not be introduced”, International Journal of Risk, Security and Crime Prevention, Vol. 1 No. 4, pp. 327-31.

Norris, C. and Armstrong, G. (1998), “Introduction: power and vision”, in Norris, C., Moran, J. and Armstrong, G. (Eds), Surveillance, Closed Circuit Television and Social Control, Ashgate, Aldershot, pp. 3-18.

Norris, C. and Armstrong, G. (1999), The Maximum Surveillance Society: The Rise of CCTV, Berg, Oxford.

Cohen, L. and Felson, M. (1979), “Social change and crime rate trends: a routine activities approach”, American Sociological Review, Vol. 44, pp. 588-608.

Skinns, D. (1997), Annual report of the safety in Doncaster evaluation, October 1995-September 1996, Safety in Doncaster, Doncaster.

Surette, R. (2005), The thinking eye: Pros and Cons of Second Generation CCTV Surveillance Systems, Policing: An International Journal of Police Strategies & Management, Vol. 28, No. 1, 2005, pp. 152-173.

Panoptic video surveillance has serious implications for *personal privacy* and our *right to anonymity*

Video surveillance is ubiquitous

1 Wide spread perception that video surveillance is essential for safety and security

Video surveillance is ubiquitous

2 Reduction in deployment and management costs due to advances in imaging & computer technologies

Video surveillance is ubiquitous

3

Legal vacuum, a lack of regulatory compliance, and a lack of understanding about the long term effects of 24/7 video surveillance

Balancing Act

The *need for video surveillance against an individual's right to privacy* is a challenge that need to be addressed within *social*, *legal* and *technical* contexts

Large Scale, Automatic Video Surveillance

Camera Networks & Smart Cameras

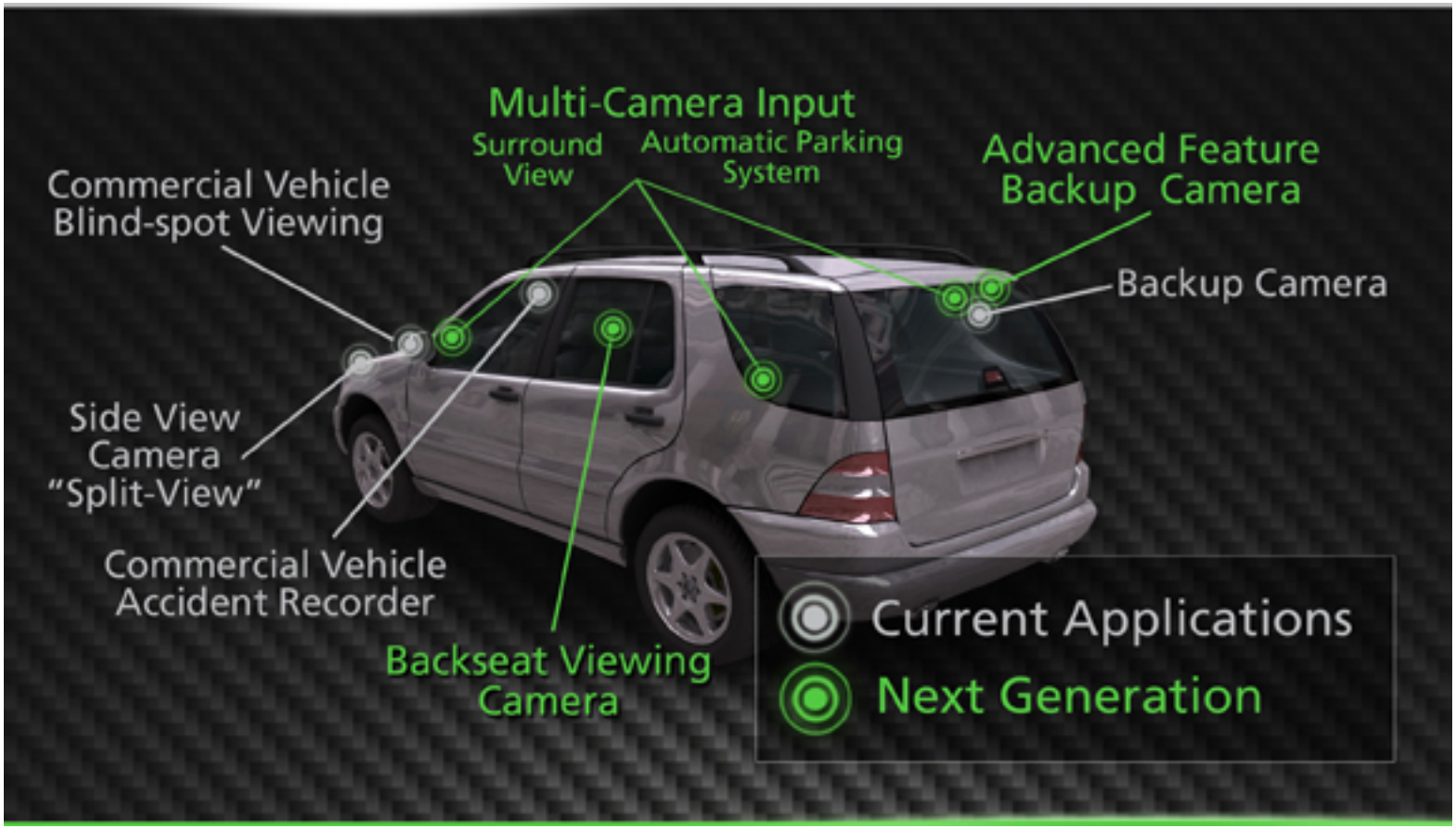
- Effective visual coverage of large spaces require multi-camera systems
- Operator monitoring is infeasible for large networks

Need networks of smart cameras capable of autonomous operation

Smart Cameras = Visual Sensor Nodes

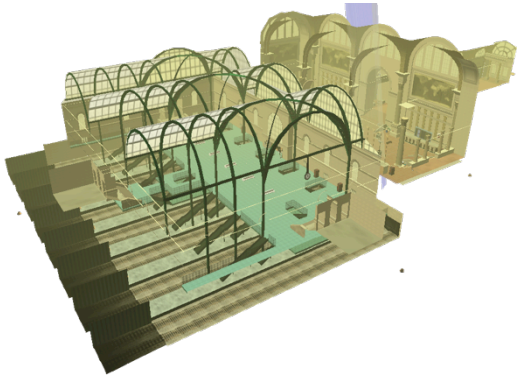
- Smart cameras networks
  - Kulkarni et al., 2005
    Gibbons et al., 2003
- Local onboard processing
- Communicate with neighbors
  - Akyildiz et al., 2002
    Priyantha et al., 2000;
    Chu et al., 2001
    Blazevic et al., 2000

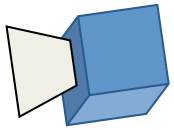
Smart Cameras = Visual Sensor Nodes



© Aptina Automobile Imaging

Software Laboratory for Camera Networks Research





Virtual Camera

Camera Model:
pan, tilt, zoom,
camera jitter,
color response,
lens distortions,
etc.

High-Level Control
camera control,
assignment,
handover,
etc.

Environment Models:
geometry, texture,
illumination

Pedestrian Models:
appearance, movement,
behavior

Reality Emulator
Virtual Penn Station

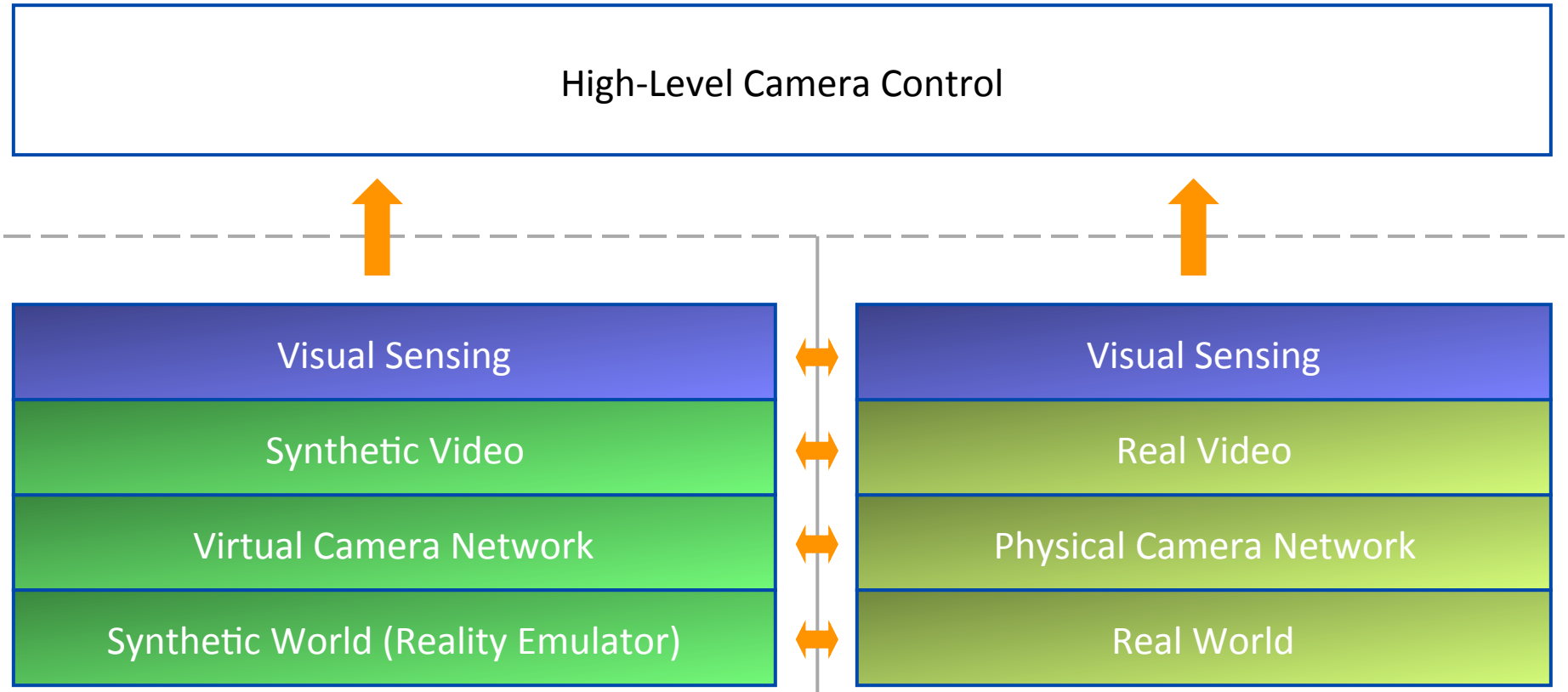
Virtual Vision

Machine Vision
tracking,
recognition,
etc.

vclab.ca

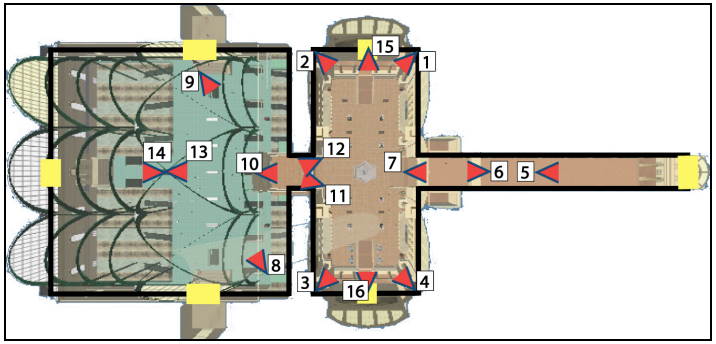
Visual Computing LAB

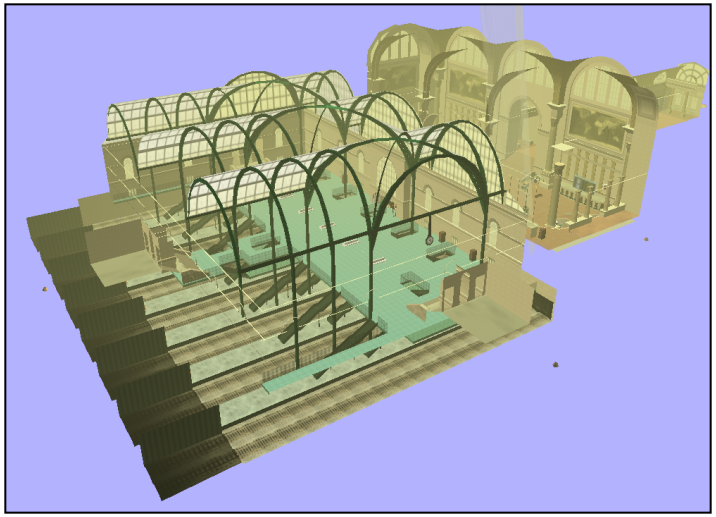
Virtual Vision:
A Tool for Visual Sensor Network Research



vclab.ca

Pedestrian Observation in an Extended Space





Advances in Computer Vision & Image Analysis

- Pedestrian tracking
- Face detection and recognition
- Activity recognition
- Anomalous behavior detection
- Visual biometrics
- Indexing and search
- Mobile vision

Advances in computer vision will lead to even more powerful and intrusive video surveillance systems

Easier integration with other sources of data

Advances in computer vision will lead to even more powerful and intrusive video surveillance systems

Complete erosion of personal privacy

Privacy Protective Video Surveillance

Even in the presence of a legal framework for or social expectation of privacy preserving video surveillance, we need better tools for privacy protective video surveillance

Privacy by Design for Video Surveillance

Video surveillance systems must have built-in privacy protecting capabilities

Good News

The same technologies that make video surveillance intrusive and can help develop privacy protective video surveillance

A Typical Video Surveillance System

Video captured by the surveillance camera is sent to the monitoring station for archiving and monitoring

Anyone with access to the cameras can view the imagery captured by these cameras

Key Idea: Privacy Protective Video Surveillance

Video captured by the surveillance camera is analyzed to find and hide unnecessary or sensitive information

Automatic video analysis (computer vision)

vclab.ca

Visual Computing LAB

Privacy Protective Video Surveillance: Current Approaches

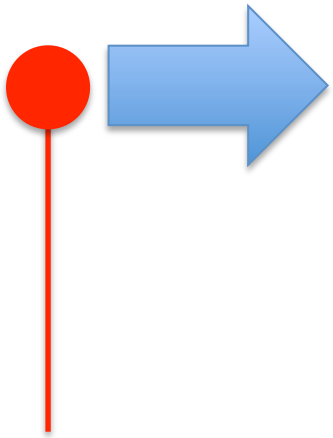
- Obscure faces (Schiff, 2007)
- Obscure people present in the video (Fan, 2005)
- Skin color removal to avoid race based discrimination (Berger, 2000)
- Identify privacy regions in pan/tilt/zoom cameras (Wada, 2001)

Key Idea: Privacy Protective Video Surveillance

Video captured by the surveillance camera is analyzed to find and hide unnecessary or sensitive information

There must be a way to recover the hidden information

Key Idea: Encryption at Source



Encrypted video is sent to the “monitoring” station for archival

Video is encrypted at source using agreed upon credentials

Privacy Protective Video Surveillance: Current Approaches

- *PrivacyCam* (Chattopadhyay, 2007)
- Region encryption (Martin, 2008)

Key Idea: Encryption at Source

Encryption

Encrypted video is sent to the “monitoring” station for archival

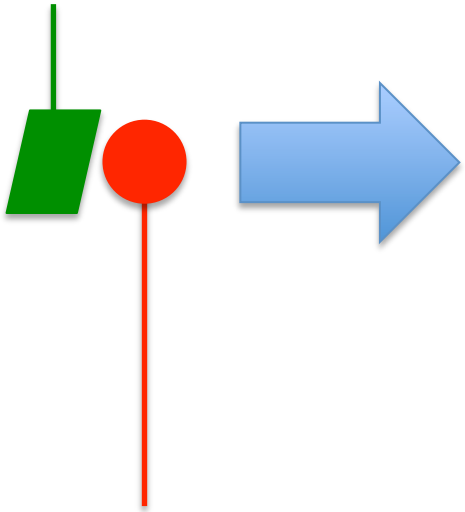
Authorization must first be obtained from appropriate legal authorities to decyrpt and view the video

Key Idea: Encryption at Source

While “encryption at source” allows law enforcement authorities to use recorded footage for forensic analysis, it does not allow for real-time monitoring of video footage

Automatic Surveillance with Encryption

Video analytics to identify “events of interest”



The video is automatically decrypted and presented to the user when an “event of interest” is detected

Video is encrypted at source using agreed upon credentials

vclab.ca

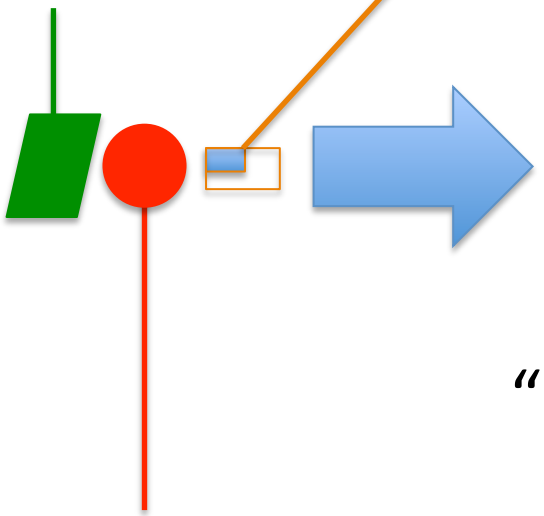
Visual Computing LAB

Automatic Surveillance with Encryption

- Video is encrypted and stored for forensic uses; however, if an “event of interest” is detected the video is decrypted on the fly and is available for real-time monitoring
  - Leverage the same advances in computer vision that makes surveillance so intrusive to design privacy preserving surveillance systems

Automatic Surveillance with Encryption

Video analytics to identify “events of interest”



Relevant portions of the video are automatically decrypted and presented to the user when an “event of interest” is detected

Video is encrypted at source using agreed upon credentials

vclab.ca

Visual Computing LAB

Automatic Surveillance with Encryption

- Provides stronger privacy preserving capabilities without compromising surveillance system's usefulness for safety and security applications

Privacy Protective Video Surveillance System Prototype

Object Video Streams
Object level video decomposition

Encrypted Video Transmission Channel

Encrypted Storage

Online Monitoring

Video Analytics
Identify events of interest

Video Encryption
Object level encryption using agreed upon credentials

Automatic *Partial* Decryption
Analytics routines determine if video should be decrypted for online viewing; object level decryption for partial viewing

vclab.ca

Visual Computing LAB

Privacy Protective Video Surveillance System Prototype

Object Video Streams

Encrypted Video Transmission Channel

Encrypted Storage

Online Monitoring

Video Analytics

Automatic *Partial* Decryption

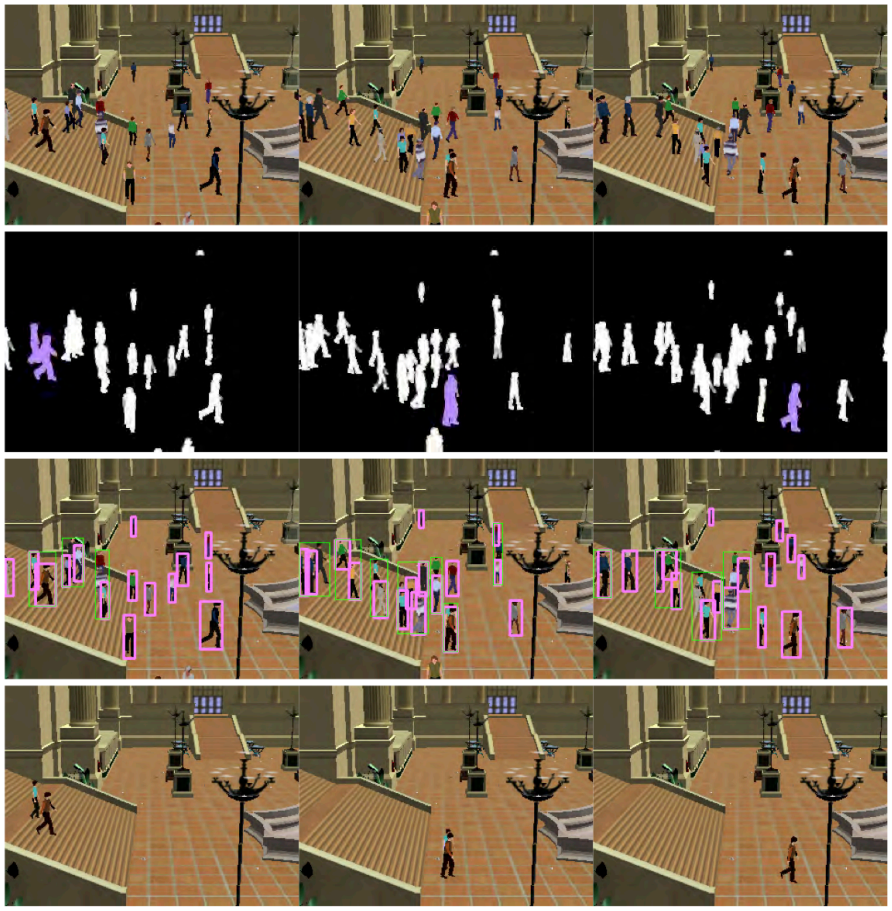
Captured Video

Video Encryption

vclab.ca

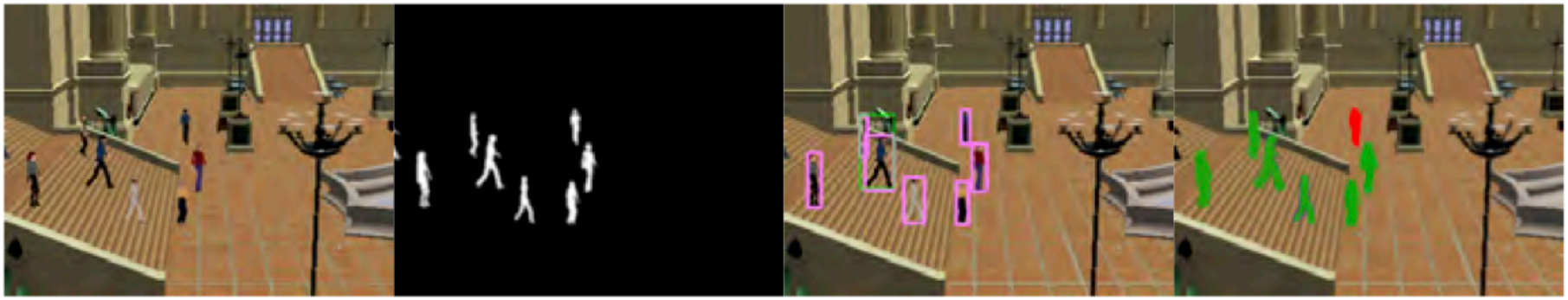
Visual Computing LAB

Object Video Streams



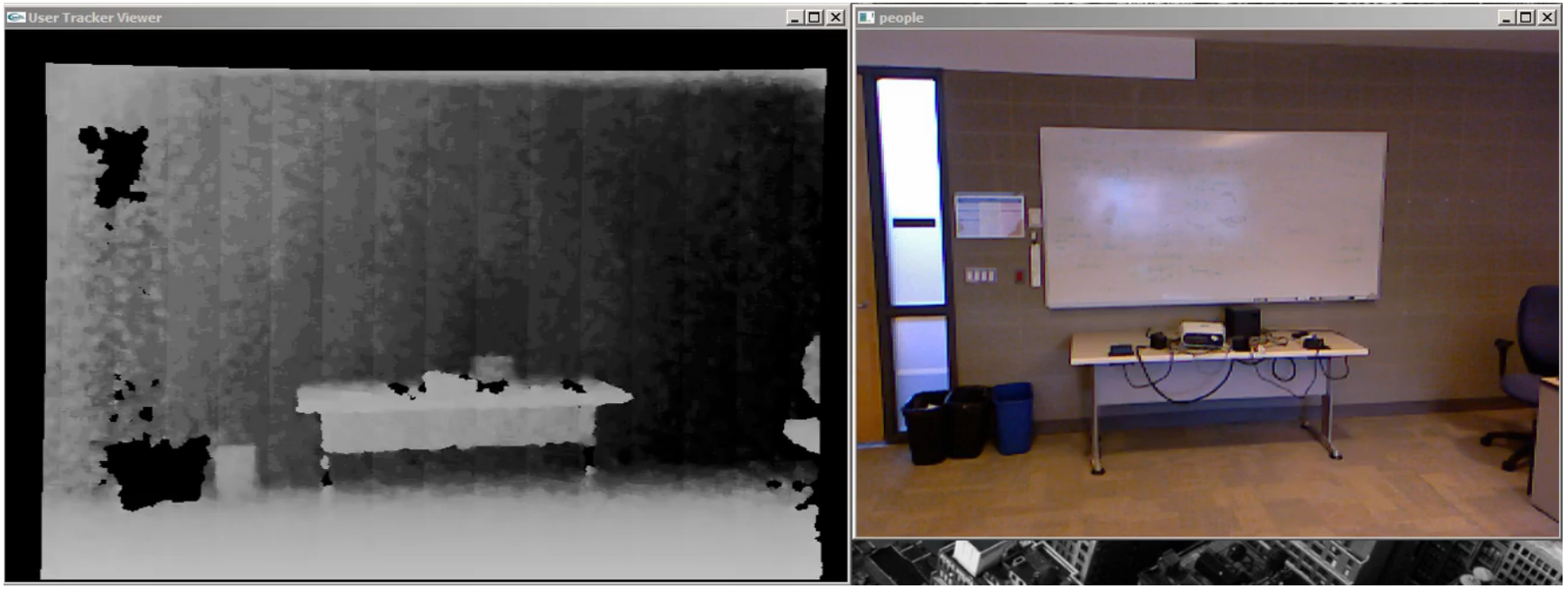
Frame 266 Frame 308 Frame 325

Object Video Streams



Object Video Streams
RGB Cameras

RGBD Sensors for Object Video Decomposition



Privacy Protective Video Surveillance System Prototype

Object Video Streams

[UOIT]

Encrypted Video Transmission Channel

[Canon]

Encrypted Storage

[UOIT]

Online Monitoring

Video Analytics

[UOIT/Canon]

Automatic *Partial* Decryption

Video Encryption

[UOIT/UofT]

Captured Video

vclab.ca

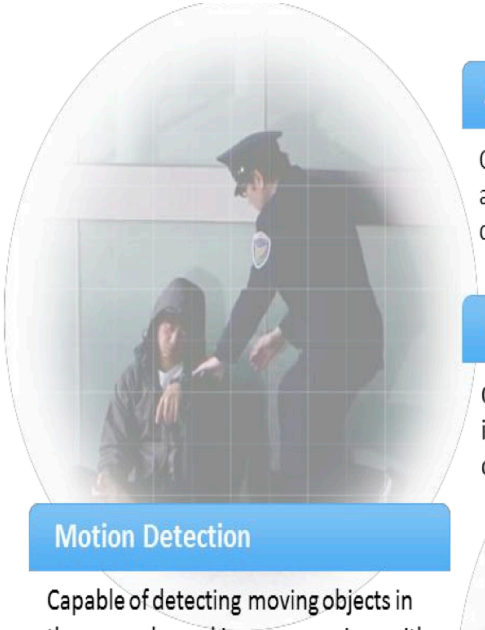
Visual Computing LAB

Image Capture & Video Analytics

UOIT & Canon Canada

- Canon IP camera provide some of the highest quality video capture
- These also provide built-in video analytics
  - Abandoned object detection
  - Camera tempering detection
  - Motion detection
  - Removed object detection
  - Passing (tripwire) detection

Canon Cameras

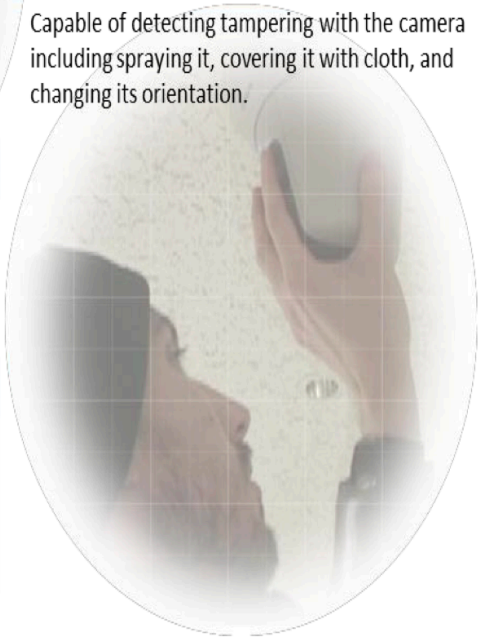


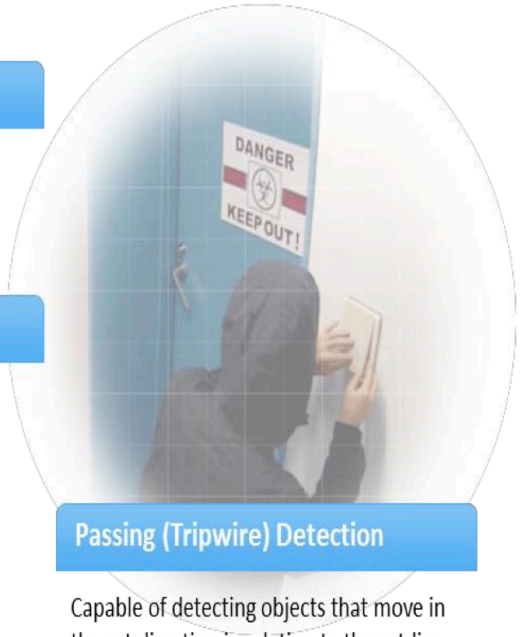
Abandoned Object Detection

Capable of detecting illegal dumping and the abandoning of suspicious items by making a comparison with the background video feed.

Camera Tampering Detection

Capable of detecting tampering with the camera including spraying it, covering it with cloth, and changing its orientation.





Motion Detection

Capable of detecting moving objects in the screen by making a comparison with the background video feed.

Passing (Tripwire) Detection

Capable of detecting objects that move in the set direction in relation to the set line.

Removed Object Detection

Capable of detecting thefts of objects such as exhibit samples by making a comparison with the background video feed.

Volume Level Detection

Capable of detecting loud sounds such as that made when window glass breaks and the stoppage of the operating sound of equipment.

Canon PTZ Cameras

Object Video Streams

UOIT

- Raw video is decomposed into two or more video streams depending upon the number of individuals present in the video
- Each stream is separately encrypted and two or more of these streams can be combined to create novel view of the scene

Encryption
UOIT/UofT

- Encrypt object video streams
  - Biometric signatures
  - Agreed upon encryption keys

Object Video Streams

- Object centric video decomposition
  - Object specific privacy policies
  - User-centric surveillance
    - Integration of mobile devices into surveillance systems

Challenge 1

Zero Tolerance for Failure

A single video-analysis failure can compromise the privacy of of an individual.

Challenge 2

Privacy Leakage

> Object removal is simply the first step towards designing privacy protective video surveillance systems.
>
> (Saini, 2012)

Thank You

Special thanks to my students:
Jordan Stadler, Wiktor Starzyk and Carly Marshall

vclab.ca

Visual Computing LAB