

Video Surveillance preserving privacy

Touradj Ebrahimi

Ecole Polytechnique Fédérale de Lausanne (EPFL)

Lausanne, Switzerland

touradj.ebrahimi@epfl.ch



Conference on Cryptology and Digital Content Security
May 14-18, 2007, CRM, Bellaterra, Spain

-
- Proliferation of advanced electronics, computers, networks
 - Sensors
 - Wireless networks
 - RFID
 - Blue tooth
 - Credit cards
 - Mobile phones
 - IP/MAC address
 - ...
 - It has become increasingly easy to monitor movements, behavior and habits of individuals
 - Data mining
 - Search
 - ...

Pros and cons of surveillance and data gathering 3

- Advantages
 - Security
 - User profiling
 - Personalization
 - Statistics
 - Increased efficiency
 - Increased quality of life
- Drawbacks
 - Unsolicited advertisement (SPAM)
 - Spy bots
 - Privacy

World Trade Center, 9/11

4



filmed by a Gas Station
surveillance camera on
September 10, 2001



Mohamed Atta



filmed by an ATM
surveillance camera on
September 10, 2001

Attack on London underground, July 7, 2005

5



On a reconnaissance mission
two weeks before the attack

Plot to attack trains in Germany, August 2006

6

Two unexploded bombs found in luggage aboard two trains

Both terrorists have been arrested thanks to the video footage



-
- Surveillance of sensitive locations
 - Embassies, airports, nuclear plants, military zone, border control, ...
 - Intrusion detection
 - Residential surveillance, retail surveillance, ...
 - Traffic control
 - Speed control
 - Access to places
 - Car license plate recognition in London
 - Event detection
 - Child/Elderly care
 - Marketing/statistics
 - Customers habits
 - Number of visitors
 - ...

Why video surveillance?

8

- Often video surveillance does not prevent crime, but:
 - Discourages crime
 - Allows quick reaction
 - Psychological dimension

- First generation
 - Analog
 - CCTV
 - Recording
- Second generation
 - Digital/Hybrid
 - Recording
 - PC based
 - IP wired/wireless

- Third generation
 - Image analysis
 - Biometrics
 - Search
- Forth generation
 - Pervasive
 - Distributed
 - Invisible
 - Multi-view

- High political appeal
 - Perception that the problem of crime is addressed
 - Not always based on the proven effectiveness of surveillance
- High psychological impact
 - UK: CCTV images of toddler Jamie Bulger led away from a shopping mall by his two ten years old killers (Liverpool, 1993)
 - USA: 9/11



- May prevent crime in numerous ways
 - Perpetrators apprehended
 - Perpetrators deterred by higher risk of apprehension
 - More people in places under surveillance
 - Security forces more effectively deployed
 - Perception to tackle crime seriously
 - Less time available to commit crime
 - Publicity

- Conflicting studies
- Welsh and Farrington (2002)
 - Analyze results from 22 studies in UK, USA and Canada
 - *City centers and public housing*
 - *Public transport*
 - *Car parks*
 - Overall crime reduction is **only 4%**
 - Evidence suggests that crime displaced beyond camera range
- Monitoring video screens is boring
 - Decreased attention after 20 minutes

- Londoner recorded **more than 300 times** a day
- Multitude of cameras
- Better cameras with high resolution and zoom
 - Even more invasive

- Criminal abuse
 - Criminal misuse by law enforcement officers
 - US: police official gathered information on a gay club to blackmail patrons
- Institutional abuse
 - Spy upon and harass political activists (Civil Rights, Vietnam war)
 - US: surveillance of political demonstrations
- Abuse for personal purposes
 - US: police officers helping friends stalk women, track estranged girlfriends/spouses
- Discrimination
 - UK: racial discrimination towards people of color
- Voyeurism
 - UK: bored male operators spying on women
 - UK: footage of public cameras made publicly available

- Principle of good faith and right to information
 - Inform everyone entering the zone with a clearly visible sign
- Data security
 - Protect personal data against unauthorized processing
- Principle of proportionality
 - Zone absolutely necessary for the purpose in the filming range
 - Data should be deleted within a short time (e.g. 24 hours)
- Purpose related principle
 - Data may only be used for the protection of persons and property
 - Identity of persons filmed may not be disclosed

-
- Convention of Human Rights and Fundamental Freedoms
 - Protection of privacy (article 8)
 - Council of Europe Convention No. 108/1981 for the protection of individuals with regard to automatic processing of personal data
 - Voices and images are considered personal data if they provide information on an individual by making him/her identifiable
 - Charter of Fundamental Rights of the European Union
 - Protection of private and family life, home and communication (article 7)
 - Protection of personal data (article 8)
 - Directive 95/46/EC
 - National provisions applying to video surveillance

- Lawfulness of the processing
 - In line with data protection principles
- Specificity, specification and lawfulness of purposes
- Proportionality of the recourse to video surveillance
- Proportionality in carrying out video surveillance activities
- Information to data subjects
 - Subjects informed when video surveillance is in operation
- Additional requirements
 - Limited number of persons to view or access the recorded images
 - Security measures to prevent dissemination or alteration of data
- Data subjects' rights
- Additional safeguards
 - Prohibited to discriminate on race, religious or political opinions, sexual habits

- No standards on
 - Where cameras can be installed
 - Who is allowed to view tapes
 - How long they are kept on file

 - It is illegal to secretly tape-record a conversation
 - But secretly videotaping is perfectly legal

- If the image is not inherently reliable, its admissibility in court is questionable
- If a poor image is ruled admissible, it will be afforded little or no weight
- For an image to be admissible, the prosecutor must prove that the image has not been altered
 - Lossy compression
 - Conditional replenishment
- Original versus copy
 - Any digital image can be thought of as being 'the original'

- Technology
- Business
- Legal
- Social

-
- Encryption
 - Secure communication
 - Conditional access
 - Data integrity
 - Digital signature
 - Proof for lack of manipulation after capture

- Fully automatic surveillance without intervention of human operators
 - False positives and false negatives
- Encrypt the whole video
 - No good for monitoring
- Replace sensitive objects with a mask
 - Limited usefulness for monitoring
- Scramble sensitive regions with a key
 - Useful for monitoring
 - Privacy preservation
 - Identification can take place when crime happens
 - Does not require major changes in the surveillance infrastructure

Masking



MPEG-7
camera



Invertible
encryption



Invertible
scrambling

Automatically identifies Regions of Interest (ROI)

People in the scene

Human faces

Car license plates

...

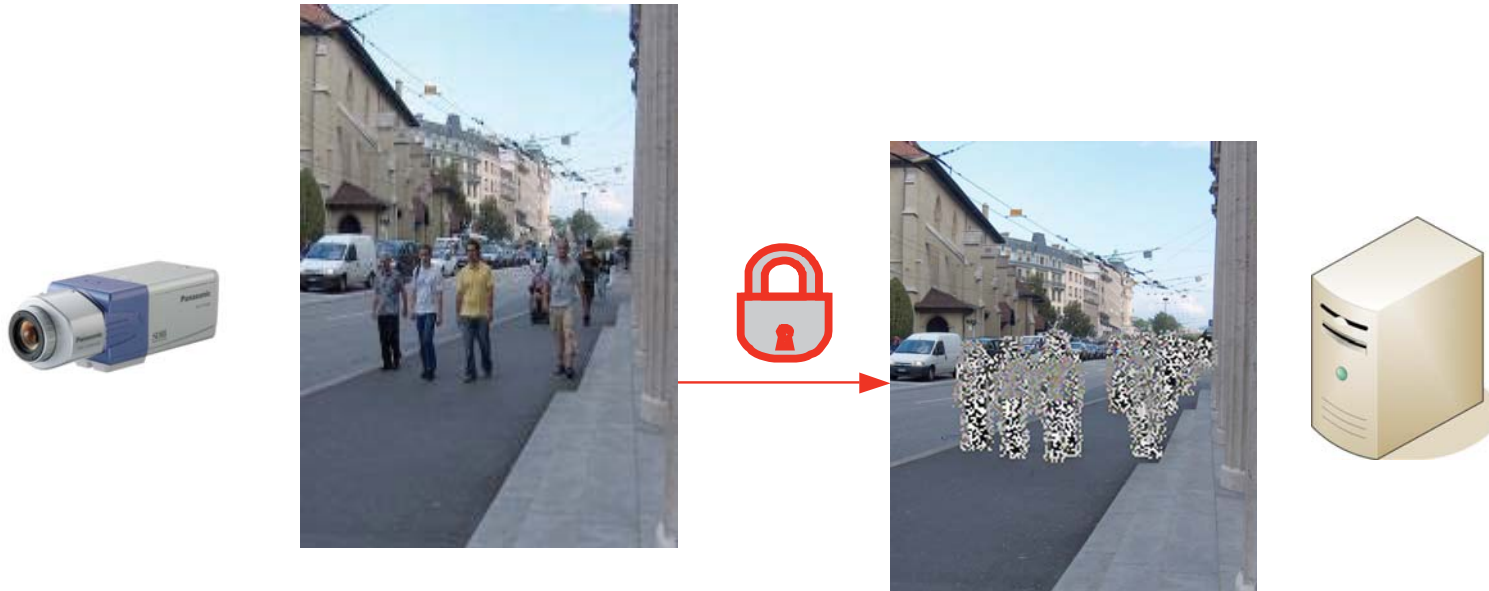
Predefined zones

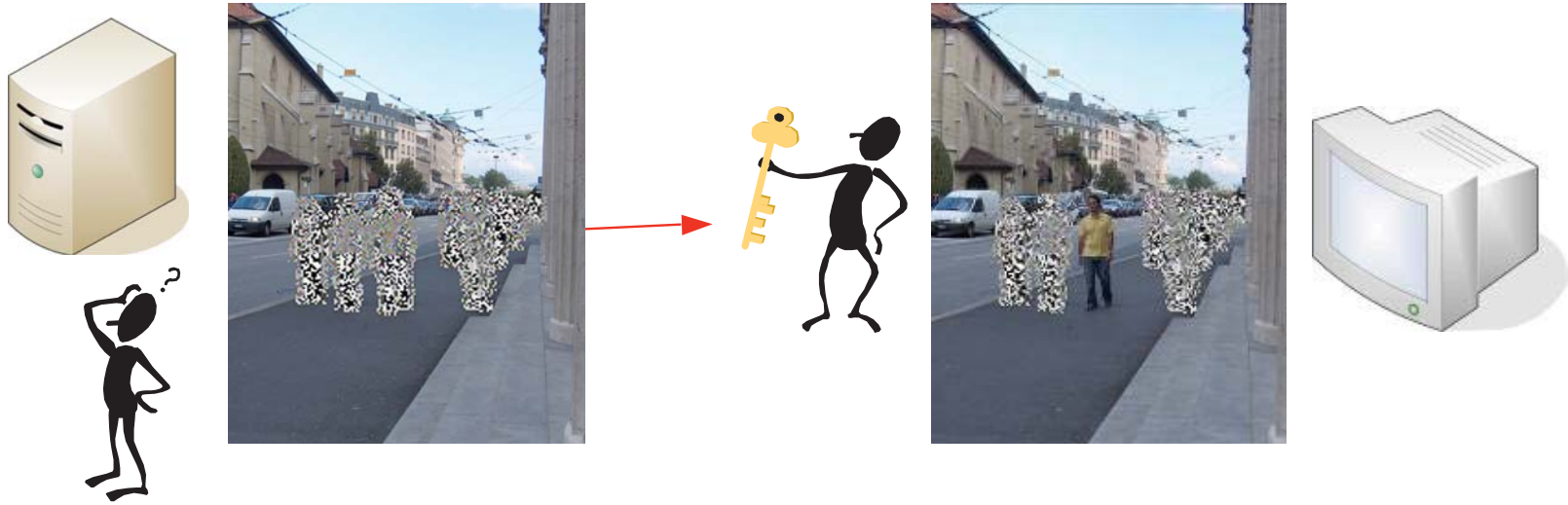
Window, door

Bank teller

Casino playing table

...





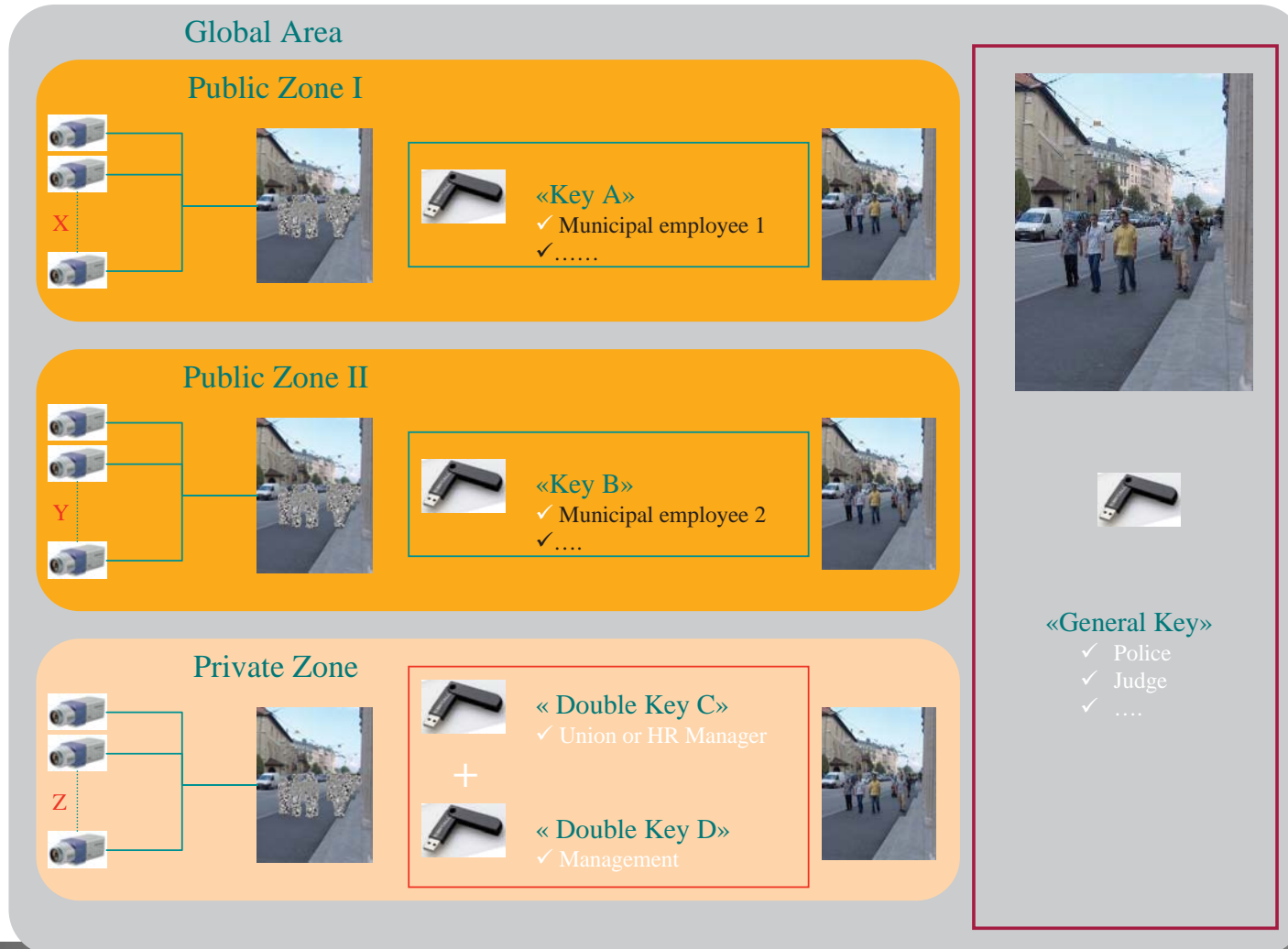




Scrambler



Unscrambler



- Video surveillance is here to stay and will only increase
- It will come with advantages and drawbacks as in many other solutions
- Technology (and specially security technologies) have proven to offer a good compromise in terms of needs for protection and preservation of privacy