4 2013

Gesichtsauflösungen

MONA KÖRTE
JUDITH ELISABETH WEISS
(HG.)

Interjekte

Herausgegeben vom Zentrum für Literatur- und Kulturforschung Berlin

INTERJEKTE ist die thematisch offene Online-Publikationsreihe des Zentrums für Literatur- und Kulturforschung (ZfL). Sie versammelt in loser Folge Ergebnisse aus den Forschungen des ZfL und dient einer beschleunigten Zirkulation dieses Wissens. Informationen über neue Interjekte sowie aktuelle Programmhinweise erhalten Sie über unseren Email-Newsletter. Bitte senden Sie eine E-Mail mit Betreff »Mailing-Liste« an *zimmermann@zfl-berlin.org*.

Bisher in dieser Reihe erschienen:

Interjekte 1 SIGRID WEIGEL: Embodied Simulation and the Coding-Problem of Simulation Theory. Interventions from Cultural Sciences (2011)

Interjekte 2 Z. ANDRONIKASHVILI, S. FRANK, G. MAISURADZE, F. THUN-HOHENSTEIN, S. WILLER: »Freundschaft: Konzepte und Praktiken in der Sowjetunion und im kulturellen Vergleich« (2011)

Interjekte 3 VANESSA LUX, JÖRG THOMAS RICHTER (HG.): »Kulturelle Faktoren der Vererbung« (2012)

Impressum

Hrsg. vom Zentrum für Literatur- und Kulturforschung Berlin (ZfL)
www.zfl-berlin.org

Direktorin Prof. Dr. Dr. h.c. Sigrid Weigel

Redaktion Dr. Christine Kutschbach

Gestaltung Carolyn Steinbeck · Gestaltung

Layout / Satz Marietta Damm, Jana Sherpa

gesetzt in der ITC Charter

Die Gesichtsauflösung in der Informationstechnologie. Wenn Maschinen erkennen sollen

Alexander Nouak

Gesichtsauflösung und Biometrie sind zunächst nur schwer zusammenzubringen. Beschäftigt man sich jedoch ein wenig mit der Informationstechnologie, so kommt man schnell darauf, dass Auflösung bei Bildern eine eklatante Rolle spielt, allerdings nicht im Sinne von wegbrechen, verschwinden sondern ganz im Gegenteil; hier meint man eher einen Detaillierungsgrad. Je höher die Auflösung eines Bildes, desto mehr kann man erkennen, desto mehr kann man aus dem Bild auslesen. Und gerade in dem Bereich, in dem ich tätig bin, ist das sehr wichtig. Weil ich aber ein fauler Mensch bin, möchte ich lieber andere für mich erklären lassen, worum es in meinen Ausführungen gehen wird.

[Film: In diesem Gebäude bringen Spitzenforscher Computern das Sehen bei. Ein kurzer Blick in die Kamera, ein Abgleich mit der Datenbank – so identifizieren Maschinen uns Menschen schon seit Jahren. Im Wesentlichen arbeiten wir zurzeit mit der so genannten 2D-Gesichtserkennung. Das heißt, es werden platte, flache Bilder analysiert. Da werden Merkmale herausgezogen und verglichen. Solche Systeme lassen sich durch simple Tricks überlisten. Damit Zugangskontrolle sicher und zuverlässig funktioniert, ist heute mehr nötig. Gesichter werden deshalb dreidimensional erfasst. Ein Vorteil ist, ich kann das Gesicht ausrichten. Ich kann es in die Position bringen, die ich brauche, um den bestmöglichen Vergleich zu erzielen. Aber dazu kommt noch, ich bin viel fälschungssicherer. Grenzkontrolle bei der Einreise, 3D-Check, hier sind Computeraugen längst technisch in der Lage, menschliches Personal zu ersetzen.]

Wir wissen also nun, es geht um Biometrie. Auch in der Biometrie gibt es eine Normung, und die entsprechenden Gremien haben festgelegt, was wir eigentlich unter Biometrie verstehen. So sagen wir zum Beispiel Biometrie und nicht Biometrik. Und das, was wir darunter verstehen, ist definiert mit: Automatische Erkennung von Individuen anhand deren Verhalten – Gangerkennung haben Sie angesprochen – und ihrer biologischen Charakteristika. Iris-Erkennung haben Sie ebenfalls angesprochen, aber es kann sich natürlich auch um das Gesicht handeln. Es ist ganz klar, wo sich der Begriff Biometrie herleitet: aus dem griechischen bios, das Leben, und metría oder metrón, die Vermessung. Die Biometrie funktioniert ähnlich, wie der Mensch auch. Zunächst muss man jemanden kennenlernen, und wenn er wiederkommt, kann ich ihn wiedererkennen. Recognition ist das bessere Wort, denn Erkennung verwechselt man gerne mit Detektion. Wir bringen übrigens nicht den Maschinen das Sehen bei – das können die selbst. Da gibt

es so Einrichtungen, die heißen Kameras, und damit können die Maschinen auch sehen. Wir versuchen allerdings, ihnen beizubringen, zu verstehen, was sie da sehen.

Wenn in einem Computer ein Vergleich stattfindet, so resultiert das in einem Vergleichswert. Dabei handelt es sich um die Wahrscheinlichkeit einer Übereinstimmung. Eine hundertprozentige Übereinstimmung wird es nicht geben, was sich als Nachteil erweist, wie wir später noch sehen werden. Wir können den Vergleich auf zwei unterschiedliche Arten anwenden: Zu einen gibt es das Verifikationsszenario. Dabei stelle ich mich dem System vor, beispielsweise durch das Einlegen meines Ausweises und in der Folge prüft das System, ob es zu dieser Identität einen Datensatz in der Datenbank finden kann. Wenn dem so ist, werden die vorliegenden Daten mit den live erfassten Daten verglichen. Das geht relativ zügig, da es sich um einen 1:1-Vergleich handelt. Zum anderen gibt es das Identifikationsszenario. Hier sieht mich das System, erfasst meine Daten und prüft nun in der Datenbank, ob vergleichbare Daten vorliegen. Und hier wie da wird ein Wahrscheinlichkeitswert errechnet, der Auskunft darüber geben soll, ob eine Übereinstimmung vorliegt oder nicht.

Und so kommen wir auch gleich zu den beiden unterschiedlichen Einsatzbereichen. Einerseits setzen wir Biometrie im Zugangskontrollszenario ein. Will ich mir also Zutritt zu einem Bereich verschaffen, werde ich mich eher kooperativ verhalten und mich dem System so präsentieren, dass es mich möglichst gut erkennt. Im Gegensatz dazu steht das Überwachungsszenario. Mehrere Kameras beispielsweise erfassen einen Raum, detektieren Gesichter und versuchen, ähnliche Gesichter in der Datenbank des Systems zu identifizieren. In diesem Anwendungsfeld muss man damit rechnen, dass ich durchaus nicht bereit bin, zu kooperieren. Wie so etwas aussehen kann, werden wir später noch sehen.

Die Biometrie hat natürlich Vor- und Nachteile. Die Nachteile werden ja lang und breit in der Gesellschaft diskutiert. Deshalb möchte ich an dieser Stelle nicht näher darauf eingehen. Aber die Biometrie hat natürlich durchaus auch Vorteile. Der Computer, mit dem ich meine Präsentation halte, verfügt über eine Kamera, das heißt, er kann sehen. Warum muss ich dann ein Passwort eintippen? Er sieht mich doch. Er könnte mich genauso gut erkennen. Das wäre für mich bequemer, weil ich mir dann kein Passwort merken muss. Insofern hätte die Biometrie für mich einen Vorteil. Die wichtigste Eigenschaft der Biometrie ist, dass eine Personenbindung hergestellt wird. Biometrie per se wird immer gerne als Sicherheitstechnologie gesehen, ist sie aber nicht. Biometrie stellt eher ein Sicherheitsrisiko dar, wie ich gleich erörtern werde. In Verbindung mit anderen Faktoren, wie zum Beispiel einem Gegenstand wie dem Pass oder Wissen wie einem Passwort oder einer PIN, kann hingegen Sicherheit verstärkt werden, weil ich diese Personenbindung herstellen kann.

Noch einmal möchte ich veranschaulichen, wie ein generisches biometrisches System funktioniert. Zwei Prozesse spielen eine tragende Rolle: der Prozess des Kennenlernens, der in unserer Sprache Enrolment-Prozess genannt wird; ein Sensor – da wir uns ja mit dem Gesicht beschäftigen, ist es wohl eine Kamera – erfasst die Daten einer Person. In weiterer Folge wird das Bild ein wenig bearbeitet und die wesentlichen Eigenschaften, die Charakteristika werden extrahiert und schließlich in der Datenbank gespeichert. Will ich eine Person identifizieren oder verifizieren, so muss ich sie erneut dem Sensor präsentieren, auch hier werden die Daten aufgearbeitet und fließen nun jedoch in das Vergleichssystem. Der Vergleichsdatensatz wird aus der Datenbank hinzugeholt und der Vergleichswert gebildet. Je nach eingestelltem Schwellwert kommt es dann zu einer Übereinstimmung oder eben nicht.

Um Biometrie betreiben zu können, müssen natürlich ein paar Voraussetzungen erfüllt sein. So muss das gewählte biometrische Charakteristikum ein gewisses Maß an Konstanz aufweisen, es muss also auf lange Sicht vorhanden sein. Das ist beispielsweise bei einem Fingerabdruck gegeben. Bereits im Mutterleib wird der Finger mit zufälligem Muster gebildet und bleibt dann mehr oder weniger – je nach Arbeitspensum – bis zum Lebensende in seiner Form erhalten. Selbst wenn Sie sich einmal in den

Finger schneiden, so werden die Fingerlinien ganz genau wieder hergestellt. Nur wenn Sie sich zu tief schneiden und dabei die untere Hautschicht verändern, kann es zu einem neuen Muster kommen. Auch das Gesicht ist relativ konstant. Wie sich das im Bezug zum Alter verhält, können uns die Doktoren und Spezialisten besser erläutern, doch man kann schon behaupten, dass sich das Gesicht im Alter zwischen 20 und 65 Jahren nicht wesentlich verändert. Danach mögen Modifikationen größeren Ausmaßes eintreten, doch hier ist noch zu prüfen, in wie weit die Erkennungssysteme davon betroffen sind. Eine weitere Voraussetzung ist die Trennschärfe; Individualität muss gegeben sein. Die Voraussetzung Universalität hingegen ist nun kritisch zu sehen. Gemeint ist, dass jeder über das Charakteristikum verfügen sollte und wir mussten ja lernen, dass dem nicht immer so ist. Doch genau betrachtet muss man sagen, dass selbst diejenigen, die ihr Gesicht verloren haben, durchaus immer noch ein Gesicht haben. Es mag nicht unserem Erscheinungsbild entsprechen, doch letztendlich ist es ein Gesicht. Biometrische Charakteristika müssen jedoch maschinell erfassbar sein. Und hier treten in Verbindung mit den Gesichtern, über die wir gelernt haben, erneut Schwierigkeiten auf. Denn für die Systeme ist das Vorhandensein gewisser Körperteile sehr wichtig. So benötigen wir in der 3D-Gesichtserkennung unbedingt die Nasenspitze und die Nasenwurzel, um daran die Gesichter auszurichten. Das wird uns mit schwer versehrten Gesichtern nur schwerlich gelingen. Und darüber hinaus müssen biometrische Charakteristika fälschungssicher sein, wir wollen keine künstlichen Merkmale akzeptieren. Ich habe ja bereits erläutert, dass Wahrscheinlichkeitswerte den Ausschlag geben. Ich muss also anhand eines sogenannten Thresholds festlegen, ab welchem Wert eine Person als wiedererkannt angesehen wird respektive als unbekannt abgelehnt wird. Mit Hilfe dieses Schwellwertes muss ich entscheiden, ob ich ein eher sichereres System betreiben möchte und dabei das Risiko eingehe, auch Berechtigte bei nicht ganz so guter Wiedererkennung abweise, oder ob ich lieber ein komfortables System bereitstelle und dabei aber auch den ein oder anderen Nicht-Berechtigten in Kauf nehme. Das sind auch die Gesichtspunkte, die wir in der Bewertung der Leistungsfähigkeit biometrischer Systeme anwenden, in unserem Evaluierungslabor.

Was ich mit dem folgenden Bild [zwei scheinbar identische auf dem Kopf stehende Gesichtsbilder; beim Drehen der Bilder wird deutlich, dass Augen und Mund in dem einen der beiden Fotos gedreht wurden] zeigen möchte, bekamen wir heute schon zur Genüge erklärt. Ich habe ein Jugendbild von mir genommen, das den Effekt verdeutlicht: Der Mensch kann Gesichter detektieren und Erkennen, wenn sie auch auf dem Kopf stehen, aber die Detailtreue ist wohl etwas in Mitleidenschaft gezogen. In der Informationsverarbeitung ist das ganz ähnlich. Es ist sicher leichter, ein Gesicht zu detektieren, wenn nur ein Kopf abgebildet ist. Die Herausforderungen steigen, wenn im Bild eine Vielzahl an Gesichtern zu erkennen sind. Für welches entscheidet sich das System? Welches der vielen Gesichter wird zuerst analysiert? Auch Verdeckungen sind in der Biometrie ein Problem oder besser: eine Herausforderung. Menschen können Menschen auch dann erkennen, wenn nur Teile des Gesichts zu sehen sind. Hier haben biometrische Systeme noch große Schwierigkeiten. Was mich persönlich jedoch noch interessiert: ich konnte feststellen, dass ich Personen auch von hinten oder von der Seite erkennen kann. Biometrische Systeme scheitern hier ja noch kläglich. Es würde mich doch sehr interessieren, warum ich als Mensch dazu in der Lage bin. Vermutlich spielen hier auch Erfahrungswerte eine große Rolle.

Was stellen wir in der Biometrie mit den Gesichtern an? Wie bringen wir den Computern bei, das, was sie da sehen, auch zu verstehen? Dazu gibt es unterschiedliche Ansätze. Einen hat uns einer meiner Vorredner schon vorgestellt: wir analysieren bestimmte markante Bereiche: Augen, Nase, Mund. Dabei haben wir noch den Vorteil, dass wir gewichten können. Ein Bart, der beispielsweise den Mund verdeckt, spielt dann keine so große Rolle mehr. Wir setzen die Priorität in der Bewertung der Augenpartie einfach höher, die der Mundpartie geringer und so kann der Bart das Erkennungsergebnis nicht mehr so tiefgreifend verändern. Denn letztendlich müssen wir ja zu einem gemeinsamen Ergebnis kommen, die Werte der

einzelnen Bereiche müssen also fusioniert werden. Alle Ergebnisse der Analysen der einzelnen Gesichter speichern wir in einer Datenbank und bilden einen Mittelwert. Wird ein einzelnes Gesicht analysiert, wird verglichen, wie stark die Bereichswerte vom Durchschnittsgesicht abweichen. Diese Abweichung ist dann der charakteristische Wert, der als Referenz für das analysierte Gesicht steht.

Ein anderer Ansatz sieht die gezielte Detektion von Landmarken vor, also charakteristischer Punkte wie Augenwinkel, Mundwinkel, Punkte um die Nase und dergleichen mehr. Diese Punkte kann ich in einem Koordinatensystem abbilden und die so erfassten Daten speichern und später vergleichen. Verfolgt man diesen Ansatz weiter, kann man ganze Gitterstrukturen entwickeln und über das Gesicht legen. Das ermöglicht mir auch, leichte Kopfdrehungen zu errechnen und so ein frontales Bild mit einem leicht gedrehten zu vergleichen. Die Methode der Eigenfaces bildet einen Durchschnitt über alle Gesichter. In der Folge wird jedes zu untersuchende Gesicht auf seine Abweichungen von diesem Durchschnittsgesicht hin analysiert. Die so entstehenden Merkmalsvektoren werden für den Vergleich herangezogen.

Ein Vorteil von Gesichtserkennungssystemen ist, dass preisgünstige Sensoren dafür verwendet werden können. Einfache Kameras, die es für wenige Euros bereits gibt, reichen völlig aus. Zudem ist es ein berührungsloses Verfahren und hinzu kommt, dass es ein akzeptiertes Verfahren ist, da wir damit bereits sehr viel Erfahrung gesammelt haben und der Mensch es tagtäglich betreibt. Das biometrische Merkmal Gesicht ist auch öffentlich zugänglich. Und genau das wirft wiederum ein Problem auf, das zurzeit in der Gesellschaft heiß diskutiert wird: wie gehen wir in Zeiten von Facebook, Google und anderer bildverarbeitender Dienste mit dem persönlichen Gut Gesicht um? Ich will auf diese Diskussionen an dieser Stelle nicht näher eingehen, doch sie sind zweifellos wichtig zu führen.

Wo können wir nun Biometrie überall einsetzen? Eines der bekanntesten Anwendungsszenarios ist die Grenzkontrolle. Seit dem Jahr 2007 bekommen wir nur noch einen "biometrischen" Pass. Ich setze "biometrisch" deshalb unter Anführungszeichen, weil die Bilder, die nun auf einem Chip im Reisepass gespeichert werden, zunächst nicht viel mit Biometrie zu tun haben. Sie werden zunächst lediglich gespeichert – in welcher Auflösung das erfolgt, werden wir gleich sehen. Breit eingesetzt wird ein darauf aufbauender Bildvergleich noch nicht, doch die Vorbereitungen wurden getroffen. Noch sind es nur Bilder – in manchen Pässen auch schon die Bilder der Fingerabdrücke – die später im Grenzkontrollprozess für den Bildvergleich herangezogen werden. Wie ein entsprechendes Grenzkontrollsystem aussehen kann, sieht man in diesem Bild: das System EasyPASS soll wohl in naher Zukunft auf allen deutschen Flughäfen zum Einsatz kommen. Es wurde in den letzten beiden Jahren intensiv getestet (bezeichnender Weise im C-Bereich des Frankfurter Flughafens, in dem nur selten jemand vorbeikommt, und auch hier nur im Ankunftsbereich. Ich hatte einmal das Vergnügen, im Bereich C anzukommen und ich musste das Personal regelrecht zwingen, mich an das System zu lassen, damit ich es mal ausprobieren kann.) Wie funktioniert EasyPASS nun? Der Pass wird auf ein Lesegerät gelegt, das zum einen die Daten aus dem Chip ausliest und zum anderen die maschinenlesbare Zone scannt. Das ist nötig, da sich aus ihr ein Schlüssel ableitet, der den Zugang zu den Daten und dem Gesichtsbild auf dem Chip überhaupt erst ermöglicht. Hat das geklappt – was nicht immer gleich da Fall ist, da die Reisenden den Pass oft zu früh wegziehen oder das Dokument schräg auflegen – öffnet sich eine Schranke und man wird in einen weiteren Bereich geführt. Man geht gewissermaßen auf eine in der Tür eingelassene Kamera zu. Die Höhe der Kamera wird auf die Größe des Reisenden angepasst und ein Bild wird von Ihnen geschossen, das in der Folge mit dem Gesichtsbild aus dem Pass verglichen wird. Danach öffnet sich – hoffentlich – die Tür und Sie haben eine Grenze überschritten. Das ist das ganze Geheimnis der „biometrischen" Grenzkontrolle und so wird das System in der nächsten Zeit ausgerollt.

[Film: Eine Grenzkontrollbeamtin prüft den Pass eines Einreisenden. Sie scheint unzufrieden mit dem Vergleich der im Pass abgebildeten Person und des Einreisenden. Dieser ahnt, was die Beamtin stört und setzt eine Sonnenbrille auf. Das Ergebnis, so ist den Reaktionen der Beamtin zu entnehmen, scheint zwar besser, aber lange noch nicht befriedigend. Der Einreisende setzt sich darauf hin auch noch ein Palästinensertuch auf den Kopf. Die Beamtin wirkt bedeutend zufriedener. Nun nimmt der Passinhaber noch ein Maschinengewehr in die Hand und präsentiert sich so der Kontrolle. Dies stellt die Grenzerin restlos zufrieden und sie lässt den Herrn passieren.]

Sie lachen, doch im Prinzip machen wir das genau so. Nur machen wir es eben schon im Vorfeld. Um ein „biometrisches" Bild im Pass abspeichern zu könne, müssen ganz bestimmte Bedingungen erfüllt sein. Ein Fotograf muss darauf achten, dass die Augen in einem bestimmten Abstand zueinander abgebildet sind. Das hat zur Folge, dass alle Gesichter etwa die gleiche Größe aufweisen, alle werden also gleich gemacht. Der Hintergrund muss einfarbig sein und darf nur einen definierten Anteil am Gesamtbild haben. Sie müssen beim Fotografieren einen neutralen Gesichtsausdruck, wie das in Wahrheit heißt, einnehmen. Das heißt, Sie dürfen weder finster dreinschauen noch lächeln, da das ja nicht ihr neutraler, entspannter Gesichtsausdruck ist. All das und mehr ist zu beachten, bevor ein Gesichtsbild im Pass gespeichert werden kann.

Wir haben ganz zu Anfang kurz das Thema Überwachungsszenario angerissen. Im Jahr 2007 hat das BKA (Bundeskriminalamt) die Qualität von auf dem Markt erhältlichen Gesichtserkennungssystemen geprüft. Schlussendlich hatte man sich für die drei größten Anbieter entschieden. 200 freiwillige Probanden hatten sich zur Verfügung gestellt und hatten die Aufgabe, die hier abgebildete Treppe oder die Rolltreppe zu benutzen, um den Mainzer Bahnhof zu verlassen. Mittels eines RFID-Chips, den sie mit sich führten, wurde die Person registriert und in der Folge geprüft, ob sie auch von den Gesichtserkennungssystemen wiedererkannt wurde. Die Ergebnisse wurden als „nicht sehr berauschend" kolportiert. Wobei hier unterstellt werden muss, dass nicht fachliche Gründe ausschlaggebend für dieses Urteil waren. Denn wir selbst hatten einen ähnlich gelagerten Test nur 3 Jahre zuvor zusammen mit dem BKA angestrengt. Dabei kam eine Erkennungsrate von etwa 20 % heraus. In dem hier vorgestellten Feldtest lagen die die Ergebnisse jedoch zwischen 60 % und 70 %. Nach einer Steigerung um das Dreifache in nur drei Jahren kann man nicht unbedingt von schlechten Ergebnissen sprechen. Zum anderen aber fiel der Versuch genau in die Zeit, als der damalige Innenminister Schäuble den sog. „Bundestrojaner" zum Einsatz bringen wollte. Da war es nicht gerade opportun für das BKA auch noch die Botschaft zu verkünden: „Gesichtserkennungssysteme im Bereich der Überwachung funktionieren wunderbar, wir werden künftig nur noch solche Systeme einsetzen!" Deshalb wurde kolportiert, die Systeme taugten nichts. Dieser Test liegt nun auch schon 6 Jahre zurück. Die damaligen Erkennungsraten bewegten sich im Bereich von 70 %. Zwar wird es zunehmend schwerer, die Raten zu verbessern, doch ich unterstelle, dass in den letzten Jahren einige Fortschritte erzielt wurden. So muss man zu dem Schluss kommen, dass Gesichtserkennung im Überwachungsszenario zweifellos einsatzfähig ist und akzeptable Ergebnisse liefern kann. So wird zurzeit überlegt, diese Technologie in (Fußball-)Stadien einzusetzen, doch da werden wohl noch andere Diskussionen auf uns zukommen (Datenschutzgesichtspunkte; die Frage: wem gehört mein Gesicht und wer darf eine Aufnahme davon machen? etc.)

Ein großes Problem in der Gesichtserkennung, und da vor allem in der 2D-Gesichtserkennung, ist das Thema Überwindungssicherheit. In einem Schaubild erkennen Sie einen meiner Mitarbeiter und nun sehen Sie die Ergebnisse eines biometrischen Systems. Auch dieses hat ein Gesicht detektiert ohne dabei zu berücksichtigen, dass es sich um einen qualitativ nicht einmal hochwertigen Schwarzweiß-Ausdruck handelt. Um diesem Problem zu begegnen haben wir uns in unserer Abteilung damit beschäftigt, wie man

die dritte Dimension in den Vergleich und die Auswertung hinzuziehen könnte. In einer Abteilung, die sich mit medizinischen Anwendungen befasst, wurde ein Vermessungsgerät entwickelt, das in der Lage ist, Objekte so zu erfassen, das ein 3D-Objekt im Computer erstellt wurde, das dort auch weiterverarbeitet werden konnte. Unsere Überlegung war nun, ob wir diesen Ansatz nicht auf Köpfe und Gesichter anwenden könnten. Der große Vorteil liegt darin, dass nun erkannt werden kann, ob es sich um einen großen oder kleinen Kopf handeln kann. Wir haben ja schon festgestellt, dass in der 2D-Gesichtserkennung alle Gesichter etwa gleich groß dargestellt werden, wir daher nicht mehr sagen können, ob es sich bei der Abbildung um einen großen Kopf handelt oder er nur sehr nahe an der Kamera stand. In der 3D-Erfassung habe ich aber auf solche Fragen eine klare Antwort. Mit der Verbindung 3D-Modelle und Gesichter lässt sich noch viel mehr anstellen, wie uns die Wissenschaftler Vetter und Blanz in diesem Video eindrucksvoll zeigen:

[Film: The morphable face model is derived from a data-set of 200 coloured 3D-scans of faces. Individual faces are combined into a single morphable model by computing dense point-to-point correspondences to a reference-face. A modified optic flow-out-rhythm establishes 3D-correspondence automatically. The morphable model combines 3D-shape- and texture-information of all example-faces into one vector space faces. We can form arbitrary linear combinations of the examples and generate continuous transitions. Starting from the average face, individual original faces are caricatured by increasing their distance from the average. Forming the average for male and female faces separately, the difference can be added to or subtracted from an individual face to change the perceived gender. Other facial attributes, such as the fullness of a face can be manipulated in a similar way. From a label set of faces, the characteristic changes are extracted automatically. In our model they are controlled by a single parameter. Differences in facial expressions captured from another face can be mapped to any individual. We now reconstruct 3D-shape and texture in order to emanate a face, given only a single photograph of a person. First we manually align the average face to the target image, roughly estimating position, size, orientation and elimination. Then a fully automated out algorithm finds the best reconstruction of the face within the morphable model. 3D-shape and texture are optimised along parameters such as size, orientation and colour-contrast. The output is a high resolution 3D-mesh of the face. It is an estimate of 3D-shape of surface colours based on a single image. Additional texture extraction improves details and texture. The reconstruction can now be rendered into the image, and a whole range of facial variations can be applied. Here we simulate weight-gain and weight-loss. Facial expression can be post-processed in images, forcing a face to frown or to smile. From this image we also estimated 3D-shape and texture and combine the photograph with 3D-computer-graphics. Cast shadows of novel objects are rendered correctly into the scene. Illumination-conditions can be changed and pose can be varied to some extent. From a single black and white image we obtain a full estimate of 3D-shape. The result of the matching procedure includes an estimate of surface colour, since the morphable model contains colour-information. Finally we show the application of our model to a painting.]

Wir arbeiten mittlerweile daran, noch mehr als nur Eigenschaften zur Wiedererkennung aus Gesichtern auszulesen, wie beispielsweise das Alter, das Geschlecht und mehr. Im Bereich der Werbung kann dies von Nutzen sein. Diesen Herren hier kennen Sie, das ist Bill Kaulitz, als er noch jung und niedlich war. Hier hat die Geschlechtsbestimmung nicht funktioniert, denn das System hat ihn als Mädchen erkannt, dafür seinen Reißverschluss als männlich ausgezeichnet. Solche Fehler können auftreten.

Da wir heute auch schon von Masken gesprochen haben, möchte ich Ihnen kurz eine interessante Geschichte erzählen. Im Jahr 2007 wurden in einer amerikanischen Stadt sechs Banken ausgeraubt. Auf Bildern der Überwachungskamera war ganz klar zu erkennen, dass es sich um einen schwarzen Täter

handeln muss. Tatsächlich aber war es ein weißer Mann, der ein Maske getragen hatte, die so gut war, dass man selbst auf Abbildungen dieser Maske nur dann erkennen kann, dass es sich um ein künstliches Gesicht handelt, wenn man es weiß. Solche Masken werden zum Beispiel in Hollywood erzeugt und werden im Internet für etwa 700 Dollar angeboten. Die kritischste Stelle in der Maske sind wohl die Augen, an denen man noch am ehesten erkennen könnte, dass es sich um Kostümierung handelt. Doch dieses Problem lässt sich ohne weiteres mit einer Sonnenbrille lösen. Dieser Herr wäre fast durchgekommen mit seinem betrügerischen Vorgehen, wenn ihn nicht jemand verpfiffen hätte. Nachdem die Polizei den Täter aufgespürt hatte, fanden sie die Maske in dem Hotelzimmer, in dem der Täter gerade wohnte.

Noch einen Dienst möchte ich Ihnen vorstellen, der sich der Vetter-Blanz-Ansätze bedient, die wir gerade im Filmbeitrag sehen konnten. Er heißt *That's my Face*[1] und bietet an, ein 3D-Modell Ihres Gesichtes anzufertigen. Auch Herr Breithaupt vom BSI, dem Bundesamt für Sicherheit in der Informationstechnik, hat diesen Dienst genutzt, um herauszufinden, wie gut solche 3D-Rekonstruktionen sind und ob man sie zur Überwindung von biometrischen Gesichtserkennungssystemen einsetzen könnte. Wie sie an den Bildern erkennen können ist das Ergebnis eine recht gute Rekonstruktion des Gesichtes. Für die Herstellung der Maske wird das Modell vom Anbieter allerdings etwas verändert und geschönt, was zwar schade, aber nicht zu ändern ist. Doch der Anbieter stellt noch weitere Möglichkeiten zur Verfügung. So lässt sich eine Vorschau anzeigen, wie Sie in 20 oder 40 Jahren aussähen, wie Sie männlicher oder weiblicher oder mit einer anderen Hautfarbe wirkten. Die so entworfene Maske können Sie sich im Anschluss zuschicken lassen. In voller Größe wären dann etwa 300 Dollar fällig, eine Minimaske, die gerade einmal in die Hand passt, wäre für 200 Dollar zu haben und – das vielleicht Interessanteste – auch einen Bastelbogen können Sie sich schicken lassen, der Sie Ihr Gesicht einfach aus Papier zusammenstecken lässt.

Zum Schluss möchte ich Sie noch auf eine der interessantesten Fragen in der Biometrie hinweisen: Wie werden biometrische Daten abgespeichert. Wir haben uns mit dieser Fragestellung intensiv auseinandergesetzt und haben Lösungen gefunden, die es möglich machen, die biometrischen Daten überhaupt nicht mehr zu speichern. Wir lösen sie auf, das heißt, wir lösen auch die Gesichter auf. Zahlreiche Informationen, die biometrische Daten begleiten, werden für die eigentliche Wiedererkennung gar nicht benötigt. Die Verfahren, die wir Template Protection nennen, speichern nur noch einen abstrakten Code, wie Sie ihn in diesem Bild erkennen können. In unserem System mit 3D-Gesichtserkennung werden zunächst mehrere 3D-Aufnahmen gemacht und in der Folge ein (Bar-)Code berechnet. Der lässt zum einen keinerlei Rückschlüsse auf die originalen Biometriedaten zu und ermöglicht zudem, dass ich die Referenzdaten, die in einem System gespeichert sind, jederzeit erneuern kann, sollte ich das wollen.

Ein Letztes wollte ich noch sagen: Herr Breithaupt hat tatsächlich versucht, mit seiner 3D-Maske unser 3D-Gesichtserkennungssystem zu überwinden. Das ist ihm aber nicht gelungen, denn so gut sind die Fälschungen dann doch wieder nicht.

1 Siehe http://www.thatsmyface.com.