Hochschule Bremerhaven
Studiengang Informatik

Gesichtserkennung

Hilfreiche Technik oder Gefahr für Privatsphäre und Datenschutz?

Von
Daniel Wagner und Simon Grass

Bremerhaven, 05.01.2012

Veranstaltung Informatik und Gesellschaft Prof. Dr. Edgar Einemann

Inhaltsverzeichnis

Gesichtserkennung

Die Gesichtserkennung ist eine Technologie, die seit Mitte der neunziger Jahre immer mehr an Bedeutung gewinnt. Nicht nur im Bereich der Kriminalitätsbekämpfung und Entwicklung von Sicherheitstechnologien, sondern auch in sozialen Netzwerken ist Gesichtserkennung ein verbreitetes, aber auch umstrittenes Thema. Zahlreiche Bürger fürchten um ihre Privatsphäre, weil die technische Gesichtserkennung einige datenschutzrechtliche Bedenken provoziert und deshalb ein weites Feld für Diskussionen schafft.
Grundsätzlich unterscheidet man zwischen zwei Arten der Gesichtserkennung. Zum einen existiert die biologische Gesichtserkennung, die aber in dieser Abhandlung nicht weiter berücksichtigt wird. Zum anderen hat sich in den letzten Jahrzehnten die technische biometrische Gesichtserkennung entwickelt. Diese unterschiedet sich grundlegend in zwei verschiedenen Techniken, die in den folgenden Ausführungen näher beschrieben werden: Die 2D-Technik, bei der „eine zweidimensionale geometrische Vermessung besonderer Merkmale"[1] durchgeführt wird und die 3D-Technik, die zusätzlich auch noch mittels Streifenprojektion weitere Informationen, unter anderem die Form des Gesichtes, auswertet.[2]

Geschichte der Gesichtserkennung

Die Geschichte der Gesichtserkennung beginnt in den sechziger Jahren. Erste Konzepte zu einer halbautomatischen Gesichtserkennung wurden entwickelt und in den siebziger Jahren von Wissenschaftlern erweitert. Das Problem dieser Gesichtserkennungstechnik bestand allerdings darin, dass sämtliche Messungen manuell durchgeführt werden mussten. Erst im Jahr 1988 wurde ein Algorithmus entwickelt, welcher der automatischen technischen Gesichtserkennung, so wie sie heute bekannt ist, am ähnlichsten ist.[3]

---

[1] Gesichtserkennung – Wikipedia. (2005). Abgerufen am 22. Dezember 2012, von http://de.wikipedia.org/wiki/Gesichtserkennung.

[2] vgl. Friedrich-Schiller-Universität Jena Angewandte Biometrie. (2012). Abgerufen am 22. Dezember 2012, von http://www.informatik.uni-jena.de/dbis/lehre/ss2010/wolf/FSU-Biometrie-Modul-9.pdf.

[3] Ebenda

FERET

Die ersten Versuche, mit einer automatischen biometrischen Gesichtserkennung zu arbeiten, fanden 1993 statt, als das Verteidigungsministerium der Vereinigten Staaten, United States Department of Defense, kurz DoD, mit dem Face Recognition Technology program (FERET) begann.[4]

Ziel dieses Programms war es, Gesichtserkennungsalgorithmen zu entwickeln, die die Strafverfolgungsbehörden bei der Erfüllung ihrer Aufgaben unterstützten und somit für eine erhöhte Sicherheit sorgten.[5]

FERET bestand aus drei Phasen: In der ersten Phase wurden die Algorithmen zur Gesichtserkennung entwickelt und versucht, sie so zu etablieren, dass diese auch in der Praxis gut einsetzbar waren. In der zweiten und dritten Phase wurden diese Algorithmen immer weiterentwickelt. Nach Abschluss der zweiten Phase folgte eine Demonstration der ersten Ergebnisse, welche eine Übertragung der FERET-Algorithmen auf Echtzeitsysteme zur Folge hatte. [6]

Weitere Elemente des FERET-Programms waren neben der Ausarbeitung der Gesichtserkennungsalgorithmen das Anlegen und Zusammenstellen von Datenbanken und eine anschließende Auswertung dieser Daten. Die Datenbanken enthielten eine große Anzahl an Gesichtsbildern, die systematisch bis zum Jahr 1996 erweitert und mit detaillierten Merkmalen ergänzt wurden. Der Schwerpunkt dieses Programms lag in der Auswertung, in der die Leistungsfähigkeit des FERET-Gesichtserkennungsalgorithmus mit Hilfe der Eigenschaften aus den Datenbanken verglichen wurde.[7] Insgesamt war das Face Recognition Technology program das erste, aber auch wichtigste Programm zur Erforschung und Ausarbeitung der Gesichtserkennungstechnologien. Die Erkenntnisse, die in diesem Programm gewonnen wurden, und die Techniken, die ausgearbeitet wurden, werden bis heute in den meisten Gesichtserkennungsprogrammen (in den häufigsten Fällen von Behörden) angewendet. FERET

---

[4] vgl. Biometrie - Gesichtserkennung - Bundesamt für Sicherheit. (2010). Abgerufen am 22. Dezember 2012, von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile.

[5] vlg. Face Recognition Technology (FERET). (2011). Abgerufen am 22 Dezember 2012 von http://www.nist.gov/itl/iad/ig/feret.cfm

[6] Ebenda

[7] Ebenda

wurde im Laufe der Zeit, besonders in den Jahren 2000 und 2002, mit dem Programm "Facial Recognition Vendor Test" um einige Testszenarien erweitert und verbessert.[8] Gerade seit dem Anschlag vom 11. September 2001 sind "Biometrische Identifikationssysteme [...] wieder in den Mittelpunkt des Interesses der Sicherheitsbehörden gelangt."[9]

BioFace

Seit dem Jahre 2002 wurden auch in Deutschland vom Bundesamt für Sicherheit in der Informationstechnik (BSI) Gesichtserkennungstechnologien und -algorithmen unter dem Namen "BioFace" untersucht und erforscht. Ziel von Bioface war es, die "Leistungsfähigkeit der Systeme bei großen Datenbeständen"[10] und die "Einflüsse von Störfaktoren"[11] bei der Gesichtserkennung zu untersuchen und zu analysieren. Dabei wurden mehrere Gesichtserkennungsysteme getestet und verschiedene Szenarien, wie größere Datenbanken, Erkennung biometrischer Zwillinge, Erfassung bei schlechten Lichtverhältnissen oder auch die Erfassung bei Bildern mit einer handelsüblichen Digitalkamera, durchgeführt.[12] Das Ergebnis war ernüchternd und konnte wie folgt zusammengefasst werden:[13] Bei größeren Datenbanken und Datenmengen lässt die Identifkation durch die Algorithmen deutlich nach, auch schlechte Lichtverhältnisse und schlechte Bildqualität erschweren die Gesichtskennungsprozesse.[14] Die

---

[8] vgl. Biometrie - Gesichtserkennung - Bundesamt für Sicherheit. (2010). Abgerufen am 22. Dezember 2012 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile.

[9] BSI: BSI-Studie: BioFace. (2010). Abgerufen am 23. Dezember 2012 von https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/BioFace/bioface.html

[10] Zusammenfassung BioFace – CCCB. (2006). Abgerufen am 27 Dezember 2012 von https://www.berlin.ccc.de/mediawiki/index.php?title=Zusammenfassung_BioFace&redirect=no

[11] Ebenda

[12] vgl. Bioface: Vergleichende Untersuchungen von Gesichtserkennungssystemem. (2003). Abgerufen am 22. Dezember 2012 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFace/BioFaceIIBericht_pdf.pdf?__blob=publicationFile.

[13] BSI-Studie bemängelt Gesichtserkennung | heise online. (2009). Abgerufen am 28 Dezember 2012 von http://www.heise.de/newsticker/meldung/BSI-Studie-bemaengelt-Gesichtserkennung-87219.html

[14] vgl. Bioface: Vergleichende Untersuchungen von Gesichtserkennungssystemem. (2003). Abgerufen am 22. Dezember 2012 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFace/BioFaceIIBericht_pdf.pdf?__blob=publicationFile.

Entwicklung der Gesichtserkennungsysteme steckte noch in den Kinderschuhen, denn in den Tests von Bioface wurde festegestellt, dass die “Tauglichkeit der Gesichtserkennungssysteme [...] nicht abschließend beweis- oder widerlegbar“[15] war.

FERET und Bioface sind die beiden wichtigsten Beispiele für Gesichtserkennungs-forschungsprogramme. Die biometrische Gesichtserkennung wurde immer weiterentwickelt und dient mittlerweile nicht nur der Verbrechensbekämpfung. Auch im öffentlichen Leben, zum Beispiel auf dem Personalausweis und in sozialen Netzwerken haben sich diese Technologien etabliert und an Bedeutung gewonnen.

Technik der Gesichtserkennung

Obwohl sich die Algorithmen der Gesichtserkennung immer verändern, sich verbessern und auch untereinander verschieden sind, bleiben doch Grundstrukturen ähnlich, die im Folgenden erläutert werden.

Die Technik, bzw. der Ablauf lässt sich in zwei Teile untergliedern. Zum einen gilt es, eine Datenbank zu erstellen oder eine vorhandene Referenzdatenbank zu nutzen, “die bekannte Gesichter und deren Identifikationszuordnung enthält”[16]. Der zweite Teil besteht darin, einen Algorithmus zu erstellen oder zu nutzen, der ein neu erfasstes Bild erkennen und den Datensätzen zuordnen, beziehungsweise, wenn noch kein Datensatz vorhanden ist, zur Datenbank hinzugefügen soll.
Auf den eingehenden Bildern muss der Algorithmus zunächst ein Gesicht erkennen. Die bekanntesten Algorithmen sind dabei das Template-Matching, die Gesichtserkennung mittels geometrischer Merkmale, und das Face Bunch Graph Matching.
Beim Template Matching wird die Erkennung des Gesichtes auf einen einzelnen Ausschnitt, auf eine Maske oder Template beschränkt. Bei der “Identifikation eines unbekannten Gesichts wird ein Vergleich dieses Gesichts mit allen in der Datenbank gespeicherten Templates

[15] Ebenda

[16] Baur, D. "Automatische Gesichtserkennung: Methoden und Anwendungen." (2006). Abgerufen am 27. Dezember 2012 von http://www.medien.ifi.lmu.de/fileadmin/mimuc/hs_ws0506/papers/Automatische_Gesichtserkennung.pdf

durchgeführt."[17] *[Siehe Abbildung 1 im Anhang]*

Das Ergebnis dieses Template Matchings ist dann "ein Vektor, der die Ähnlichkeit zu den Merkmalen des jeweiligen Templates enthält"[18] Letztendlich wird daraus die Ähnlichkeit des Gesichtes und des in der Datenbank vorhandenen Templates gelesen und verglichen. Diese Methode ist allerdings sehr stark davon abhängig, wie gut die Qualität der in der Datenbank vorhandenen Templates ist.[19] Das Template Matching ist ein vergleichsweise alter Gesichtserkennungsalgorithmus mit einer nicht so großen Genauigkeit.

Bei der Gesichsterkennung mit Hilfe geometrischer Merkmale werden die besonderen Merkmale, wie Auge, Nase und Mund vermessen und "deren Position, Abstand und Lage zueinander bestimmt"[20] Auch hierbei werden die Ergebnisse in Vektoren gespeichert, die dann zur Berechnung der Ähnlichkeit zwischen den Gesichtern dienen sollen.[21] *[Siehe Abbildung 2 im Anhang]*

Zuletzt noch wird das Bunch Graph Matching erläutert, bei dem für die Gesichterkennung ein Face Bunch Graph erstellt wird. Zunächst funktioniert der Algorithmus so, dass das Gesicht

---

[17] Einleitung - merkmalbasiert oder holistisch? - arlbergnet.com. (2002). Abgerufen am 28 Dezember 2012, von http://www.arlbergnet.com/design/biometrics/face/fs_face05.htm

[18] Friedrich-Schiller-Universität Jena Angewandte Biometrie Modul 9. (2012). Abgerufen am 28 Dezember 2012 von http://www.informatik.uni-jena.de/dbis/lehre/ss2010/wolf/FSU-Biometrie-Modul-9.pdf

[19] Einleitung - merkmalbasiert oder holistisch? - arlbergnet.com. (2002). Abgerufen am 28 Dezember 2012 von http://www.arlbergnet.com/design/biometrics/face/fs_face05.htm

[20] Gesichtserkennung – Wikipedia. (2005). Abgerufen am 22. Dezember 2012 von http://de.wikipedia.org/wiki/Gesichtserkennung.

[21] Friedrich-Schiller-Universität Jena Angewandte Biometrie Modul 9. (2012). Abgerufen am 22. Dezember 2012 von http://www.informatik.uni-jena.de/dbis/lehre/ss2010/wolf/FSU-Biometrie-Modul-9.pdf>

in ein “festgelegtes Raster aus Knoten und Kanten”[22] integriert wird. Dabei werden dann “mithilfe sogenannter Jets , einem Bündel von bestimmten Knoten und Wavelets, das dem Knoten umgebene (Farb-)Muster gespeichtert.”[23] Zuletzt werden dann die “erzeugten Jets mit den Modellgraphen der Datenbank verglichen, um das Gesicht einer Person zuzuordnen”[24] Das Bunch Graph Matching ist die ausgereifste Gesichtserkennungsmethode, da sie sowohl “unempfindlich gegen Schwankungen in Bildhelligkeit und -kontrast”[25] ist, als auch das Gesicht dreidimensional erfassen und analysieren kann. *[Siehe Abbildung 3 im Anhang]*

Aktuelle Entwicklungen der Gesichtserkennung sind die 3D-Techniken, bei denen meistens die Streifenprojektion zur Erfassung der Gesichter benutzt wird.[26] Die 3D-Technik verläuft ähnlich bei der Verwendung der Algorithmen und ist am besten mit dem Bunch Graph Matchting vergleichbar. Die Gesichterkennung mit Hilfe von Dreidimensionaler Aufnahmen ist vielverspreched aber nicht so weit fortgeschritten, wie die 2D-Techniken und -Algorithmen.[27]

Insgesamt ist es so, dass Algorithmen der Gesichtserkennung ähnlich sind, allerdings werden oft unterschiedliche Merkmale erfasst und zur Erkennung hinzugezogen, sei es bei der einen Technik, die Position gewisser Kriterien oder bei der anderen einfach nur die Ähnlichkeit von Templates. Allen ist eines gemeinsam: Es werden Vektoren erzeugt, die dann durch verschiedene Prozesse zur Identifikation von Gesichtern beitragen. Die Algorithmen verbessern sich kontinuierlich und es fließen immer mehr Details zur Auswertung ein, so dass sich

---

[22] Baur, D. "Automatische Gesichtserkennung: Methoden und Anwendungen." (2006). Abgerufen am 28. Dezember 2012 von http://www.medien.ifi.lmu.de/fileadmin/mimuc/hs_ws0506/papers/Automatische_Gesichtserkennung.pdf

[23] Ebenda

[24] Ebenda

[25] Ebenda

[26] Gesichtserkennung – Wikipedia. (2005). Abgerufen am 22. Dezember 2012 von http://de.wikipedia.org/wiki/Gesichtserkennung.

[27] vgl. Gesichtserkennung – Wikipedia. (2005). Abgerufen am 22. Dezember 2012 von http://de.wikipedia.org/wiki/Gesichtserkennung.

mittlerweile die Gesichterkennung auf einem guten Weg befindet, produktiv und zuverlässig eingesetzt werden kann und sich immer weiter verbessert.

Einsatzmöglichkeiten einer Gesichtserkennung

Die Einsatzmöglichkeiten der biometrischen Gesichtserkennung sind sehr vielfältig. So werden sie sowohl zur Sicherheit, beispielsweise in Zugangsüberwachungen bei Spielkasinos[28], und Kontrolle eingesetzt, aber mittlerweile auch in sozialen Netzwerken und Software für Privatanwender zugänglich gemacht. Bei der Photoverwaltungssoftware iPhoto ist es zum Beispiels hauptsächlich Sinn und Zweck der Gesichtserkennung, bekannte Personen oder Freunde auf den eigenen Bildern zu finden, zu taggen und somit gezielt nach Bildern mit den entsprechenden Personen zu suchen.

Gesichtserkennung wird allerdings vorwiegend in Zugriffskontrollsystemen eingesetzt, aber auch im Bereich der Industrie genutzt. An öffentlichen Plätzen wie Bahnhöfen, Flugplätzen oder im Bereich des öffentlichen Personennahverkehrs wird eine Gesichterkennung ausgiebig getestet, jedoch nicht immer mit Erfolg. Beispielsweise scheiterte ein “Feldversuch des Bundeskriminalamtes (BKA) zur biometrischen Kameraüberwachung im Mainzer Hauptbahnhof [..] 2007 an schlechten Lichtverhältnissen und ständig versagender Kameratechnik.”[29] Auch die Berliner Verkehrsbetriebe testeten den Ausbau der Videoüberwachungssysteme mit Gesichtserkennung und erhofften sich dabei weniger Kriminalität auf den Bahnhöfen.[30]

Die Polizei der vereinigten Staaten ist mit der Forschung, der Entwicklung und dem Ausbau und produktiven Einsatz von Gesichtserkennungsystemen durchaus fortgeschrittener. So setzt die Polizei mittels einer Applikation einfach und schnell Gesichterkennungstechniken zur Kriminalitätsbekämpung ein. Mit der Kamera des Smartphone, in diesem Fall ein iPhone, wird

---

[28] vgl. Biometrie - Gesichtserkennung - Bundesamt für Sicherheit. (2010). Abgerufen am 27. Dezember 2012 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile.

[29] Videoüberwachung im U-Bahnhof: BVG lässt tief blicken - Taz. (2011). Abgerufen am 27. Dezember 2012 von http://www.taz.de/!22702/

[30] vgl. Berlin will Videoüberwachung mit biometrischer Gesichtserkennung. (2009). Abgerufen am 27. Dezember 2012 von http://www.heise.de/newsticker/meldung/Berlin-will-Videoueberwachung-mit-biometrischer-Gesichtserkennung-testen-204147.html

das Gesicht erfasst und mit den Servern abgeglichen. [31]

In Deutschland wiederum ist ebenfalls ein sehr wichtiges Einsatzfeld biometrischer Techniken im neuen biometrischen Personalausweis entstanden.

Insgesamt kann man sagen, dass die Gesichtserkennung zunehmend bei Sicherheitsbehörden produktiv eingesetzt werden kann, da die Technik schon sehr weit fortgeschritten ist. Momentan glänzt die USA aber mit einem weiter fortgeschrittenen Ausbau dieser Techniken. Die Entwicklung ist aber noch lange nicht vorbei, das BKA beispielsweise setzt nun schon seine "Hoffnung auf künftige Anlagen mit 3D-Gesichtserfassung."[32]

Gesichtserkennung in sozialen Netzwerken

Soziale Netzerke, wie Facebook oder Google+, haben mittlerweile auch die Gesichtserkennung implementiert. Es ist ein wichtiges Feature von sozialen Netzwerken, Photos hochzuladen, die meistens mit Freunden enstanden sind, um diese dann darauf markieren zu können. Um diesen Vorgang zu automatisieren und den Nutzern den Umgang mit der Software zu erleichtern, haben Facebook, Google+ aber auch Privatanwendersoftware wie iPhoto eine Gesichtserkennung eingebaut. Durch die Gesichtserkennung können die Nutzer Freunde und andere Menschen auf den Photos taggen, eine Funktion, die schon lange vorhanden war, aber durch die Gesichtserkennung fast automatisiert ablaufen kann. Diese Gründe sind aber nur werbewirksamer Natur, natürlich wollen die Netzwerke auch Verbindungen zwischen den Menschen analysieren und auswerten. Dabei kommt die Gesichtserkennung gelegen. Während bei Google+ und anderer Software vorher über diese Funktion informiert wird und sich der Nutzer aussuchen kann, ob er gerne die Gesichtserkennung nutzen möchte, führte Facebook seit dem 7. Juni 2011 offiziell auch in Deutschland die Gesichtserkennung ein, die schon seit Ende 2010 geplant, ausgiebig getestet und nach und nach in den Ländern, beginnend mit den

[31] vgl. Police Adopting iPhone-Based Facial-Recognition Device by BI2. (2011). 27. Dezember 2012 http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html

[32] Berlin will Videoüberwachung mit biometrischer Gesichtserkennung. (2009). Abgerufen am 27. Dezember 2012 von http://www.heise.de/newsticker/meldung/Berlin-will-Videoueberwachung-mit-biometrischer-Gesichtserkennung-testen-204147.html

Vereinigten Staaten, ausgerollt wurde, ohne die Nutzer darüber zu informieren.[33] [34] Abschalten konnte man diese Funktion nur im nachhinein auf eine für den normalen Anwender sehr komplizierte Art und Weise. Natürlich sorgte die Aktion für mediales Interesse und Kritik von Datenschützern und Nutzern. Vier Wochen nach dem Börsengang, also am also am 18. Juni 2012, kaufte Facebook das israelische Unternehmen Face.com, welches für die genaueste Gesichtserkennung bekannt ist.[35] Daran kann man deutlich erkennen, dass Facebook der Ausbau der Gesichtserkennungsfunktion im sozialen Netzwerk sehr wichtig ist. Große Kritik an der Gesichtserkennung blieb allerdings nicht aus. So beanstandete die von Max Schrems, ein Jurastudent aus Österreich, gegründete Bewegung “Europe vs Facebook” viele Datenschutzvergehen des sozialen Netzwerkes Facebook und zeigte Facebook diesbezüglich an.[36] Unter diesen Datenschutzvergehen ist auch die Gesichtserkennung zu finden, die als “ein unverhältnismäßiger Eingriff in die Privatsphäre der Nutzer”[37] bezeichnet wird. Auch Johannes Caspar, Hamburger Beauftrager für Datenschutz und Informationsfreiheit, übte Kritik an der Gesichtserkennung und verpflichtete Facebook Inc. in einer Verwaltungsanordnung “das seit langem als rechtswidrig in der Kritik stehende Verfahren der Gesichtserkennung auch rückwirkend datenschutzkonform zu gestalten.”[38] Am 21. September 2012 lenkte Facebook ein und schaltete die Gesichtserkennung in Europa ab und und versprach, sämtliche durch die

---

[33] Markus Beckedahl. Facebook aktiviert automatische Gesichtserkennung. (2011). Abgerufen am 30. Dezember 2012 von https://netzpolitik.org/2011/facebook-aktiviert-automatische-gesichtserkennung/

[34] Datenschutz: Facebook erlaubt Gesichtserkennung bei Fotos - FAZ.net. (2012). Abgerufen am 1. Januar 2013 von http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/der-facebook-boersengang/datenschutz-facebook-erlaubt-gesichtserkennung-bei-fotos-1574791.html

[35] Awesome News – Facebook Acquires Face.com | face.com. (2012). Abgerufen am 1. Januar 2013 von https://face.com/blog/facebook-acquires-face-com/

[36] vgl. 22 Anzeigen - europe-v-facebook.org. (2011). Abgerufen am 2. Januar 2013 von http://www.europe-v-facebook.org/DE/Anzeigen/anzeigen.html

[37] 22 Anzeigen - europe-v-facebook.org. (2011). Abgerufen am 2. Januar 2013 von http://www.europe-v-facebook.org/DE/Anzeigen/anzeigen.html

[38] Anordnung gegen Facebook erlassen - Detail (2012). Abgerufen am 2. Januar 2013 von http://www.datenschutz-hamburg.de/news/detail/article/anordnung-gegen-facebook-erlassen.html

Gesichtserkennung gesammelten Daten bis zum 15. Oktober zu löschen.[39] Wie oben schon erwähnt, ist Wettbewerber Google mit dem sozialen Netzwerk Google+ anders verfahren und hat die Gesichtserkennung datenschutzkonformer gestaltet, indem die Nutzer vorher informiert wurden und auswählen konnten, ob sie die standardmäßig abgeschaltete Funktion nutzen möchten oder nicht.[40] Somit ist viel Ärger erspart geblieben. Die Gesichtserkennung in sozialen Netzwerken ist daher nicht per se schlecht, sondern sollte eine optionale Funktion sein, die die Nutzer von sich aus aktivieren können, wenn sie wollen. Dann ist auch die Kritik nicht so groß.

Kritik an der Gesichtserkennung

Kritik an der Gesichtserkennung finden wir nicht nur im Bereich der sozialen Netzwerke, sondern auch außerhalb. Die Gesichtserkennung wird im Allgemeinen als Eingriff in die Privatsphäre bezeichnet und würde eher der Freiheit der Bürger schaden, als der Sicherheit zu nutzen. Im Folgenden wird erörtert, ob diese Kritik gerechtfertig ist, oder ob die Gesichtserkennung tatsächlich eine hilfreiche Technik ist, die keine Gefahr mit sich bringt.

Geheimdienst, Polizei und andere Organe der Kriminalitätsbekämpfung, Innen- und Außenverteidigung können die Gesichtserkennung nutzen, um wie oben bereits erwähnt, Kriminelle schnell zu erkennen und eine große Datenbank über sämtliche Straftäter mit biometrischen Daten anzulegen. Damit kann so schnell wie möglich vor Kriminalität geschützt und vorzeitig bei Erkennung des Gesichtes eingegriffen werden, wenn sich eine Person verdächtig verhält. Des Weiteren kann die immer weiter fortschreitende Technik dazu genutzt werden, um terroristische Angriffe oder geplante Attentate zu verhindern oder schnellstmöglich aufzuklären.

Auch der Einsatz einer Gesichtserkennung bei Zugriffskontrollsystemen ist eine gute Möglichkeit, um schnell und zuverlässig Personen zu verifizieren. Hinzu kommt noch, dass im Privatanwenderbereich und in Sozialen Netzwerken eine Gesichtserkennung eine sinnvolle Funktion ist, die den Nutzern helfen kann, gezielt nach Bildern mit bestimmten Personen zu suchen und diese dort zu markieren. Durch das intelligente System der Gesichtserkennung wird dann einiges an Arbeit erleichtert.

---

[39] vgl. Umstrittene Funktion: Facebook stoppt Gesichtserkennung - FAZ.net. (2012). Abgerufen am 2 Januar 2013 von http://www.faz.net/aktuell/wirtschaft/umstrittene-funktion-facebook-stoppt-gesichtserkennung-11899152.html

[40] vgl. Online-Netzwerke: Google+ führt Gesichtserkennung ein. (2011) Abgerufen am 5. Januar 2013 von http://www.zeit.de/digital/datenschutz/2011-12/google-gesichtserkennung

Auf der anderen Seite sträuben sich Datenschützer gegen eine Gesichtserkennung.
Zum einen stellt die Gesichtserkennung für die Privatsphäre eine Gefahr dar, weil bei der "Auswertung der Gesichtsphysiognomie Rückschlüsse auf Alter, Geschlecht oder ethnische Herkunft möglich"[41] sind. Zum anderen ist es nicht ausgeschlossen, eine eventuelle Erkrankung identifizieren zu können. Auch wenn der letzte Punkt noch nicht beweisbar ist, so „wird der Kern der Gefährdung deutlich"[42].
Des Weiteren ist es der Person unmöglich, die Nutzung und Weiterverwertung der Daten zu kontrollieren oder zu verhindern. Die Speicherung solcher Daten verstößt zudem gegen die verfassungsrechtlich geschützte Anonymität.[43] Jede Person sollte selbst bestimmen können, was mit den eigenen Daten geschieht. Jeder Bürger hat ein Recht auf Freiheit und Anonymität. Dies wird mit Gesichtserkennungsprogrammen nicht garantiert. Nutzer müssen die volle Kontrolle über ihre biometrischen Daten erhalten können und von den Vereinen oder Behörden die „Tragweite ihrer Entscheidung die Einwilligung erteilen und diese ohne äußeren Zwang treffen"[44] können. Im Allgemeinen ist die Speicherung solcher Daten nur durch ein klares Einverständnis seitens der Nutzer möglich. Ist dies nicht der Fall, so verstößt es gegen § 4a des Bundesdatenschutzgesetzes (BDSG).[45] Es wäre laut des BDSG möglich, das Gesichtserkennungssystem zu verwenden, wenn die Bilder und Daten nach der Abfrage sofort und unwiderruflich gelöscht werden. Unter den heutigen Umständen ist es möglich, die Bilder zu speichern, wenn vorher versichert wird, dass diese weder verkauft noch weitergegeben werden und nur zu betrieblichen Zwecken dienen, wie zum Beispiel als Zugangsbestätigung in einem Flughafen oder Ähnliches. Die Daten dürfen ebenfalls nur gespeichert werden, wenn sichergestellt ist, dass auch darüber hinausgehende Auswertungen nicht erfolgen, d.h. die

---

[41] Humboldt Forum Recht (HFR) - Moritz Karg: Biometrische Verfahren. (2012) Abgerufen am 4. Januar 2013 von http://www.humboldt-forum-recht.de/deutsch/7-2012/beitrag.html

[42] Ebenda

[43] vgl. Humboldt Forum Recht (HFR) - Moritz Karg: Biometrische Verfahren. (2012) Abgerufen am 4. Januar 2013 von http://www.humboldt-forum-recht.de/deutsch/7-2012/beitrag.html

[44] Humboldt Forum Recht (HFR) - Moritz Karg: Biometrische Verfahren. (2012) Abgerufen am 4. Januar 2013 von http://www.humboldt-forum-recht.de/deutsch/7-2012/beitrag.html

[45] vgl. 4a BDSG - Gesetze im Internet. (2006). Abgerufen am 5. Januar 2013 http://www.gesetze-im-internet.de/bdsg_1990/__4a.html

Feststellung der Identität der abgebildeten Person nicht anderweitig realisiert wird.

Die Nutzung und der Gebrauch ist nur unter den oben genannten Bedingungen nach § 4a des BDSG möglich und vertretbar. Jede nicht den Vorschriften nach korrekte Nutzung ist strafbar und damit verboten, auch wenn die Gesichtserkennung hilfreich für Polizei und andere Sicherheitsorgane ist.

Um dieses Problem beseitigen zu können, sollten vorher Gesetze oder Regelungen verabschiedet werden, die den Gebrauch, die Nutzung und Weiterverwertung eben dieser ganzen Daten regelt und versichert, dass die Daten nicht missbraucht werden. Bei ausstehender Regelung ist die Gesichtserkennung ein Verstoß gegen das Bundesdatenschutzgesetz. In den meisten Fällen werden die gegebenen Gesetze nicht beachtet. So ist es auch bei Facebook gewesen, die eine Gesichtserkennung eingeführt haben, ohne die Nutzer zu informieren. In öffentlichen Bereichen ist eine Ausstattung mit Gesichtserkennungsystemen von den bisherigen Überwachungssystemen ebenfalls datenschutzrechtlich bedenklich. Der Gedanke eines gläsernden Bürgers wird immer naheliegender und eine Gesichtserkennung ist daher eine deutliche Gefahr für die Privatsphäre. Wenn man dann noch bedenkt, dass die Gesichtserkennung trotz der enormen Entwicklung viele Fehler aufweist, sind Irrtümer und ungerechte Verurteilen aufgrund der fehlerhaften Systeme ein Zeichen dafür, dass im sicherheitstechnischen Bereich auf eine Gesichtserkennung vorerst noch kein Verlass ist.

Fazit

Zusammenfassend ergibt sich, dass die Gesichtserkennung eine sich sehr schnell entwickelnde und schon recht fortgeschrittene Technologie ist, die man sowohl in Privatanwendersoftware als auch in großen sicherheitstechnischen Bereichen durchaus ernst nehmen sollte. Allerdings ist die Technologie immer noch nicht komplett ausgereift und weist einige Mängel auf. Zudem ist eine Gesetzgrundlage noch nicht gegeben, die den Einsatz von Gesichtserkennung gerechtfertigt. Laut des Bundesdatenschutzgesetztes ist eine Gesichtserkennung im öffentlichen Bereich in den meisten Fällen nicht erlaubt. Aus diesem Grund ist zwar die Gesichtserkennung eine hilfreiche Technik, die aber definitiv eine Gefahr für die Privatsphäre darstellt und nicht datenschutzkonform ist.

Anhang

Abbildung 1: *Beim Template-Matching wird das Gesicht in mehrere Templates zerlegt.*[46]

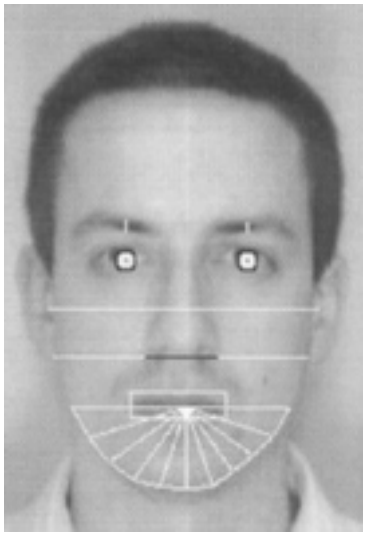

Abbildung 2: *Bei der Gesichtserkennung mit Hilfe geometrischer Merkmale werden die Gesichtsmerkmale vermessen.*[47]

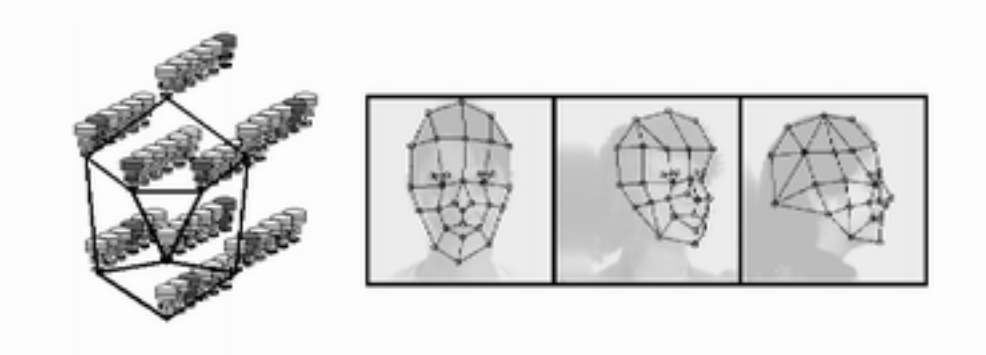

Abbildung 3: Beim Bunch Graph Matching wird das Gesicht dreidimensional erfasst und analysiert.[48]

---

[46] Bildquelle: Friedrich-Schiller-Universität Jena Angewandte Biometrie Modul 9. (2012). Abgerufen am 22. Dezember 2012 von http://www.informatik.uni-jena.de/dbis/lehre/ss2010/wolf/FSU-Biometrie-Modul-9.pdf

[47] Bildquelle: Ebenda

[48] Bildquelle: Baur, D. "Automatische Gesichtserkennung: Methoden und Anwendungen." (2006). Abgerufen am 28. Dezember 2012 von http://www.medien.ifi.lmu.de/fileadmin/mimuc/hs_ws0506/papers/Automatische_Gesichtserkennung.pdf

Quellenverzeichnis

Gesichtserkennung – Wikipedia. (2005). Abgerufen am 22. Dezember 2012, von http://de.wikipedia.org/wiki/Gesichtserkennung.

Friedrich-Schiller-Universität Jena Angewandte Biometrie. (2012). Abgerufen am 22. Dezember 2012, von http://www.informatik.uni-jena.de/dbis/lehre/ss2010/wolf/FSU-Biometrie-Modul-9.pdf.

Biometrie - Gesichtserkennung - Bundesamt für Sicherheit. (2010). Abgerufen am 22. Dezember 2012, von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile.

Face Recognition Technology (FERET). (2011). Abgerufen am 22 Dezember 2012 von http://www.nist.gov/itl/iad/ig/feret.cfm

Biometrie - Gesichtserkennung - Bundesamt für Sicherheit. (2010). Abgerufen am 22. Dezember 2012 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile.

BSI: BSI-Studie: BioFace. (2010). Abgerufen am 23. Dezember 2012 von https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/BioFace/bioface.html

Zusammenfassung BioFace – CCCB. (2006). Abgerufen am 27 Dezember 2012 von https://www.berlin.ccc.de/mediawiki/index.php?title=Zusammenfassung_BioFace&redirect=no

Bioface: Vergleichende Untersuchungen von Gesichtserkennungssystemem. (2003). Abgerufen am 22. Dezember 2012 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFace/BioFaceIIBericht_pdf.pdf?__blob=publicationFile.

BSI-Studie bemängelt Gesichtserkennung | heise online. (2009). Abgerufen am 28 Dezember 2012 von http://www.heise.de/newsticker/meldung/BSI-Studie-bemaengelt-Gesichtserkennung-87219.html

Baur, D. "Automatische Gesichtserkennung: Methoden und Anwendungen." (2006). Abgerufen am 27. Dezember 2012 von http://www.medien.ifi.lmu.de/fileadmin/mimuc/hs_ws0506/papers/Automatische_Gesichtserkennung.pdf

Einleitung - merkmalbasiert oder holistisch? - arlbergnet.com. (2002). Abgerufen am 28 Dezember 2012, von http://www.arlbergnet.com/design/biometrics/face/fs_face05.htm

Friedrich-Schiller-Universität Jena Angewandte Biometrie Modul 9. (2012). Abgerufen am 28 Dezember 2012 von http://www.informatik.uni-jena.de/dbis/lehre/ss2010/wolf/FSU-Biometrie-Modul-9.pdf

Gesichtserkennung – Wikipedia. (2005). Abgerufen am 22. Dezember 2012 von http://de.wikipedia.org/wiki/Gesichtserkennung.

Videoüberwachung im U-Bahnhof: BVG lässt tief blicken - Taz. (2011). Abgerufen am 27. Dezember 2012 von http://www.taz.de/!22702/

Berlin will Videoüberwachung mit biometrischer Gesichtserkennung. (2009). Abgerufen am 27. Dezember 2012 von http://www.heise.de/newsticker/meldung/Berlin-will-Videoueberwachung-mit-biometrischer-Gesichtserkennung-testen-204147.html

Police Adopting iPhone-Based Facial-Recognition Device by BI2. (2011). 27. Dezember 2012 http://online.wsj.com/article/SB10001424052702303678704576440253307985070.html

Markus Beckedahl. Facebook aktiviert automatische Gesichtserkennung. (2011). Abgerufen am 30. Dezember 2012 von https://netzpolitik.org/2011/facebook-aktiviert-automatische-gesichtserkennung/

Datenschutz: Facebook erlaubt Gesichtserkennung bei Fotos - FAZ.net. (2012). Abgerufen am 1. Januar 2013 von http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/der-facebook-boersengang/datenschutz-facebook-erlaubt-gesichtserkennung-bei-fotos-1574791.html

Awesome News – Facebook Acquires Face.com | face.com. (2012). Abgerufen am 1. Januar 2013 von https://face.com/blog/facebook-acquires-face-com/

22 Anzeigen - europe-v-facebook.org. (2011). Abgerufen am 2. Januar 2013 von http://www.europe-v-facebook.org/DE/Anzeigen/anzeigen.html

Anordnung gegen Facebook erlassen - Detail (2012). Abgerufen am 2. Januar 2013 von http://www.datenschutz-hamburg.de/news/detail/article/anordnung-gegen-facebook-erlassen.html

Umstrittene Funktion: Facebook stoppt Gesichtserkennung - FAZ.net. (2012). Abgerufen am 2 Januar 2013 von http://www.faz.net/aktuell/wirtschaft/umstrittene-funktion-facebook-stoppt-gesichtserkennung-11899152.html

Online-Netzwerke: Google+ führt Gesichtserkennung ein. (2011) Abgerufen am 5. Januar 2013 von http://www.zeit.de/digital/datenschutz/2011-12/google-gesichtserkennung

Humboldt Forum Recht (HFR) - Moritz Karg: Biometrische Verfahren. (2012) Abgerufen am 4. Januar 2013 von http://www.humboldt-forum-recht.de/deutsch/7-2012/beitrag.html

4a BDSG - Gesetze im Internet. (2006). Abgerufen am 5. Januar 2013 http://www.gesetze-im-internet.de/bdsg_1990/__4a.html

Eigenständigkeitserklärung

Wir erklären hiermit,
• dass wir die vorliegende Arbeit ohne fremde Hilfe und ohne Verwendung anderer als der angegebenen Hilfsmittel verfasst haben.
• dass wir sämtliche verwendeten Quellen erwähnt und korrekt zitiert haben.

_____	_____
Daniel Wagner	Simon Grass