Security and Privacy in Video Surveillance: Requirements and Challenges

Qasim Mahmood Rajpoot, Christian Damsgaard Jensen

Security and Privacy in Video Surveillance: Requirements and Challenges*

Qasim Mahmood Rajpoot and Christian Damsgaard Jensen

Department of Applied Mathematics & Computer Science
Technical University of Denmark
DK-2800 Kgs. Lyngby, Denmark
{qara,cdje}@dtu.dk

Abstract. Use of video surveillance has substantially increased in the last few decades. Modern video surveillance systems are equipped with techniques that allow traversal of data in an effective and efficient manner, giving massive powers to operators and potentially compromising the privacy of anyone observed by the system. Several techniques to protect the privacy of individuals have therefore been proposed, but very little research work has focused on the specific security requirements of video surveillance data (in transit or in storage) and on authorizing access to this data. In this paper, we present a general model of video surveillance systems that will help identify the major security and privacy requirements for a video surveillance system and we use this model to identify practical challenges in ensuring the security of video surveillance data in all stages (in transit and at rest). Our study shows a gap between the identified security requirements and the proposed security solutions where future research efforts may focus in this domain.

Keywords: Video Surveillance, Security, Privacy, Monitoring, Storage, Access Control, Encryption

1 Introduction

Video surveillance is often considered one of the first applications of pervasive computing [1]. Its usage has significantly increased over the last two decades, firstly due to continuously decreasing hardware costs including camera, storage or networking and secondly due to the increased sense of insecurity caused by incidents like 9/11 and the Madrid and London bombings.

Traditional video surveillance systems are either simple recording systems or they are monitored by human observers without automated technological assistance. This makes them very expensive in terms of installation and operation. They are mainly used as deterrents and the recordings help investigation once an incident has occurred. Compared to these traditional solutions, modern digital solutions are less expensive while offering much better quality. Modern systems make use of advanced techniques such as object-detection, -identification, -tracking and event-detection, exploiting algorithms

* The work presented in this paper is supported by a grant from the Danish National Advanced Technology Foundation.

from the fields of computer vision, image processing and pattern recognition [2]. These techniques potentially allow recognizing a target object e.g. a vehicle, or even automatically tracking an individual spanning over multiple areas in a surveillance network [1], with trivial effort. Having such systems installed throughout the major public places in a city, for example, at bus stops, in train stations, near ATMs, in shopping malls, streets, etc., may lead to a big brother society in which all the activities of an individual can be profiled, allowed legally by law enforcement authorities or performed out of curiosity by an operator. Doing so requires a significant amount of time and effort in traditional surveillance systems, so the privacy concerns are obviously much more serious in modern video surveillance systems compared to traditional ones.

Consequently, there have been a lot of research efforts on developing privacy enhancing technologies (PETs) in video surveillance during last few years. This is achieved by hiding privacy sensitive regions like faces by means of obfuscation [3] or scrambling [4]. However, little research has focused on effectively making use of these techniques in ensuring privacy and controlling access to the data [1], [5]. Similarly, little research is found in literature that addresses the security of video streams and the associated data while they are transmitted or stored. In this paper, we propose a general model of video surveillance to help identify a list of security and privacy requirements in a video surveillance system. We provide an overview of existing solutions proposed to fulfill the major requirements identified through our model and point out their problems. Our study identifies a potential gap where research efforts need to be put in by pointing out challenges that need to be considered while designing security solutions in this regard.

The rest of the paper is organized as follows. In section II, we present the architecture of a video surveillance system to help the reader understand the security and privacy requirements identified through our model in section III. An overview of privacy enhancing technologies is presented in section IV. We examine the existing work related to security requirements in video surveillance and outline the associated challenges in section V. Section VI concludes the paper.

2 Architecture of a Video Surveillance System

In this section we present a simplified architecture of a modern video surveillance system. The aim of this section is to give a brief overview of a video surveillance system, and its related issues, which serves as background to understand the model and the security and privacy requirements that we identify in the next section.

Modern video surveillance systems primarily use the internet as a channel to transfer data to intermediary servers, storage systems and the users. Such a system normally employs a network of several cameras which capture video data at their respective locations, as depicted in Fig. 1. This data is sent to the storage server responsible for securely storing the data. Depending on the application requirements, this could be a centralized or distributed storage solution. The data may be accessed by users, wishing to see the live or recorded data of a desired location, e.g. live video feeds are often sent to a special monitoring room, and this live or stored data may also be watched on hand-held devices or a workstation. We refer to such users as observers. The control

unit handles access requests from the observers and allows them to access data as per the specified policy.

Consider the video surveillance system deployed at Technical University of Denmark (DTU). This system consists of several cameras which are employed on the entrances of different departments and in the parking lots. The captured data is continuously monitored manually, along with the technological assistance by the system which generates an alarm upon detection of an anomalous event e.g. crossing a fence or gate in a parking lot. The observers are associated with different areas in the university and on generation of an alarm they investigate closely what happened and call security, if required. The observers may access the data in the monitoring room or on their handheld devices when they are approaching towards the place of incident. However, notice that the observers are normally pre-associated with the specific areas and are already granted access to watch videos of those areas, independent of the alarm generation. This static access control leads to privacy issues where observers are always allowed to access the data.

An alternative approach could make use of dynamic access control where access to data is granted to the nearest available mobile observers upon detection of an event. Considering the proportionate access principle, observers in the monitoring room may be given regular access with less privileges (low resolution) in normal situations and higher privileges in an emergency situation.

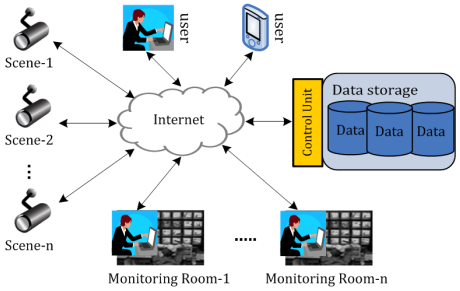

Fig. 1. Architecture of a video surveillance system

Allowing access of data to certain individuals only in case a specific event occurs or an emergency situation, addresses the privacy concerns raised because of continuous video surveillance. Using these techniques can prove to be immensely useful in public video surveillance too, conducted by Birmingham city council, for instance. In this video surveillance system, cameras are deployed in the major public places all over the city. Suppose there is a fire incident reported in the city center. Upon detection of this emergency situation, along with the observers assigned to this location, the nearest fire-brigade and police stations are also informed about the event and the system allows access of data to the respective employees of these stations. Allowing access to the video stream to the fire-brigade and police station would help them understand the severity of the situation and to come prepared with appropriate tools and man-power to better combat such situations. Although the system should allow advanced functionalities such as searching, tracking an individual and automatically identifying an individual,

however, appropriate access control mechanisms must be adopted in order to minimize the chances of performing voyeurism by the observers, reduce privacy invasion and to make these systems widely acceptable.

3 Video Surveillance Model

In this section, we generalize the architecture, presented in Section 2, into an abstract model of video surveillance as a method to identify the manifold security and privacy requirements in a video surveillance system. Fundamentally, a video surveillance system must include elements to capture video, to store/record video and to display video to the users, as well as a mechanism to transport video data between these elements. Figure 2(a) shows the main elements of our model, which includes four components, namely: video capture, -transport, -monitoring, and -storage. The video capture component includes the cameras, their local infrastructure, and the area which can be captured by the cameras. Once the data is captured, it needs to be securely transported; this is typically done over the internet, so we have included this as a component in our model. It is important that video transport is done in a way that ensures the confidentiality and integrity of data while in-transit. The transport component considers transport of data from cameras to storage servers, between storage servers, and while watching either live- or stored video data. The monitoring component includes the different elements that are necessary to allow somebody to watch the video. The monitoring component must consider all security and privacy concerns that arise when the captured data (live or stored) is watched by the observers. Finally, the storage component is responsible

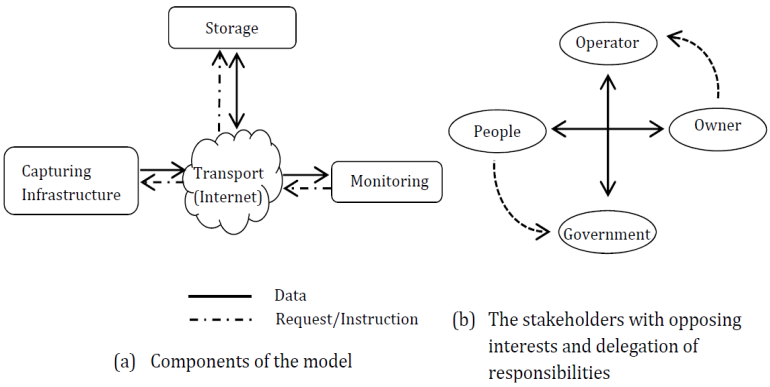

Fig. 2. Video surveillance model

for securely storing the data and restricting the access of stored data to the authorized individuals only. Monitoring includes any automatic or manual processing for the purpose of observing live or stored data, therefore when the stored data is watched by the observers, it falls under the monitoring component.

The four components identified in Fig. 2(a), allow us to identify the domain and scope for many of the security and privacy requirements that may arise in video surveillance systems. We do, however, also need to consider the different stakeholders and

interests in order to identify all the security and privacy requirements in video surveillance systems. There are two principal stakeholders in all video surveillance systems, the owner, who commissions and is responsible for the system, and the people who are being watched by the system; these are shown as principal opposing forces in Fig. 2(b) In practice, however, normally owners do not operate the video surveillance systems themselves, but instead delegate this task to another organization, e.g. a guard company; this organization is referred as operator. Similarly, most people are unable to determine whether video surveillance is fair and warranted or excessive, so it is typically an elected government which regulates video surveillance through legislation and guidelines. This means that, in practice, the video surveillance operator and the government become the real opposing forces in a video surveillance system. The term observer used in the previous section holds a subset of responsibilities of the operator, as the operator may have additional responsibilities other than merely watching the video streams. For the sake of simplicity, we will use the term operator in rest of the paper.

People are the core of our model, because they may have certain expectations from each component of the video surveillance system, whereas the other entities strive to live up to the expectations of the people. It is the combined responsibility of the owner and the operator to ensure the security of the system and the privacy of the people as it is defined by the government. Privacy of people should be protected both from outside attackers and the personnel within the owner and operator organizations. The operator is responsible for performing his duties while being least intrusive as far as the privacy of people is concerned. Based on our model, requirements capturing consists of two stages. In the first stage, we map the requirements from the perspective of each of the stakeholders for each of the four components in the model. In the second stage, we remap these requirements in terms of privacy and security aspects. The first stage ensures that we identify the requirements that can be specified by the people and/or the government, owner and operator in the form of security and privacy related functionalities and features in the system.

Based on the requirements specified by the people/government, owner and operator, we then derive further requirements from the implementation point of view. For instance, the proportionate access requirement specified by the owner is divided into multiple requirements including data hiding, dynamic access control and voyeurism protection when looked in the implementation perspective. Table 1 presents the security and privacy requirements in video surveillance identified as a result of the first stage.

Based on our model, the first stage produces a large number of requirements. However, it contains certain overlapping and repetitive requirements too. This is because our model identifies each requirement in the perspective of the individual stakeholders. Thus in the second stage, we remap those requirements considering the conventional security and privacy aspects that allows us to combine the repetitive requirements together. Table 2 depicts this mapping. We briefly describe these requirements in greater details below.

Privacy:

Consent and Signage: Consent of the people who can potentially be recorded by the video surveillance system needs to be taken in advance, either explicitly or implicitly.

Table 1. Security and privacy requirements in different phases of video surveillance corresponding to all the stakeholders. The last column derives implementation requirements from the ones on left

Phase/ Stakeholders	**People/ Government**	**Owner**	**Operator**	**Implementation requirements**
Capture	*c1.* Consent *c2.* Signage *c3.* Anonymity	*c4.* No data missing *c5.* Availability *c6.* Video properties	None	*c7.* Security of software and hardware infrastructure
Transport	*t1.* Confidentiality *t2.* Integrity *t3.* Authenticity	*t1.* Confidentiality *t2.* Integrity *t3.* Authenticity	None	*t4.* Camera authentication *t5.* Data encryption *t6.* Key management *t7.* No deletion of data
Monitoring	*m1.* Privacy safeguards *m2.* Authorized access *m3.* Public access to their data	*m4.* Continuous monitoring *m5.* Proportionate access *m6.* Occasional access *m2.* Authorized access	*m7.* Data freshness *m8.* Time-stamping *m9.* Easy to search	*m10.* Dynamic access control *m11.* Data hiding *m12.* Voyeurism protection *m13.* User management *m8.* Time-stamping
Storage	*s1.* Secure storage	*s2.* Secure data storage as per law *s3.* Deletion after retention period	None	*s3.* Deletion after retention period *c7.* Security of software and hardware infrastructure *t2.* Integrity *t6.* Key management

One way to take consent is by informing the people about video surveillance through *signage* i.e. displaying clear and visible symbols in the area where video surveillance takes place.

Anonymity, Data Hiding and Privacy Safeguards: While the system is supposed to monitor the behavior of the people, it should strive to maintain the *anonymity* of the people by hiding their identity using certain *privacy safeguarding mechanisms*. Therefore the system must implement *data hiding* techniques which obfuscate the identity-revealing regions in the images when the operators monitor video streams in a normal situation. Needless to say, these data hiding techniques should be reversible such that identity could be revealed if required, for example while investigating a murder.

Video properties: The owner needs to determine whether cameras with advanced functionalities such as pan-tilt-zoom, night-vision and high-resolution are really required to be used, with respect to the purpose of the surveillance conducted.

Voyeurism protection: In order to restrict voyeurism, advanced functionalities such as searching, identifying and tracking an individual are only to be made available when an operator explicitly requests them. While granting these privileges the system logs the request along with the information about the circumstances.

Confidentiality:
The people and owner desire that the data is accessible only to the intended recipients. *Confidentiality* ensures privacy protection against outsiders mainly when data is in transit, whereas *privacy* is a much broader concept that covers privacy protection against insiders too. *Confidentiality* can be ensured by using appropriate *encryption algorithms* and taking care of *key management* issues. Because of the nature of the system, the encryption mechanism should be efficient enough enabling the data to reach the other end in real-time.

Integrity:
Any unauthorized change in the data should be detectable. Appropriate measures should be taken to ensure the *integrity* of data. Moreover, it should not be possible to *delete chunks of data* while leaving other data intact so as to hide the data captured in a specific time interval.

Authenticity:
Camera authentication: In order to ensure the authenticity of the captured data, each camera may be required to authenticate itself to the server.
Data freshness: The operator requires newly captured data in live streaming rather than previously captured data being replayed. *Time-stamping:* The recorded data must include verifiable time-stamping helping to ensure that the data was captured at a specific time and also to search videos specifying the time interval later on.

Availability:
The services offered by the system should of course be *available* when needed. If surveillance takes place upon detection of an event e.g. motion detection then such a mechanism is to be made perfectly reliable such that no event goes uncaptured i.e. *data missing should not be possible*.
Continuous monitoring: The owner requires that the captured data is continuously monitored manually and/or by using automated tools.
Easy search: The operators require that advanced functionalities such as searching, identifying and tracking an individual are available whenever required so they can effectively perform their duties.

Access Authorization:
Public access to their data: Certain countries, for example Canada and France, allow an individual to watch their own images captured by the surveillance system. Therefore, people should be able to get access to the images containing them, through a predefined procedure.
Proportionate access: In order to protect the privacy of people, the owner requires that the proportionate access principle is implemented in the system and that the operators are given the minimum access to the data required to fulfill their duties. This can be achieved by implementing dynamic access control.
Dynamic Access Control: The system must take the context pertinent to a situation into account when authorizing access to data so that different access levels (e.g. blurred, original images) are maintained in different situations (e.g. normal, emergency) and privacy of people is preserved to the maximum extent. In short, the access level should change appropriately depending upon the situation.

Table 2. Remapping of the requirements in Table 1 in terms of privacy & security aspects

Components/ P&S Aspects		**Capture**	**Transport**	**Monitoring**	**Storage**
Privacy	**1. Privacy**	*1a.* Consent (c1) *1b.* Signage (c2) *1c.* Anonymity (c3) *1d.* Video properties (c6)	None	*1e.* Privacy safeguards (m1) *1f.* Data hiding (m11) *1g.* Voyeurism protection (m12) *1c.* Anonymity (c3)	*1g.* Voyeurism protection (m12)
Security	**2. Confidentiality**	Covered by 7a, below	*2a.* Data encryption (t5) *2b.* Key management (t6)	None	*2a.* Data encryption (t5) *2b.* Key manageent (t6)
	3. Integrity	Covered by 7a, below	*3a.* No deletion of data (t7) *3b.* Integrity (t3)	*3c.* Data freshness (m7)	*3b.* Integrity (t3)
	4. Authenticity	Covered by 7a, below	*4a.* Camera authentication (t4) *4b.* Time-stamping (m8)	*4b.* Time-stamping (m8)	None
	5. Availability	*5a.* No data missing (c4)	None	*5b.* East search (m9) *5c.* Continuous monitoring (m4)	Covered by 7a, below
	6. Access authorization	None	None	*6a.* Authorized access (m2) *6b.* Public access to their data (m3) *6c.* Occasional access (m6) *6d.* Dynamic access control (m10) *6e.* User management (m13) *6f.* Logging (m14) *6g.* Proportionate access (m5)	None
	7. Others	*7a.* Security of software and hardware infrastructure (c7)	None	None	*7a.* Security of software and hardware infrastructure (c7) *7b.* Deletion after retention period (s3)

User management: This involves all the issues related to the users of the system including user enrollment, permission assignment, changing permissions, permission revocation, user deletion etc.
Occasional access: As explained in section 2, occasional access to the data might need to be given to certain public organizations; the system needs to build a mechanism to enable such access.
Occasional access: As explained in section 2, occasional access to the data might need to be given to certain public organizations; the system needs to build a mechanism to enable such access.
Logging: All activities performed by the operators should be securely logged, especially those permissions requested explicitly.
Others:
Deletion after retention period: Depending upon the regulations of the region where video surveillance takes place, the captured data must be automatically deleted as soon as the retention period expires.
Security of software and hardware infrastructure: It is to be ensured that the security of the underlying infrastructure is well protected against the attacks exploiting software vulnerabilities or physical access to the hardware.

Considering the concerns of each party involved to maintain security and privacy, it is reasonable to expect that our model has identified a comprehensive set of requirements, though a complete set of requirements is not guaranteed. As mentioned previously, there exists a large amount of work on protecting privacy in video surveillance. The next section briefly summarizes the major types of available techniques for protecting privacy, followed by the state of the art of security research in video surveillance system and the associated challenges.

4 Privacy in Video Surveillance

A pervasive video surveillance system may be exploited by the operators for unauthorized collection of data on the activities of an individual [6]. In the United Kingdom, a report discovered that operators have used video surveillance for voyeurism [7]. In another report by the BBC, council workers in Liverpool spied on a womans apartment using a CCTV street camera. Possibilities for such misuse are further increased with the advent of modern video surveillance systems that facilitate rapid data retrieval enabled by indexing and searching and advanced imaging technology allowing high-resolution and zooming-in. Moreover, pervasive surveillance networks may enable linking the activities of a target in multiple video streams [1].

Considering the above-mentioned issues, several techniques to protect the privacy of the observed individuals have been proposed. In order to hide the identity of observed subjects, identity revealing sensitive areas are first determined and then removed or de-identified depending upon the approach used. Several types of techniques to hide privacy-sensitive areas have been proposed. A simple technique is to fully remove the sensitive regions but this not only hides the identity but in some cases also the behavior, see for example [8] [9] [10]. Another type of approach is to reduce the level of detail of privacy-sensitive areas, with the help of blurring or pixilation, leaving the subject

unidentifiable yet the behavior remains recognizable, [3] [11] [12] to name only a few. The third approach, called abstraction, is to remove the sensitive regions and replace them with dummy objects such as silhouettes or skeletons. Some of the key works in this area are [5] [13] [14]. Yet another technique proposed in literature, called scrambling, is to encrypt the sensitive regions with a key allowing the area to be decrypted only by authorized personnel possessing the key, see for instance [4] [15] [16]. As compared to other techniques, this approach offers the benefit of perfectly reconstructing the original image.

This section explored the major privacy enhancing techniques in order to enable us to identify the research gaps, in the next section. Addressing the identified research gaps may also need to exploit these techniques while suggesting new security and access control mechanisms.

5 Security in Video Surveillance

A study of the relevant literature so far, reveals that many solutions, discussed below, addressing the security requirements including integrity, authentication and confidentiality have been proposed in multimedia systems e.g. video on demand and business video conferencing. However the factors involved in video surveillance systems are quite different than multimedia systems hence these solutions cannot be directly applied in video surveillance systems, although a few commonalities exist.

Due to the communication over public networks, the security aspects are to be addressed when data is transferred from camera to server, server-to-server and server to handheld devices or monitoring room. We discuss here why the security requirements in video surveillance systems are important and identify the challenges to be addressed when designing security solutions for them.

Integrity and Authenticity:

An important security consideration is integrity protection and authentication of recorded video data. This is important for two reasons [17]: i) to accept the recordings as evidence in a court of law, and ii) to avoid framing an individual by tempering with the recordings of a crime scene, for example. Two major techniques to address integrity exist [18]: using cryptographic hash functions along with digital signatures or by making use of watermarks in the video recordings. Solutions proposed in multimedia systems mostly use cryptographic techniques [18] [19]. The integrity protection solution is desired to be robust against certain modifications such as scaling and compression and images should be verifiable despite such benign modifications [19]. In order to ensure authenticity, cameras need to authenticate themselves to the server. Some of the key solutions proposed in this respect require to use Trusted Platform Module in each camera [20] [21] [22]. This approach is prohibitively expensive. Furthermore, performance and scalability remain issues to be resolved too.

Confidentiality:

Similar to integrity and authentication, there are several solutions presented for confidentiality mainly targeting multimedia applications [23] [24] [25]. In order to fulfill these requirements, the existing solutions essentially use cryptography. However, the conventional cryptographic algorithms used in these solutions are not especially de-

signed to encrypt video data [26]. Their usage on video data, although compressed, requires significant processing power, for instance, an MPEG-2 video stream requires a bit rate ranging between 4 to 9 Mbps [27]. Because of the huge amount of data and real-time requirement, efficient usage of cryptography is far from the desired efficiency level in conventional multimedia applications [26], whereas its usage in video surveillance introduces further challenges. In video surveillance systems, unlike multimedia applications, there are several video producers (cameras) with limited processing capabilities. A major challenge, therefore, is to devise encryption algorithms which may efficiently encrypt the large amounts of continuously produced video data, transferred in real-time to the server side, by the cameras. Another relevant issue is key management. Along with encrypting the data from each camera with a different key, the keys may also need to differ for each chunk of data, for instance different key for each 24 hours of data recorded by a camera.

A few solutions addressing confidentiality in video surveillance systems have been proposed in [28] [29] [30]. In order to protect the privacy of individuals and to ensure efficient retrieval of data, modern video surveillance systems extract metadata such as object identification, number of objects and the object types contained in the video streams in real-time [2]. This data is normally extracted at the server, therefore the server must be able to access decrypted data. Solutions proposed in [28] and [30] fail to consider this aspect and share the keys among operators requiring them to collaborate when data is to be decrypted. Another reason for the server to access plain data contents is to be able to send modified video streams (low resolution, obfuscated privacy regions) to different users depending on their access authorization, discussed later in this section. Once metadata has been extracted at the server, another interesting research issue is to securely store the data along with the associated metadata in a manner that it is possible to efficiently retrieve metadata and its associated video streams later, based on query language, for example.

Access Authorization:
Another important challenge which we believe requires major research effort is access authorization in video surveillance systems. Controlling the access to data is of critical importance, as the potential capabilities offered by modern video surveillance systems such as searching for an individual or an event, and monitoring the activities of an individual spanning over multiple locations [1], makes it very easy to invade the privacy of individuals. Clearly video surveillance is expected to become more pervasive and this leaves us with only two choices: either entrust the operators or to devise a mechanism for watching the watchers and minimizing the chances to use such systems abusively [31].

Similar to the above-mentioned security requirements, there exist several solutions regarding access control mechanisms for online and other payment-based video databases such as [32] [33] [34]. Bertino et al. [32] argue that an effective and efficient access control mechanism in video databases requires advancements in extraction of meaningful metadata, furthermore, such mechanism must take benefit of the indexing structure used to store the video data. This is even more important in video surveillance systems as the access control mechanisms are to be applied to live video streams, continuously produced by several cameras, in real-time. With advancements in indexing and metadata

extraction techniques in video databases, we believe that the research efforts now need to focus on devising access authorization techniques for video surveillance systems.

There are only a few research attempts that address the challenge of access authorization in video surveillance. Senior et al. [5] present the idea of using multiple privacy levels in video surveillance systems where different operators are provided different levels of information and actions to be performed, depending on the access privileges of the operator. Different information levels may include for example access to behavioral information where objects are replaced with silhouettes. Similarly different levels of actions to be performed include restrictions over playback, zooming-in and searching functions, offered by the system. The authors suggest using a privacy-preserving console manager that makes use of encryption and access control mechanisms and reveals the data to the operator by extracting information components from video streams as per the authorization level of the operator. In order to use this approach, a large-scale video surveillance system requires a sophisticated access control model. However, the paper presents only the concept without providing details of the privacy-preserving console manager, encryption and access authorization.

Moncrieff et al. [1] argue that using static security policies in video surveillance is either too intrusive for privacy or it hinders the usability of the system. They identify the challenge of utilizing the video surveillance system by exposing sufficient need-specific data to the operators while preserving the privacy of people. The authors suggest that one possible way of protecting privacy in video surveillance while retaining its useful functionality is to use dynamic access control mechanisms. They propose to incorporate the context of the requestor in the access authorization, where privacy is maintained using data hiding techniques in normal situations, whereas a request to data in certain situations, e.g. emergency cases, would enable the operators to access full information with less focus on protecting privacy. Similar to [5], this paper also does not provide an access control mechanism. The main contribution of this paper is presenting the idea of dynamic access control in video surveillance while leaving the designing of dynamic access control model as a goal to be achieved in future research. Our model emphasizes this challenge and demands that the context of requestor is taken into consideration while granting the access.

To the best of our knowledge, no comprehensive access control mechanism in video surveillance has been proposed. An access control model proposed by Thuraisingham et al. [35] makes use of metadata extracted from the video streams. It presents a grammar that allows referring to video streams by the information contained within them, such as timestamp, location, events occurred and objects. Access privileges for operators can be specified using predefined credential expression templates based on their id, group and/or a set of credentials. The solution, however, offers a static access control model and does not allow the access privileges of an operator to be changed dynamically based on the changing context.

Finally, in a large-scale video surveillance systems requiring occasional access by multiple public organizations such as the police and fire-brigade, management of users is also a challenge. This may require using federated identity management allowing each participating organization to manage its own users. Existing federated identity

and access management solutions like SAML [36] and WS-Federation [37] may be investigated for this purpose.

Table 3 provides a list of future challenges in security of video surveillance systems. Each challenge refers to the related requirements given in Table 2. Based on our model and the discussion, it is evident that many security requirements in video surveillance systems still require further research in this domain. Certain privacy requirements are dependent on some security requirements as a result it is not possible to effectively ensure privacy without the security requirements being addressed. Protecting the privacy of individuals without compromising the functionality of the system demands an access control mechanism that makes use of privacy enhancing technologies in order to hide the privacy sensitive regions in the video frames while making them available when required. Clearly there exists a gap demanding further research in this domain in order to satisfy the security requirements in video surveillance systems and to increase their acceptability in society.

Table 3. Future research challenges in security of video surveillance systems

Security aspect	**Future research challenges**
1. Confidentiality	*1.1.* Novel efficient real-time encryption algorithms for large-scale video data from multiple sources (2a) *1.2.* Duration-specific key management techniques for data produced by several cameras (2b) *1.3.* Secure storage of video data and the associated metadata while enabling efficient retrieval (5b, 6a)
2. Integrity & Authenticity	*2.1.* Integrity protection solutions having robustness against benign modifications (3b, 3c) *2.2.* Scalable and efficient authenticity mechanisms for large-scale video surveillance data (4a, 4b)
3. Access authorization	*3.1.* Multiple privacy levels in the video surveillance data, making use of existing privacy enhancing techniques, with each level accessible to different access privileges (1c, 1e, 1f, 6g) *3.2.* Dynamic access control that enable preserving the privacy of people yet exposing maximum data to the operators when needed (6a, 6c, 6d, 6g) *3.3.* Novel access control mechanisms utilizing the indexing structure of video data and the extracted metadata (6a, 6b) *3.4.* Federated identity and access management solutions for access authorization of video surveillance data (6c, 6e)

6 Conclusion

Modern video surveillance systems provide an effective mechanism to combat security threats. Advanced functionalities offered by these systems, however, greatly threaten the privacy of the individuals under surveillance. Aside from protecting privacy from outside attackers by securing the video streams using cryptographic mechanisms, it is equally important to protect the privacy of individuals from the insider personnel involved in monitoring surveillance data. We identify the security and privacy requirements in a video surveillance system and outline a number of challenges and directions

for future research to accomplish these requirements. Our study unveils that existing solutions for security and access authorization in multimedia systems cannot be used in video surveillance hence further research efforts are required to devise security solutions in video surveillance. We have also outlined the further research challenges to be solved for ensuring the security of video surveillance systems.

References

1. Moncrieff, S., Svetha V., Geoff A.W.: Dynamic Privacy in Public Surveillance. Journal of Computer 42, 22-28 (2009)
2. Hampapur, A.: Smart Video Surveillance for Proactive Security. IEEE Signal Processing Magazine 25, 136 (2008)
3. Saini, M. K., Atrey, P. K., Mehrotra, S., Kankanhalli, M. S.: Privacy Aware Publication of Surveillance Video. International Journal of Trust Management in Computing and Communications 1, 23-51 (2013)
4. Frederic D., Ebrahimi T.: Scrambling for Privacy Protection in Video Surveillance Systems. IEEE Transactions on Circuits and Systems for Video Technology 18, 1168-1174 (2008)
5. Senior, A., Sharath P., Arun H., Lisa B., Ying-Li T., Ahmet E., Jonathan C., Chiao F.S., Max L.: Enabling Video Privacy Through Computer Vision. Journal of Security & Privacy 3, 50-57 (2005)
6. Cavallaro, A.: Privacy in Video Surveillance. IEEE Signal Processing Magazine 24, 168169 (2007)
7. Norris, C., Armstrong, G.: The Maximum Surveillance Society. Berg (1999)
8. Criminisi, A., Perez, P., Toyama, K.: Object Removal by Exemplar-Based Inpainting. In: 13th IEEE Computer Visioin and Pattern Recognition, pp. 721-728. IEEE (2003)
9. Criminisi, A., Prez, P., Toyama, K.: Region Filling and Object Removal by Exemplar-Based Image Inpainting. IEEE Transactions on Image Processing 13, 1200-1212 (2004)
10. Tang, F., Ying, Y., Wang, J., Ping, Q.: A novel texture synthesis based algorithm for object removal in photographs. In: 9th Asian Computing Science Conference, pp. 248-258. Springer (2004)
11. Schiff, J., Meingast, M., Mulligan, D. K., Sastry, S., Goldberg, K.: Respectful cameras: Detecting visual markers in real-time to address privacy concerns. In: Senior, A. (eds.) Protecting Privacy in Video Surveillance, pp. 65-89. Springer (2009)
12. Yu, X., Chinomi, K., Koshimizu, T., Nitta, N., Ito, Y., Babaguchi, N.: Privacy Protecting Visual Processing for Secure Video Surveillance. In: 15th IEEE International Conference on Image Processing, pp. 1672-1675. IEEE (2008)
13. Haritaoglu, I., Harwood, D., Davis, L. S.: W4: Real-Time Surveillance of People and their Activities. IEEE Transactions on Pattern Analysis and Machine Intelligence 22, 809-830 (2000)
14. Koshimizu, T., Toriyama T., Babaguchi N.: Factors on the Sense of Privacy in Video Surveillance. In: 3rd ACM Workshop on Continuous Archival and Retrival of Personal Experiences, pp. 35-44. ACM (2006)
15. Boult, T. E.: Pico: Privacy through Invertible Cryptographic Obscuration. In: IEEE Computer Vision for Interactive and Intelligent Environment, pp. 27-38, IEEE (2005)
16. Carrillo, P., Kalva, H., Magliveras, S.: Compression Independent Object Encryption for Ensuring Privacy in Video Surveillance.In: 9th IEEE International Conference on Multimedia and Expo, pp. 273-276, IEEE (2008)
17. Atrey, P. K., Yan W., Kankanhalli M.S.: A Scalable Signature Scheme for Video Authentication. Journal of Multimedia Tools and Applications 34, 107-135, Springer (2007)

18. Schneider, M., Chang, S.: A Robust Content Based Digital Signature for Image Authentication. In: International Conference on Image Processing,pp. 227-230, (1996)
19. Sun, Q., He D., Tian, Q.: A Secure and Robust Authentication Scheme for Video Transcoding. IEEE Transactions on Circuits and Systems for Video Technology 16, 1232-1244 (2006)
20. Winkler, T., Rinner, B.: Securing Embedded Smart Cameras with Trusted Computing. EURASIP Journal on Wireless Communications and Networking, 2011:20 (2011)
21. Winkler, T., Rinner, B.: TrustCAM: Security and Privacy-Protection for an Embedded Smart Camera Based on Trusted Computing. In: 7th IEEE Advanced Video and Signal Based Surveillance, pp. 593-600, IEEE (2010)
22. Winkler, T., Rinner, B.: A Systematic Approach Towards User-Centric Privacy and Security for Smart Camera Networks. In: 4th ACM/IEEE International Conference on Distributed Smart Cameras, pp. 133-141, ACM (2010)
23. Liu, X., Ahmet, M.E.: Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions. In: 2nd IASTED Conference on Communications, Internet & Information Technology, (2003)
24. Liu, F., Koenig H.: Puzzlea Novel Video Encryption Algorithm. In: 9th International Conference on Communications and Multimedia Security, pp. 88-97. Springer (2005)
25. Socek, D., Magliveras S., Marques O., Kalva H., Furht, B.: Digital Video Encryption Algorithms Based on Correlation-Preserving Permutations. EURASIP Journal on Information Security (2007)
26. Liu, F., Hartmut K.: A Survey of Video Encryption Algorithms. Journal of computers & security 29, 3-15 (2010)
27. Haskell, B.G., Puri A., Netravali A.N.: Digital Video: an Introduction to MPEG-2. Kluwer Academic Publishers (1998)
28. Schaffer, M., Peter, S.: Video Surveillance: a Distributed Approach to Protect Privacy. In: 9th International Conference on Communications and Multimedia Security, pp. 140-149, Springer (2005)
29. Liu, Z., Peng D., Zheng Y., Liu J.: Communication Protection in IP-Based Video Surveillance Systems. In: 7th IEEE International Symposium on Multimedia, pp. 69-78. IEEE (2005)
30. Castiglione, A., Cepparulo M., Santis A.D., Palmieri F.: Towards a Lawfully Secure and Privacy Preserving Video Surveillance System. In: 11th International Conference on E-Commerce and Web Technologies, pp. 73-84. Springer (2010)
31. Brin, D.: The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom, Perseus Publishing (1999)
32. Bertino, E., Fan J., Ferrari E., Hacid M., Elmagarmid A.K., Zhu X.: A Hierarchical Access Control Model for Video Database Systems. ACM Transactions on Information Systems 21, 155-191 (2003)
33. Bertino, E., Moustafa A.H., Walid A.G., Elmagarmid, A.K.: An Access Control Model for Video Database Systems. In: 9th International Conference on Information and Knowledge Management, pp. 336-343. ACM (2000)
34. Pan, L., Zhang C.N.: A Web-Based Multilayer Access Control Model for Multimedia Applications in MPEG-7. International Journal of Network Security 4, pp. 155-165 (2007)
35. Thuraisingham, B., Lavee G., Bertino E., Fan J., Khan L.: Access Control, Confidentiality and Privacy for Video Surveillance Databases. In: 11th ACM Symposium on Access Control Models and Technologies, pp. 1-10. ACM (2006)
36. Security Assertion Markup Language, OASIS Standard, http://saml.xml.org/wiki/saml-introduction
37. Web Services Federation Language (WS-Federation) Version 1.2, http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html