

Increasing the Security at Vital Infrastructures: Automated Detection of Deviant Behaviors

Gertjan J. Burghouts*^a, Richard den Hollander^a, Klamer Schutte^a
Jan-Willem Marck^a, Sander Landsmeer^b, Eric den Breejen^a
^aTNO, The Hague, ^bS&T, Delft, The Netherlands

ABSTRACT

This paper discusses the decomposition of hostile intentions into abnormal behaviors. A list of such behaviors has been compiled for the specific case of public transport. Some of the deviant behaviors are hard to observe by people, as they are in the midst of the crowd. Examples are deviant walking patterns, prohibited actions such as taking photos and waiting without taking the train. We discuss our visual analytics algorithms and demonstrate them on CCTV footage from the Amsterdam train station.

Keywords: Abnormal behavior, automated detection, pattern recognition, tracking, features, observables, CCTV.

1. INTRODUCTION

Amsterdam, The Netherlands, 27th of May 2010. The national security authorities call out to secure the area around the central train station. 150 Security officers, both military and police, are instructed to guard the area and to report people of whom the behavior is deviant. Here, ‘deviant’ is relative to what is normal at a train station, with all its commuters.

At TNO, psychologists have compiled a list of deviant behaviors. Some are very subtle and therefore better observed by human professionals. Others are hard to observe in the midst of the crowd, for instance, deviant walking patterns. For these cases, we have developed visual analytics. Our approach starts with tracking people, including re-tracking a person after occlusions. From the tracking and bounding box, more detailed behavioral indicators are extracted, using both whole-body and patch-based features. Our visual analytics software is able to detect the deviant trajectories, aggression, and suspicious interactions between people.

We have experimented with the four hours of video data that were recorded at Amsterdam Central Station. The data is very challenging: 100s of people, partially visible, many trajectories, similar clothes. In this presentation, we will show our tracking algorithm, behavioral features and the inference of which behaviors are deviant. We show our recent work that multiple indicators together are discriminative: the ‘0+0+0=1’ principle. Our results discover persons who are avoiding the police, taking photos where this is not allowed, and waiting without taking the train.

Contribution of this paper

In this paper, we provide insight in the Amsterdam experiment and what type of abnormal behaviors are observed around this train station, the second largest in the Netherlands. The objective of this paper is to give the reader a view on the type of indicators that follow from our psychology research and how they can be translated into technology to aid in the process of monitoring people’s behavior at one of the most important infrastructures in the Netherlands. To demonstrate this, we show some examples of behaviors that were automatically detected during the experiment. We motivate the need for a carefully designed monitoring concept where humans and machines complement each other. Finally, we share our conclusions from this experiment. Our findings are summarized at the end of this paper.

As implementation and surveying is not the goal of the paper, we briefly mention some algorithms and methods, without discussing or referencing related literature. For those readers who are interested in the background of the results presented in this paper, or more pointers to literature, we have included a few references to our recent work, at the end of this paper.

* gertjan.burghouts@tno.nl

2. A REAL-WORLD EXAMPLE OF A THREAT

On July 31, 2006, two suitcase bombs were placed on commuter trains at the Cologne main train station. One of the suitcases was put on a train headed for the city of Hamm, north of Cologne, and the other was deposited on a train headed for Koblenz, south of Cologne. The suitcase in the northbound train was discovered in Dortmund, and the other bomb was found when the southbound train reached Koblenz. Because of a minor design flaw involving the amount of fuel placed in the bombs, detonators set for 2:30 p.m. failed to ignite the charge.

A closer look at the persons who placed the bombs, learns that they arrived together at this train station, while after a while they separate and pretend that they do not know each other. This is summarized in Figure 1. The images that are used in the figure, are obtained from public resources. The two men split after a while. This is abnormal behavior. In this case, such an abnormality is very informative about the threat that they posed later. This motivates the search for particular behaviors that may hint at hostile intentions.

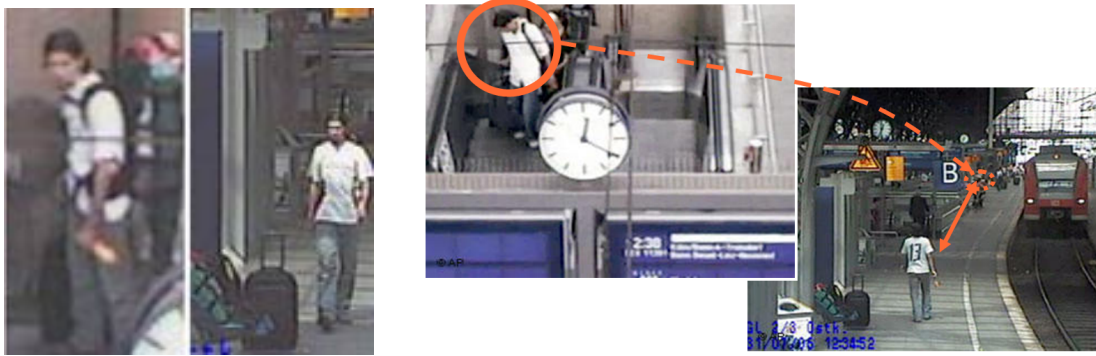


Figure 1. Footage from the Cologne threat, illustrating the motivation to search for abnormal behaviors: two men arrive together but split later to continue separately to place two explosives.

Train stations are arguably among the most vital infrastructures in a country. As airports have received the highest degree of attention with respect to security measures, the authorities have broadened their focus to train stations. Train stations are interesting because the required balance between security, comfort and free mobility of the traveller. A few potential suspects in the midst of 1000s of commuters every day, makes the train station an interesting testing platform. This motivates us to choose a train station as a vital infrastructure of interest.

3. OUR EXPERIMENT AT THE CENTRAL STATION OF AMSTERDAM

We choose the Amsterdam Central Station, the second largest train station in the Netherlands. On average 20K commuters everyday. The exercise of the police, as mentioned in the Introduction, gave us the opportunity to install our test equipment and to perform an experiment with our sensor technology.

3.1 Experimental setup

The location of the radar and cameras was above the entrance, at a height of approximately 5 m. The FMCW radar recorded in stereo, such that we were able to reconstruct a persons position later. The combination of wide and narrow field of view cameras gives both the overview and opportunity to see details. For more information on our sensors and the localization by the stereo radar, see our SPIE'09 paper [2].



Figure 2. The setup of our cameras and stereo radar at the Amsterdam Central Station.

3.2 Which behaviors are of interest?

Our psychologists made an analysis of the behaviors of interest, prior to the experiment, specific for a train station. In an earlier confidential study for the Netherlands' national coordinator on counterterrorism, a list was created of deviant behaviors. Although the list itself is confidential, the categorization of behaviors is public. The main discriminators of the deviant behaviors are location (this station is different from the station in Rotterdam, the difference with a football stadium is even bigger, e.g. because people need a ticket to get in), time (e.g. during rush hour it is much busier than around lunch time), type of threat (e.g. a pickpocket shows different behavior than a drug dealer) and, for about 7% of the behaviors, culture (e.g. Dutch and Asian people respond to authorities much differently). The deviant behaviors that are considered in this paper include abnormal walking patterns and particular actions that are not allowed at parts of the station.

4. HOSTILE INTENT TECHNOLOGY

Our sensor technology is coined "Hostile Intent Technology" (HIT). It is a collection of algorithms that together detect a set of relevant behaviors. The behaviors and examples of detections are discussed below.

4.1 Trajectory analysis

Usual walking patterns have the tendency to be straight towards a goal. There is little variation in heading orientation and velocity. Significant changes in the orientation and velocity may hint at interesting events. The recent history of the walking pattern can be stored in a histogram that captures the orientations and velocities over the last few seconds. Outliers of such histograms appeared to be very informative of people that try to avoid the police officers, like in Figure 1. This figure shows the track that was generated by our tracking algorithm. The overall algorithm consists of a foreground-background tracker and a person-matcher. The person-matcher is applied to re-connect tracks after temporary occlusions. This matching functionality is crucial in real-world situations such as illustrated in Figure 3.

Interactions between people have a very profound constellation in space and time. For instance, the gathering of a group of people looks like a star where all tracks end in the middle. This is illustrated in Figure 3, on the right. Few of the resulting track interactions are interesting. People that cross are not interesting. Gathering of people, or sudden break-ups, are relevant. A selection procedure keeps only those interactions that remain stable for at least a short while. In Figure 3, in the right panel, our algorithm has faded the irrelevant walking patterns to highlight only the relevant events. For more details on trajectory analysis, see our SPIE'09 paper [2].

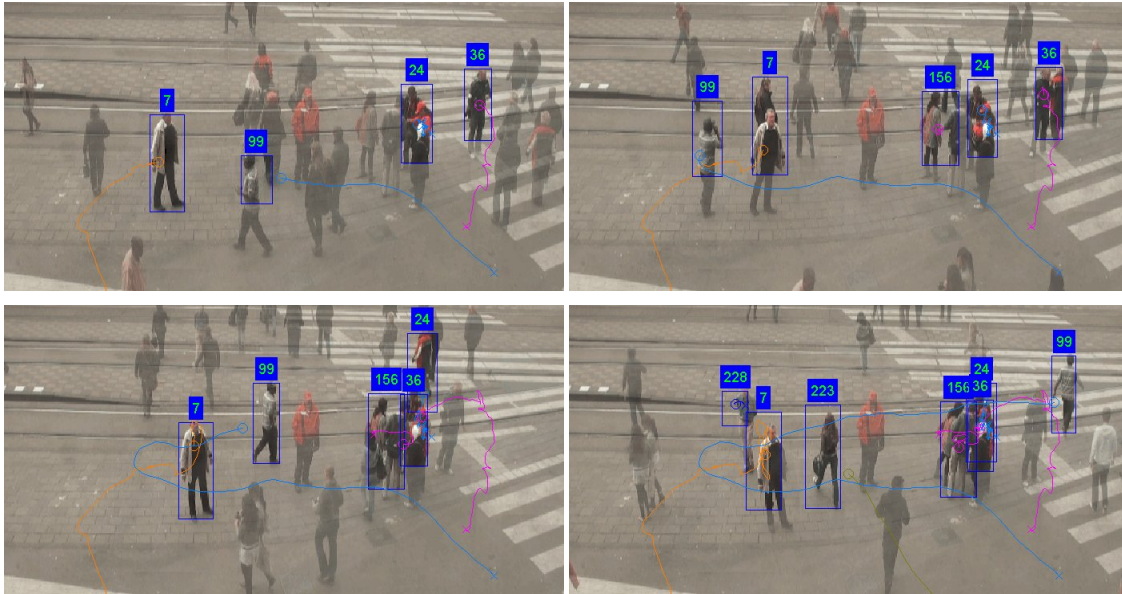


Figure 3. Deviant walking patterns: a U-turn (see track ‘99’), a group formation (tracks ‘24’, ‘156’, ‘36’) and somebody who has been there for several minutes (track ‘7’).

4.2 Clues from body parts

In some cases, a more detailed analysis is needed. The integral appearance may not be discriminative enough and the dynamics of the individual body parts need to be investigated. This is, for instance, the case with the assessment whether somebody is taking a picture. In Figure 4, the relevant parts of the hypothesis are shown: hands and heads (i.e. pieces where skin are detected) and how these pieces interact. If they come sufficiently close, after an upwards motion, the hypothesis is confirmed. For more details on analysis of body parts, see our ICDP’09 paper [1].

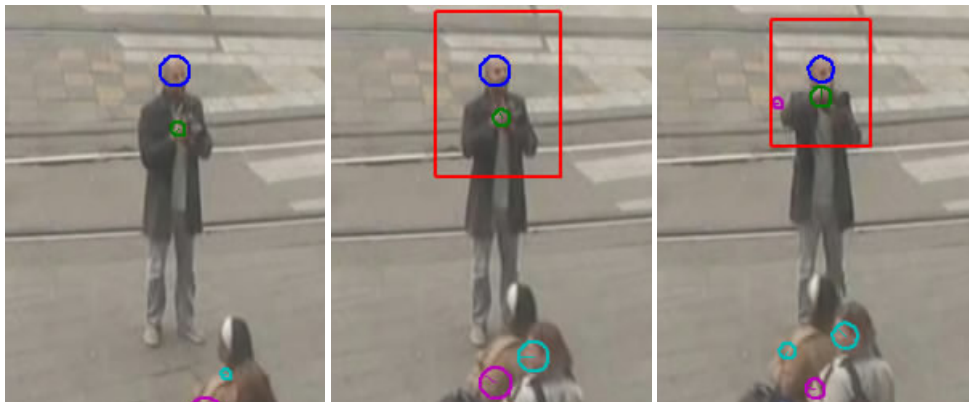


Figure 4. Detailed analysis of body parts reveals a person who is taking a photo.

5. INTERESTING FINDINGS FROM THE AMSTERDAM EXPERIMENT

5.1 Combining behavioral indicators

In a real-world application, the behavioral indicators need to be discriminative of suspicious events. The application should be of added value to the users who need to decide on follow-up actions. Hence alarms should be both reliable and sensitive. If this can be achieved, the application is arguably an appropriate way to deal with privacy and to work

towards societal acceptance: the application is well capable of selecting those people that behave suspiciously. We believe that the focus on behavior (rather than e.g. identity or ethnicity) and a adequate selection (rather than to look at everybody) are requirements for future applications. This implies that some improvements need to be made: some of the behavioral indicators are in themselves not discriminative. For instance, the detection that somebody carries a bag is not informative. The training of police officers, called Search, Detect, React, instructs to look for a combination of indicators to increase certainty of the assessment. The same strategy can be taken in technology, by the fusion of multiple behavioral indicators into a single assessment. In our IEEE'11 paper [3] we propose a model to do this.

5.2 Where are humans better, and where machines?

Although the police officers were very effective in assessing people's nervousness and where they were looking, - a lot of other indicators were hard for them to recognize, such as somebody that is hanging around a particular spot for a while. Obviously, it is hard for a human to focus on many people at the same time. Also, the area of focus is very limited: to watch all people within e.g. 10 meters, is impossible. This became very clear with the U-turn, which was missed by the officers because it happened at about 7 meters: just a little bit beyond their area of focus. The officers are very well capable of seeing the details that we believe are impossible to implement with current state-of-the-art algorithms. Examples are the assessment of somebody's viewing direction (e.g. somebody looking at the cameras, or somebody looking at a partner that is a few meters apart), nervousness, and small movements of the hand (e.g. in a pocket). Hence, we believe that effective security concepts need to take the strengths of both human observers and technology into account.

6. CHECK US OUT ON YOUTUBE

The Amsterdam experiment, our psychology research and the HIT technology are explained in more detail in a short movie on YouTube: www.youtube.com/watch?v=wJ7H_AxZQ8E. Our vision towards optimal detection of hostile intent using sensory observations is elaborated in our NATO'11 paper [4]. In that paper, we also discuss our contributions to the DARPA Mind's Eye program on Visual Intelligence to recognize 48 behaviors.

SOME REFERENCES TO MATERIAL PRESENTED IN THIS PAPER

- [1] G. J. Burghouts, B. van den Broek, B. G. Alefs, E. den Breejen, K. Schutte, 'Automated indicators for behavior interpretation', International Conference on Crime Detection and Prevention (2009).
- [2] B. van den Broek, G.J. Burghouts, S.P. van den Broek, R. Hagen, L. Anitori, W. van Rossum, and A. Smith, 'Automatic detection of hostile behavior', SPIE Defence Europe (2009).
- [3] G. J. Burghouts, J-W. Marck, 'Reasoning about threats: from observables to situation assessment', IEEE Transactions on System, Man and Cybernetics, special issue on Pattern Recognition for Anti-terrorism Applications, pending minor revision (2011).
- [4] G. J. Burghouts, K. Schutte, 'A vision towards automatic inference of hostile intent from sensory observations', NATO MSS conference (2011).