Kinect – eine Revolution nicht nur im Kinderzimmer

Neue Möglichkeiten und potenzielle Gefahren

Durch die Entwicklung neuer Sensortechniken und insbesondere auch der intelligenten Weiterverarbeitung ergeben sich neue Möglichkeiten in der Analyse personenbezogener Daten. Einerseits erfreuen sich die ganz neuen Formen der Mensch-Maschine-Interaktion immer grösserer Beliebtheit sowohl in Kinder- und Wohnzimmern zum Steuern von Computerspielen als auch im Kunst- und Medizinbereich. Andererseits birgt diese Technik aber auch erhebliche Gefahren.

Matthias Wölfel

Die rasante Entwicklung der Sensortechnik und der dahinterliegenden digitalen Datenverarbeitung und Datenauswertung ermöglicht ganz neue Formen der Mensch-Maschine-Interaktion. So wandelte sich z.B. durch die Auswertung von Position und Beschleunigung in der Wiimote (Gamecontroller der 2006 veröffentlichten Spielkonsole Wii von Nintendo) die bis dato maus-, keyboard- und joystickbasierte Steuerung von Computerspielen zu einer gestenbasierten Steuerung durch Armbewegungen im Raum. Der nächste Evolutionsschritt wurde durch den Kinect-Sensor von Microsoft für die Spielekonsole Xbox 360 eingeleitet **(Bild 1)**. Durch diesen wurde es möglich, ohne Berührung – sei es Tastatur, Maus, Gamepad, sensitive Oberfläche oder eine Wiimote – mit der Spielekonsole zu interagieren. Aber bereits kurze Zeit nachdem Microsoft, Anfang November 2010, den Kinect-Sensor als Steuerung für die Spielekonsole Xbox 360 auf den Markt gebracht hatte, entwickelte sich rasch eine schnell wachsende Community, die den Sensor nicht wie von Microsoft vorgesehen an der Xbox, sondern am Computer verwendet, um insbesondere die zahlreichen neuen Möglichkeiten der kostengünstigen Tiefenkamera für ihre Zwecke zu nutzen. Neben Hackern und Medienkünstlern bedienen sich auch immer mehr Firmen, Universitäten und Forschungseinrichtungen dieser Technik, um beispielsweise Innovationen im Gesundheitswesen voranzutreiben. Aber auch Grosskonzerne möchten die neuen Möglichkeiten der heutigen Sensortechnik und Verarbeitungsalgorithmen für ihre Zwecke nutzen, um Benutzer noch besser beobachten und analysieren und somit effektiver mit Werbung «versorgen» zu können.

Hacking the Kinect

Wie bei vielen anderen Gadgets, die in letzter Zeit auf den Markt gekommen sind, wurde auch der Kinect-Sensor[1)] von einer breiten Masse an Hackern und Bastlern unter die Lupe genommen. Bereits kurz nach Verkauf des ersten Sensors war es möglich, den Kinect von einem Windows-, Mac-OS-X- oder Linux-Betriebssystem aus anzusprechen und auf die Sensordaten zuzugreifen. Durch diese Möglichkeit entstanden inzwischen nicht nur viele künstlerische Arbeiten, sondern auch ein breites Spektrum an Anwendungen.

Recht früh entstand eine Arbeit «Be your own souvenir» von Blablablab [1], bei der es möglich war, sich auf einem öffentlichen Platz von dem Kinect-Sensor scannen zu lassen und sich selbst als Figur aus einem 3D-Druck mit nach Hause zu nehmen. Ein weiteres Projekt, das sich direkt mit der Auswertung des Tiefenbildes befasst, diesmal von Microsoft Research in England, ist KinectFusion [2]. Es ermöglicht das schnelle Erfassen eines 3D-Modells einschliesslich Textur aus einer realen Umgebung. Hierdurch wird es z.B. möglich, ein reales Objekt sehr einfach in eine virtuelle Umgebung einzubinden oder die Beleuchtung einer realen Szene, im Nachhinein, zu verändern.

Beispiele, die auf der Auswertung der Skelettstruktur beruhen, finden sich insbesondere in der Musik- und Performanceszene, wo die Koordinaten der Hand oder der Füsse direkt dazu verwendet wurden, um Töne zu manipulieren oder Lichteffekte zu steuern. So lässt sich sogar eine Luftgitarre spielen, die «echte Töne» erzeugt [3]. Ein weiteres Beispiel der Verwendung der Skelettstruktur ist die Steuerung von virtuellen Figuren.

Evan-Amos

Bild 1 Seit Anfang November 2010 ist die Kinect-Sensorleiste zur Steuerung der Videospielkonsole Xbox 360 erhältlich.

Wölfel

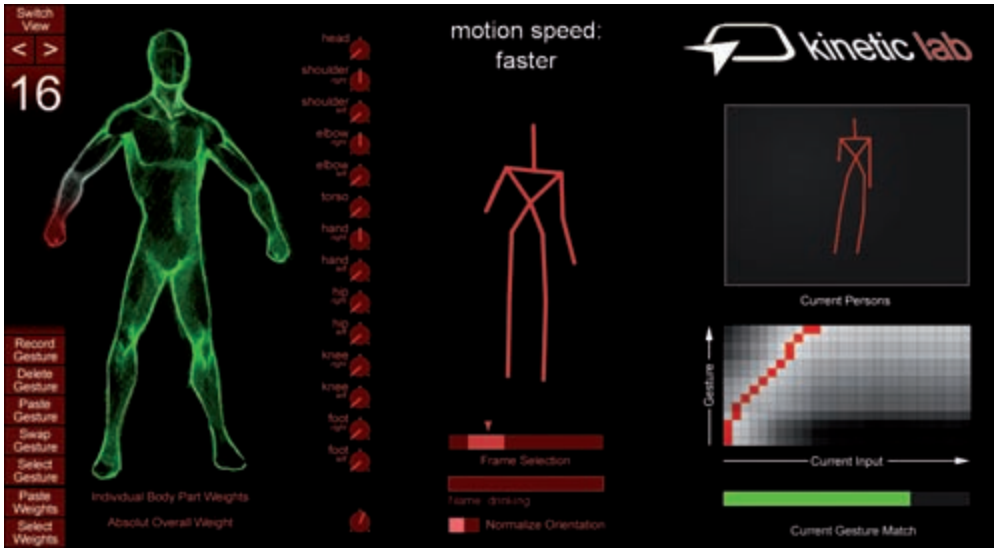

Bild 2 Kinetic-Space-Programm in der «Lab»-Ansicht.

Hier werden die einzelnen Körperteile und die Körperbewegung auf einen 3D-Charakter übertragen [4]. Um die Abbildung des virtuellen Charakters zu vervollständigen, lassen sich durch den Abgleich von Gesichtsmasken mit dem Tiefenbild eines Gesichtes auch die Gesichtsmimiken auf ein 3D-Gesicht abbilden [5].

Mit der durch den Verfasser entwickelten Software Kinetic Space [6] zum Lernen und Erkennen beliebiger Gesten durch simples Vormachen, anstatt sie mittels Programmcode zu beschreiben, ergeben sich weitere interessante Anwendungen: So ist es z.B. möglich, nicht nur durch simple Gesten Anwendungen wie PowerPoint zu bedienen, sondern auch durch eintrainierte Bewegungen. Akustische und optische Ereignisse lassen sich also auch durch komplexe Bewegungsabläufe, wie sie unter anderem im Tanz vorkommen, steuern. Diese neue Möglichkeiten fanden insbesondere in der Medienkunst interessante Anwendungen: So verwendet der Künstler Chico Macmurtrie Kinetic Space, um Posen von Besuchern im Museum zu erkennen, um darauf mit entsprechenden Posen von maschinenartigen, humanoiden Robotern zu reagieren (gezeigt in der Ausstellung «Art and Artificial Life», Espacio Fundacion Telefonica, Calle Fuencarral 3, Madrid, Spanien, vom 10.5.2012 bis 6.1.2013). Paul Stoffregen in Oregon, USA, baut pyrotechnische «Heavy Metal»-Installationen, bei denen mehrere Feuerwerfer durch verschiedene Gesten gesteuert werden. Elke Reinhuber dreht einen interaktiven Film, dessen Handlung von bewussten und unbewussten Gesten des Publikums beeinflusst wird. Aber auch in der Medizintechnik haben diese Möglichkeiten ein reges Interesse hervorgerufen. So können in der Physiotherapie und Krankengymnastik Bewegungsabläufe der Patienten kontrolliert und gegebenenfalls korrigiert werden.

Die Ansicht (Bild 2) unterteilt sich in vier Bereiche:

- Aktuelle Pose (rechts oben). Hier wird die Pose der Person vor dem Sensor dargestellt.
- Gestenanalyse und Best Match (rechts unten). Hier wird der Vergleich der beiden Gesten über die Zeit grafisch dargestellt (je ähnlicher die Pose in der Referenz mit den Sensordaten, umso heller die Fläche) und der optimale Pfad, in Rot, hervorgehoben. Direkt unter dieser Information befindet sich ein Balken, dessen Länge die Übereinstimmung zwischen der ausgeführten Bewegung und der gelernten Geste anzeigt.
- Visualisierung der Gesten (Mitte). Hier wird die «aktuelle» Geste (ID oben links) über ihren jeweiligen Bewegungsablauf als Skelettstruktur abgespielt.
- Analyse der einzelnen Körperteile (links). Die Skizze einer Person zeigt anhand von Farbwerten, für jedes Körperteil, ob die ausgeführte Bewegung der gelernten Geste entspricht (Körperteil in Grün dargestellt) oder davon abweicht (in Rot dargestellt).

Microsofts Antwort

Schon sehr kurze Zeit nach dem Verkaufsstart des Kinect-Sensors bemerkte Microsoft, dass sich immer mehr Menschen – die nicht unbedingt Spielefans sind – mit dem Sensor beschäftigten und ihn sozusagen zweckentfremdeten, um ihn wie erwähnt im wissenschaftlichen und künstlerischen Umfeld zu nutzen.

Erst betrachtete Microsoft das sogenannte «Kinect Hacking» mit Argwohn, ohne jedoch gerichtlich gegen die Hacker vorzugehen. Dann aber erkannte auch Microsoft das grosse kreative und wirtschaftliche Potenzial des Kinect auch ausserhalb des Computerspielemarktes, welches sie bis dato völlig unterschätzt hatte.

Microsoft entschloss sich nicht nur dazu, selbst die kostenfreie Entwicklungsumgebung «Kinect Software Development Kit» anzubieten (natürlich nur für Windows, erste öffentliche Beta im Juni 2011, erster Release im Februar 2012), sondern auch ein Programm namens «Kinect Accelerator» aufzusetzen, um Start-ups zu fördern, die neue Anwendungen für Kinect entwickeln. Im Rahmen dieses Programms wurden 11 Firmen mit einem Startkapital von je 20 000 US-Dollar ausgestattet und nach Seattle eingeladen, um dort im Zeitraum von April bis Juni 2012 von Microsofts Support und Technologie zu profitieren und die Ideen Realität werden zu lassen.

Zurzeit ist aber schwer abzuschätzen, welche Strategie Microsoft mit einem solchen Programm verfolgt. Inzwischen hat Microsoft den Bewegungssensor Kinect auch in einer Version für Computer auf den Markt gebracht. Die Besonderheit ist hier ein sogenannter Near-Mode, der bereits Objekte im Abstand von 40 cm erkennen kann (mit der Xbox-360-Sensorversion waren bisher mindestens 80 cm nötig), wodurch

sich weitere Anwendungen erschliessen lassen.

Gefahren

Neben der Euphorie um Kinect und dessen zahlreiche Anwendungsgebiete sollte man aber die Gefahren, die er mit sich bringt, nicht vergessen. Denn alle Sensoren, die in Kinect enthalten sind, egal ob Mikrofon, Kamera oder Tiefenkamera, ermöglichen durch ihre gesammelten Daten auch umfangreiche Kontroll- oder Überwachungsmassnahmen. Insbesonders ergeben sich durch die zuvor beschriebenen Analysemöglichkeiten des Kinect ganz neue Einsatzgebiete: Es könnten somit anhand der beobachten Gesten automatisierte Rückschlüsse auf Handlungen, die mit dem Sensor aufgenommen wurden, erfolgen, z.B. Aufbrechen eines Autos oder Ausüben von Gewalt, und ein Alarm könnte automatisch ausgelöst werden.

Da der Kinect-Sensor noch recht neu ist, gibt es noch keine bekannt gewordenen Beispiele für eine Auswertung der Tiefenkamera. Aber die klassischen Sensoren lieferten in der Vergangenheit bereits viele Beispiele. Daher wollen wir uns im Folgenden mit diesen auseinandersetzen. So wurde z.B. bekannt, dass Webcams von Unbefugten durch entsprechende Software ausgelesen werden können. Im Oktober 2011 stand deshalb ein 44-jähriger Mann vor Gericht, der sich so (virtuell) in Hunderte von Kinderzimmern eingeschlichen hatte, um Jungen und Mädchen unerlaubt und (zuerst unbemerkt) zu beobachten.

Noch beunruhigender aber als der unerlaubte Zugriff von aussen durch Hacker, die dafür belangt werden können, ist die immer tolerantere Auslegung der Grosskonzerne an der Nutzung persönlicher Daten in Kombination mit der automatischen Auswertung der Sensorinformationen. So war es in einer Studie der Carnegie Mellon University möglich, durch die Kombination von drei gängigen Technologien – öffentlich verfügbare Informationen aus sozialen Netzwerken, Cloud Computing sowie einer handelsüblichen Gesichtserkennung – fremde Personen zu identifizieren und deren persönliche Informationen herauszufinden (in manchen Fällen bis zur Sozialversicherungsnummer).

Ein weiteres Beispiel findet sich in der Gesichtserkennung von Facebook, mit der automatisch die Bilder ganzer Online-Alben nach bekannten Gesichtern oder nach frisch veröffentlichten Prominentenfotos durchsucht werden können. Wie wichtig eine solche Technologie für Facebook ist, zeigt sich durch die Übernahme des Gesichtserkennungsdienstes «Face.com». Durch diese Übernahme kann Facebook Nutzer und deren Freunde (sogar wenn diese selbst nicht bei Facebook angemeldet sind) auch ausserhalb von Facebook besser verfolgen und mit passender Werbung bombardieren. Eine weitere Hiobsbotschaft für den Datenschutz ist der von Microsoft eingereichte Patentantrag, bei dem das Gefühl des Nutzers ausgewertet wird, um solche Werbung zu zeigen, die bei dem erkannten emotionalen Zustand die höchste Wirkung verspricht. So kann eine Werbung gezeigt und anhand der Reaktion des Verbrauchers entschieden werden, welche Werbung als nächste am wirksamsten sein könnte. Da für diese Erkennung viele menschliche Hinweise, wie z.B. Gesichtsausdruck, Blickrichtung, Körpersprache, Charakteristik der Stimme, ausgewertet werden, müssen sehr viele persönliche Daten in einer Datenbank abgelegt sein.

Dem gegenübergestellt ist die Auswertung des Geschlechts oder Alters, die bereits heute schon stattfindet, eher harmlos. Eine Microsoft-Sprecherin betonte Cnet News gegenüber zwar, dass laut der Microsoft-eigenen Bestimmungen (bisher) keine von Kinect gesammelten Daten für Werbezwecke genutzt würden. Ist aber erst einmal eine solche Möglichkeit geschaffen, werden die wenigsten Firmen (freiwillig) darauf verzichten. Dies zeigt sich schon daran, dass nur eine aus 100 der populärsten Websites der USA keine Daten über seine Nutzer sammelt: Wikipedia, also ein nicht kommerzielles, ausschliesslich aus Spenden finanziertes Angebot.

Insbesondere Firmen wie Facebook und Google, die sich primär durch eine zwar indirekte Vermarktung der Nutzerdaten bzw. des Nutzerprofils finanzieren, werden es sich vielleicht gar nicht leisten können, von diesen neuen Möglichkeiten keinen Gebrauch zu machen, um nicht Marktanteile an die Konkurrenz zu verlieren. Wirkt der von Google selbst gewählte Slogan «Don't be evil» nicht doch etwas ironisch? Denn demonstrierte Google in der Vergangenheit nicht schon oft genug, dass alle nur erdenklichen Daten, die gesammelt werden können, auch gespeichert werden? So wurden beispielsweise bei der Aufnahme für «Google Street View» nicht nur Bilddaten gesammelt und gespeichert (was bereits eine entsprechende Diskussion ausgelöst hat), sondern auch WLAN-Daten, worunter sich E-Mails, Passwörter, Browser-Historien und auch gerade angesurfte Websites der jeweiligen Nutzer befanden. Ein weiteres bekanntes Beispiel der von den Nutzern zunächst unbemerkten Sammlung von Daten, dieses Mal von Apple, ist das Speichern der GPS-Daten des iPhone-Standortes.

Nicht vergessen sollte man in diesem Bezug auch die Möglichkeiten des Staates, auf die Sensordaten zuzugreifen. Ob diese Online-Durchsuchungen rechtlich erlaubt sind, ist weder in Deutschland noch in der Schweiz gesetzlich geregelt. Ganz unbeachtet dessen hat die Bundesregierung Deutschland ein Programm entwickeln lassen, das unter dem Namen Staatstrojaner bekannt geworden ist. Dieses Programm, mit dem es unter anderem möglich ist, Voice-over-IP-Gesprä-

Résumé

Kinect: une révolution qui ne se passe pas uniquement dans la chambre d'enfant

Nouvelles possibilités et risques potentiels

Le développement de nouvelles technologies pour les capteurs, et notamment du traitement intelligent de leurs données, permet de créer de toutes nouvelles possibilités en matière d'analyse et d'évaluation de données personnelles. D'une part, les dernières formes de l'interaction entre l'humain et la machine jouissent d'une popularité grandissante tant à l'intérieur des chambres d'enfant et des salons quand il s'agit de jouer aux jeux d'ordinateur que dans les domaines de l'art et de la médecine. D'autre part, une telle technologie présente également des risques considérables : d'un côté, une évaluation, jusqu'ici tolérée par la loi, des données personnelles afin de compléter les profils d'utilisateur destinés à un marketing ciblé et, de l'autre, un accès non autorisé à de telles données obtenu par les hackers. Ces derniers sont même susceptibles de servir des régimes totalitaires à des fins de surveillance.

Le présent article expose, à l'aide d'exemples multiples, les nombreuses et nouvelles possibilités offertes par la technologie des capteurs et notamment par les données rendues disponibles par le capteur Kinect. Il aborde également la question des risques, déjà réels, que représente une telle technologie.

No

che vor der Verschlüsselung abzuhören, wurde vom Chaos Computer Club am 8. Oktober 2011 aufgedeckt. Wobei eine Software, die ausschliesslich zur Überwachung von VoIP verwendet werden kann, rechtlich erlaubt ist. Mit diesem Trojaner ist es aber auch möglich, auf andere Daten zuzugreifen, sogar auf das Kamerabild. Golem kommentierte hierzu: «Experten halten einen legalen Staatstrojaner für unmöglich, das Bundeskriminalamt versuchte es dennoch und versagte.»

Die gezeigten Beispiele verdeutlichen, dass wir auch in Zukunft nicht vor unerlaubtem Zugriff auf unsere persönlichen Daten und die von Sensoren zur Verfügung stehenden Daten geschützt sind, sei es gegenüber Hackern, Konzernen oder dem Staat.

Ausblick

Wie so oft gilt es auch hier, die richtige Balance zu finden: Die riesigen Chancen zu nutzen, die diese Technologie erst ermöglicht, und die Gefahren rechtzeitig zu erkennen, um diese durch entsprechende Gesetze (durch die Politik) oder Selbstregulierung (durch die Konzerne) einzugrenzen. Denn sonst wird aus einer Revolution eventuell schon bald ein Spion – nicht nur im Kinderzimmer!

Literatur

- Matthias Wölfel: Kinetic Space – 3D-Gestenerkennung für Dich und Mich, Konturen 2012, Pforzheim, Deutschland.
- Achim Sawall: Bundeskriminalamt kann keinen Trojaner entwickeln, http://www.golem.de/news/staatstrojaner-bundeskriminalamt-kann-keinen-trojaner-entwickeln-1205-91764.html, 13.5.2012.
- Alessandro Acquisti, Ralph Gross, Fred Stutzman: Faces of Facebook: Privacy in the Age of Augmented Reality. Präsentiert auf der BlackHat Konferenz, Las Vegas, August 4, 2011.
- Wook Jin Chung et al.: Targeting Advertisements Based on Emotion, United States Patent Application 20120143693.

Links

Eine gute Übersicht über Kinect-Hacks findet sich auf den Websites http://www.kinecthacks.com und http://kinect.dashhacks.com.

Referenzen

[1] www.blablablab.org.
[2] http://research.microsoft.com/apps/video/dl.aspx?id=152815.
[3] www.youtube.com/watch?v=8DmOux4IdAE.
[4] www.ni-mate.com.
[5] www.faceshift.com.
[6] http://kineticspace.googlecode.com.

Angaben zum Autor

Dr. **Matthias Wölfel** ist Professor für Interaction- und Interfacedesign im Studiengang Intermediales Design der Fakultät für Gestaltung an der Hochschule Pforzheim, Deutschland, und Gründer der Firma ColorfulBit, die in den Bereichen Design, Signalverarbeitung, Sensorik und Mensch-Maschine-Interaktion tätig ist. Er hat an der Technischen Universität Karlsruhe, jetzt Karlsruher Institut für Technologie (KIT), Deutschland, sowie der University of Massachusetts, USA, und der Carnegie Mellon University, USA, Elektrotechnik und Informationstechnik studiert und wurde in Informatik promoviert.

Hochschule Pforzheim, DE-75175 Pforzheim, matthias.woelfel@hs-pforzheim.de

ColorfulBit, matthias.woelfel@colorfulbit.com

[1)] Obwohl es eine ganze Reihe von alternativen Tiefensensoren gibt, ist der Kinect-Sensor der bei Weitem erfolgreichste. So wurde er bisher 18 Millionen Mal abgesetzt. Leider gibt es bisher keine Zahlen, wie viele von diesen Sensoren tatsächlich an einer Xbox angeschlossen sind und wie viele zweckentfremdet wurden.