

Abstract

The move from analog to fully digital systems in conjunction with continuous technological advances in the fields of optics, image sensors, embedded processing systems, communication networks and computer vision have fostered the rapid development of smart camera systems. A primary area of application for these systems is video surveillance in public as well as in private environments. With widespread adoption, concerns about security and privacy protection are increasing. If at all, these concerns are currently addressed by detecting and obfuscating sensitive image regions. Integration of this high-level protection with the underlying embedded computing system and established IT security concepts is rarely investigated.

This thesis captures the state of the art of security and privacy research in the context of smart camera systems. Based on the derived observations, a design of a security-enhanced, privacy-preserving smart camera system is proposed. It follows a hardware-based security approach and explores the integration of Trusted Computing technology with high-level, computer vision-based protection concepts to achieve increased levels of overall security and privacy protection. As part of this effort, a set of primary security targets is defined. These include the reliable status monitoring of remote cameras as well as providing integrity, confidentiality and authenticity guarantees for delivered video and image data. Based on these fundamental security guarantees, a multi-level privacy protection concept is presented. Via on-board detection of sensitive image regions such as human faces, various abstractions of a single video stream are created. Individual abstraction levels reveal or protect the behavior and identities of captured persons. Depending on the sensitivity of the contained information, the individual layers are separately protected by encryption to ensure that only authorized parties can access the data.

Transparency is a crucial aspect of increasing public confidence and acceptance of video surveillance. Therefore, this work investigates an approach that allows monitored people to directly and reliably check the status of a camera. This mechanism provides people with an insight into the properties of a camera including the implemented privacy protection techniques.

The concepts proposed in this thesis are implemented in a custom-built prototype system called TrustCAM. The prototype implementation covers both hard- and software aspects of the system. The prototype not only illustrates the practical feasibility of the proposed concepts but also allows realistic performance evaluations to be presented. The achieved results indicate that the performance impact due to the added security functionality is relatively small and does not limit the usefulness of the camera system.