Face(book)ing the Future of Person-Identification

In den vergangen zehn Jahren wurden biometrische Verfahren in der breiten Öffentlichkeit vorrangig unter der Anwendung der Zugangskontrolle insbesondere im Zusammenhang mit elektronischen Reisedokumenten (ePass, nPA) diskutiert. Biometrische System messen und analysieren ein biometrisches Charakteristikum wie etwa die Fingerkuppen oder das Gesicht einer Person. Der Vorgang der biometrischen Authentisierung liefert eine eindeutige Verknüpfung einer Person mit ihrer Identität unabhängig davon, wo diese Identität gespeichert ist. Der Vorgang der biometrischen Wiedererkennung lässt sich in die folgenden Schritte untergliedern:

- Erfassung der biologischen Charakteristika mit geeigneten Sensoren (Kamera, Mikrofon etc.) und Speicherung als digitale Repräsentation.
- Vorverarbeitung zur Datenverbesserung oder –bereinigung.
- Merkmalsextraktion zur signifikanten Beschreibung der Muster.
- Vergleich der Merkmale mit den Referenzdaten.

Der Vorgang bedingt, dass grundsätzlich eine Person vorab eingelernt (Enrolment) wurde, um die notwendigen Referenzdaten zu bilden. Biometrische Systeme können als Verifikationssysteme oder als Identifikationssysteme ausgelegt sein. Bei einem Verifikationssystem gibt der Nutzer eine Identität vor, zu der im System eine Referenz vorliegt. Sofern biometrische Systeme mit einem authentischen Dokument (zum Beispiel dem ePass) kombiniert werden, kann das Referenzbild auf diesem Dokument abgelegt sein. Zum Zeitpunkt der Verifikation wird ein Vergleich mit genau diesem einen Referenzbild durchgeführt (1:1 Vergleich). Bei einem Identifikationssystem hingegen wird das erfasste Bild mit vielen eingelernten Bildern verglichen und aus dieser Menge das am besten passende Muster ermittelt (1:n Vergleich). Die Ähnlichkeit zwischen beiden Bildern muss jedoch ein definiertes Mindestmaß erreichen, damit eine zuverlässige Zuordnung der mit dem Referenzbild verbundenen Identität vorgenommen werden kann.

Die Gesichtserkennung ist das biometrische Verfahren, das der Mensch selbst am häufigsten zur Erkennung verwendet. Die in der biometrischen Gesichtserkennung bislang eingesetzten Systeme verwenden im Normalfall eine Standard-Fotokamera, um zweidimensionale Frontalbilder zu erfassen. Die 3D-Erfassung ist zwar technisch möglich, aber noch wenig verbreitet. Bei der zweidimensionalen Gesichtserkennung ist es vorteilhaft, dass das Bildmaterial in sehr guter Bildqualität vorliegt. Wichtige Kriterien sind dabei eine ausreichende Ausfüllung des 2D-Bildes durch das Gesicht (etwa zu 70%), eine Frontalaufnahme, guter Kontrast, Bildschärfe, gleichmäßige Ausleuchtung, ein neutraler Gesichtsausdruck und keine Verdeckung des Gesichtes bzw. der Landmarken (z.B. Augenwinkel bzw. Mittelpunkte der Augen) durch Haare, Brillen oder Kopfbedeckungen. In den vergangen Jahren konnte eine deutliche Leistungssteigerung der kommerziellen Gesichtserkennungsprodukte beobachtet werden. Seit 1993 werden solche Produkte regelmäßig vom US National Institute of Standards and Technology (NIST) getestet. Das erste Testergebnis zeigte für eine feste False-Match Fehlerrate von 0.001 noch eine unakzeptabel hohe False-Non-Match Fehlerrate von FNMR=0,79, wie es im FERET-Report dokumentiert ist. Diese Fehlerraten konnten reduziert werden von FNMR=0,54 im FERET-Report 1997 auf FNMR=0,2 im FRVT 2002 Test. Seitdem fanden zwei weitere Tests statt, die mit FNMR=0,026 im FRVT 2006 und im vergangenen Jahr mit FNMR=0,003 im MBE 2010 eine eindrucksvolle Leistung zeigten. Diese verbesserten Leistungen machen es inzwischen möglich, dass Gesichtserkennung auch in einem Identifikationssystem eingesetzt werden kann selbst dann, wenn die Anforderungen an gute Bildqualität des Probenbildes

nicht erfüllt werden. Anwendungen in der polizeilichen Forensik sind in den letzten Jahren eingeführt worden. In den USA wird die Gesichtserkennung eingesetzt, um Duplikate von Personen mit mehrfachen Führerschein-Identitäten aufzuspüren.

Auch jenseits von polizeilichen oder hoheitlichen Anwendungen verbreitet sich die Gesichtserkennung in unserem Lebensumfeld. Besitzer eines Macintosh-Rechners können ihre vielen digitalen Bilder inzwischen mit Unterstützung der Gesichtserkennung schneller sortieren und verwalten. Dazu müssen die Gesichter von Freunden und Verwandten nur wenige Male mit einem Tag versehen – also eingelernt werden. Diese Anwendung ist sicher positiv belegt und erfreut die Anwender. Weit weniger positiv belegt ist die im Sommer 2011 von Facebook eingeführte Gesichtserkennung. Wie schon bei anderen die Privat-Sphäre beeinträchtigenden Facebook-Funktionen wurden die Nutzer darüber nicht explizit informiert. Das Einverständnis wurde stillschweigend vorausgesetzt. Zudem sind Informationen zur eingesetzten Technik oder zur Konfiguration bzw. Deaktivierung dem einfachen Facebook-Nutzer mit mittlerem Aufwand nicht zugänglich. Wie diese Vorgehensweise des Unternehmens mit Europäischen Datenschutz-Prinzipien wie etwa der Transparenz vereinbar sein soll, ist unerklärlich. Die Risiken wurden kürzlich in der Öffentlichkeit aufgeregt diskutiert. Wird damit eine globale Datenbank von Gesichtsbildern denkbar? Wird mich in Zukunft der Nachbar im Kaffee mit Namen ansprechen, der ihm für ein Foto, das er mit seiner Handy-Kamera erstellt, von Facebook geliefert wurde? Das Szenario rückt technisch in den Bereich der Möglichkeiten und wird unsere Kommunikations-Kultur vermutlich negativ verändern.

Wie jedes biometrische System kann eine Facebook-Gesichtserkennung nur funktionieren, wenn Referenzdaten eingelernt wurden. Wie ist das Szenario also zu bewerten?
Erstens ergibt sich weiter die Notwendigkeit zur Warnung an Facebook-Nutzer: Wer seine **eigenen** Bilder mit Name-Tag bei Facebook einstellt ist selbst verantwortlich, dass er durch Facebook biometrisch eingelernt wird und in der Folge durch eine Facebook-Anwendung von einem anderen Facebook-Nutzer im öffentlichen Raum biometrisch erkannt werden kann.
Zweitens sollte man aus Sicht des Datenschutzes den Vorgang des Einstellens und Markierens (Tagging) eines Bildes **einer Dritten** Person neu bewerten: Das Publizieren von Bildern ohne explizite Zustimmung der abgebildeten Person muss man als Eingriff in das Persönlichkeitsrecht der betroffenen Person sehen. Dieser Eingriff kann konkret mit unangenehmen Folgen für den Dritten versehen sein. Wie kann das juristisch betrachtet werden? Ist ein solcher Eingriff unter Strafe zu stellen?
Drittens wird es technisch spannend werden, wie die Facebook-Gesichtserkennung mit Duplikaten umgehen wird. Und darin liegt auch meines Erachtens ein ganz pragmatischer Weg, um die Erkennung im öffentlichen Raum und die unerwünschte Profil-Bildung zu verhindern. Ich konnte schon nicht verstehen, warum ich als Nutzer Facebook mein tatsächliches Geburtsdatum anvertrauen soll. Warum sollte ich dann Facebook meinen Namen **und** mein Foto (in hoher Auflösung) anvertrauen. Nun habe ich mir in Facebook unter einem Pseudonym ein zweites Nutzerkonto angelegt und dort ein Foto von mir in hoher Auflösung hinterlegt. Ich bin gespannt, ob und wann ich im öffentlichen Raum mit meinem Pseudonym-Namen angesprochen werde.

Prof. Dr. Christoph Busch,
Fraunhofer IGD
Fraunhoferstr. 5
D-64283 Darmstadt, Germany
Tel: +49-6151-155-536
email: christoph.busch@igd.fraunhofer.de http://www.igd.fraunhofer.de http://www.christoph-busch.de