



Daumen als Schlüssel

Die Biometrie wertet Körpereigenschaften aus und besitzt damit wesentliche Vorteile gegenüber traditionellen Techniken der Identifikation. Denn jeder Mensch trägt seine Körpermerkmale stets bei sich. Diese Merkmale sind eindeutig und sehr schwer nachzuahmen.

Von
Dr. Manfred Bromba,
Gerd Hribernig und
Dr. Thomas Scheiter

Das Computerzeitalter hat uns neue Formen des Zugangsschutzes beschert, Wissen erlaubt den Zugriff auf PCs oder Mobiltelefone. Ein Paßwort hier, ein PIN-Code (Personal Identification Number) dort: Je mehr wir im Alltag mit Maschinen an Stelle von Menschen kommunizieren, desto unbequemer gerät dieser Paßwort-Mechanismus. Darüber hinaus sinkt die Sicherheit sofort auf Null, wenn jemand über die Schulter sieht oder ein Paßwort errät. Biometrische Systeme überwinden all diese Schwächen. Zur biometrischen Authentifikation sind etwa Sprache, Irismuster und, wie hier betrachtet, auch Fingerlinien geeignet. Bei einer Authentifikation beweist eine Person, daß sie die ist, für die sie sich ausgibt. Für diese Merkmale gibt es bereits Erkennungssysteme. Besonders die Identifikation anhand der Fingerlinien besitzt allerdings die folgenden Vorteile gegenüber den meisten anderen Verfahren:

- Die Kriminaltechnik beschäftigt sich seit vielen Jahrzehnten mit dem Fingerabdruck. Sogar ein Gericht erkennt ihn als eindeutiges Merkmal an.
- Jeder Mensch hat eindeutige Abdrücke. Niemals wurden identische Fingerabdrücke von unterschiedlichen Personen gefunden.
- Die Aufnahme geschieht kurz und schmerzlos: Ein Druck auf einen Sensor genügt. Es ist nicht nötig, in unangenehmen Positionen zu verharren. Die Abgabe des Fingerabdrucks ist ein bewußt gesteuerter Vorgang im Unterschied etwa zur Gesichtserkennung.
- Die Fingerlinien bleiben während des gesamten Lebens nahezu unverändert.

Prinzipiell gibt es zwei Arten, eine Anfrage an ein Fingerabdrucksystem zu stellen: Bei der Authentifikation gibt der Benutzer seine Identität etwa mit einer Chipkarte bekannt, das System überprüft dann seine Identität. Bei der Identifikation sind hingegen die Daten mehrerer Personen gespeichert, das System ermittelt die Identität der Anfrageperson.

► Den Fingerabdruck verarbeiten

Das bekannteste biometrische Verfahren ist die Ausweiskontrolle. Der Kontrollleur vergleicht die im Ausweis vermerkten Kennzeichen, etwa Gesicht, Größe, Augenfarbe und Unterschrift, mit denen des Ausweisbesitzers. Aufgrund des Identitätsnachweises lassen sich dem Besitzer weitere Daten wie Name

und Adresse zuordnen. Es ist auch möglich, nach der Kontrolle bestimmte Maßnahmen zu ergreifen, zum Beispiel den Zutritt zu einem Raum gewähren. Eine elektronische Identifikation läuft ganz ähnlich ab. Zunächst wird das biometrische Kennzeichen, in unserem Fall der Fingerabdruck, über einen geeigneten Sensor erfaßt. Bekannte Sensoren basie-

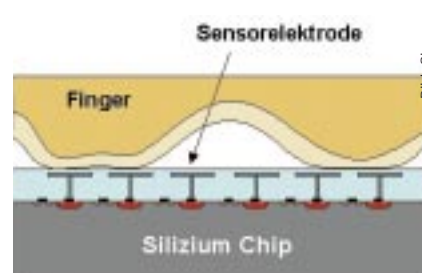


Bild: Siemens

Ein Feld von 256*256 Zellen mißt über die Kapazität den Abstand der Haut zur Sensorfläche

ren auf optischen, drucksensitiven, akustischen oder kapazitiven Messungen. Eine akustische Messung ist zum Beispiel die Ultraschallabtastung.

Nachdem ein Sensor ein Merkmal erfaßt hat, vergleicht ein Rechner die aufgenommenen Daten mit den gespeicherten Referenzmerkmalen berechtigter Personen. Gegenüber einem einfachen PIN-Code ist der Vergleich bei einem biometrischen Verfahren naturgemäß komplexer. Das Abbild des Fingerabdrucks ist typischerweise 50 kByte groß. Ein 1:1-Vergleich zwischen zwei zu unterschiedlichen Zeiten aufgenommenen Fingerabdrücken

würde nahezu automatisch zur Abweisung des Berechtigten führen. Grund dafür ist die statistische Natur der vom Sensor aufgenommenen biometrischen Daten, die neben den eigentlichen Merkmalen noch einen hohen Anteil an redundanter Information enthalten. Es ist nämlich nicht alles, was in der bildlichen Darstellung sichtbar ist, charakteristische Information.

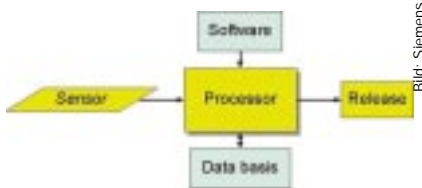


Bild: Siemens

Der Sensor leitet die Bilddaten an den Prozessor weiter, der sie mit den gespeicherten Daten vergleicht

Weiterhin ändert sich die Position des auszuwertenden Fingers von Mal zu Mal. Ein Finger läßt sich nicht wie ein harter Gegenstand exakt ausrichten, so daß gelegentlich Merkmale wegfallen, ein anderes Mal welche hinzukommen. Je nach Auflagedruck und Rauschen, etwa durch Verschmutzung des Fingers, ist damit zu rechnen, daß der Sensor mitunter einzelne Merkmale nicht erkennt. Nicht zuletzt spiegelt sich sogar die psychische Verfassung des zu Überprüfenden in der Qualität des aufgenommenen Bildes wieder.

Die Software muß deshalb redundante Daten und Störungen entfernen. Anschließend findet ein statistischer Vergleich der verbleibenden Merkmalsätze statt. Ein Programm prüft, wie genau die Aufnahme mit dem Referenzabdruck übereinstimmt. Ab einem einzustellenden Schwellwert gilt der Fingerabdruck als erkannt, andernfalls wird er abgewiesen. Über diesen Schwellwert kann der Administrator das System zwischen den beiden Extremen „sehr sicher“ und „sehr bequem“ konfigurieren. Ist die Schwelle hoch, wird mit Sicherheit nur der Berechtigte zugelassen, allerdings wird er gelegentlich auch abgewiesen. Ein ähnlicher Effekt tritt auch bei Paßwörtern auf: Mit der Länge des Paßworts steigt nicht nur die Sicherheit der Kontrolle, sondern wegen der unvermeidlichen Tippfehler auch die Wahrscheinlichkeit, daß ein Berechtigter möglicherweise zurückgewiesen wird.

Bei Übereinstimmung erfolgt die Freigabe etwa für die Benutzung eines Rechners oder eines Netzwerks. Je nach Software liegt der Rechenaufwand für den Prozessor bei ungefähr 10 Millionen Operationen. Der benötigte Arbeitsspeicher kann bei einer optimierten Lösung unter 100 kByte liegen. Für den Programcode ist mit 10 kByte zu rechnen, und die extrahierten Merkmale in der Datenbasis bean-

spruchen etwa 200 Bytes pro Fingerabdruck. Darin ist noch eine Menge Redundanz enthalten, denn 200 Bytes entsprechen 2^{600} (10^{181}) Möglichkeiten, während es bisher nur vielleicht 10^{11} Menschen auf der Erde gegeben hat. Auch die Zahl der unterscheidbaren Fingerabdrücke liegt wesentlich niedriger, nämlich bei etwa 10^{14} .

► Ein Sensor erfaßt 65.536 Meßpunkte

Der von Siemens entwickelte Fingerabdruck-Sensorchip wurde in 0,8 µm-Standard-CMOS-Technologie hergestellt. Das Sensorzellenfeld besteht aus einem Array von 256 x 256 Sensorelektroden, die in einem Raster von 50 µm angeordnet sind. Daraus resultiert eine Sensoraufösung von 500 dpi (dots per inch). Die aktive Sensorfläche beträgt ungefähr 160 mm². Im Unterschied zu den bereits verfügbaren optischen Sensoren zur Aufnahme von Fingerabdrücken ist der Siliziumsensorchip lediglich Bruchteile eines Millimeters dick und läßt sich mit Hilfe der VLSI-Technologie (VLSI = Very Large Scale Integration) sehr kostengünstig produzieren. Die Aufnahme der Hautstruktur der Fingerkuppe erfolgt mit Hilfe einer kapazitiven Abstandsmessung.

Die Kapazitätsmessung jeder einzelnen der über 65.000 Sensorelektroden wird auf dem Chip gemessen und in einen digitalen Grauwert des Fingerabdruckbildes umgewandelt. Auf dem Chip sind neben dem Sensorzellenfeld noch folgende Einheiten untergebracht:

- ein Analog/Digital-Wandler für die gemessenen Kapazitäten,
- eine Steuereinheit,
- ein 1 MHz Taktgeber sowie
- eine parallele Schnittstelle, die 8 bit/Pixel digitaler Daten an die Auswerteeinheit liefert. Es ist also keine weitere Schnittstellenschaltung notwendig, um den Chip zum Beispiel direkt an einen PC anzuschließen.

► Die Software-Auswertung

Es gibt zwei Wege, Körperdaten darzustellen: bildgebende und nicht bildgebende Verfahren. Die nicht-bildgebenden Verfahren er-

fassen beispielsweise Frequenzspektren der Fingerlinien. Charakteristische Frequenzspektren haben den Vorteil, daß unter anderem sogenannte Rotationsvarianzen elegant umgangen werden können. Größter Nachteil dieser Verfahren ist jedoch die schlechte Transparenz bei der Beurteilung der Ergebnisse, da es keinerlei interpretierbare Schnittstelle in der Verarbeitungskette gibt und damit mögliche Fehler schwer zu lokalisieren sind.

Bei bildgebenden Verfahren erzeugt ein Sensor ein Rohbild. Das aufgenommene Bild ist nur ein Ausschnitt des Fingerabdrucks. Eine Filterstufe bereitet dieses Rohbild auf, um im nächsten Schritt Fingerlinien und Elementarmerkmale aus dem Bild zu extrahieren und mit den Merkmalen anderer Fingerabdrücke zu vergleichen. Wie bei vielen Bildverarbeitungsaufgaben versucht man im ersten Schritt die Schwächen der Aufnahmetechnik und Störungen herauszufiltern. Die Einflüsse unterschiedlicher Quellen und Sen-



Bild: Siemens

Biometrische Verfahren bieten zahlreiche Vorteile gegenüber der klassischen Identifikation mit Wissen und Besitz. Ein Paßwort und eine Smart Card kann man schließlich leicht vergessen

soren müssen entfernt beziehungsweise normiert werden.

Neben stochastischen Störungen wie etwa Pixelrauschen gibt es bedingt durch die Aufnahme schwerwiegende negative Einflüsse auf die Bildinterpretation. Schmutz auf der Haut oder auf dem Sensor erzeugt flächige Störungen; bedingt durch das Auflegen des Fingers kommt es zu Dynamikdrifts über das Bild. Aus der Problembeschreibung kann man die Anforderungen an die Bildvorverarbeitung erkennen. Zum Einsatz kommen dabei Methoden zur Linienvollständigkeit (Dilation), die auf unterschiedliche Weise die lokalen Unterschiede zwischen Fingerlinienberg und Fingerliniental verstärkt. Die Linien werden dabei voll durchgezogen, Einschnitte und Poren werden geschlossen. Durch Schmutz oder Hautfalten entstehen sehr oft Unterbrechungen mehrerer paralleler Linien, auch diese Fehler sind zu be-

seitigen. Anschließend wird der Grundtyp des Linienmusters eines Fingers bestimmt, und daraus werden zusätzliche globale Merkmale wie etwa der Abstand zwischen ausgezeichneten Punkten abgeleitet. Anhand dieser globalen Beschreibung lassen sich die Abdrücke grob kategorisieren. Der exakte Vergleich erfolgt dann auf Basis lokaler Merkmale. Diese lokalen Merkmale, auch Minutien genannt, werden in zwei Grundtypen geteilt: Divergenz oder Linienende beziehungsweise Bifurkation oder Gabelung. Je nach Anwendung werden diese Merkmale noch zu höherwertigen Merkmalen zusammengefaßt, zum Beispiel zu Inseln oder Punkten. Es gibt Richtlinien, wie viele Elementarmerkmale übereinstimmen müssen, damit das Ergebnis eindeutig ist. Zwölf Merkmale gelten in der Kriminaltechnik als si-

chere Identifikation einer Person. Allerdings kommen für gerichtsrelevante Gutachten zusätzlich noch weitere Informationen zur Auswertung.

Die Möglichkeiten der Bildnormierung sind um so größer, je höher die Grauwert- und die laterale Auflösung sind. Die Grauwertaufklärung liegt meist bei 256 Graustufen, in der Praxis werden diese Stufen jedoch niemals ausgenutzt, da durch die Intensität der Tinte beim Papierverfahren oder durch das Meßprinzip nur ein Teil der Dynamik in jedem Fingerabdruckbild enthalten ist. Die laterale Auflösung muß nach dem Abtasttheorem von Shannon mindestens doppelt so hoch wie die kleinste im Bild enthaltene Struktur sein. Das bedeutet für die Fingerabdruck-Erkennung eine laterale Auflösung von mindestens

300 dpi (dots per inch). Das Ziel des ersten Verarbeitungsschrittes ist es, ein normiertes Bild ohne Störungen und mit Betonung der Linien zu erzeugen. Der nächste Arbeitsschritt, die sogenannte Encodierung, erfaßt die Elementarmerkmale. Die Merkmale werden in ihrer Lage absolut zu einem Fixpunkt oder relativ zueinander erfaßt. Zusatzinformation, wie etwa der Winkel, verbessern die Genauigkeit bei der Beurteilung der Musterübereinstimmung. Zum Auffinden der Elementarmerkmale gibt es verschiedene Methoden. Der „klassische Ansatz“ geht von den Fingerlinien aus und ermittelt die Tangenten zu den Fingerlinien. Schneiden sich diese Tangenten auf bestimmte Weise, befindet sich ein Merkmal an dieser Stelle. In der Mustererkennung sehr bewährt haben sich neuronale Netze.

INFO

Sicherheit versus Komfort

Bild: Siemens



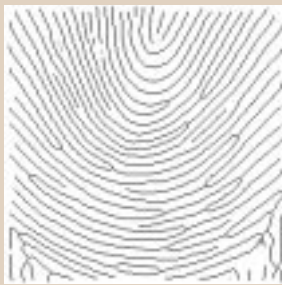
Der Sensor erzeugt ein Rohbild des Fingerabdrucks

Bild: Siemens



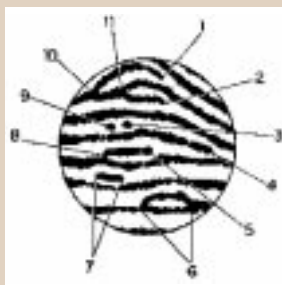
Eine Filterstufe entfernt Bildstörungen etwa durch Schmutz

Bild: Siemens



Anschließend normiert ein Programm das Bild und extrahiert die Fingerlinien

Bild: Siemens



Die Elementarmerkmale eines Fingerabdrucks: Divergenz (1, 2, 4, 5), Bifurkation (8, 10, 11), Insel (6), kurze Linie (7) und Punkte (3, 9)

durch eine Art „Lebenderkennung“ durch die Kontrollperson ausgeschlossen. Es darf nicht reichen, dem Kontrolleur ein Foto seines Gesichts hinzuhalten. An dieser Stelle machen sich die Unterschiede der einzelnen Sensorprinzipien bemerkbar: Teilweise ist eine Lebenderkennung nämlich Bestandteil des Funktionsprinzips. Ein Drucksensor läßt sich nicht von einem Foto und ein optischer Sensor, je nach Meßprinzip, nicht von einem Wachsabdruck täuschen.

Während bei der Fingerprintauthentifikation die Sicherheit gegen unberechtigten Zugriff im Vordergrund der Diskussion steht, sind bei vielen Anwendungen auch die unberechtigten Zurückweisungen von großer Bedeutung. Für einen verletzten Finger ist es recht einfach, eine Abhilfe zu finden: Es müssen lediglich mehrere Finger als Referenzfinger gespeichert werden. Schwieriger ist es hingegen in vielen Fällen, mit trockenen, kalten oder sehr feuchten Fingern zurechtzukommen. Hier ist in besonderem Maß der Sensor gefordert, aber auch die Software muß solche Fälle erkennen und berücksichtigen. Die Referenzfingerabdrücke zu speichern, auch Enrollment genannt, ist übrigens ein besonders kritischer Arbeitsschritt. Die dazu erforderliche Autorisierung muß besonders gesichert werden. Dies kann etwa durch eine spezielle PIN geschehen, die nach Gebrauch sicher verwahrt wird. Beim Enrollment ist weiterhin darauf zu achten, daß die Referenzabdrücke eine hohe Qualität besitzen, denn diese bestimmt insbesondere die Wahrscheinlichkeit einer unberechtigten Zurückweisung.

Trotz jahrelanger kriminalistischer Erfahrung mit Fingerabdrücken ist die Fingerprint-Identifikation nur dann sicher, wenn alle Angriffsmöglichkeiten genau betrachtet und so gut wie möglich ausgeschlossen werden. Wie bei allen Sicherheitssystemen gilt: Ein Authentifikationssystem ist korrumpierbar, die Frage ist nur, mit welchem Aufwand. Jeder einzelne erfolgreiche Angriff muß teuer sein als der potentielle Schaden.

Ein Angreifer kann das Sensorsignal kopieren, er kann die Referenzen in der Datenbasis von außen ersetzen, er kann die Software manipulieren und schließlich kann er das Freigabesignal beson-

ders einfach fälschen, wenn es unverschlüsselt ist. All diese Alternativen sind aber aus anderen Anwendungen bereits bekannt und lassen sich am einfachsten dadurch lösen, daß man wie bei der Chipkarte die Zahl der Schnittstellen nach außen reduziert. Da das Freigabesignal allerdings extern gebraucht wird, kommt hier nur eine Verschlüsselung zum Beispiel in Verbindung mit einem sogenannten Challenge-Response-Verfahren in Frage.

Zunächst ist sicherzustellen, daß der Finger auch wirklich echt ist und nicht aus Wachs oder Silikon. Bei der menschlichen Ausweiskontrolle ist diese Manipulation

Diese Netze lernen Merkmale von Nichtmerkmalen zu unterscheiden und ermitteln dadurch die Position der Minuten. Die ermittelten Minuten werden in Merkmalslisten gespeichert. Dadurch sinkt der Speicherbedarf von typisch 50-100 kByte für das Bild auf wenige 100 Byte pro gespeichertem Abdruck. Der Vergleich zweier Merkmalslisten, das sogenannte Matchen, bringt einige Probleme mit sich. Je nach Aufnahmetechnik und Einsatzszenario müssen Änderungen in den Positionen der Elementarmerkmale berücksichtigt werden. Das System muß mit Rotation, Translation und Skalierung zurecht kommen können. Schwierigkeiten gibt es zusätzlich mit Schmutz auf dem Sensor oder auf dem Finger. Mit geeigneten Algorithmen beim Matchen lassen sich diese Hürden im allgemeinen umgehen.

► *Der Finger ersetzt das Gedächtnis*

Das Handy ist ein sehr gutes Beispiel für eine sinnvolle Anwendung des Fingerprintsensors. Für das Mobilnetz GSM ist bereits viel unternommen worden, um Mißbrauch zu verhindern. Das war hauptsächlich notwendig, um den Netzzugang gegen unbefugte Nutzung zu sichern. Hier könnte ein Mißbrauch schon mal Tausend Mark Gebühren pro Tag verursachen.

Je nach Netzbetreiber sind mehr als fünf PIN-Codes zulässig, um Dienste einzeln abzusichern. Sämtliche Sicherheitsfunktionen werden über die SIM-Karte (Subscriber Identification Module) abgewickelt, was sich als eine sehr zuverlässige Methode erwiesen hat. Die eigentliche PIN kann je nach Sicherheitsbedürfnis des Nutzers zwischen vier und acht Stellen betragen. Die SIM-Karte fragt beim Einschalten des Handys die PIN ab und schützt vor unberechtigter Netzbenutzung. Vorausgesetzt, das Handy war ausgeschaltet! Wer die PIN vergessen hat, benötigt die achtstellige Master-PIN, um eine neue PIN auszuwählen. Ein vier- bis achtstelliger Gerätecode, den der Handybesitzer eingeben muß, macht den Diebstahl des Handys sinnlos, da der Code beim Einsetzen einer SIM-Karte erneut einzugeben ist. Andernfalls ist das Gerät nicht weiter zu benutzen. Die eigene SIM-Karte kann der Besitzer durch Sperrung beim Netzbetreiber umgehend deaktivieren.

Verglichen mit anderen biometrischen Verfahren zeichnet sich die Fingerprint-Identifikation dadurch aus, daß sie wenig Strom verbraucht und in absehbarer Zeit sehr kostengünstig realisierbar sein wird. Auf der CeBIT '98 zeigte Siemens ein Demonstrationsmodell eines Fingertip-Handys, das die Einbuchung



Ein Handy, das einen Fingerabdruck erkennt, kann Gebührenmißbrauch verhindern. Hier ein Prototyp der Firma Siemens: Ein umgebautes SL10.

in das Mobilfunknetz steuerte. Die Fingerprint-Software lief noch in einem externen Notebook, ist aber prinzipiell auch auf dem handy-eigenen DSP (Digital Signal Processor) implementierbar. Da der DSP während der Identifikationsphase für weitere Aufgaben nicht benötigt wird, wäre dies sogar eine sehr kostengünstige Lösung.

Wichtigster Vorteil des vorgestellten Prototypen des Fingertip-Handys ist die komfortable Bedienung: Anstelle von bis zu neun Tastendrücken bei der PIN-Eingabe ist lediglich ein einziger „Fingertip“ erforderlich. Da keine zusätzlichen Tasten nötig sind, ist die Identifikation mit Fingerabdruck ein geeigneter Kandidat für zukünftige tastenarme „Easyphones“. Dieser Komfort ließe sich wiederum dadurch in zusätzliche Sicherheit ummünzen, daß nicht nur der Einschaltvorgang, sondern jedes einzelne Telefonat per „Fingertip“ bestätigt wird. So dürfte ein Fingertip-Handy auch schon mal im eingeschalteten Zustand unbewacht liegenbleiben, ohne daß der Besit-

zer sich allzu sehr um eine hohe Telefonrechnung sorgen müßte.

Neben dem Wegfall aller Nachteile einer PIN ist beim Fingertip-Handy auch an zusätzliche Anwendungen und Dienste wie Home-Banking, Authentifizierung an Kassenautomaten und Türöffnerfunktionen zu denken. Mit dem Fingertip-Handy wäre es recht einfach, Familien- oder Abteilungsmitglieder zuzulassen, die über Fingertip automatisch erkannt würden. So könnte wiederum eine automatische Zuordnung der Gebühren zu den Benutzern der Handys erfolgen.

► *Die Karten der Zukunft*

Auch der Chipkartenmarkt wird von dem System profitieren. Eine zukunftsweisende Lösung besteht darin, sämtliche Funktionen von Fingertip, also den Sensor, den Prozessor, die Datenbank und die Software in einem Chip zu vereinen. Das klingt derzeit noch visionär, wird aber in wenigen Jahren keine Utopie mehr sein. Integriert die Karte alle Komponenten, sind Schnittstellen, die sonst Angriffen ausgesetzt sein könnten, nicht mehr von außen zugänglich. Ebenso sind alle Referenzfingerabdrücke nur in der Karte gespeichert, womit die persönlichen Merkmale im Besitz des Karteninhabers verbleiben und die Risiken einer zentralen Datenbank elegant umschifft werden. Besitzt man eine solche Fingertip-Chipkarte, ist diese im Prinzip für alle Authentifikationsaufgaben geeignet, in denen heute noch eine PIN- oder Paßworteingabe gefordert ist. Das löst auch gleich das Problem der Vandalismussicherheit, das auftritt, wenn der Sensor zum Beispiel in einen Bankautomaten eingebaut ist. Selbst beim Handy könnte man daran denken, das gesamte Fingertip-System auf einer SIM-Karte unterzubringen, die dann zentral im Bedienfeld zu plazieren ist.

Mit dem Fingerprintsensor auf Siliziumbasis ist eine deutliche Reduktion der Kosten gegenüber bisherigen Verfahren verbunden. Da es sich beim Handy und bei der Chipkarte jedoch um extrem kostensensitive Produkte handelt, wird noch einiges an Entwicklung zu leisten sein, bevor sich die Fingertip-Authentifikation in diesen Anwendungen durchsetzen kann. Dies dürfte in etwa zwei Jahren erreicht sein, wenn es gelingt, noch preiswertere Substrate als Silizium einzusetzen. Auch im Hinblick auf eine Standardisierung ist einiges zu tun, da GSM eine biometrische Identifikation in seiner derzeitigen Fassung noch nicht berücksichtigt.

Literatur: Woop, M.-B.; Baltus, R.: „Biometrische Identifikation“, Funkschau 1997, Ausgabe 20, Seite 65-66. (72)

INFO

Die Autoren

Die Autoren arbeiten in verschiedenen Projekten bei Siemens, die eng mit der Entwicklung neuer biometrischer Verfahren zu tun haben.

Dr. Manfred Bromba ist für das Fingertip-Projekt im Siemens-Bereich Private Kommunikationssysteme verantwortlich. Gerd Hribernig ist Leiter der Softwareentwicklung für Fingerabdruck-Erkennung bei Siemens in Graz. Dr. Thomas Scheiter leitet die Entwicklung des Sensors im Siemens-Bereich Halbleiter.