Privacy-Aware Object Representation for Surveillance Systems

Hauke Vagts
Karlsruhe Institute of Technology
Adenauerring 4, 76131 Karlsruhe, Germany
vagts@kit.edu

Alexander Bauer
Fraunhofer IOSB
Fraunhoferstr. 1, 76131 Karlsruhe, Germany
alexander.bauer@iosb.fraunhofer.de

Abstract

Real-time object tracking, feature assessment and classification based on video are an enabling technology for improving situation awareness of human operators as well as for automated recognition of critical situations. To bridge the gap between video signal-processing output and spatio-temporal analysis of object behavior at the semantic level, a generic and sensor-independent object representation is necessary. However, in the case of public and corporate video surveillance, centralized storage of aggregated data leads to privacy violations. This article explains how a centralized object representation, complying with the Fair Information Practice Principles (FIP) privacy constraints, can be implemented for a video surveillance system.

1. Introduction

Recent advances in multi-camera real-time object tracking have opened new opportunities for video surveillance systems. Trajectories of people, cars and other mobile objects can be tracked over multiple camera views with growing reliability [1]. Tracking information is already used to annotate video with semantic information in order to facilitate browsing of stored video streams [2], for example for forensic analysis or shop efficiency monitoring. In the long run, surveillance systems are envisioned to be able to recognize or even predict abnormal or dangerous behavior [3], allowing the operator to take appropriate actions to prevent critical incidents.

The field of situation recognition has recently gained increasing attention. Recognizing behavior or critical situations requires very different methods compared to video signal-processing, as the input information is not about signal amplitudes but rather on objects, attributes and relations. Still, these methods have to account for uncertainty and imperfection of object assessments at the signal-processing level [4].

Regardless of the method used to represent and match situations against predefined models, as a first step, a canonical representation of objects, their attributes and relations has to be established. To design such an object representation, Bauer et al. [5] have developed an Object-Oriented World Model (OOWM) for surveillance applications, based on the ideas of Beyerer et al. [6]. Their OOWM system fuses arbitrary uncertain object observation into a common object representation and provides a general high-level interface for visualization, track analysis and situation recognition. As a central source of object information it is meant to facilitate the development of such surveillance system components, independent from the sensor and signal-processing domain. At the same time however, the centralized aggregation of object information leads to severe implications for privacy violations as soon as people are part of the supervised area.

Surveillance systems have become increasingly powerful and conventional camera-based systems are extended with all kinds of sensors. The number of data sources increases, hardware and video processing algorithms improve, and data can potentially be shared between interlinked networks. Hence, modern surveillance systems pose a threat at privacy. Surveillance solutions that can be used in practice must be compliant with current and future law, and must be accepted by society.

The objective of a surveillance system is usually specified at the application level, e.g., “Notification about abnormal behavior at a station platform” or “Monitor guests on a way to a meeting room”. Information used to fulfill such a task is gained at sensor-level. Conventional sensor-oriented systems collect all available information, even if it is not relevant for the overall objective of the system. Video is rich of information and traditional surveillance cameras cannot distinguish between important and unimportant data or identify data that is worth of protection.

Thus, privacy-aware solutions must bridge the gap between semantic-level and sensor-level to ensure that privacy is enforced during the entire surveillance process, beginning with the collection of relevant data. Task-oriented processing in conjunction with the OOWM offers great possibilities for the enhancement of privacy. The OOWM acts as a central data hub that can potentially

978-0-7695-4264-5/10 $26.00 © 2010 IEEE
DOI 10.1109/AVSS.2010.73

integrate any kind of sensor service. Thus privacy can be enforced for any information source.

Following a brief overview of related work (Section 2) and an introduction to OOWM systems (Section 3), Section 4 proposes technical solutions for privacy enforcement in the described context and in accordance with the current legislative constraints.

2. Related work

In the field of video surveillance, much focus has been on the development of reliable computer vision algorithms for tracking and assessment of objects, which are the basis for advanced surveillance systems. With the increasing use of video surveillance in public space, several approaches to ensure privacy have appeared in literature. Most of the approaches perform a blurring, blanking-out, pixelation, or scrambling of Regions of Interest (RoI) that might imperil privacy, e.g. [7]. In [8] Senior et al. propose a "privacy-preserving video console"" for video surveillance. The console rerenders the video stream and hides sensitive details, detected by video analysis. Depending on the authorization level, access is granted to the rerendered videos (e.g. with blurred faces or even enriched with additional information) or the raw video stream. They also propose a "privacy cam", which processes the video sources and transmits encrypted information streams. In [9] Chattopadhyay and Boult also present a privacy cam, which is implemented on a Blackfin DSP and blurs RoI based on cryptographic obscuration [10]. In [11] Schiff et al. propose a "respectful camera" which reacts on visual markers worn by the subjects. In [12] the usage of "talking cameras" is reported, if a camera detects motion, it sends an acoustic message to a subject. Even if such cameras should prevent vandalism, they can ensure privacy as well, e.g., a camera can vocalize a countdown, before it starts recording. Fleck's approach to privacy [13] is based on smart cameras, which transmit events instead of video data. Fidaleo et al. present in [14] a privacy enhanced software architecture with a centralized server that hosts a privacy buffer, which can remove private or identifiable information from the stream. Schaffer and Scharter propose a flexible secret sharing approach to enhance privacy in [15].

A second aspect, which is closely linked to privacy, is security. Security techniques such as encryption or digital signatures are required to ensure authenticity and confidentiality of sensor information. One way to provide confidentiality, integrity and authenticity in video surveillance systems is to use video independent solutions that have proved to be successful, as symmetric and asymmetric encryption, signatures, certificates and public key infrastructures (PKI), and existing security protocols (SSL, IPSec, Kerberos, etc.). However, in case of video data more specific methods have been proposed taking advantage of video characteristics. To ensure authenticity of images and video, a lot of research has been done in the area of (robust) watermarking, e.g., [16].

To achieve confidentiality of transmitted video data several approaches exist that achieve better performance by utilizing video specific characteristics, e.g. [17].

The mentioned approaches are focused on video surveillance and new approaches are required that also cover new sensors (e.g., GPS, RFID, acoustic) that are integrated in modern systems. However, existing solutions can be used to store video data, i.e., multiple versions of a scene can be stored, but an open issue is the robustness. If a RoI is not detected correctly in a single frame, privacy can be compromised completely. In general, most of the existing approaches only try to enforce privacy on the raw data at sensor-level, which is insufficient, if more abstract information is extracted (e.g., names of persons in a specific region) and processed in the system. Furthermore, whether collected information imperils privacy or not, is highly dependent on the objective of the surveillance installation. Therefore privacy enforcement has to be dependent on the tasks currently performed by the system. A task-oriented approach for privacy enforcement, which is described below, makes use of the OOWM to decouple raw sensor data and information. Due to the higher level of abstraction, privacy can be enforced from signal-level to semantic-level. The proposed approach can be seen as consequent development of the idea presented by Senior et al. [8].

3. Object-oriented world model (OOWM)

An object-oriented world model, as part of a surveillance system, is meant to transform object observations collected from multiple and heterogeneous sensor systems into a consistent object representation, in order to provide a unified information source for application-level software such as visualization, track analysis or online behavior recognition. Sensor systems in this context are defined as any combination of physical sensor deployments and corresponding signal-processing software, able to extract object information from raw sensor data (e.g. person tracking, face recognition, etc.). Figure 1 shows a sketch of an OOWM system in the context in a video surveillance system.

Similar approaches for object-oriented modeling are found in the development of cognitive systems, such as in robotics. For example, Kuhn et al. developed an OOWM system for an indoor robot [18].

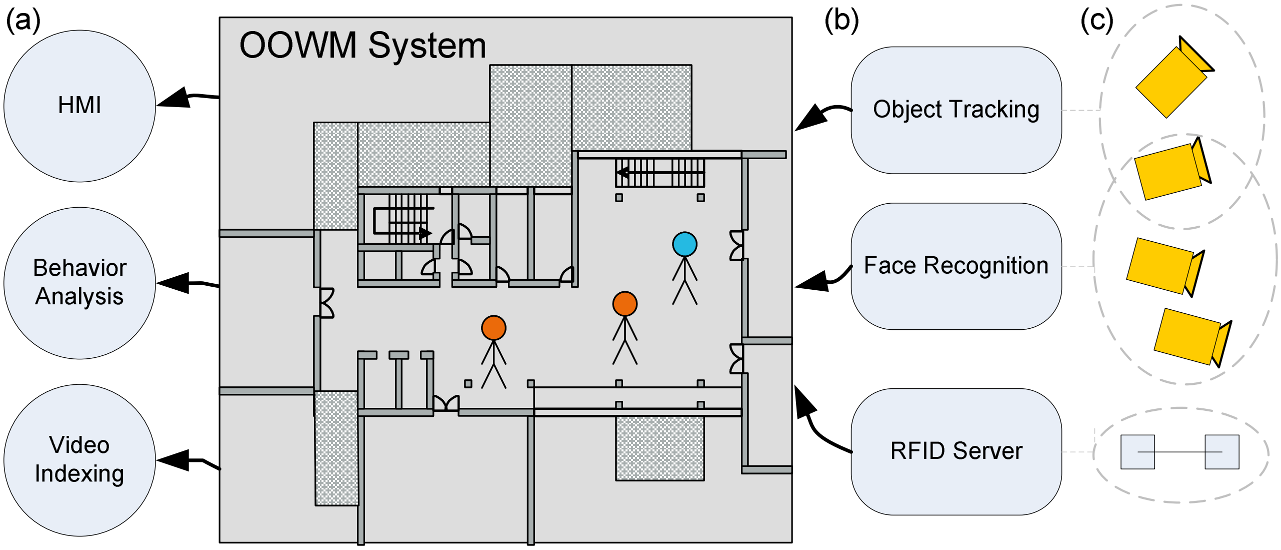

Figure 1: An OOWM in the surveillance system context: (a) Application-level modules, (b) Signal-Processing modules, c) Sensor Deployment

In order to serve its objective, an OOWM has to perform several challenging tasks, which are closely linked to high-level data fusion [19]:

1) *Information Representation and Distribution:* An application independent representation of objects, its features and uncertainty about their assessment has to be developed. To distribute object information to high level applications, a unified access and query mechanism has to be established.
2) *Data Association:* For each new object observation, it has to be decided if it corresponds to a new object or represents updated information about a previously observed object.
3) *Data Fusion and Tracking:* Updated information from new observations has to be fused with previously assessed information.
4) *Information Aging and Management:* First, it has to be managed, whether objects which have not been observed for a longer time period can be removed from the object representation. Secondly, it has to be decided if enough observations supporting the existence of a new object have been collected.

As it is responsible for the fusion of all object observations, an OOWM represents a critical element of the information processing chain, so algorithms for information fusion must be selected carefully. The main benefit of the use of an OOWM is the establishment of a generalized object representation, which is designed to be independent of application and signal-processing level. This can enormously facilitate the extension of a video surveillance system with new modules on the application-level as well as on the signal- level. Detailed explanations about the technical implementation of an OOWM can be found in [5].

4. Privacy enforcement

Privacy law is heterogeneous and even the current legal situation for conventional video surveillance systems is not fully explored. As a result the FIP (explained in Section 4.1) are still the minimum requirements for surveillance systems and should be adhered by any surveillance system. In Section 4.2 the task-oriented approach for privacy enforcement is described in more detail. A framework for privacy enforcement is presented in Section 4.3. It is finally shown in Section 4.4 how the task-oriented approach and the framework achieve compliance with the principles.

4.1. Legislation and the fair information practice principles

Although the legal situation concerning privacy and data protection should be the same throughout the EU, surveillance and data protection is handled differently in every member state. The legal status in the US is also different [20]. Even if data protection law is existent, it is not ensured that it is enforced properly, e.g., it is estimated that 80% of existing CCTV installations in the UK are not compliant with existing privacy law [21]. To make things worse, many people do not care about privacy anymore and release their personal data without hesitation (social networks, loyal shopping cards, etc.). However, the current legal situation is not even fully explored for conventional systems and it cannot be foreseen in what manner Privacy Enhancing Technologies (PETs) can be applied to ensure privacy or if the collection of data will still be restricted.

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [22] serve as a rule for the EU directives on data protection (95/46/EC, 2002/58/EC), which must be enforced by the member states. The guidelines have been published by the OECD in 1980. The Guidelines contain eight principles for privacy, which are still valid and should be considered by any legislation. Due to the heterogeneous law, these principles can be considered as the minimum requirements for surveillance systems. Solutions that enforce privacy must deal with all principles, but must be flexible enough to adapt privacy according to future requirements. Due to the named shift in the sense of privacy the principles *P1*and *P4* should be called into question, but in general it is a good idea to aim for maximum privacy, i.e., all principles should be adhered:

(P1) Data Collection Limitation Principle - There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

(P2) Data Quality Principle - Personal data should be relevant to the purposes for which they are to be used, should be accurate, complete and kept up-to-date.

(P3)Purpose Specification Principle - The purposes for which personal data are collected should be specified not later than at the time of data collection.

(P4) Use Limitation Principle - Personal data should not be disclosed or otherwise used for purposes other than those specified in accordance with P3. Except: (a) with consent of the data subject, or (b) by the authority of law.

(P5) Security Safeguard Principle - Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

(P6) Openness Principle - There should be a general policy of openness about developments, practices and policies with respect to personal data.

(P7) Individual Participation Principle - An individual should have the right to obtain confirmation of whether or not data relating to him has been collected. To request data relating to him and to have the data erased, rectified, completed or amended.

(P8) Accountability Principle - A data controller should be accountable for complying with measures which give effect to the principles stated above.

4.2. Task-oriented privacy enforcement

Conventional surveillance systems follow a sensor-orientated approach, i.e., all available data is collected, stored and finally processed to fulfill a specific surveillance task. This leads to complex approaches to cope with privacy and data protection. Hence, it is apparent to apply a task-orient approach to surveillance systems. When following such an approach, only data that is required for a surveillance task, is collected, stored and processed, and the task itself must be specified beforehand. Thus data protection and privacy policies are straightforward to implement as they can be tied to specific objects, persons of interest and surveillance scenarios. If a task is specified strictly according to its purpose, a task-oriented system ensures best possible privacy and data protection for the observed subjects. As processing is task-oriented, person related data can be isolated in case of multiple surveillance tasks and privacy protection mechanisms can be established very granularly according to the requirements of the task. Hence a task-oriented system is efficient and privacy-aware.

A task-oriented approach directly enforces the purpose specification principle, i.e., the purpose of a surveillance task must be specified exactly before the task is started and acquired information can only be used for this specific task. The principle of collection limitation can be extended to a more common data minimization principle, which includes minimal collection, processing and storing of surveillance data. This can be realized at best by the task-oriented approach. The individual participation principle and national legislations require that a surveillance subject can obtain data related to him. The subject can provoke erasure, correction or completion of related data (depending on weighting of other interests). A task-oriented system assures that only a minimum of the surveillance tasks is affected and that the overall surveillance is not at risk. If data must be exchanged between security systems or should be reused in a new task, data access can be granted task-oriented and hence according to least privilege. If a task expires or no new task is approved, usage of protected information is denied. Finally a task-oriented approach facilitates surveillance in a large region without being area-wide. An example for task-oriented surveillance system is the NEST architecture [23] that allows the operator to specify surveillance tasks at semantic level. The OOWM acts as central information hub (see Figure 2). Any information that is requested by application-level modules is compliant with privacy policies.

To extend the surveillance area, multiple OOWMs can be connected and exchange data. In most cases only little

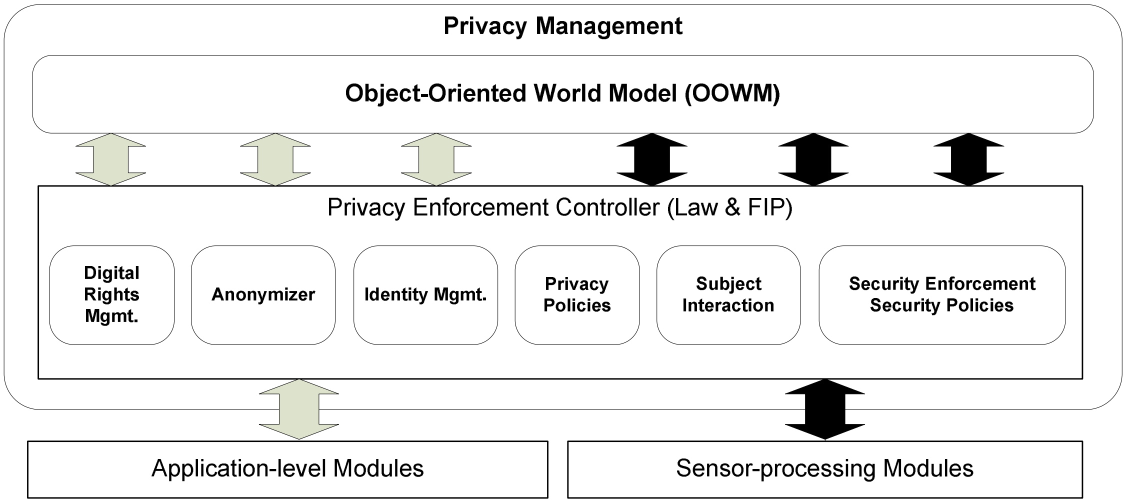
Privacy Management
Object-Oriented World Model (OOWM)
Privacy Enforcement Controller (Law & FIP)
Digital Rights Mgmt.
Anonymizer
Identity Mgmt.
Privacy Policies
Subject Interaction
Security Enforcement Security Policies
Application-level Modules
Sensor-processing Modules

Figure 2: A framework for privacy enforcement

information is exchanged with other OOWMs. OOWMs should be connected with caution, as it can result in extensive surveillance, which is forbidden by most legislations. Besides, application-level modules, data subjects can also interact with the system to request personal data related to them *P7*. The *Privacy Management (PM)*, see Figure 2) and its modules are highlighted in the next section. The PM intercepts the communication requests and responses between the OOWM and the modules.

Access is only granted to an application module, if it is required for fulfillment of a surveillance task (the module is authorized). Furthermore only as few as possible information is released (see *P1* and *P4* below). In addition, the *Task Management* is also relevant to enforce privacy. Although it is not shown in Figure 2, it is also connected to the OOWM, thus information about existing and planned tasks are present.

4.3. A framework for privacy enforcement

Privacy compliance is enforced by the PM, restricting the access to the OOWM according to the deployed privacy policies for guidelines and law. It is directly connected with the OOWM and hosts *Security Enforcement Sub-Module (SESM).* The latter enforces the actual access controls that are derived from the privacy policies, performs authenticity checks, and manages cryptographic keys. The framework contains modules for anonymization, identity management, user interaction (erasure as well as correction of personal data) and a policy repository. If data is exchanged with other surveillance systems the PM attaches digitals rights to ensure that information can only be used for a specific task. All components in the PM are geared to task-orientation and enforce privacy according to the FIP.

4.3.1 Privacy Enforcement Controller (PEC)

The Privacy Enforcement Controller is the central interface; it receives and processes data requests from application-level modules and controls all privacy-related modules. All information that is used must pass the PEC, Hence, privacy-aware data processing can be ensured. The SESM is also controlled by the PEC.

4.3.2 Identity Management (IdM)

To guarantee privacy, the Identity Management performs multi-layer identity management that handles object IDs at sensor level, operational level (in the OOWM), and access level (semantic level). For the latter, the IdM keeps track of surveillance tasks and corresponding application-level modules, and creates virtual IDs to hide the real identity of observed objects. It must be infeasible to combine information of different surveillance tasks, separation is also addressed by virtual IDs. At the operational level problems occur, if access controls change dynamically, e.g., if a person is identified as an employee during a tracking process, access to particular attributes might be restricted. At sensor level, it must be ensured that collected information is assigned to the proper objects in the OOWM.

4.3.3 Anonymizer (AM)

The Anonymizer is closely linked to the IdM and ensures privacy-aware access on information about objects. The AM enforces maximum privacy for different accesses by anonymization. If possible (depending on the surveillance task) location requests and attribute requests are anonymized. In most cases sensitive attributes are not accessible for specific tasks or modules executed during a task. In general, as less as possible information of an object should be provided to a module. Depending on the surveillance task, imprecision or artificial errors can be added intentionally.

4.3.4 Digital Rights Management (DRM)

Objective of this Module is to attach digital rights to any information that is sent to an application module or to another surveillance deployment (OOWM). This guarantees that data is only accessible during execution of a surveillance task. Lifetime of data is restricted and data is only available for authorized modules. However, even if the information flow can be controlled, surveillance module providers (operators) must be trusted. Once information has been observed, it might be reproduced and misused. Only if a system is certified and sealed, it can be ensured that data is not used in a prohibited context.

4.3.5 Subject Interaction (SI)

The Subject Interaction module handles the interaction between an observed subject and the surveillance system. The subject can request personal data related to him and can induce correction or erasure. In some surveillance scenarios a subject can import his own policies. Different options for interaction with a surveillance system are imaginable, for instance: a personal device, a kiosk or simply pen and paper.

4.3.6 Privacy Policies

Privacy policies ensure a proper level of privacy for the surveillance deployment. Policies concern one or more surveillance tasks (global policies) or can be user specific (personal policies). Global policies are enforced to achieve compliance with data protection law and the FIP. By using personal policies the observed subject can specify a personal trade-off between functionality and privacy.

4.3.7 Security Enforcement and Security Policies

As mentioned, security is closely related to privacy. However, the SESM manages cryptographic keys and certificates, thus ensuring authenticity of application modules and confidentiality of transmitted data. The SESM also logs any (attempted) access to the OOWM. The SESM deploys and enforces the access controls derived from the privacy policies and security policies. The latter specify authorizations for application modules and resources that are not privacy related.

4.4. Achievement of the fair information principles

The presented framework can ensure compliance with the FIP. Following it is shown how the components interact to enforce privacy according to the principles

(P2) Data Collection Limitation Principle - The collection of data is firstly minimized at sensor level, i.e., the sensor modules only select the potentially required sensors for a surveillance task. As a result only potentially relevant information is fused in the OOWM and the relation to a specific task exists right from the start. However, sensors can still deliver information for a specific surveillance task that is not required. Hence the AM removes irrelevant information before the response or event is sent back. Strategies for anonymization differ depending on the surveillance task (tracking of group, statistical requests, surveillance of an area). Hence, the Anonymizer can be customized to achieve best possible privacy. Strategies are stored in the Privacy Policy repository.

(P4) Use Limitation Principle - Usage of data is restricted according to the surveillance task. Therefore access controls are enforced by the SESM, i.e., access is only granted to all involved modules during the duration of the task, and such general Security Policies are stored in the SESM. To enhance privacy, more specific privacy policies that describe which attributes are accessible by particular modules can be specified. A possible enhancement would be to deploy and remove these privacy policies according to the surveillance workflow, i.e., a module is only allowed to access data at a specific point in time. However, this may lead to complications in case of exceptions or other unforeseen activities, and hence requires more research. Data should only be used in a specific context and only during execution of the corresponding task. Hence any information that leaves the OOWM is coupled with digital rights to restrict lifetime and usage. This is done by the DRM. This is especially important, if data is exchanged between OOWMs. A module or an OOWM must have the valid credential to process the requested data, e.g., if a credential has expired, the module or the OOWM cannot process information of a subject and the credential must be requested again.

(P5) Security Safeguard Principle - A lot of video-specific approaches exist that try to achieve the standard security objectives: Confidentiality, Integrity and Availability (CIA). The OOWM deals with more abstract data, hence these approaches are not applicable, and established security mechanisms and protocols are used to achieve CIA in a task-oriented surveillance architecture. For instance, certificates (PKI) or IPSec. Although, these methods are sufficient more specific security mechanisms would enhance efficiency. In [31] a web of trust for surveillance sensors is proposed to enhance trust in the authenticity of surveillance sensors. Hence only sensor modules that are assumed to be trusted are allowed to deliver information into the OOWM.

(P7) Individual Participation Principle - Besides the general privacy policies mentioned above (P4), data subjects can also specify personal privacy policies, i.e., a data subject can specify his personal trade-off between efficiency and privacy. For instance, information about a vehicle can be released voluntarily to enable its monitoring

in a parking garage. Naturally not all surveillance tasks (e.g. thievery protection) allow personalization. These personal policies must be brought into the system, hence the Subject Interaction Module, handles interaction between the data subject and the surveillance system. This can be realized by personal assistants which communicate with the OOWM, but other methods, e. g., terminals or pen and paper, can be used as well. The interaction module also empowers user subjects to request the personal data related to them. They can induce erasure (if it is compliant with the surveillance task) or correction of their personal data.

(P8) Accounting principle - Any services performed by a module inside the OOWM, any external access by an actor and any data integration by a sensor is logged. If, for some reason, a violation of access rules occurs, the operator is notified about it. These logs cannot be altered by the operator. Hence they can be used to prove proper processing of personal data.

Principle *P3* and *P6* can by definition not be achieved by the PM. The purpose for which personal data is collected must be specified before the surveillance task is started. Most legislations require that the entire surveillance task (purpose) is specified before it is started. *P6* cannot be achieved by the PM and SESM as well. Information about the architecture, policies and operators must be easily accessible for surveillance subjects.

5. Conclusion

Modern surveillance systems are extended with all kind of sensors and process information on a high level of abstraction. Hence, privacy cannot be enforced on sensor-level. Abstract object representation as in the OOWM is required and task-oriented approach for privacy enforcement is well suited. The proposed framework that makes use of an OOWM copes with privacy regulations according to the FIP. It has been shown that modern surveillance systems do not only imperil privacy, but also allow more sophisticated methods to improve privacy.

6. References

[1] E. Monari, J. Maerker, and K. Kroschel. A robust and efficient approach for human tracking in multi-camera systems. In Proc. IEEE International Conference on Advanced Video and Signal Based Surveillance AVSS, 2–4 Sept. 2009.

[2] A. Hampapur, L. Brown, J. Connell, A. Ekin, N. Haas, M. Lu, H. Merkl, and S. Pankanti. Smart video surveillance: exploring the concept of multiscale spatiotemporal tracking. Signal Processing Magazine, IEEE, 22(2):38–51, 2005.

[3] J. Gonzàlez, F. X. Roca, and J. J. Villanueva, "Research steps towards human sequence evaluation," in *Advances in Computational Vision and Medical Image Processing*, J. M. Tavares and R. M. N. Jorge, Eds. Dordrecht: Springer Netherlands, 2009, vol. 13, ch. 6, pp. 105-115.

[4] P. Turaga, R. Chellappa, V. S. Subrahmanian, and O. Udrea, "Machine recognition of human activities: A survey," Circuits and Systems for Video Technology, IEEE Transactions on, vol. 18, no. 11, pp. 1473-1488, September 2008.

[5] A. Bauer, T. Emter, H. Vagts, and J. Beyerer. Object oriented world model for surveillance systems. In P. Elsner, editor, Future Security: 4th Security Research Conference, pages 339–345. Fraunhofer Verlag, Oct. 2009.

[6] T. Emter, I. Gheta and J. Beyerer. Object oriented world model for video surveillance systems. In P. Elsner, editor, Future Security: 3rd Security Research Conference, pages 315-320, Fraunhofer Verlag, 2008.

[7] F. Dufaux and T. Ebrahimi. Scrambling for video surveillance with privacy. Computer Vision and Pattern Recognition Workshop, 2006. CVPRW '06. Conference on, pages 160–160, June 2006.

[8] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, A. Ekin, J. Connell, C. F. Shu, and M. Lu. Enabling video privacy through computer vision. IEEE Security and Privacy, 3(3):50–57, 2005.

[9] A. Chattopadhyay and T. E. Boult. Privacycam: a privacy preserving camera using uclinux on the blackfin dsp. In CVPR, 2007.

[10] T. Boult. Pico: Privacy through invertible cryptographic obscuration. pages 27–38, Nov. 2005.

[11] J. Schiff, M. Meingast, D. Mulligan, S. Sastry, and K. Goldberg. Respectful cameras: detecting visual markers in real-time to address privacy concerns. Intelligent Robots and Systems, 2007. IROS 2007. IEEE/RSJ International Conference on, pages 971–978, 29 2007- Nov. 2 2007.

[12] Associated Press. Talking camera tackles city crime. http://www.cbsnews.com/stories/2005/11/17/tech/main1054526.shtml (last access 15.06.09), November 2005.

[13] S. Fleck and W. Strasser. Smart camera based monitoring system and its application to assisted living. Proceedings of the IEEE, 96(10):1698–1714, Oct. 2008.

[14] D. A. Fidaleo, H.-A. Nguyen, and M. Trivedi. The networked sensor tapestry (nest): a privacy enhanced software architecture for interactive analysis of data in video-sensor networks. In VSSN '04: Proceedings of the ACM 2nd international workshop on Video surveillance & sensor networks, pages 46–53, New York, NY, USA, 2004. ACM.

[15] M. Schaffer and P. Schartner. Video surveillance: A distributed approach to protect privacy, 2005.

[16] R. Du and J. Fridrich. Lossless authentication of mpeg-2 video. In Image Processing. 2002. Proceedings. 2002 International Conference on, volume 2, pages II–893–II–896 vol.2, 2002. (10)

[17] T. Chattopadhyay and A. Pal. Two fold video encryption technique applicable to h.264 avc. In Advance Computing Conference, 2009. IACC 2009. IEEE International, pages 785–789, March 2009.

[18] B. Kuhn, A. Belkin, A. Swerdlow, Timo Machmer and Jürgen Beyerer. Knowledge-driven opto-acoustic scene

analysis based on an object-oriented world modelling approach for humanoid robots, VDE Verlag, 2010.

[19] S. Das, High-Level Data Fusion. Artech House Publishers, September 2008.

[20] H. Vagts and J. Beyerer. Security and privacy challenges in modern surveillance systems. In P. Elsner, editor, Future Security: 4th Security Research Conference, pages 94–116. Fraunhofer Verlag, Oct. 2009.

[21] M. Mccahill and C. Norris. Estimating the Extent, Sophistication and Legality of CCTV in London. Palgrave Macmillan, Basingstoke, Hampshire, England, 2003.

[22] O. for Economic Cooperation and Development. OECD guidelines on the protection of privacy and transborder flows of personal data. OECD Publishing, 2002.

[23] J. Moßgraber, F. Reinert and H. Vagts. An architecture for a task-oriented surveillance system - a service and event based approach, Proc. Fifth International Conference on Systems ICONS, 2010