Observing Taxi Behaviour at Charging Stations and Taxi Stands Using Image Recognition

Groen, Maarten; Piersma, Nanda

Observing Taxi Behaviour at Charging Stations and Taxi Stands Using Image Recognition

by Maarten Groen (Amsterdam University of Applied Sciences) and Nanda Piersma (Amsterdam University of Applied Sciences, CWI)

City authorities want to know how to match the charging infrastructures for electric vehicles with the demand. Using camera recognition algorithms from artificial intelligence we investigated the behavior of taxis at a charging stations and a taxi stand.

In Amsterdam, the municipality has placed fast charging stations throughout the city to support electric taxi ownership. This represents a step towards its ambitious goals, which include prohibiting all vehicles except "green taxis" from using taxi stands in prime city locations, such as train stations and inner-city tourist attractions, and even entire city areas.

Because of the proactive attitude of all stakeholders, increasing numbers of charging stations are being established throughout the city. When a taxi is connected to a charging pole, both the transaction for each car and the usage of each station is registered in a central database. However, since information is only collected when vehicles are connected to stations, we lack data about drivers that fail to charge their vehicle when all stations are occupied. Additionally, it is unclear how often taxi-stands are still being used by customers with the increased availability of taxi-apps. These datapoints are the missing link for policy making on charging infrastructure demand and the usage of taxi stands.

In a joint project with the Municipality of Amsterdam, the use of charging stations and taxi stands is monitored to better understand charging demand and taxi-stand customer activity. This information will help the municipality in getting to more informed policy decisions for their ambitious 'green taxi' plan. With an image recognition algorithm, we observed a fast charging station and a taxi stand in Amsterdam, the Netherlands and counted events related to taxis. The automation of the observation was found to be non-trivial.

The challenge

Ideally, for the sake of privacy, camera footage should not be stored when it may contain images of individuals such as taxi drivers or members of the public and when tracking of movement of found objects is required. For this reason, the speed of the algorithm to process the camera footage so that no data has to be stored was an important consideration when developing the algorithm.

State-of-the-art object detection algorithms have been rapidly improving in accuracy and speed [R1]. It is now easy to find cars, trees, people or charging stations (after some training) within an image. In this project the algorithm used object detection and object tracking ([R2],[R3]) as the major building-blocks to be able to distinguish between: taxis and other vehicles using the charging stations, cars waiting for a charging station, taxis waiting for customers or taxis taking a break, and the interpretation of drive-by cars leaving because the charge stations are full. Finally, the algorithm should use as many generally available trained elements as possible to facilitate transfer of the algorithm to other locations without extra location-specific training.

Results

We collected and analyzed data at two locations, a fast charging location and a taxi pickup location. The fast charging location, shown in Figure 1, opened in May 2019 with four fast charging stations. The location can only be reached through a dedicated road with a dead end. Figure 2 represents an overview of the taxi stand at the Amsterdam main train station, showing four places where taxis can pick

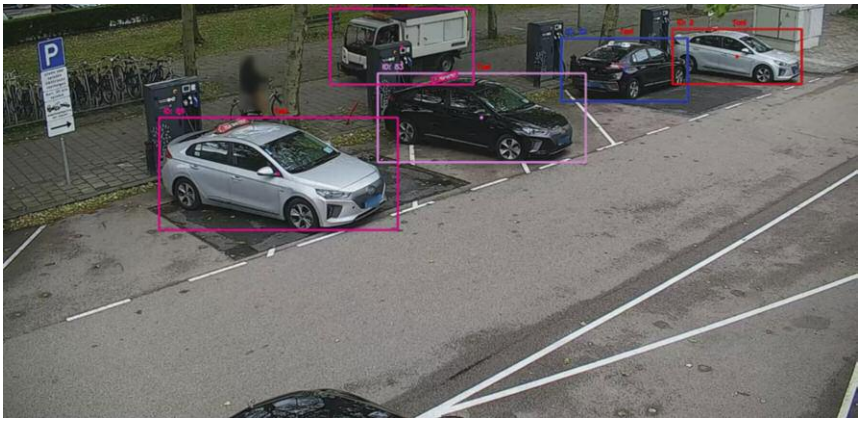

Figure 1: Example from data collected at the fast charging location.

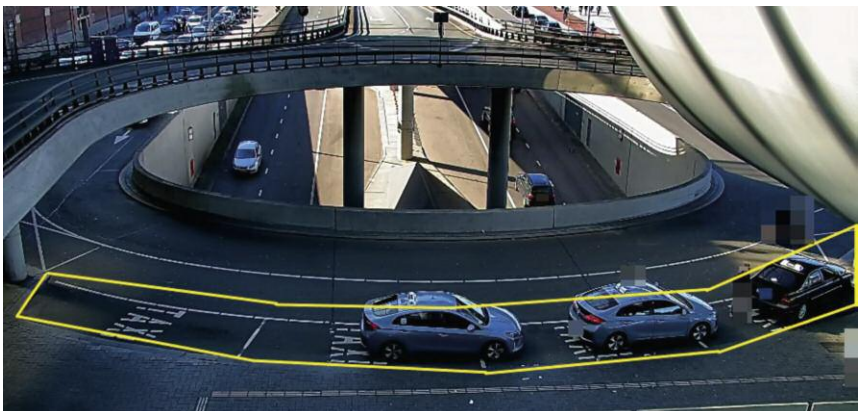

Figure 2: Example from data collected at the taxi stand.

up customers. Taxis are directed to the pickup location with an automated number plate-based system. We focused on the pickup location to count the taxis leaving with customers (versus taxis leaving without customers).

We successfully identified car types (taxi or other), charging taxis, taxis waiting to charge and

taxis driving away. This enabled us to count taxis using the fast charging stations, with duration (time) slots for all activities. The taxi stand was much busier than the fast charging station, with many pedestrians and cars not related to the taxi pick up process moving through the video. We could identify and count the number of taxis picking up customers (per time slot). Owing to the many passers-by in the vicinity of the taxis, the algorithm could not be trained to identify the number of customers entering a taxi. The object tracking task was especially challenging due to unexpected walking patterns at this location; people passing the waiting taxis and leaving the images were often recorded as entering the taxi. In addition, owing both to the camera position and the fact that taxi drivers often leave the car multiple times, drivers are difficult to distinguish from customers.

The simpler tasks can be done in real time, taking an average of 13 minutes to analyze a 15-minute video. This includes tasks such as identifying and counting taxis and determining time slots. More complex tasks, such as counting the number of people entering a car, require more computational power and more location-specific training to achieve acceptable results.

The Municipality of Amsterdam is considering applying the new algorithms to new taxi stands and to other use-cases. This research is part of the research on energy transition of the Intelligence and Autonomous Systems group of the CWI and the IDOLAAD project [L1] at the Amsterdam University of Applied Science. Future research will focus on exploring ways to further automate the more complex tasks.

Link:
[L1]: https://www.idolaad.com/research/research.html

References:

[1] J. Redmon, A. Farhadi: "Yolov3: An incremental improvement", arXiv preprint arXiv:1804.02767, 2018.
[2] L. Leal-Taixé, et al.: "Tracking the trackers: an analysis of the state of the art in multiple object tracking", arXiv preprint arXiv:1704.02781, 2017
[3] S. R. E. Datondji, et al.: "A survey of vision-based traffic monitoring of road intersections", IEEE transactions on intelligent transportation systems, 17(10), 2681-2698, 2016

Please contact:

Maarten Groen, Amsterdam University of Applied Science, Netherlands, m.n.groen@hva.nl

Nanda Piersma, Amsterdam University of Applied Science, CWI, Netherlands, nanda.piersma@cwi.nl

Securing Home Automation Systems against Sensor Manipulation

by Albert Treytl, Edith Huber, Thilo Sauter (Danube University Krems) and Peter Kieseberg (St. Pölten University of Applied Sciences)

Home automation systems (HAS) can be important attack vectors, yet research on securing sensors is sparse, especially with respect to the analogous side of these components, i.e., detecting manipulations of the sensors themselves. Metadata together with the combination of several sensor nodes can be used to thwart such manipulation attacks.

The Internet of Things is a wide and diverse ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context, automate tasks and provide better situation awareness to react to customer needs. Home automation systems (HAS), which are commonly based on IoT, are a growing field for many applications, such as comfort, surveillance and access and energy saving. Since HAS generate a lot of private data, they are very appealing to attackers, who can use them to spy on or stalk inhabitants, or use them to facilitate more traditional criminal activities like burglaries [1]. The comprehensive interconnection of systems to an Internet of Things offers enormous potential to HAS, but also generates new cyber-risks. This has been discussed in-depth by many other researchers, often in the context of industrial or workplace environments, such as building automation and industrial IoT, pointing out that the quality and/or veracity of the source information, typically provided through sensors, forms the basis for securing IoT systems. Thus, both the acquisition and the communication of this information requires special attention in an IoT-environment.

Most of the basic HAS standards currently in use were developed the from the late eighties to early nineties, and IT-security, such as KNX, was added later on. There remain many open questions and challenges, especially in relation to security measures that rely directly on the sensor data and related meta-information. While there are several approaches to use meta-information to discover malicious software (e.g., [2]), the analogue side of the sensors (hardware) is typically neglected, even though manipulation on this side makes typical countermeasures obsolete. This also applies to the extraction of meta-information in the analogue sensor circuit, which could help detect such manipulations and thus help close the security gap in sensor systems [3]. Thus, two different attacker approaches must be considered for home automation systems:

- An attacker could manipulate the data in the digital realm, i.e., the sensor sends correct information, but it is modified in the network. This typical approach is often referred to in the academic literature. Even in this context new tech-