

Einsatz von Deep Learning Frameworks für die Anonymisierung von mobil erfassten 3D-Bilddiensten

Aus Datenschutzgründen müssen Personen und Nummernschilder in 3D-Bilddiensten anonymisiert werden. Da mit modernen Aufnahmeverfahren riesige Datenmengen erfasst werden, ist eine manuelle Erfassung der betroffenen Objekte mit hohem Aufwand verbunden. In dieser Master Thesis wurde daher untersucht, ob dies mit Deep Learning automatisch geschehen könnte. Zudem wurde getestet, welchen Einfluss auf die Resultate die Verwendung der Tiefeninformation hat. Die Resultate, welche mit den trainierten Modellen erreicht wurden, zeigen das vorhandene Potential des Einsatzes von Deep Learning auf. Für den produktiven Einsatz müssten die Modelle allerdings weiter optimiert werden.

Motivation und Zielsetzung

Derzeit wird die Anonymisierung von 3D-Bilddiensten von Hand erledigt, was bei den immer grösseren Datenmengen sehr lange dauert und auf Dauer monoton wird. Eine automatische Detektion der zu anonymisierenden Objekte wäre daher wünschenswert.

In dieser Master Thesis wurde untersucht, ob eine Objektdetektion mittels Deep Learning möglich ist, und welchen Einfluss die Verwendung von Tiefeninformation auf die Resultate hat.

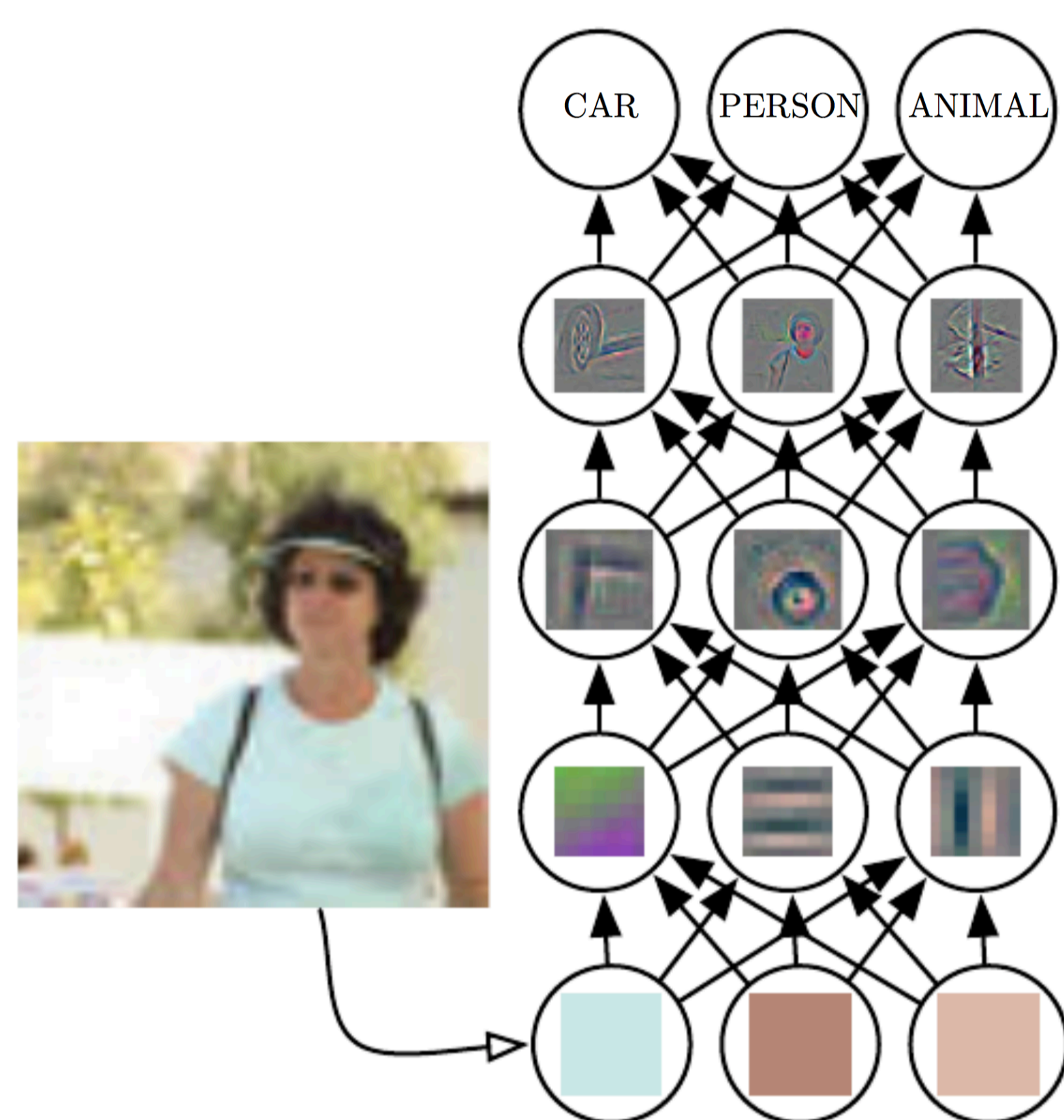


Abb. 1: Stark vereinfachtes Netzwerk (Goodfellow et al., 2016)

Deep Learning

Neuronale Netzwerke sind Modelle, deren Grundkonzept vom menschlichen Gehirn übernommen wurde. Sie bestehen aus unzähligen Neuronen, die zu einem Netzwerk zusammengefügt sind. Werden dafür tiefe Modelle mit vielen aufeinander folgenden Schichten verwendet, spricht man von Deep Learning (Goodfellow et al., 2016).

Die Neuronen im Netzwerk senden Signale aus, die jeweils von den Neuronen in der nächsten Schicht verarbeitet werden (Abb. 1). Durch Gewichte wird definiert, welche Neuronen wie stark voneinander abhängen. Diese Gewichte werden zunächst zufällig initialisiert. Durch das Training mit tausenden Datensätzen werden die Gewichte so angepasst, dass die Ausgaben des Netzwerks möglichst nahe an die Werte der Trainingsdaten herankommen.

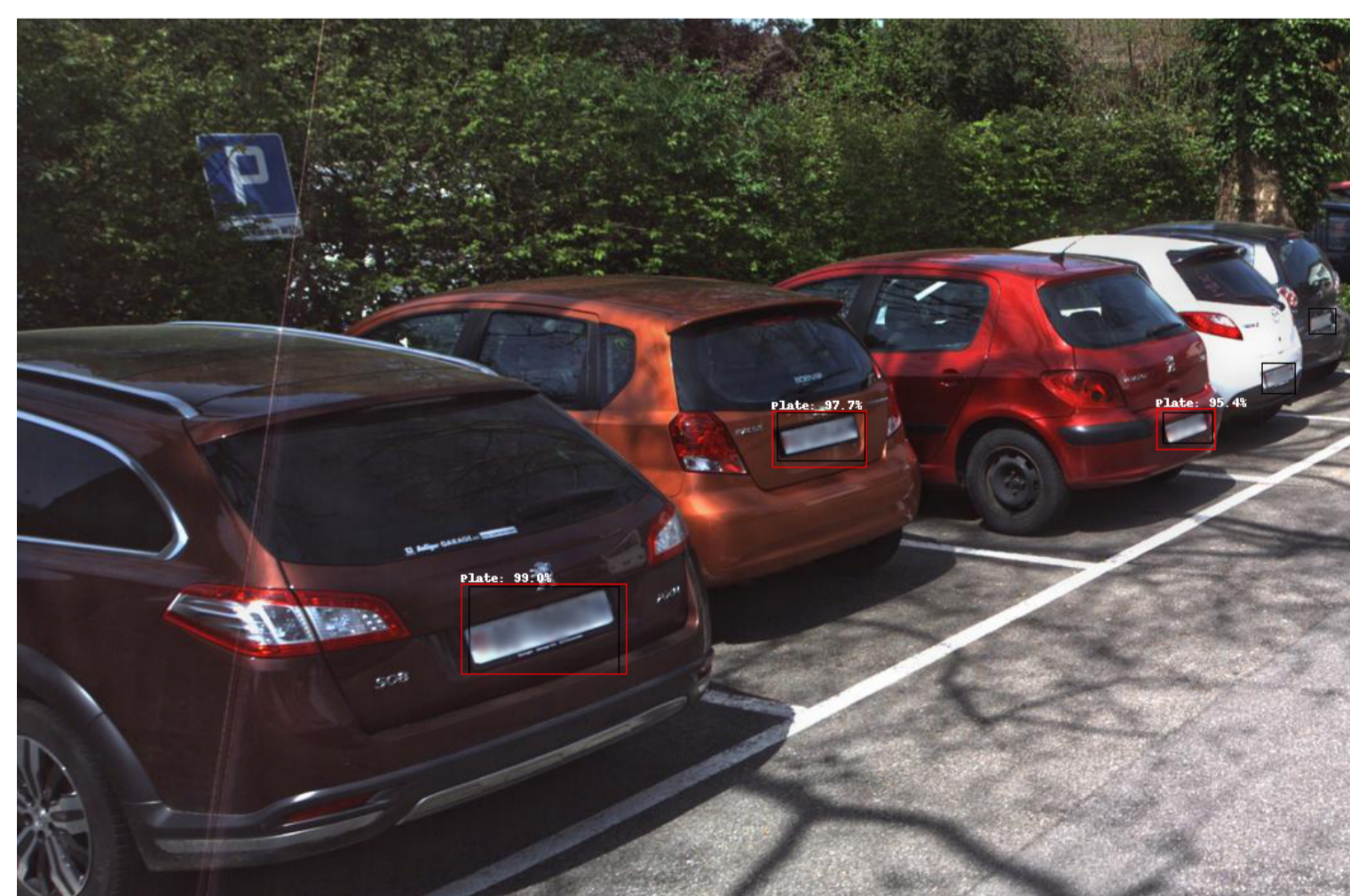


Abb. 2: Einige Detektionen aus dem Test-Datensatz

Referenzen:

Chen, X. & Gupta, A., 2017. *An Implementation of Faster RCNN with Study for Region Sampling*. arXiv preprint, arXiv: 1702.02138.

Goodfellow, I., Bengio Y. & Courville A., 2016. *Deep Learning*. Cambridge, MA: MIT Press.

Ren, S., He, K., Girshick, R. & Sun J., 2015. *Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks*. In: Cortes, C. et al. (Eds.), 2015. *Advances in Neural Information Processing Systems*. Red Hook, NY: Curran Associates.

Autor: Daniel Rettenmund
Examinatoren: Prof. Dr. Stephan Nebiker
Martin Christen
Experte: Dr. Hannes Eugster

Implementierung

Faster R-CNN ist ein Verfahren zur Detektion von Objekten mit Deep Learning (Ren et al., 2015). Basierend auf der Faster-R-CNN-Implementierung von Chen & Gupta (2017) wurde ein Objektdetektionssystem erstellt und verschiedene Modelle trainiert. Dafür wurde das Framework TensorFlow von Google verwendet, welches es erlaubt, mit Python Deep Learning-Modelle zu implementieren.



Resultate

Für die Beurteilung der Resultate können die Genauigkeit (Anteil korrekter Detektionen) und die Trefferquote (Anteil detektierter Objekte) betrachtet werden. Dabei fallen die grossen Differenzen zwischen den trainierten Modellen auf (Tab. 1). Dies ist zum einen in der unterschiedlichen Tiefe der verwendeten Netz-Architekturen (34 bzw. 101 Schichten) begründet. Zudem könnten wahrscheinlich auch mit einem längeren Training Verbesserungen erreicht werden. Dafür hat im Rahmen dieser Arbeit jedoch die Zeit gefehlt. Allerdings wird ersichtlich, dass die Integration der Tiefenkarten als vierter Bildkanal nicht zielführend ist.

	Genauigkeit	Trefferquote
34 Layer (RGB)	60 %	64 %
34 Layer (RGB-D)	30 %	43%
101 Layer	86 %	78 %

Tab. 1: Vergleich der Modelle

Fazit

Die trainierten Modelle zeigen das Potential für den Einsatz von Deep Learning für die Anonymisierung von 3D-Bilddiensten zweifellos auf. Die vom Datenschützer geforderte Genauigkeit (99%) kann derzeit aber noch nicht erreicht werden. Wenn Tiefenkarten zur Genauigkeitssteigerung verwendet werden sollen, müssen sie besser in das Modell integriert werden als beim getesteten Ansatz.

