Eingriff in die Privatsphäre der Endanwender durch Augmented Reality Anwendungen

Matthias Neges und Jan Luca Siewert

Einleitung und Problemstellung

Augmented Reality (AR) Anwendungen finden zunehmend den Weg auf Smartphones und Tablets und etablieren sich stetig weiter in unseren Alltag. Bislang waren spezielle Drittanbieter-Entwicklungsumgebungen (SDKs) wie Vuforia für die Entwicklung von AR Anwendungen notwendig, um die teils komplexe Erkennung von Objekten und Umgebungen für eine positionsgetreue Darstellung von Texten und virtuellen 3D-Modellen zu ermöglichen. Heutet bieten die Hersteller der mobilen Betriebssysteme eigene SDKs, wie z.B. Google mit ARCore für eine Reihe von Smartphones und Tablets auf Android-Basis, an. Apple kaufte 2015 die Firma metaio, welche bis dato eines der leistungsstärksten AR-SDKs angeboten hat. Seit 2017 ist das SDK vollständig in das Betriebssystem integriert und lässt sich von jedem Entwickler wie jede andere Standardfunktionalität des Betriebssystems nutzen.

Neben einigen AR-Spielen, wie „PokemonGo“, verbreiten sich die AR-Anwendung auch in anderen Bereichen, wie z.B. im Marketing. IKEA bietet mit seiner kostenlosen „IKEA Place“-App eine Möglichkeit, alle verfügbaren Einrichtungsgegenstände in die eigenen Wohnräume virtuell zu projizieren. Der Kunde kann so die Möbel in seiner realen, vertrauten Umgebung mit Hilfe seines Smartphones virtuell platzieren und hinsichtlich Design und Größe beurteilen.

Ermöglicht wird die virtuelle Positionierung über die visuell-inertiale Odometrie (VIO), bei den markanten Punkten in jedem einzelnen Kamerabild des Videostreams der Smartphone Kamera verglichen und zusätzlich mit den detektierten Bewegungen über die integrierte Bewegungs-und

Beschleunigungssensoren des Smartphones abgleichen werden. Durch dieses Verfahren lassen sich digitale, dreidimensionale Abbilder der Umgebung erzeugen, ohne spezielle Kameras mit Tiefensensoren oder Stereokameras nutzen zu müssen.

Die Nutzung von AR erfreut sich unter den Anwendern immer größerer Beliebtheit. Dabei ist den Anwendern häufig nicht klar, dass die anfallenden Daten, welche durch die VIO generiert werde, auch Auswertungen ermöglichen, die einen erheblichen Eingriff in die Privatsphäre bedeuten. Zwar sind solche Auswertungen in den Datenschutzrichtlinien der Hersteller der Anwendungen geregelt, laut Statista jedoch lesen 31,8% der Befragten Datenschutzbestimmung im Internet gar nicht erst. Weitere 50% lesen diese selten oder nur manchmal. Als Folge werden den Datenschutzrichtlinien vor der ersten Verwendung solcher Apps blind zugestimmt, um z.B. die neuen AR-Funktionalitäten nutzen zu können.

3D-Tracking in AR-Anwendungen

Heutige Augmented Reality (AR) Anwendungen basieren auf speziellen AR-SDKs, wie z.B. Vuforia oder Wikitude. Zeit kurzem bieten aber die Betriebssysteme selbst integrierten APIs wie das ARCore von Google oder das ARKit von Apple an. Hierbei lassen sich zum einen eine klassische Registrierung des Anwenders im Raum über 2D-Marker realisieren. Es existieren jedoch auch 3D-Trackingverfahren, wie die visuell-inertiale Odometrie (VIO), welches mit nur einer 2D-Kamera am Endgerät auskommt (Munguia & Grau, 2007). Entscheidend hierfür ist der kontinuierliche Abgleich der verschiedenen Kamerabilder mit der dazwischen detektierten Bewegung des Endgerätes. Die Qualität und Robustheit dieses Verfahrens hängt daher maßgeblich von der Genauigkeit und der Kalibrierung der internen Sensoren ab um die erfolgte Translation und Rotation des Endgerätes zwischen zwei Kamerabilder möglichst exakt aufzeichnen zu können (Matt Miesnieks, 31.07.17/2017). Ein Algorithmus erkennt innerhalb der beiden Kamerabilder markante Punkte, gleicht diese ab und berechnet die Verschiebung identischer Punkte unter Berücksichtigung der aufgezeichneten Bewegung des Endgerätes. Somit ist es möglich, sich in einem Raum frei zu Bewegen und dorthinein virtuelle Objekte zu positionieren und virtuell zu fixieren. Ein entscheidender Unterschied zu bekannten Marker-basierten Trackingverfahren liegt darin, dass

kein definierter Ausgangspunkt für das Tracking existiert. Das Tracking beginnt beim Starten der Anwendung und wird dann kontinuierlich weiterverfolgt. Dabei wird der Anwender angehalten, beim Start der Anwendung seine Umgebung aus verschiedenen Perspektiven aufzunehmen, damit der Algorithmus bereits zu Beginn viele Merkmale erkannt hat. Das System lern somit seine Umgebung erst kennen und erweitert fortwährend sein Arbeitsraum. Als Ergebnis entsteht eine 3D-Punktwolke aus markanten Punkten in der realen Umgebung. Diese Punktwolke kann gespeichert und wiederverwendet werden und stellt voran eine Digitalisierung des realen Raumes dar, in welchem der Anwender interagiert. Häufig wird die VIO auch mit dem SLAM (Simultaneous Localization and Mapping) – Tracking gleichgesetzt, welches heute als eine Standard-Trackingmethode in den AR-SDKs von Vuforia, Google und Apple integriert ist. Im Zuge von kollaborativen AR-Anwendungen sind heut Mechanismen in den AR-SDKs implementiert, die die aufgezeichneten Punktwolken mehreren Anwendern zur Verfügung stellen und gegenseitig abgleichen (Apple, 2018). Als Konsequenz muss die erstellte Punktwolke über das Internet hochgeladen und bereitgestellt werden. Dies kann jedoch weitreichende Folgen für den Anwender haben, wenn die darin enthaltenen Informationen für anderen Zwecke genutzt und durch eine entsprechende KI ausgewertet werden.

Datenschutz in AR-Anwendungen

Das Thema Datenschutz ist vielschichtig. Bezogen auf die hier angeführte Thematik lassen sich jedoch grundlegen zwei Quellen von Information festhalten. Zum einen die Informationen, welche aus den Daten der integrierten Sensorik, wie die Inertaialsensorik, gewonnen werden und zum anderen die Visuellen als Extraktion aus den Kamerabildern. Komplexe AR-Anwendungen greifen heute auf eine Vielzahl von Sensorwerten zurück. Je nach Anwendung werden zusätzliche Daten, z.B. GPS-Positionsdaten oder Aufnahmen eines Mikrofons verwendet (Roesner, Kohno & Molnar, 2014). Diese Sensoren lassen zum Teil Rückschlüsse auf sensitive Daten des Anwenders zu. So kann die Kamera beim Aufnehmen der Umgebung z.B. handschriftliche Notizen auf einem Schreibtisch oder einem Whiteboard aufnehmen (Jana et al., 2013).

Spezielle Bilderkennungsalgorithmen, die häufig auf Methoden des maschinellen Lernens (ML) basieren, ermöglichen eine automatische Erkennung der Objekte auf den Kamerabildern wodurch sich diese wiederum mit Ihren 3D-Koordinaten im Raum lokalisieren lassen. Heute stehen eine Vielzahl unterschiedlicher Algorithmen und trainierte ML-Modelle zur Verfügung, die in der Lage sind, prominente Objekte auf einem Kamerabild zu lokalisieren und kategorisieren (Borji, Cheng, Hou, Jiang & Li, 2014; Han, Zhang, Cheng, Liu & Xu, 2018). Google bietet eine API an, bei denen auf Kamerabildern Texterkennung, Objektkategorisierung und -lokalisation, aber auch eine Produktsuche über eine einfache REST API verfügbar ist (Google, 2019). Mit Hilfe solcher Verfahren lassen sich unter Umstände persönlichste Daten der Anwender extrahieren, ohne dass dieser Kontrollmöglichkeiten über die gesammelten Informationen besitzt.

Eine diskutierte Lösung beschreibt das Verwenden von sogenannten Recognizern. AR-APIs erlauben Anwendungen dabei keinen direkten Zugriff auf die gesamten Sensordaten, sondern geben nur abstrahierte Informationen weiter. Das Framework übernimmt dabei die Analyse der Sensorwerte sowie die eigentliche Überlagerung zwischen Kamerabild und virtuellen Inhalten, sodass Anwendungen keinen direkten Zugriff auf diese benötigen. Dies wird z.B. bei der Posen-Erkennung der Microsoft Kinect angewandt (Jana et al., 2013). Alternativ dazu werden Ansätze diskutiert, bei denen der Anwender aktiv Bereiche markiert, die von einer Kamera aufgenommen und analysiert werden dürfen (Raval et al., 2016).

Ein weiteres Problem ist der Eingriff der Privatsphäre von unbeteiligten Dritten, die z.B. über die Kamera aufgenommen werden. Dieses Problem wiege nochmals schwerer, wenn die Analyse der Daten nicht ausschließlich auf lokalen Geräten ausgeführt wird, sondern an Cloud-Dienste ausgelagert werden, da hier der Anwender die Kontrolle über seine Daten verliert. Ausgereifte Datenschutzeinstellungen sind daher ein wichtiger Schritt, damit z.B. AR-Brillen, die dauerhaft Daten aufnehmen, sozial akzeptiert werden (van Krevelen & Poelman, 2010).

Problemstellung und Implementierung einer AR-KI-Anwendung

Der in diesem Paper vorgestellte Prototyp greift diese Thematik auf. Als Use-Case wird eine AR-Anwendungen nach dem Beispiel der IKEA Place App implementiert. Mit der Ikea Place App ist es möglich 3D-Modelle der einzelnen Möbelstücke und Accessoires aus dem Ikea Produktkatalog in der jeweiligen 1:1 Größe in der Umgebung des Anwenders, z.B. in seinem Wohnzimmer, virtuell zu platzieren. Hierfür wird im Hintergrund Apples ARKit verwendet, welches sich die VIO für die Registrierung des Anwenders im Raum zu Nutze macht (Williams, 2018). Ziel ist die Entwicklung eines Prototyps, welcher im Hintergrund und ohne Wissen des Anwenders Zugriff auf die Sensordaten und Kamerabilder während der Nutzung der Anwendung gewährt.

Der Prototyp ist als iOS Anwendung auf einem iPad implementiert. Als AR-Framework wird das ARKit 2.0 verwendet. Als Server wird ein auf NodeJS basierender Express-Server eingesetzt, mit dem das iOS-Gerät über eine REST-API kommuniziert. Nachdem der Anwender Datenschutzrichtlinien akzeptiert hat, stellt das iOS-Gerät im Hintergrund selbständig eine Verbindung mit dem Server her und startet die Kamera. Vordergründig sieht der Anwender die AR-Anwendung und kann Gegenstände platzieren, wobei er angehalten wird, für ein besseres Tracking seine Umgebung genau zu scannen. In einem Hintergrundprozess werden laufend die aktuellen Kameraframes analysiert. Bei Erkennung eines Gegenstandes wird das entsprechende Kamerabild inklusive zusätzlicher Informationen, wie die Systemzeit und Informationen über die Position des Objektes, über die REST-API an den Server gesendet.

Auf diesem ist eine Objektdatenbank angelegt, in der jeder Gegenstand einer einfachen ID und weitere Metadaten zugeordnet ist. Sendet das Gerät Informationen über einen erkannten Gegenstand, wird dieser mit der Datenbank abgeglichen und abgespeichert. Zu einem späteren Zeitpunkt kann sich der Anwender auf einer Übersichtsseite alle gespeicherten Bilder, erkannte Objekte und verknüpfte Metdaten im Webbrowser ansehen.

Der Prototyp wird in einer Studie zum Einsatz kommen. Die daran teilnehmenden Probanden bekommen die Aufgabe, mit der Anwendung Gegenstände und Möbel in einem definierten Raum virtuell zu platzieren. Beim Start der Anwendungen müssen die Probanden zunächst die Datenschutz-

vereinbarung akzeptieren. Darin enthalten ist eine Passage, die es dem Anbieter der Anwendung erlaubt, die generierten Daten während der Nutzung weiter zu verwenden.

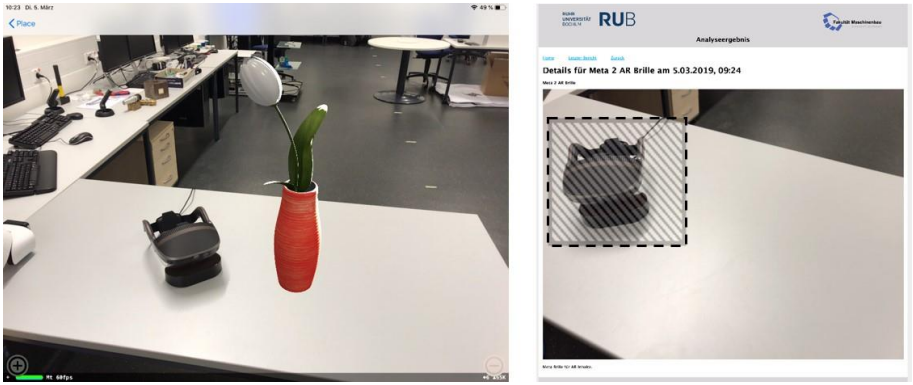

Abbildung 1: Sichtweise des Anwenders bei Verwendung der Anwendung (rechts) und Identifizierung von Objekten auf der Serverseite (links)

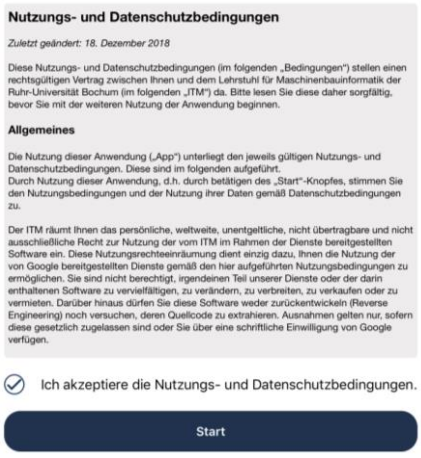

Abbildung 2: Anzeige der Datenschutzbestimmung vor Verwendung der Anwendung

Es wird erwartet, dass ein Großteil der Probanden die Datenschutzrichtlinie ungelesen akzeptieren. Ein kleiner Teil wird diese zwar lesen, aber aufgrund der Vorteile und Funktionsweise in Anlehnung an die IKEA Place App dennoch akzeptieren. Nach Verwendung der App werden den Probanden die

Auswirkungen aufgezeigt, welche durch die Bereitstellung der Daten und die Objekterkennung hat. Hierbei werden verschieden Stufen von zielgerichteter Werbung, über Aussagen über den Lebensstil und den Gesundheitszustand des Anwenders bis hin zur Verwendung für Einbruchs/-Diebstahlplanung krimineller Dritte. Es wird ebenfalls erwartet, dass die Probanden nach Aufzeigen dieser Konsequenzen eine Verwendung solcher AR-Anwendungen zukünftig ablehnen werden. Somit lassen sich die beiden Kernfragstellungen der geplanten Studie wie folgt definieren:

1. Wie sorglos wird heutigen Datenschutzbestimmung bei der Verwendung von mobilen Anwendungen zugestimmt?
2. Wie verändert sich der Umgang mit AR-Anwendungen, wenn die Konsequenzen durch einen Datenmissbrauch aufgezeigt werden?

Fazit und Ausblick

AR-Anwendungen etablieren sich zunehmen in unserem Alltag. Dabei bieten heutige 3D-Trackingingverfahren bei kommerziellen Anwendungen die Möglichkeit eine freie Registrierung des Anwenders im Raum. Im Hintergrund wird hierzu eine Digitalisierung der realen Umgebung vorgenommen, welche in Kombination mit einer KI zahlreiche Informationen über den Anwender und dessen Umgebung preisgibt. Im vorliegenden Betrag wurde ein Prototyp vorgestellt, welcher die Funktionen der IKEA Place App nachbildet und das AR-Tracking mit einer im Hintergrund und serverseitig laufenden KI kombiniert. Dieser Prototyp ist die Basis für eine Studie, bei der die Teilnehmer die Anwendung nutzen und erst im Nachgang aufgezeigt bekommen, welche Informationen sich aus den generierten Daten gewinnen lassen. Beispielsweise kann der Anbieter viele Informationen über die Alltagsgewohnheiten alleine aufgrund der Kamerabilder und späteren Auswertung durch Bilderkennungsalgorithmen ziehen und so gezielt Werbung anbieten. Den Probanden wird darüber hinaus aufgezeigt, wie problematisch es werden kann, wenn kriminelle Gruppe Zugriff auf die Daten erhalten und so beispielsweise Wertgegenstände identifizieren oder Sicherheitsmechanismen gegen Einbrüche lokalisieren können. Als Ergebnis der Studie wird zum eine Sensibilisierung der Anwender erwartet, sowie eine Handlungsanweisung für die Anbieter

dieser AR-Anwendungen hinsichtlich der Transparenz und der erforderlichen Sicherheitsmechanismen zum Schutz der Daten der Anwender.

Literaturverzeichnis

Apple (Apple, Hrsg.). (2018). Creating a Multiuser AR Experience. Apple Developer Documentation. Zugriff am 26.02.2019. Verfügbar unter https://developer.apple.com/documentation/arkit/creating_a_multiuser_ar_experience

Borji, A., Cheng, M.-M., Hou, Q., Jiang, H. & Li, J. (2014). Salient object detection. A survey. arXiv preprint arXiv:1411.5878.

Google. (2019). Google Vision API. Zugriff am 06.03.2019. Verfügbar unter https://cloud.google.com/vision/docs/reference/rest/?hl=de

Han, J., Zhang, D., Cheng, G., Liu, N. & Xu, D. (2018). Advanced deep-learning techniques for salient and category-specific object detection. A survey. IEEE Signal Processing Magazine, 35 (1), 84-100.

Jana, S., Molnar, D., Moshchuk, A., Dunn, A., Livshits, B., Wang, H. J. et al. (Hrsg.). (2013). Enabling fine-grained permissions for augmented reality applications with recognizers.

Matt Miesnieks. (2017). Why is ARKit better than the alternatives? Verfügbar unter https://medium.com/super-ventures-blog/why-is-arkit-better-than-the-alternatives-af8871889d6a

Munguia, R. & Grau, A. (2007). Monocular SLAM for Visual Odometry. In Proc. IEEE International Symposium on Intelligent Signal Processing 2007 (S. 1-6). IEEE.

Raval, N., Srivastava, A., Razeen, A., Lebeck, K., Machanavajjhala, A. & Cox, L. P. (Hrsg.). (2016). What you mark is what apps see: ACM.

Roesner, F., Kohno, T. & Molnar, D. (2014). Security and privacy for augmented reality systems. Commun. ACM, 57 (4), 88-96.

Van Krevelen, D. W.F. & Poelman, R. (2010). A survey of augmented reality technologies, applications and limitations. International Journal of Virtual Reality, 9 (2), 1-19.

Williams, R. (Mobil Marketer, Hrsg.). (2018). Ikea Place ranks as No. 2 free ARKit app. Zugriff am 06.03.2019. Verfügbar unter *https://www.mobilemarketer.com/news/ikea-place-ranks-as-no-2-free-arkit-app/520761/*

Kontakt

Dr.-Ing. Matthias Neges
Ruhr Universität Bochum
Lehrstuhl für Maschinenbauinformatik
Univ.-Prof. Dr.-Ing. Detlef Gerhard
Fakultät für Maschinenbau
Universitätsstr. 150
44801 Bochum
www.itm.rub.de

Jan Luca Siewert, B.Sc.
Ruhr Universität Bochum
Lehrstuhl für Digital Engineering
Univ.-Prof. Dr.-Ing. Detlef Gerhard
Fakultät für Maschinenbau
Universitätsstr. 150
44801 Bochum
www.itm.rub.de