Andrea Cavallaro

Privacy in Video Surveillance

In recent months, *wired.com* and other media outlets have published articles that discussed the trade-off between privacy and security. More specifically, these reports referred to the fact that "giving up privacy does not necessarily result in greater security, and greater security does not necessarily require a loss of privacy"[1]. Various technologies that protect privacy in video surveillance exist, but their implementations in current security systems have been limited compared to those of surveillance technology. In this article, we comment on how recent advances in video surveillance threaten privacy and how emerging signal processing technologies can protect privacy without risking security.

Video surveillance has become commonplace in recent years. By means of closed circuit television (CCTV) technology, individuals are observed without their knowledge in public buildings, train stations, stores, elevators, locker rooms, and school hallways. They're caught at ATMs and when stopped by the police in patrol cars. In London, the average citizen is caught on CCTV cameras 300 times a day, and in the United Kingdom alone there are more than 4 million CCTV cameras. This growing number of cameras is due to technological advances in manufacturing tiny sensors with processing and communication capabilities, and the increased availability of storage capabilities and searchable video databases. However, the features that have enabled the diffusion of CCTV also facilitate the collection of information about an individual and increase the risk of misuse and abuse of surveillance data. These issues are further amplified by high-definition color cameras and face recognition software, which make the "people google" scenario possible. People search engines like Zabasearch can be extended to enable the input of passport pictures of individuals, thereby enabling one to obtain the location and time the individual was last caught on camera, as well as the history of their displacements through vast networks of interconnected cameras.

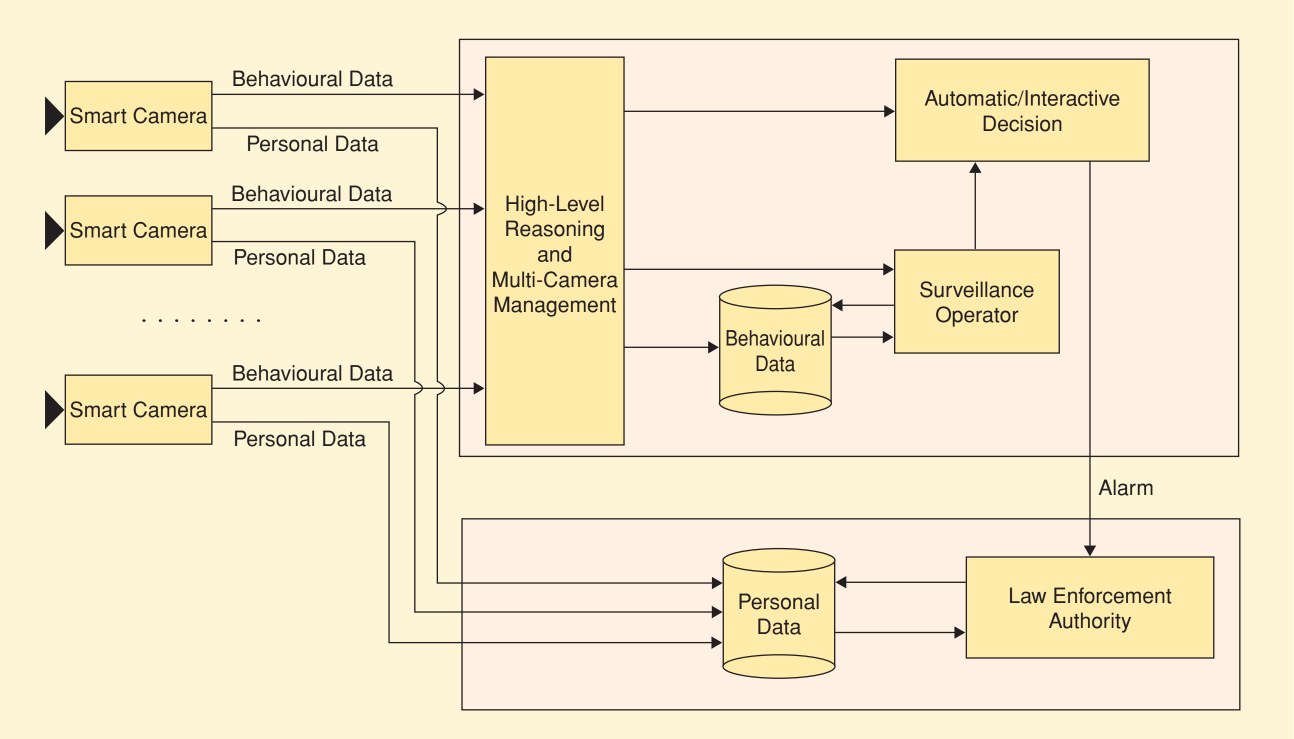
The pervasiveness of surveillance cameras in public places concerns civil libertarians and portions of the general public [2]. Consequently, initiatives such as the Isee project in Manhattan and Boston, and the Observing Surveillance Project in Washington D.C., have distributed city maps indicating the location of CCTV cameras to help people organize their displacements to avoid being caught on camera. Privacy concerns have also arisen over the Community Safety Channel, which is offered alongside traditional video-on-demand TV services to residents in Shoreditch (United Kingdom), allowing them to monitor CCTV cameras in their neighborhood from their own TVs or home computers. Current privacy legislation includes time limitations for the storage of recorded material and address the need for masking regions of the CCTV video that capture private windows. However, legislation does not prevent a number of misuses, such as voyeurism and the unauthorized collection of data on activities or behaviors of an individual. For instance, according to the BBC, four council workers in Liverpool used a street CCTV pan-tilt-zoom camera to spy on a woman in her apartment. There is also a risk that this kind of misuse is extended to spying on government officials or public figures. For instance, an investigation was recently launched after a museum's CCTV camera was used by a security guard to spy on the private apartment of the German Chancellor Angela Merkel.

To address the challenges that stem from the interaction of technological advances in video surveillance and individual privacy requirements, the signal processing community can offer solutions such as:

- Traditional data encryption schemes–These can be used to prevent eavesdropping, but they cannot prevent the misuse of CCTV video by authorized personnel, as in the cases of voyeurism and criminal purposes mentioned earlier.
- Smart cameras–These can be used to embed privacy constraints in the design of a surveillance system. Smart cameras are surveillance cameras equipped with a digital signal processor (DSP). In surveillance tasks such as street and traffic control, the DSP is programmed so as to selectively de-identify [3], mask [4], or scramble [5] the regions revealing the identity of an individual (or license plate) in the transmitted video. In tasks such as area monitoring, smart cameras activate transmission (or remove the selective masking) when they detect an event (for instance, an individual entering a protected area or a crowd gathering in a small area) or recognize gestures (for example, a person raising a fist or pointing a gun). As an alternative to transmitting video, smart cameras can produce two separate data streams: a metadata stream describing, for instance, trajectories of people or vehicles (behavioral data) and a stream of images capturing the identity

(continued on page 166)

1053-5888/07/$25.00©2007IEEE



[FIG1] Block diagram of a privacy-preserving video surveillance system with smart cameras.

of a person or a vehicle (personal data) [6]. As illustrated in Figure 1, the metadata stream is then rendered on the display of the surveillance operator or the shop keeper, whereas the stream of images is sent to a different location to be used solely for law enforcement purposes.

The success of smart cameras will depend on the accuracy and robustness of the image processing and pattern recognition algorithms that detect events and localize the portions containing personal data in real operating conditions. Face detection, skin color segmentation, and license plate detection strategies have progressed greatly in recent years and can operate in real scenarios with illumination variations and crowded scenes. However, additional progress is required in other domains such as action recognition, unusual event detection, and target tracking, especially across multiple cameras.

Given the existing and pervasive surveillance infrastructure, the cost incurred to change the concept of surveillance to accommodate privacy protection will mainly depend on the affordability of cameras with embedded DSPs. The popularity and increased demand for these cameras in areas ranging from industrial inspection to consumer electronics, and the possible introduction of legislation (as demanded by civil libertarian groups), can accelerate cost reductions. Managing these costs, as well as enabling advanced video surveillance in public places while protecting privacy, is a major interdisciplinary challenge that the signal processing community–together with scientists from other disciplines such as the social sciences–must address to adapt to changing demands from citizens. Including privacy constraints in the design of a surveillance system is essential for the perception of video surveillance as a true security tool and not as a threat to privacy.

AUTHOR

Andrea Cavallaro (andrea.cavallaro@elec.qmul.ac.uk) is a lecturer at Queen Mary University of London, United Kingdom.

REFERENCES

[1] Jennifer Granick, 2006, May 24 “Security versus privacy: The rematch,” Wired News, [Online]. Available: http://www.wired.com/news/columns/0,70971-0.html

[2] J. Kumagai and S. Cherry, “Sensors and sensibility,” *IEEE Spectr.*, vol. 41, no. 7, pp. 22–26, July 2004.

[3] R. Gross, L. Sweeney, F. de la Torre, and S. Baker. “Model-based face de-identification,” in *Proc. IEEE Computer Vision and Pattern Recognition Workshop on Privacy Research in Vision*, p. 161, June 2006.

[4] A. Senior, S. Pankati, A. Hampapur, L. Brown, Y.-L. Tian, and A. Ekin. “Enabling video surveillance privacy through computer vision,” *IEEE Security Privacy*, vol. 3, no. 3, pp. 50–57, May-June 2005.

[5] F. Dufaux and T. Ebrahimi, “Scrambling for video surveillance with privacy,” in *Proc. IEEE Computer Vision and Pattern Recognition Workshop on Privacy Research in Vision*, p. 160, June 2006.

[6] A. Cavallaro, “Adding privacy constraints to video-based applications.” in *Proc. European Workshop on the Integration of Knowledge, Semantics and Digital Media Technology*, Nov. 2004, pp. 257-264.