S 5.2

NEW APPROACHES FOR DATA PROTECTION AND ANONYMIZATION IN SURVEILLANCE SYSTEMS

H. Vagts[1,2] and J. Beyerer[1,2]
[1] Fraunhofer Institute of Optronics, System Technologies and Image Exploitation, Fraunhoferstr. 1, Karlsruhe, Germany
[2] KIT – Institute for Anthropomatics – Vision and Fusion Lab, Adenauerring 4, 76131 Karlsruhe, Germany
hauke.vagts@iosb.fraunhofer.de

Motivation

Conventional video systems collect all available information, store it and perform situation analysis on the raw material. With the growing number of cameras and other sensors it is essential to extract required information as soon as possible to reduce the amount of data. In addition, data collected by other sensors (RFID, acoustics, etc.) must be combined with the information gained out of the video material. Hence, data must be represented and processed on a high level of abstraction. The abstraction leads to new opportunities for privacy enforcement and a framework for surveillance systems that follows the fair information practice principles [1]. It is possible to maximize privacy and efficiently fulfill surveillance tasks at the same time.

All previous work in the field of privacy protection in surveillance focuses on video. Many approaches blur out sensitive regions. Detection and recognition algorithms are error-prone, especially in bad lighting conditions or similar. Moreover, blurring can't be applied, if information is collected by heterogeneous sensors. The system proposed in [2] rerenders video to remove sensitive information. The approach in [3] follows the same idea in an extremer way. No video is presented to the users. Instead, only avatars of the observed objects are shown in a virtual model of the real world. As long as the surveillance data is represented virtually, anonymization strategies can be applied. Each object has several attributes (e.g., size, age, color of upper body) that can be anonymized.

Absolute anonymization can only be achieved, if the data is totally scrambled and cannot be linked to the original data. Obviously, such data is not useful for all kinds of tasks. Hence, data must be anonymized at a reasonable level. When anonymizing raw video, it is not possible to specify objective privacy levels. Sensitive information may either be blurred or not. A high level of data abstraction allows to apply metrics for anonymization. Consequently, it can be ensured that surveillance systems fulfill a certain level of privacy, respectively that specific surveillance tasks have access to data of a proper level only.

Due to the fact that there are different metrics for anonymization, it must be determined, which ones are suitable for surveillance. Privacy-aware surveillance systems can be successfully designed only, if they are based on appropriate metrics.

Solutions for surveillance can never rely on technology only; but they must also comply with existing law. Furthermore, they must be accepted by the observed people. However, privacy enhancing technologies, such as anonymization algorithms, could be used to create legal surveillance systems.

Scope of Surveillance for Surveillance Systems

Surveillance systems have a huge scope of application, e.g., they can be used to detect thievery or to protect workers in a danger area. Exemplarily, two contrary categories were selected to point out the different requirements for surveillance data.

Tracking of a single object: This is a typical category in surveillance, e.g., for tracking a visitor from the reception to a meeting room. Tasks of this category focus on position data, which is quite special in the context of surveillance (see below). All other attributes of a person are either not relevant as in the named example, or all attributes are extremely relevant, e.g., surveillance of a suspect of crime.

Collection of data for statistical reasons: Statistical data can be collected for diverse reasons. Contrary to the upper task, a single position is not relevant or does not have to be accurate. In general, only a subset of all available attributes of objects (e.g., viewing direction, gender) is relevant. A typical task would be the detection of consumer behavior, e.g., identification of the perfect spot for a product in a grocery store.

In a modern surveillance system (e.g., [4]), services belonging to different surveillance tasks can request information about objects and they can all receive differently anonymized data. A task of the latter category can, e.g., receive an anonymized table of all persons that have crossed a specific area. The accurate position is substituted by the Boolean attribute “has crossed important area” and only the gender of all these people is revealed, no additional information is provided.

Metrics for Surveillance Systems

Metrics for Anonymization are usually applied to tables. Surveillance data at a high level of abstraction can be expressed in tables also. Hence, metrics are potentially applicable. A table containing non-anonymized data is named *private* table, an anonymized one is referred to as *release table*. In such tables, an *explicit identifier* is an attribute that identifies an object directly, e.g., a tax number. Obviously, such objects must be removed or anonymized. Moreover, there are attributes that can be used to identify objects, if they are combined with other attributes; such an attribute is denoted as *Quasi-Identifier attribute (QIA)*. A set of these object identifying attributes is named *Quasi-Identifier (QI).* An equivalence class of QIs (QI-EC) is the set of tuples with the same QIA values. Non-identifying attributes that must be hidden from attackers are named *sensitive*.

In most work, QIs and sensitive attributes are considered to be not disjunct. This assumption cannot be made in surveillance. For instance, the position of an object can act as QI (e.g., in combination with the height) and is also a sensitive attribute that should not be released. In addition, position data has its own semantic, which does not allow the use of regular methods for anonymization of numeric attributes. The information content does not change, if it is changed by a few inches or yards. Hence, position data must be treated in a special manner.

Numerous metrics for anonymization exist (e.g., [5]) and two of them have been identified to be appropriate for surveillance data, when considering its special characteristics: *k-anonymity* [6] and *l-diversity* [7].

If a release table fulfills k-anonymity, each combination of QIs must be assignable to at least k objects. This definition does not consider sensitive attributes. A QI-EC fulfills l-diversity, if it contains at least l well-defined values for the sensitive attribute. A table fulfills l-diversity, if all QI-EC fulfill l-diversity.

However, k-Anonymity is not appropriate for position data. If many people are at a small spot, the semantic information of each position is the same, i e., all tuples of the QI's equivalence class have the same sensitive attribute and a known user attack can be performed.

One solution is to decouple the aspects of being a QI and a sensitive attribute for position data. Therefore, the attribute *region* is introduced as well as a function f_h of a position (x, y) to a region r: $f_h : (x,) \rightarrow r$. Region now contains the sensitive information and the exact arrangement is depending on the specific context. As a consequence, position data is a QI only. The differentiation of the semantic information is performed in the attribute region. Two metrics can be used to measure the differentiation of the sensitive aspect: l-Diversity and t-Closeness. The later has several disadvantages, if used in surveillance. When observing a single object, always exactly one equivalence class is created, which contains the object. Hence, t-Closeness is fulfilled trivially. Even when collecting data for statistical investigation with multiple objects, t-Closeness can be used only, if a critical amount of data is collected.

A Framework for Anonymization

Based on the determined metrics, a framework for anonymization must consist of the following modules. Figure 1 shows the progress of anonymization that can be split in three parts (1.x, 2.x and 3). At the left side, users can interact with the system. The core component is the *Privacy Manager* that contains modules for anonymization and a module for Identity Management (IdM). The collected surveillance data is stored at a central server (right side).

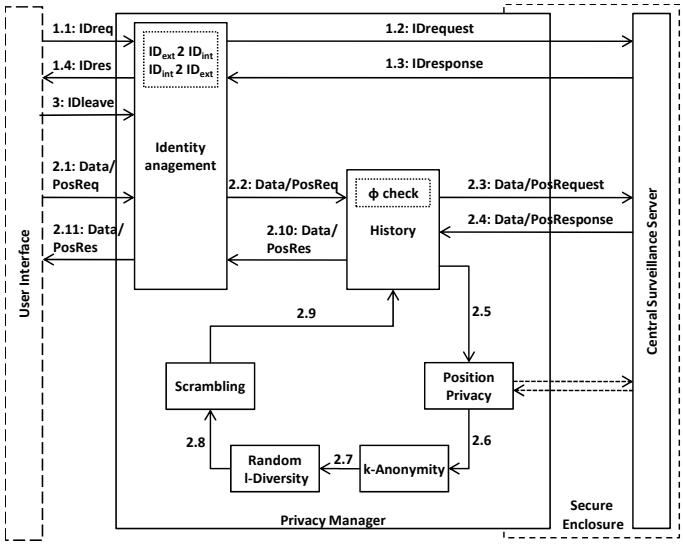

Fig. 1. Framework for Anonymization.

All communication in 1.x is for handling IDs. The IdM module is responsible for mapping internal (private) IDs ID_{int} to external IDs ID_{ext}. The external IDs can then be used to perform requests (2.1/2.2) for position or data (all other attributes). The Anonymization proceeds in 2.x. At first, the maximal request rate is checked to prevent location tracking by repeatedly sending requests. The *History* module logs performed anonymization to prevent that attacks can be performed by combining released tables. The module for *Position privacy* ensures k-anonymity and l-diversity of a released position data by generalization, based on the Algorithm from Bamba and Lui [8]. For each response regarding a specific object, it is ensured that the returned area (generalization of an exact position) contains at least k-1 other objects. Furthermore, a response must span l regions (which must be defined beforehand). The module *k-Anonymity*

enforces k-anonymity for all other attributes. The l-diversity Module applies the second metric to all other attributes as well. Therefore, a random part of other private data containing the same private attributes is selected and its distribution of values is applied to the release table. In conclusion, the records in the release table are mixed to prevent attacks on too static tables. The final private table is then released to a service or user (2.10/2.11). After finishing a surveillance task, internal IDs that are blocked by the IdM (to prevent further attacks) are released (3).

Legislation

From a legal point of view, modern and intelligent surveillance systems have several pros and cons. One disadvantage is that modern IP-based systems can be easily linked with each other. Hence, area-wide surveillance is possible. In addition, modern systems can autonomously identify objects. Data collected by multiple sensors is fused to an early point in time and as in conventional systems, information about objects is stored.

On the other hand, sensors used in modern systems are less intrusive, i.e., they only transmit relevant and abstract data. Furthermore, these sensors can be activated selectively for specific surveillance tasks. Task-oriented systems also ensure that data is only used for the specified purpose and can easily be deleted. Anonymization strategies can be applied to data and the linkage to the private material can only be revealed, if necessary (e.g., if it is requested by court).

In summary, an intelligent surveillance is a huge invasion of privacy, especially of the right to self-determination. Nevertheless, if it is based on the technological realization of data protection, a modern surveillance system can be evaluated to be less invasive then a conventional surveillance system.

Summary

It has been shown that existing metrics can be applied to surveillance systems, if the characteristic of surveillance data is considered. As a result, privacy can be measured in systems that handle privacy on a high level of abstraction. Based on the metrics, privacy can be enforced by a *Privacy Manager* framework. Task-oriented surveillance and anonymization lead to less invasive surveillance systems. It remains, however, an open question, whether these systems will be accepted by the users, the society.

References

[1] Vagts, H. and Beyerer, J.: Security and privacy challenges in modern surveillance systems, in Future Security: 4th Security Research Conference, Peter Elsner, Ed. Oct. 2009, Fraunhofer Verlag, p. 94.
[2] Senior, A., Pankanti, S., Hampapur, A., Brown, L., Tian, Y.L., Ekin, A., Connell, J., Shu, C.F., Lu, M.: Enabling video privacy through computer vision. Security & Privacy, IEEE 3) (May-June 2005), p. 50–57.
[3] Bauer, A., Emter, T., Vagts, H., Beyerer, J.: Object oriented world model for surveillance systems. in Future Security: 4th Security Research Conference, Peter Elsner, Ed. Oct. 2009, Fraunhofer Verlag, p. 339–345.

[4] Moßgraber, J., Reinert J. and Vagts, H.: An architecture for a task-oriented surveillance system - a service and event based approach, Proc. Fifth International Conference on Systems ICONS, 2010.
[5] Andersson, C. and Lundin R., On the Fundamentals of Anonymity Metrics, in: The Future of Identity in the The Future of Identity in the Information Society, Bd. 262, 2008, p. 325.
[6] Sweeney, L.: Achieving K-Anonymity Privacy Protection Using Generalization and Suppression, in: International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10 2002.
[7] Machanavajjhala et al.: L-diversity: Privacy beyond k-anonymity, ACM Transactions on Knowledge Discovery from Data, 2007, p. 3.
[8] Bamba, B. und Liu L.: PRIVACYGRID: Supporting Anonymous Location Queries in Mobile Environments, Techn. Ber., GIT-CERCS, 2007.