Das Gesicht als Passwort

Biometrische Methoden wie Gesichtserkennung oder Iris-Scan kommen in Smartphones als Alternative zur PIN zum Einsatz.

Bernd Müller

Bei der dreidimensionalen Gesichtserkennung erfasst die Kamera des Smartphones mehrere zehntausend Lichtpunkte, um die charakteristischen Merkmale zu identifizieren.

Biometrische Methoden werden immer beliebter, um elektronische Geräte wie Smartphones oder Computer vor unberechtigtem Zugriff zu schützen. Dabei werden Merkmale, die für jeden Menschen einzigartig sind, erfasst und mit einem hinterlegten Muster verglichen. Beispiele sind der Fingerabdruck, ein Bild der Iris oder markante Merkmale des Gesichts. Bei letzterem erlaubt die neueste Technik mittlerweile einen dreidimensionalen Abgleich.

Das Vergleichsmuster muss beim ersten Registrieren angelegt werden und verbleibt auf dem Mikrochip des Geräts. Üblicherweise reichen 512 oder 1024 Bytes aus, um die Merkmale in einer mathematischen Repräsentation zu beschreiben. Als einfachste optische biometrische Methode gilt die zweidimensionale Gesichtserkennung. Dabei erstellt der Nutzer das Vergleichsmuster mit Hilfe der Frontkamera des Geräts. Ein Bilderkennungsalgorithmus bestimmt so genannte Face-Landmarks. Diese 60 bis 80 Punkte, darunter sechs bis acht Punkte um jedes Auge, liefern über ihre Koordinaten und die Winkel zwischen Verbindungslinien eine charakteristische Repräsentation des Nutzers. Bei der Verifikation ermittelt ein Algorithmus diese Werte anhand der aktuellen Aufnahme und berechnet, ob die geometrischen Abweichungen innerhalb der vom Hersteller festgelegten Grenzen liegen. Früher geschah dies mittels einer Wavelet- oder Hauptkomponentenanalyse.

Heute kommt bei der Verifikation auch Deep Learning zum Einsatz. Neuronale Netzwerke bestimmen die biometrischen Merkmale von Millionen Gesichtern. Durch ein automatisiertes Training optimiert das Netzwerk seine Erkennungsrate. Daher ist nicht klar, welche Merkmale der Gesichter wie stark gewichtet in den Vergleich eingehen. Allerdings zeigt sich, dass Augen und Nase besonders wichtig sind, gerade wenn eine Brille oder ein Bart das Aussehen signifikant verändern. Das Ergebnis des Trainings – ein Algorithmus, der die Eigenschaften des Netzwerks abbildet – ist auf dem Smartphone gespeichert und prüft bei jedem Versuch, das Gerät zu entsperren, wie gut die Merkmale zusammenpassen. Anders als bei den Face-Landmarks versteckt sich diese Information in einem Zahlenwert, den der Algorithmus mit Hilfe komplexer Mathematik bewertet. Dabei kommen Klassifikationsverfahren zum Einsatz, welche die Ähnlichkeit zwischen den Werten des neuen Bildes und des gespeicherten errechnen. Eine gewisse Toleranz ist unumgänglich, damit die Verifikation gelingt. Um diese gering zu halten und damit die Sicherheit zu optimieren, gleicht der Algorithmus Schwankungen aus, indem er in regelmäßigen Abständen einen neuen Referenzwert generiert. So passt dieser sich beispielsweise auch beim Altern automatisch an.

Um schlechte Lichtverhältnisse auszugleichen, arbeiten einige Geräte mit Infrarotlicht aus einer LED. Eine spezielle Kamera nimmt ein Bild der reflektierten Strahlung auf. Infrarotlicht mit einer Wellenlänge zwischen 870 und 950 Nanometern ist auch Basis der dreidimensionalen Gesichtserkennung, die in Smartphones der neuesten Generation zum Einsatz kommt. Licht dieser Wellenlänge ist für das menschliche Auge nicht sichtbar und blendet den Nutzer bei der Aufnahme somit nicht. Um eine Tiefeninformation zu generieren, müssen zwei räumlich leicht versetzte Systeme zusammenarbeiten. Eine Kamera nimmt das Bild eines Netzes von mehreren 10 000 regelmäßig angeordneten Lichtpunkten auf, die ein Projektor auf das Gesicht wirft. Bei der Reflexion verzerrt die dreidimensionale Form des Gesichts das Muster, sodass ein Algorithmus auf die Position der Punkte im Raum schließen kann.

Beim erstmaligen Registrieren muss der Nutzer seinen Kopf bei der

Aufnahme leicht drehen, um Aufnahmen aus unterschiedlichen Perspektiven zu erzeugen (**Abb. 1**). Eine Software bringt die Punktwolken der verschiedenen Bilder durch Rotation und Translation zur Deckung. Dazu wird beim Closest-Point-Algorithmus für jeden Punkt aus der einen Wolke der jeweils nächste Punkt aus der anderen bestimmt. Die Summe der Quadrate der Abstände über alle Punktepaare ist ein Maß für die Güte der Übereinstimmung zwischen den Punktwolken. Ziel ist es, eine Rotation und Translation zu finden, welche die Summe minimieren.

Eine Frage der Sicherheit

Die Hersteller der Geräte müssen einen Kompromiss eingehen zwischen möglichst einfacher und schneller Nutzung und möglichst hohem Schutz. Damit das Entsperren des Geräts deutlich unter einer Sekunde oder sogar unter einer Zehntelsekunde dauert, dürfen nicht zu viele Merkmale in den Vergleich eingehen. Aber weniger Merkmale reduzieren die Sicherheit, wie ein Vergleich von zwei- und dreidimensionaler Gesichtserkennung zeigt.

Die zweidimensionale Gesichtserkennung arbeitet mit einem Sicherheitslevel von 99 Prozent. Bei hundert Versuchen schlägt also einer fehl, wobei entweder ein rechtmäßiger Zugriff verweigert (false negative) oder ein unerlaubter Zugriff genehmigt wird (false positive). Weil bei der dreidimensionalen Gesichtserkennung deutlich mehr Merkmale in den Vergleich eingehen, steigt das Sicherheitslevel auf 99,9 Prozent.

Um eineiige Zwillinge sicher zu unterscheiden, braucht es andere Methoden, wie das Erkennen des Fingerabdrucks oder des Irismusters, weil nur diese beiden biometrischen Merkmale für jeden Menschen verschieden sind. Mit dem Irismuster lässt sich ein Sicherheitslevel von 99,999 Prozent erreichen, das gegenüber der Gesichtserkennung deutlich erhöht ist. Zum Vergleich: Bei einer vierstelligen PIN liegt die Trefferwahrscheinlichkeit bei 1:10 000.

Die Werte für die biometrischen Methoden gelten aber nur, wenn die Systeme nicht willentlich getäuscht werden. Weil die zweidimensionale Gesichtserkennung keine Tiefenmerkmale abgleicht, ist es hier möglich, den Algorithmus mit einem ausgedruckten Foto des eigentlichen Nutzers zu überlisten. Bei der dreidimensionalen Variante braucht man dagegen eine Maske des Gesichts: Mit der entsprechenden Software ließe sich aber auch diese aus Fotografien mit einem 3D-Drucker erstellen. Und selbst der Abgleich des Irismusters lässt sich austricksen: Dem Chaos Computer Club gelang es, das Infrarotbild einer Iris aufzunehmen und auf eine Kontaktlinse zu projizieren. Hundertprozentige Sicherheit gibt es also nicht.

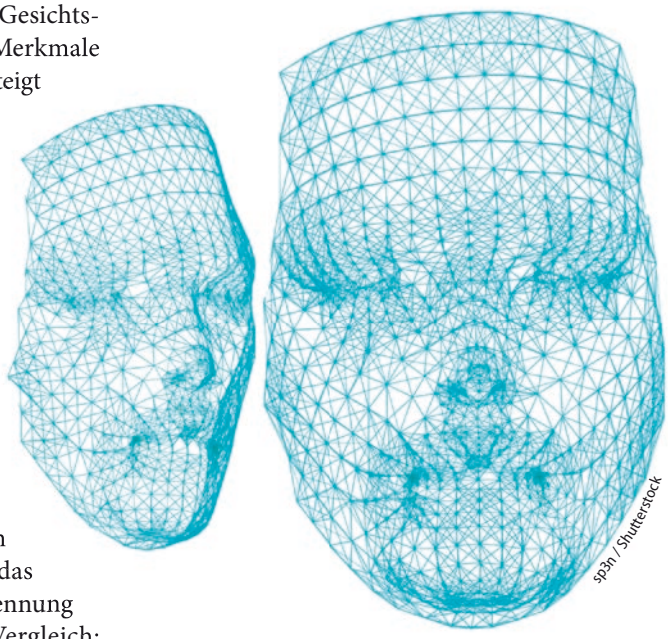

Abb. 1 Die Konturen des Gesichts reflektieren die Lichtpunkte leicht verzerrt. Daraus lässt sich eine dreidimensionale Repräsentation des Gesichts berechnen, die an eine Maske erinnert.

*

Ich danke Dr. Andreas Braun, Biometrie-Experte bei PwC in Luxemburg, für seine Unterstützung.