

■ Fingerabdruck als Passwort

Passwörter und PINs könnten bald der Vergangenheit angehören, wenn künftig unser Fingerabdruck als Identifikation dient und uns Zugang zu Laptops oder Geldautomaten gewährt.

Fingerabdrücke nützen längst nicht mehr nur der Polizei, um Verbrecher zu überführen. Schon heute finden sich in einigen Laptops, Handys und Memory-Sticks Sensoren, die den Benutzerzugriff nur nach erfolgreicher Erkennung des richtigen Fingerabdrucks gewähren und so eine unberechtigte Nutzung des Gerätes verhindern sollen. Digitale Fingerabdrücke könnten in Zukunft als personen- gebundene Merkmale auch an vielen anderen Stellen PINs und Passwörter ersetzen: etwa als Zugangsschlüssel für hochsensible Sicherheitsbereiche (z. B. in Flughäfen), für Geldautomaten oder beim Einkaufen („touch and pay“).

Im November 2007 soll der deutsche ePass der zweiten Generation¹⁾ eingeführt werden, auf dessen Chip die Fingerabdrücke zusammen mit dem digitalen Foto des Passinhabers gespeichert sind. Diese biometrische Authentisierung²⁾ setzt voraus, dass jeder Fingerabdruck einzigartig und unveränderlich ist. Unter zehn Millionen Menschen finden sich nur zwei zum Verwechseln ähnliche Muster. Dafür verantwortlich sind die feinen Linien auf der Fingerkuppe – die sog. Papillarleisten –, die ein charakteristisches Muster aus Wirbeln, Bögen oder Schleifen bilden, das tief in der oberen Hautschicht verankert ist.

Im Gegensatz zu PINs und Codewörtern lässt sich ein Fingerabdruck theoretisch nicht stehlen. Zuverlässige Fingerabdruck-Sensoren müssen allerdings hohe Anforderungen erfüllen: Sie sollen nicht nur anwenderfreundlich einen Fingerabdruck in wenigen Sekunden erfassen und erkennen, sondern auch gelungene Silikon-Kopien entlarven. Daher werden ergänzende Verfahren entwickelt, die den Puls bzw. den Sauerstoffgehalt im Blut messen oder ein Wärmebild aufnehmen.

Fingerabdruck-Sensoren arbeiten heute meist mit optischen



Gemeinsam mit Siemens hat die Luft-hansa ein biometrisches Check-in- und Boarding-Verfahren getestet, das Flug-gäste per Fingerabdruck identifiziert.

Das System wandelt charakteristische Merkmale der Fingerkuppe in einen zweidimensionalen Code um und druckt ihn auf eine Bordkarte.

oder kapazitiven Verfahren. Bei optischen Sensoren vermeiden dreieckige Glasprismen, deren große Basisfläche als Auflage für den Finger dient, Verzerrungen, die bei der zweidimensionalen Abbildung eines dreidimensionalen Objekts auftreten können (Abb. 1a). Eine LED als Lichtquelle, eine Linse und eine CCD-Zeilenkamera vervollständigen den Sensor, dessen Funktionsweise – wie beim Regensensor³⁾ – auf der Totalreflexion beruht.

Die LED beleuchtet die transparente Sensorfläche durch das Prisma hindurch unter einem Winkel von 45°, der größer ist als der Grenzwinkel der Totalreflexion. Ohne Finger auf der Sensorfläche wird daher das gesamte einfallende

Licht an der Grenzschicht total reflektiert. Liegt nun ein Finger auf dem Sensor, so ist zwischen den einzelnen Papillarleisten Luft eingeschlossen, sodass das Licht auch hier total reflektiert wird. Nur dort, wo die Papillarleisten in direktem Kontakt mit der Sensoroberfläche stehen, erhöht sich aufgrund des geänderten Brechzahlverhältnisses der Grenzwinkel, sodass keine Totalreflexion mehr stattfindet. Eine Linse (in der Grafik nicht eingezeichnet) sammelt das am Fingermuster reflektierte Licht und lenkt es auf die CCD-Zeilenkamera, die anhand der detektierten Signale den Fingerabdruck in Graustufen abbildet. Für ein vollständiges Bild wird die Fingerkuppe zeilenweise

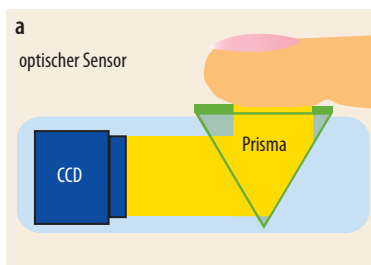
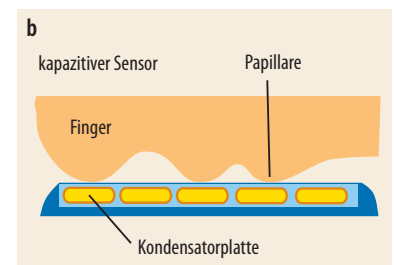


Abb. 1 Optische Fingerabdruck-Sensoren arbeiten mit Glasprismen (a). Bei kapazitiven Sensoren verändert die



Struktur der Fingerkuppe den Abstand des Minikondensators und damit die gemessene Kapazität (b).

1) Informationen zum ePass: www.epass.de

2) Biometrische Verfahren nutzen personen- gebundene (Gesichts- form, Handgeometrie, Iris) oder verhaltens- bezogene Merkmale (Stim- me, Anschlagrhythmus auf einer Tastatur).

3) vgl. Physik Journal März 2007, S. 64

abgetastet. Die so entstandenen Bilder haben eine Auflösung von bis zu 500 dpi mit immerhin 20 Bildpunkten pro Millimeter.

Im Vergleich zu den relativ großen optischen Sensoren bestehen kapazitive Fingerabdruck-Sensoren, die u. a. in Laptops oder Handys integriert sind, durch ihre Kompaktheit und ihren geringen Preis. Als Auflagefläche dient eine etwa 1,5 Quadratzentimeter große, mit einem dünnen Schutzfilm versehene Siliziumschicht, die aus etwa 65 000 winzigen, regelmäßig angeordneten Kondensatorzellen besteht. Dieses Array bildet zusammen mit der aufliegenden Fingeroberfläche einen Kondensator. Durch die Hauttrillen ergeben sich unterschiedliche Plattenabstände d für die einzelnen Minikondensatoren, wonach sich die Kapazitäten C gemäß $C = \epsilon_0 A/d$ (A : Fläche des Kondensators und ϵ_0 : Dielektrizitätskonstante) ändern (Abb. 1b). Aus diesem kapazitiven Ladungsbild des Fingerabdrucks lässt sich ein Graustufenbild generieren, dessen Auflösung durch die Anzahl der Kondensatorzellen bestimmt ist und ebenfalls etwa 500 dpi beträgt.

Neuere Sensoren nutzen Ultraschall zur Abtastung der Fingerkuppe und bilden diese anhand der Echostärke ab. Da Ultraschallwellen weit in menschliches Gewebe eindringen, liefert ein Ultraschallsensor sogar bei verletzten, ver-



Cross Match Technologies

Ein neuartiger Fingerabdruckscanner für die Einführung des deutschen e-Passes der zweiten Generation

schmutzten, zu feuchten oder zu trockenen Fingern zuverlässige Ergebnisse. Ultraschallwellen, deren Wellenlängen mit etwa 0,1 mm den Abständen und Breiten der Papillarleisten entsprechen, tasten die Fingeroberfläche aus unterschiedlichen Winkeln ab. Die reliefartigen Strukturen an der Fingerkuppe zeigen ein unterschiedliches Reflexionsverhalten. Aus der Laufzeit und Größe der detektierten Echos berechnet sich der Abstand des jeweiligen Empfängers zur Fingeroberfläche. Daraus wird ein dreidimensionales Bild von dessen Struktur erzeugt.

Um eine Person anhand ihres Fingerabdrucks möglichst schnell zu identifizieren, muss die Größe des digitalen Datensatzes reduziert werden. Aus diesem Grund wird in

der Regel nicht der gesamte Fingerabdruck, sondern eine Kombination aus charakteristischen Punkten auf der Fingerkuppe gewählt. Dabei handelt es sich um sog. Minutien, also unterschiedlich orientierte Endungen und Verzweigungen der Papillarleisten, deren Position spezielle Algorithmen aus dem vollständigen Datensatz extrahieren.

Auf jedem Finger finden sich gut 40 Minutien, deren Muster sich in Sekundenschnelle mit einem hinterlegten Referenzmuster vergleichen lassen. Fingerabdrücke sind identisch, wenn eine hohe Anzahl gleicher Minutien erkannt wird. Meist genügen bereits 14 Minutien für eine sichere Identifikation.

Da ein Finger bei jedem Scan anders auf der Sensorfläche liegt, sind zwei digitale Abbilder eines Fingerabdrucks niemals identisch. Die Parameter, die über den Toleranzbereich entscheiden, müssen entsprechend eingestellt sein, damit ein Nutzer nicht zu häufig, z. B. beim Einloggen in seinen Computer, zurückgewiesen wird. Fingerabdrücke werden daher meist nicht auf ihre Gleichheit, sondern nur auf eine hinreichende Ähnlichkeit untersucht. Aus diesem Grund wird bei hohen Sicherheitsanforderungen eine Kombination verschiedener Methoden, wie z. B. die Identifikation über Fingerabdruck und Iris-Scan, favorisiert.

Katja Bammel

Dr. Katja Bammel,
science & more
redaktionsbüro,
kb@science-and-
more.de