Towards building a robust video sensor network

Sen-ching S. Cheung (sen-ching.cheung@uky.edu) and Thinh Nguyen (thinhq@eecs.oregonstate.edu)

Wide-area visual sensor networks are becoming more and more common. They have wide-range of commercial and military applications from video surveillance to smart home and from traffic monitoring to anti-terrorism. The design of such a visual sensor network is a challenging problem due to the complexity of the environment, self and mutual occlusion of moving objects, diverse sensor properties and a myriad of performance metrics for different applications. As such, there is a need to develop a flexible sensor-planning framework that can incorporate all the aforementioned modeling details, and derive the sensor configuration that simultaneously optimizes the target performance and minimizes the cost. We have been tackling this optimal sensor problem by developing a general visibility model for visual sensor networks and solving the optimization problem via Binary Integer Programming (BIP) [1], [2]. Our proposed visibility model supports arbitrary-shaped 3D environments and incorporates realistic camera models, occupant traffic models, self occlusion and mutual occlusion.

Another area of growing concerns in widespread deployment and increased sophistication of video sensor networks is their threat to individuals right of privacy. Privacy protection technologies developed thus far have focused mainly on different visual obfuscation techniques but no comprehensive solution has yet been proposed. We have been developing a prototype system for privacy-protected video sensor networks that advances the state-of-the-art in three different areas: First, after identifying the individuals whose privacy needs to be protected, a fast and effective video in-painting algorithm is applied to erase individuals images as a means of privacy protection [3]. Second, to authenticate this modification, a novel rate-distortion optimized data-hiding scheme is used to embed the extracted private information into the modified video [4]. While keeping the modified video standard-compliant, our data hiding scheme allows the original data to be retrieved with proper authentication. Third, we view the original video as a private property of the individuals in it and develop a secure infrastructure similar to a Digital Rights Management system that allows individuals to selectively grant access to their privacy information [5], [6].

The security of the distributed computation itself within a video sensor network is also highly important, especially if it is deployed in hostile environments such as battlefields or correctional facilities. Individual sensors can be comprised by attackers to obtain useful information or even disrupt the normal operations of the network. While simple scrambling or encryption can protect the signal in transit, the signal must be fully decrypted before any processing can be performed and a malicious receiver can easily obtain sensitive information. We have considered a number of linear algorithmic building blocks for secure distributed image processing that partition information into sensitive and non-sensitive components, and only non-sensitive components are shared with other sensors [7], [8]. While these techniques are computationally efficient, there is a leakage of information which might not be tolerable in some applications. Recently, we have begun to apply cryptographical primitives to enhance security in many signal processing algorithms [9]. The proper use of cryptographical primitives can provide provable guarantee on privacy in the processing of multimedia data. On the other hand, this is a very challenging problem because typical video sensor applications are characterized by the need of processing high-dimensional data at a very high data rate with real or close to real-time response. In [10], we have developed a distributed iris biometric access control system with the matching process carried out entirely in encrypted domain. Using our system, the server can verify if the input probe is similar to any entries in the gallery but will not be able to pinpoint which entries so as to protect user anonymity. In [11], we further extend the concept and incorporate a new framework based on k-anonymity to provide a controllable trade-off of privacy and computational efficiency.

REFERENCES

[1] J. Zhao, S.-C. Cheung, and T. Nguyen, "Optimal camera network configurations for visual tagging," *IEEE Journal on Selected Topics in Signal Processing*, vol. 2, no. 4, pp. 464–479, Aug. 2008.

[2] ——, "Camera network configuration and its application in privacy protected video surveillance," in *Multi-Camera Networks: Concepts and Applications*, H. Aghajan and A. Cavallaro, Eds. Elsevier, 2009.

[3] M. V. Venkatesh, S.-C. Cheung, and J. Zhao, "Efficient object-based video inpainting," *Pattern Recognition Letters : Special issue on Video-based Object and Event Analysis*, 2008.

[4] J. K. Paruchuri and S.-C. Cheung, "Joint optimization of data hiding and video compression," in *Proceedings of IEEE International Symposium on Circuists and Systems (ISCAS 2008)*, 2008, pp. 3021–3024.

[5] J. K. Paruchuri, S.-C. Cheung, and T. Nguyen, "Managing privacy data in pervasive camera networks," in *Proceedings of IEEE International Conference on Image Processing (ICIP 2008)*, 2008, pp. 1676–1679.

[6] M. V. Venkatesh, S.-C. Cheung, J. Paruchuri, J. Zhao, and T. Nguyen, "Protecting and managing privacy information in video surveillance systems," in *Protecting Privacy in Video Surveillance*, A. Senior, Ed. Springer, 2009.

[7] N. Hu and S.-C. Cheung, "Secure image filtering," in *Proc. of IEEE International Conference on Image Processing (ICIP 2006)*, Oct 2006, pp. 1553–1556.

[8] N. Hu, S.-C. Cheung, and T. Nguyen, "A new security model for secure thresholding," in *Proc. of IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP 2007)*, April 2007, pp. 273–276, http://www.vis.uky.edu/∼cheung/doc/icassp07.pdf.

[9] S.-C. Cheung and T. Nguyen, "Secure signal processing between distrusted network terminals," *EURASIP Journal on Information Security*, 2007, http://www.hindawi.com/GetArticle.aspx?doi=10.1155/2007/51368.

[10] Y. Luo, S.-C. S. Cheung, and S. Ye, "Anonymous biometric access control based on homomorphic encryption," in *IEEE International Conference on Multimedia & Expo*, Cancun, Mexico, June 2009.

[11] S. Yee, Y. Luo, J. Zhao, and S.-C. Cheung, "Anonymous biometric access control," *Submitted to EURASIP Journal of Information Security*, 2009.