A Socio-Technical Approach for Event Detection in Security Critical Infrastructure

Philipp Blauensteiner, Martin Kampel
Institute of Computer Aided Automation
Vienna University of Technology, Austria
{blau, kampel}@prip.tuwien.ac.at

Christoph Musik, Stefan Vogtenhuber
Institute for Advanced Studies
Vienna, Austria
{musik, vogten}@ihs.ac.at

Abstract

In recent years, surveillance and monitoring have become topics of increased interest for not only research active in computer vision, but also for many scholars in the field of social sciences and the humanities. Joint research becomes important when effective surveillance systems are deployed in public spaces. This paper focuses on designing and developing a socio-technical surveillance application in a security critical infrastructure like a bank. The technical system presented is designed to detect specific events like abnormal or suspicious behaviour. A close collaboration between scientists from Computer Science and Sociology actively reflects the development of the new surveillance technology. The novelties of the paper are rather a socially intelligent surveillance system coordinating human and non human actions then technical achievements. Based on interviews several behaviours of interest as well as an interaction between the system and its users are defined. Experiments and results are shown based on a real life installation.

1. Introduction

The goal of our inter- and transdisciplinary research project is to develop a system for automated event recognition within security-critical infrastructure. More specifically, a smart CCTV system is to be designed and implemented in the customer area of a bank branch not only to support and improve investigation but to prevent crimes by detecting suspicious behaviour. Thus, one of the main questions is whether "abnormal or suspicious behaviour" can be identified in the context of a bank and if yes, how this can be translated into a program code of the technical system. Designing and implementing a socio-technical surveillance application in close collaboration between scientists from different disciplines (Computer Science and Sociology) and consumer bodies (Bank, Austrian Federal Police Office, and a Software Consulting company) from the very beginning offer the genuine possibility to not only getting inside the production and implementation of software, but to actively reflect, design and shape this process during the development of new intelligent surveillance technologies. This also involves the participation of bank customers, bank officers and security personnel in this specific case. Integrating the views of relevant stakeholders and social groups as well as cultural aspects in the development of surveillance systems can be regarded as a precondition for a successful implementation of such a system. This is especially important to note here, because we know that technological systems can fail or collapse, if they are designed inappropriate and do not suit employee's needs [14]. For example, staff members of the bank could be overstrained by a high alarm rate, resulting in a loss of attention to possible detections. Yet alone the use of the word "alarm" might be counterproductive (see Section 4.3). One consequence is that a system under development must support the complex sociality of the specific work setting, in which it is going to be implemented [11]. The production of code, which classifies and categorises behaviour, cannot be successful without taking into account the specific situated action [26] and setting. This setting can be historically, geographically, socially and culturally diverse. Furthermore the development of a new intelligent surveillance system must take into account the distribution of actions in socio-technical work practices. This means that technology is distributed to actions of humans, machines and programs altogether [24]. There are many different human as well as non-human actors involved and they all have different actions and tasks that have to be co-ordinated. We speak about a socio-technical approach, because the event detection is especially distributed to the technical system and to the bank officers using the system. How much autonomy is going to be allowed for the technical surveillance system? What kind of and to what extent is intervention possible for the bank officer? And how transparent the system should be for the bank officer? To add a data protection and civil rights view here, the question of

978-1-4244-7028-0/10/$26.00 ©2010 IEEE

how transparent an algorithmic surveillance system should be for the "watched" emerges here.

The remainder of the paper is organised as follows: Section 2 gives an overview of the related work. Section 3 discusses the specific scenario of bank robberies as a testcase for describing possibilities of prevention and investigation. In Section 4, the surveillance framework applied within the project is presented. Section 5 concludes this paper.

2. Related Work

Since we are dealing with an inter- and transdisciplinary research project, this section is divided into two parts. Firstly, we give an overview of the current research in the area of surveillance studies, followed by a brief discussion of the state of the art for visual surveillance and event detection systems.

2.1. Surveillance Studies

In recent years, surveillance and monitoring have become topics of increased interest for not only researchers active in computer sciences, but also for many scholars in the field of social sciences and the humanities. After a brief introduction to the field of "surveillance studies", we focus on algorithmic surveillance technologies and the matter of classification in this context. We show that classification processes being inscribed in technology and software can have serious consequences like the discrimination of specific social groups or individuals.

Seeing that there is a considerable number of publications about surveillance and the notion of surveillance society, it is now possible to speak of "surveillance studies" as a distinct academic discipline [9]. Surveillance studies are mainly dealing with "the rapidly increasing ways in which personal details are collected, stored, transmitted, checked, and used as means of influencing and managing people and populations" [18]. Here has to be mentioned that surveillance may be not only technologically mediated, but also direct or face-to-face [18]. Beginning in the 1990s there has been a qualitative transformation of surveillance which among others can be explained by the computerization of surveillance practices [32]. In this context the term algorithmic surveillance was coined by Norris and Armstrong in their pioneering book "The Maximum Surveillance Society" [3] and was also adopted by Introna and Wood in the context of Facial Recognition Systems [12]. The latter define algorithmic surveillance as surveillance that makes use of automatic step-by-step instructions and especially of computer systems to provide more than the raw data observed. One crucial aspect in this process is both in the technical video surveillance context and in social surveillance studies classification and categorization of behaviour or groups. In computer vision and pattern recognition classification means to decide whether a specific behaviour is suspect or not-suspect, usual or unusual, normal or abnormal and so on. In surveillance studies the term classification has to be understood as social sorting and therefore tends to highlight social and economic categories [19, 20]. Another important aspect of classification as social sorting is the production of computer codes by which personal data is organised with a view to influence and manage people by redefining behaviour expectations [19]. There is no clear understanding of how suspicious or abnormal behaviour in a specific context looks like, it has to be defined. So the production of a computer code contains the production of suspectedness in such a case. The crux of the matter is that classification, especially relating to computer codes, does never occur in an objective or neutral way, in each specific case it has a career and may be biased. Bowker and Star see software as "frozen organizational and policy discourse" [6], in which policy is coded into software. In this view, software is, like technology, society made durable [16]. This means that specific social practices, norms and cultural values are either consciously or tacitly inscribed in the software. A characteristic of classification is that it can create advantage and disadvantage for individuals or social groups [6]. This can have consequences especially for those singled out for attention [18]. But it is not only the individual person singled out, in some circumstances classification processes may have profound effects on the shaping and ordering of human life in general, creating new social classes [18]. behaviour of certain social groups or individuals may also be shaped by classification, for example when they get feedback to fit an expected pattern of behaviour [18]. The consequences of classification can be serious and in specific cases the grounds of discrimination, especially when the classification processes are biased. Socially intelligent surveillance or monitoring has to bear in mind these possible consequences when producing classification codes. There are often subtle ways in which they are created. These ways have to be made visible before such a policy will start to make a difference [18].

2.2. Visual Surveillance and Event Detection

A variety of methods have been proposed to detect and recognise events of interest in video sequences. Ali and Shah [1] use optical flow information to derive kinematic features such as divergence and flow-fields in order to recognise human actions in image sequences. However, the proposed features are not view-invariant. Furthermore, the approach fails in presence of moving occlusions.

Lavee et al. [17] propose a framework for event detection based on the assumption that actions and events can be regarded as temporal stochastic processes [30]. Local features at various temporal scales are taken as samples for the distributions. Clustering is applied on these samples,

thus gaining a non-paramterical model of different events in videos. This approach has its merits in a context where no a-priori knowledge of the possible events is available. In the specific application discussed in this paper, this knowledge is not only available, but the events of interest have to be clear to the operators (bank staff) and, if possible, to the customers (as discussed in the next section).

Zhang and Gong [31] utilise hidden conditional random fields in order to categorise human actions based on silhouette-based features. However, in presence of occlusions, obtaining these features poses a severe problem. Since the video input in our project suffers from a high level of occlusions, a robust extraction of the silhouettes cannot be guaranteed.

Another group of event detection algorithm is based on trajectory analysis: Ma and Li [21] use fuzzy support vector machines on the trajectories in order to recognise suspicious events. Piciarelli and Foresti [23] apply on-line clustering for the trajectory classification. Parameswaran and Chellapa [22] model events in term of trajectories and body view invariant poses. Calderara et al. [7] analyze the shape of trajectories in their surveillance and forensic application. The main advantage of this group of algorithms is that there exists a plethora of pedestrian tracking algorithms, that hold for real-time constraints and deliver reliable results for the event detection:

Siebel and Maybank [25] use a combination of a region tracker and an active shape tracking algorithm in order to track pedestrians also in crowded scenes. Seitner and Lovell track pedestrians based on color features and spatial information. Fuentes and Velastin [8] propose a blob tracker, utilizing the input of a simple luminance based motion detector. Kahn and Shah [13] use a multi-view approach with an early fusion stage to reliably track people even in occluded areas. Andriluka et al. [2] combine pedestrian tracking and pedestrian detection, in order to overcome the weaknesses of each approach.

3. Prevention and Investigation of Bank Robberies in Austria

Possible approaches aiming at the prevention of criminal acts like bank robberies are through criminal prosecutions or the adaption of a wide range of opportunity structures [10]. For investigation, pictures of CCTV cameras are very useful. In case of a bank robbery, the security staff has to browse through the recorded material manually in order to get video material of the crime scene. For prevention, CCTV cameras do not act as a deterrent. But security experts of the bank and of the Austrian Federal Police Office proceed on the assumption that virtually all bank robbers explore the branch of the bank in order to get information about staff and spatial structure. In addition to that, there is the assumption that potential robbers will choose another bank branch, if they are addressed in person by a staff member during the spy out within the bank. And, the security experts mentioned their gut feeling that those potential robbers exploring a bank branch when preparing the crime can be detected. In order to clarify the possibility to use this "gut feeling" to design a smart system that automatically detects suspicious behaviour, we carried out interviews with security experts and staff members, visited special security training seminars of staff members including simulations of bank robberies, and talked to various other experts in the field of surveillance, data protection and civil rights. One important statement is that in this specific case the ground truth of suspicious behaviour is not there from the beginning, but has to be defined first. Tacit and practical knowledge has to be transformed into explicit knowledge, it has to be segmented in simple and distinct commands to be able to form a ground truth [24]. This first sociological step led to a predefinition of suspicious behaviour of interest in cooperation with all project partners. This includes staying at the bank foyer without using a machine (e.g. the ATM), without interacting with a member of staff over an extended period of time or staying at a machine for an unusual long time. However, we were unable to gather accurate knowledge about the actual behaviour of bank robbers exploring objects. Thus the determined criteria remained questionable regarding their relevance for implementing an effective and applicable system. So in a further step we analyzed the behaviour of people staying in a bank branch to learn about the "usual" or "normal" behaviour of bank customers. For this purpose we used the method of non-participant observation combined with video-analysis in Social Research [15]. The observation aimed at describing and analyzing social space, actions, interactions between humans and interactivities between humans and machines in a bank branch. Within four observation sessions (two non-participant directly in two different bank branches, and two based on video recordings in another branch) we got a sample of 236 people. These three branches are quite typical for Austria, with foyer sizes of about 20 to 30 square meters. The foyers are equipped with about 6 machines (2 ATM, 2 bank statement printers, cash deposit machine, prepayment meter) and offer the possibility to enter bank transfers. The machines are also accessible outside opening hours between 5 am and 12 pm. To open the door, one have to insert an ATM card, a customer card. Of course it is not unusual to slip in with another customer. During opening hours, usually one staff member is serving at the counter. The observations in the branches were conducted in July 2009 after lunch break and outside weather conditions were warm and dry. Most of the observed customers entered the bank branch alone (86.4%). Ten persons have been wearing sunglasses and 35 persons wearing a head covering (hat, cap, beanie, or headscarf) in-

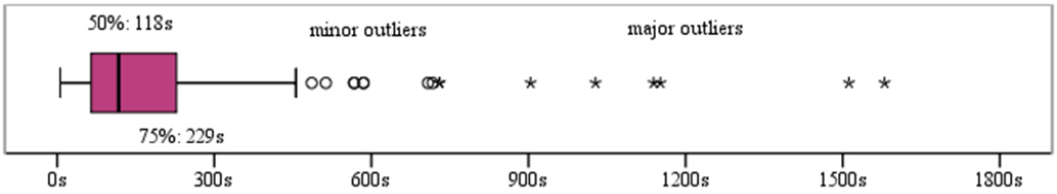

Figure 1. Customer's duration of stay in bank foyers in seconds. n=236, median=118s, IQR=164s

side the bank. People are on average 3 min. 53 sec. (median 02 min. 13 sec.) inside a bank branch. This includes also those persons that are going through the foyer to an office for further talks with bank officers. The average time of people staying only in the foyer (where machines like ATM, bank statement printer etc. as well as bank counters can be found) is 03 min. 08 sec. (median 01 min 58 sec., see Figure 1). Three quarters of these people are staying in the branch within a period of 03 min. 49 sec. There have been 38 out of 236 people (16%) staying longer than 5 minutes and 10 out of 236 (4%) staying longer than 10 minutes. The outlier percentage concerning attendance time of bank clients is quite high, so a simple detection of those is on the one hand not practically, on the other hand there is no evidence for a longer attendance time being unusual or even suspicious behaviour. In fact, all longer attendance time periods can be explained and appear as usual behaviour: Many bank clients had to wait in the line in front of ATM or bank counter, others had problems with a machine, calling and waiting for a bank officer, and some just took their time filling in a transfer form.

Facing people staying at the bank foyer without using a machine (e.g. the ATM) or without interacting with a member of staff over an extended period of time could be another interesting point. 17 out of 236 (7%) people entering and leaving a bank branch did not do any usual activity: almost 50% of these accompanied somebody performing an usual activity. The other half has been inside the bank foyer for a very short period of time. Most of these just had a glimpse inside noticing many people standing in the line. An elder man seemed to be confused.

One main conclusion of our observation is that usual behaviour in bank foyers is very diverse, although the specific context of a bank determines the expected human behaviour to a considerable extent. There is a great range of different behaviour, making the detection of unusual or suspicious behaviour difficult. One way could be to detect those with a specific deviation from the mean. In our view this is questionable, because on the one hand there is no evidence that those differing from the mean are suspicious. Additionally we have information that many bank robbers exploring a bank branch behave like ordinary customers or even are bank customers. On the other hand, in the case of detecting those with a specific deviation from the mean the usual would become the normative. This may have serious consequences for the watched: The pressure to adapt may increase for those entering a bank foyer. And if they do not behave flawlessly, they might provoke adverse consequences. They do not want to do anything wrong, and if they do so, they have to fear adverse consequences. Those diverging from the norm are coming to the fore instead of real bank robbers. One must consider that the detection of suspicious behaviour of bank robbers is like finding a needle in a haystack. In Vienna's 512 bank branches there are estimated 70 million people entering and leaving a bank branch in one year. By comparison there have been 63 bank robberies in Vienna in 2008.

Interviews with the Austrian Data Protection Commission as well as with other civil rights advocates raised concerns about the proportionality principle: They question the pre-emptive aspect and indicate proportionality only in the case of a criminal offence. Every video surveillance measure should be reviewed, if it really is proportionate and if there are any alternatives. In the case of bank robbery there are many other possible ways to prevent further bank robberies, e.g. through criminal prosecution or the adaption of opportunity structures [10]. Many bank officers name guards in the bank foyer to offer the best security.

4. The Surveillance System

As depicted in the previous sections, the main focus of our system is two-fold: to detect situations of interest to inform the members of staff on the one hand and to gather forensic data and to label suspicious situations for later investigation (in case an incident actually has taken place) on the other hand. Therefore, the system has to work in real-time and to provide a resolution as high as possible.

4.1. The Setup

In order to create a real-world testbed for bank surveillance, six indoor cameras, one outdoor camera and a dynamic PTZ camera were installed in the foyer of a bank branch in Vienna. The intrinsic and extrinsic calibration data of the static cameras is known.

The video streams are subject to motion detection and shadow suppresion [5]. The foreground-regions are input to the tracking system, which itself consists of a combina-

tion of several trackers (namely, a blob tracker and an active shape tracker, similar to [25]). At this time, the tracking is conducted on each camera separately. The tracked targets are mapped to the ground plane, where a single representation of the scenes activity is modelled by data fusion according to [4].

This setup allows real-time tracking ($>$ 10 fps) on 800×600 images using one CPU core per camera on a standard workstation (Xeon 8x2.0 GHz, 8 GB RAM). However, it has its limits in the bank's peak-time – typically on Monday at lunch time – where more than 20 customers may be present in the foyer of approximately 30 square meters.

4.2. Trajectory Analysis

Based on the sociological findings discussed in the previous sections, amongst others, the following scenarios of interest were defined, which can be detected by means of trajectory analysis:

1. wandering around in the branch without using a machine (e.g., the ATM) or contacting a member of staff over an extended period of time
2. operating a machine over an unusual long period of time
3. more than one person operating a machine at the same time
4. people moving fast or running around

In order to analyze the trajectories for behaviour of interest, the foyer was divided into several areas, namely device zone, counter zone, table zone; the remaining area was defined as open area (see Figure 2). If a person is standing within a designated zone, the person is marked as *operating*. People in the open area may be *queueing*, *standing* or *moving*. To determine if a person is queuing, an action radius is defined. A person is marked as queueing, if another person within this action radius is either queueing or operating a device.

In order to detect Scenario 1, the history of a person is analyzed. The trajectory of a normal acting person is shown in Figure 3 together with the trajectory of a behaviour of interest. In the latter case, no actual action was undertaken. For Scenario 2, temporal thresholds were defined based on the average time spend to operate a certain device, to use the table (e.g. for filling out forms) and to interact with bank staff at the counter. The average speed of a person (Scenario 3) can be calculated directly since we are dealing with a calibrated setup.

4.3. The Interaction

The interviews with members of staff and unionists delivered insight, which influenced the system's user interaction. Wordings as "alarm" and "suspicious behaviour" have to be avoided, since it signals a potentially dangerous situation and bank clerks argue that they are employed to serve customers and not to serve as security agents. The

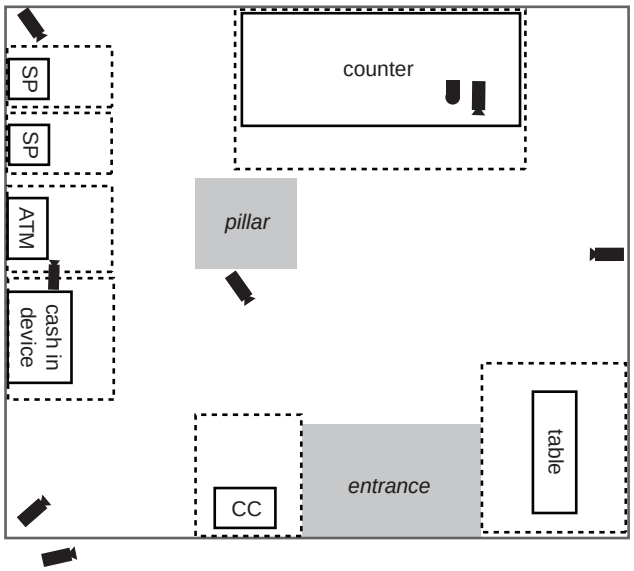

Figure 2. Sketch of the foyer including the position of the 7 static and the PTZ camera, the position of the counter and of the devices (SP: statement printer; CC: coin counting device). The dashed lines mark the zones of the

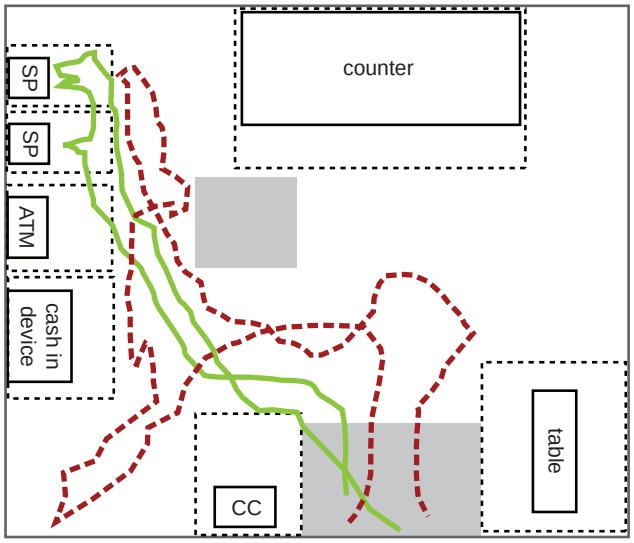

Figure 3. Two sample trajectories plotted onto the ground map. The solid green line shows a normal trajectory extracted during the normal operation of the system. The dashed red line represents a trajectory of a behaviour of interest, since no interaction with a device was detected - the data was acquired in a special session where suspicious behaviour was re-enacted under the supervision of the bank's security expert.

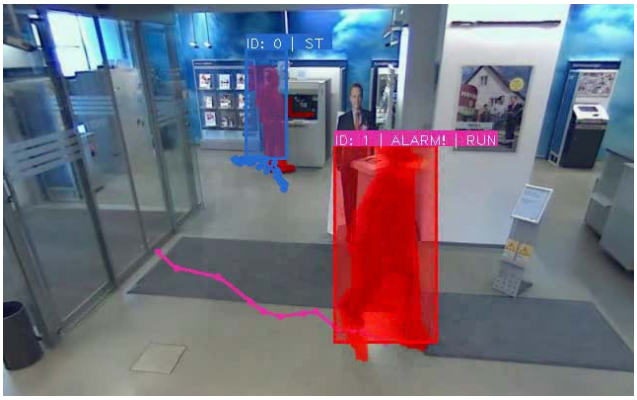

Figure 4. Examplaric situation for Scenario 3: the system detected a running person.

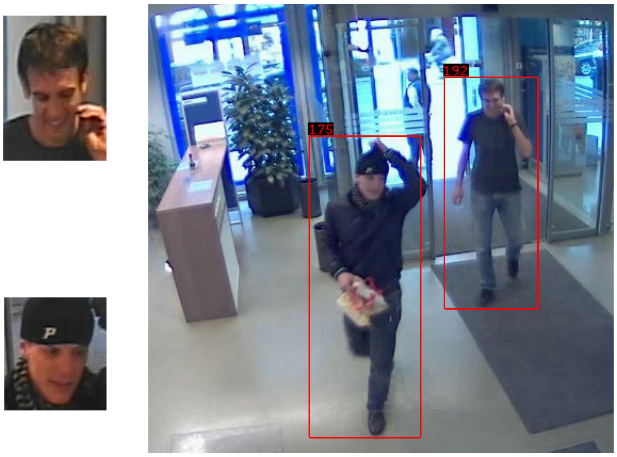

Figure 5. Detected persons with the estimated height and the higher quality facial image. The face images were recorded by the PTZ camera.

very same argumentation was also used in the perspective of false alarms: the members of staff - as end users - do not want to be disturbed "too often" by the system. Additionally, resentments occured due to the fact, that the members of staff fear that they are made responsible, if they misjudge a situation and classify a system notification as false alarm.

In case of contacting a member of staff, the facial image of the person of interest is transmitted together with the description of the scenario detected.

In case a crime cannot be prevented, the system should be able to provide information usable by the police, such as a detailed high-quality view f the face and an accurate estimation of the size of a suspect (see Figure 5). Facial images (gathered by a combination of the tracker and a face detector [27]) are stored together with image sequence and the trajectory information [29]. Since the extrinsic calibration of the cameas is availble, extracting the height of a person is straight forward.

	Tag Video		Contact staff	
	DR	**FAR**	**DR**	**FAR**
Scenario 1	0.8	0.3	0.65	0.1
Scenario 2	0.8	0.2	0.7	0.05
Scenario 3	0.95	0.05	0.8	0

Table 1. Preliminary Results - Detection Rate (DR) vs. False Alarm Rate (FAR)

4.4. Evaluation

As mentioned in the previous section, availability for real life video material of suspicious behaviours is limited. In order to obtain data for evaluating the system, in addition to real life recordings such behaviours were re-enacted on site under the supervision of security experts responsible for the bank's internal security trainings.

In order to evaluate the system, video sequences were chosen and labelled manually according to the findings depicted in the previous sections. The true positive sequences showing behaviour of interest were taken from the re-enacted recordings, whereas the true negatives were chosen from the real life videos.

The results of our preliminary evaluation are shown in Table 1. Following the results of the interviews, for each scenario two thresholds have been defined based on the empirical observations in the bank: a threshold for marking a scene as suspicious in the video archive and a second threshold (including the minor outliers observed, see e.g., Figure 1) for contacting a member of staff. This is to ensure a high detection rate at tagging sequences of interest for later scrutiny (if necessary), while at the same time granting a low false alarm rate for contacting employees and therefore not bothering the staff with a high amount of system messages and thereby lowering the acceptance of the system.

5. Conclusion and Discussion

In this paper we presented a recent inter- and transdiciplinary research project for surveilling the customer area of bank branches. We analyzed the current situation in technological as well as in sociological context. Based on the results of interviews with bank staff and security experts, we devised several behaviours of interest and defined the interaction between the system and the members of staff.

An open issue is the performance during the peak time. To overcome the problems of large scale occlusion, further investigation in early fusion (as proposed in [13]) are going to be undertaken. Furthermore, an in-depth evaluation of the system as well as of the underlying tracking process (such as depicted in [28]) has yet to be conducted.

In our view a socially intelligent surveillance system has to be a socio-technical system, which co-ordinates human and non-human actions. Such a system has to take situ-

ated actions [26] and situated settings into account. This is essential, because there is no distinct definition of suspicious behaviour in bank branches. In providing hints of unusual behaviour, the system can contribute to heighten attention of bank officers, which maybe can have positive effects for preventing bank robberies. Bank officers can follow a hint and confirm or falsify it by using their location- and situation-dependent, practical knowledge, which is impossible to integrate in a generalised system. E.g., if the system detects a man standing in the bank foyer for an extended period of time not using a machine or interacting with any member of staff, this does not indicate anything about his intention. The man can come to meet his wife working in the bank, he can be confused because he is a foreigner and does not know how to behave, he can take cover from rain or, highly improbable but possible, to explore the bank foyer preparing for a bank robbery. In any case the bank officer can apply the attention to this man and see, if it is necessary to address him. Hugely important is the notion that no person detected by this system is suspicious, but is standing there for a specific period of time doing nothing. This has to be made clear to bank staff operating with the system. Otherwise they can get the impression everybody being detected is a potential bank robber. Consequences of this impression can be false alarm, fear and insecurity.

Acknowledgement

This work was supported by the Austrian Research Promotion Agency (FFG) under the KIRAS initiative (project *tripleB ID, number 818783).*

References

[1] *S. Ali and M. Shah. Human action recognition in videos using kinematic features and multiple instance learning.* IEEE Transactions on Pattern Analysis and Machine Learning*, 32(2):288–303, 2010.*

[2] *M. Andriluka, S. Roth, and B. Schiele. People-tracking-by-detection and people-detection-by-tracking. In* Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR 2008)*, 2008.*

[3] *G. Armstrong and C. Norris.* The Maximum Surveillance Society: The Rise of CCTV. *Berg publishers, Oxford, 1999.*

[4] *J. Batista. Tracking Pedestrians under Occlusion using Multiple Cameras. In* Proc. of the Intl. Conf. on Image Analysis and Recognition*, pages 552–562, 2004.*

[5] *P. Blauensteiner, H. Wildenauer, A. Hanbury, and M. Kampel. Motion and Shadow Detection with an Improved Colour Model. In* Proc. of the IEEE Int. Conf. on Signal and Image Processing (ICSIP06)*, Hubli, India, Dec 2006.*

[6] *G. Bowker and S. Leigh Star.* Sorting Things Out. Classification and its Consequences*. The MIT Press, Cambridge and London, 2000.*

[7] *S. Calderara, A. Prati, and R. Cucchiara. Video surveillance and multimedia forensics: an application to trajectory analysis. In* MiFor '09: Proceedings of the First ACM workshop on Multimedia in forensics*, pages 13–18, Beijing, China, 2009. ACM.*

[8] *L. Fuentes and S. Velastin. People tracking in surveillance application.* Image and Vision Computing*, 24(11):1165–1171, November 2006.*

[9] *B. Goold. Editorial. Making Sense of Surveillance in Europe.* European Journal in Criminology*, 6(2):115–117, 2009.*

[10] *C. Hille.* Handbuch Bankraub*. digidruck, Wien, 2008.*

[11] *J. Hughes, J. O'Brian, T. Rodden, and M. Rouncefield.* Workplace Studies. Recovering Work Practice and Informing System Design*, chapter Ethnography, Communication and Support for Design, pages 187–215. Cambridge University Press, 2000.*

[12] *L. Introna and D. Wood. Picturing algorithmic surveillance: The policies of facial recognition systems.* Surveillance and Society*, 2(2/3):177–198, 2004.*

[13] *S. M. Khan and M. Shah. Tracking multiple occluding people by localizing on multiple scene planes.* IEEE Transactions on Pattern Analysis and Machine Intelligence*, 31(3):505–519, 2009.*

[14] *H. Knoblauch and C. Heath. Technologie, interaktion und organisation: Die workspace studies.* Swiss Journal of Sociology*, 25(2):163–181, 1999.*

[15] *H. Knoblauch, B. Schnettler, J. Raab, and H. Soeffner.* Video Analysis: Methodology and Methods. Qualitative Audiovisual Data Analysis in Sociology. *Peter Lang Publishing, frankfurt am main edition, 2006.*

[16] *B. Latour.* A Sociology of Monsters: Essays on Power, Technology and Domination*, chapter Technology is Society Made Durable, pages 103–131. Routledge, 1991.*

[17] *G. Lavee, L. Khan, and B. Thuraisingham. A framework for a video analysis tool for suspicious event detection. In* MDM '05: Proceedings of the 6th international workshop on Multimedia data mining*, pages 79–84, New York, NY, USA, 2005. ACM.*

[18] *D. Lyon. Editorial. surveillance studies: Understanding visibility, mobility and the phonetic fix.* Surveillance and Society*, 1(1):1–7, 2002.*

[19] *D. Lyon, editor.* Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination*. Routledge, London and New York, 2003.*

[20] *D. Lyon.* Surveillance Studies: An Overview. *Polity Press, Cambridge and Malden, 2007.*

[21] *Y. Ma and M. Li. Detection for Abnormal Event Based on Trajectory Analysis and FSVM. In* International Conference on Intelligent Computing*, pages 1112–1120, Qingdao, China, 2007.*

[22] *V. Parameswaran and R. Chellappa. View invariance for human action recognition.* Intl. Journal of Computer Vision*, 66:81–101, 2006.*

[23] *C. Piciarelli and G. Foresti. On-line trajectory clustering for anomalous events detection.* Pattern Recognition Letters*, 27(15):1835–1842, 2006.*

[24] *W. Rammert.* Technik - Handeln- Wissen. Zu einer pragmatischen Technik- und Sozialtheorie*. VS-Verlag für Sozialwissenschaften, Wiesbaden, 2007.*

[25] *N. Siebel and S. Maybank. Fusion of multiple tracking algorithmis for robust people tracking. In* Proc. of the 7th European Conf. on Computer Vision (ECCV 2002)*, Copenhagen, Denmark, 373–387 2002.*

[26] *L. Suchman.* Human-Machine Reconfigurations. Plans and Situated Actions. *Cambridge University Press, 2nd editoin edition, 2007.*

[27] *P. Viola and M. Jones. Robust real-time face detection.* International Journal of Computer Vision*, 57(2):137–154, 2004.*

[28] *H. Wu, A. C. Sankaranarayanan, and R. Chellappa. Online empirical evaluation of tracking algorithms.* IEEE Transactions on Pattern Analysis and Machine Intelligence*, 99(PrePrints), 2009.*

[29] *S. Zambanini, P. Blauensteiner, and M. Kampel. Automated Multi-Camera Surveillance for the Prevention and Investigation of Bank Robberies in Austria: A Case Study. In* 3rd International Conference on Imaging for Crime Detection and Prevention*, page P31, London, United Kingdom, Dec. 2009.*

[30] *L. Zelnik-Manor and M. Irani. Event-based analysis of video. In* Proc. of the IEEE Conf. on Computer Vision and Pattern Recognition (CVPR 2001)*, volume 2, pages 123–130, 2001.*

[31] *J. Zhang and S. Gong. Action categorization with modified hidden conditional random field.* Pattern Recognition*, 43:197–203, 2010.*

[32] *N. Zurawski.* Surveillance Studies. Perspektiven eines Forschungsfeldes*, chapter Einleitung, pages 7–24. Barbara Budrich, Opladen and Farmington Hills, 2007.*