Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 86 (1995)

Heft: 1

Artikel: Biometrische Personenidentifikation mit elektronischen Mitteln

Autor: Brüderlin, René

DOI: https://doi.org/10.5169/seals-902411

Vor etwa zehn Jahren begann man in unserem Land in breiterem Ausmass elektronische Systeme für die Zutrittskontrolle von Gebäuden einzurichten. Die grosse Mehrheit dieser Anlagen basierte auf Personenidentifikation mit PIN-Code oder mit maschinell lesbaren Ausweiskarten. Vor ebenfalls zehn Jahren kamen die ersten sogenannten biometrischen Systeme auf den Markt, Systeme, die die Identität einer Person automatisch unter Verwendung von biologischen oder verhaltensmässigen Merkmalen feststellen. Preis und Arbeitsgeschwindigkeit dieser Systeme haben sich inzwischen so verbessert, dass an eine breitere Anwendung gedacht werden kann. Nachstehend folgt eine Übersicht über heute verfügbare biometrische Identifikationssysteme.

Biometrische Personenidentifikation mit elektronischen Mitteln

■ René Brüderlin

Seit Jahren werden automatische Hilfsmittel eingesetzt, um die Identität und die Berechtigung von Personen für die Durchführung verschiedener Transaktionen festzustellen. Darunter fallen: Eintritt in Gebäude und Areale, Zeiterfassung in Betrieben, Zugriff auf Datenverarbeitungsgeräte und -netze, Zugriff auf Spezialfunktionen von Geräten und Anlagen (z. B. Schlüssel von Chiffriergeräten), Bezug von Bargeld (Postomat, Bancomat), Zugriff auf Bankkonten, bargeldloser Zahlungsverkehr usw. In allen diesen Fällen geht es darum, die Identität einer Person festzustellen, zusammen mit der Berechtigung, die entsprechende Handlung zu vollziehen. Personen können auf drei Wegen identifiziert werden (Bild 1):

- durch das, was eine Person besitzt
- durch das, was eine Person weiss
- durch charakteristische Eigenschaften einer Person
- durch Kombinationen dieser drei Identifikationsmittel

Die schon am längsten angewendete Methode ist der *Besitz:* der Schlüssel. In unserer Zeit kamen Sichtausweise (Pass, Identitätskarte usw.) und automatisch lesbare Karten (Karten mit Magnetstreifen, Induktionsschaltkreisen, eingebetteten integrierten Schaltungen, passiven oder aktiven Sendern oder anderen physikalischen Effekten) dazu, die ebenfalls zur Kategorie «Besitz» gehören. Vor- und Nachteile dieser Methoden sind bekannt: Sie sind vor allem einfach und verhältnismässig billig, anderseits kann Besitz verlorengehen, gestohlen oder an Unberechtigte weitergegeben werden. Mit automatischer Lesung von Karten lässt sich die Berechtigung dieser Karte differenziert nach Zeit und Ort, aber nicht die Berechtigung der sie besitzenden Person feststellen.

Zur zweiten Kategorie, *Wissen*, gehören die sogenannte PIN (Persönliche Identifikations-Nummer) und das Passwort, die vor allem im Zusammenhang mit dem Zugang zu Computereinrichtungen populär wurden. Sofern keine triviale Zahlen-

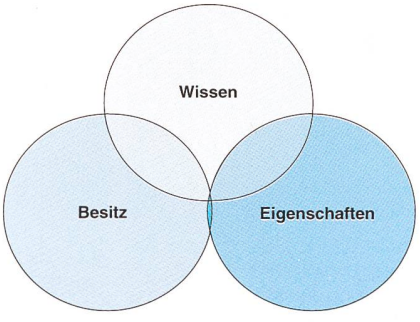


Bild 1 Mittel der Personenidentifikation

Adresse des Autors:
René Brüderlin, Dipl. El.-Ing. ETH, Identix AG (Europe), 8003 Zürich.

Buchstaben-Kombination gewählt wird (wie z. B. das eigene Geburtsdatum, die Telefonnummer oder ähnliches) und häufig genug gewechselt wird, bieten PIN und Passwort eine recht gute Sicherheit. Daneben ist das Verfahren einfach und verhältnismässig kostengünstig. Nachteile sind: das Vergessen, das Notieren an leicht zugänglichen Orten, die Weitergabe an Nichtberechtigte. Die Verwaltung von Passwort und PIN kann deshalb zum Problem werden.

Die Kombination maschinell lesbare Karte und PIN bietet eine nochmals höhere Stufe der Sicherheit, besonders gegen Diebstahl und Verlust. Leider wird auch hier die Sicherheit häufig eingeschränkt durch den falschen Gebrauch: Eine auf der Karte notierte PIN reduziert im Verlustfall deren Sicherheitswert auf praktisch null.

Methoden und Kriterien der biometrischen Identifikation

Bei den Verfahren zur biometrischen Personenidentifikation werden physiologische Eigenschaften und/oder wiederkehrende, aber individuell differenzierbare Verhaltensmuster zur Identifikation benutzt. Als eine frühe Anwendung biometrischer Merkmale zur Identifikation können die in jedem Reisepass festgehaltenen Angaben angesehen werden: die Fotografie des Trägers, zusammen mit den (meist nicht kontrollierten) Angaben zu Grösse, Haar- und Augenfarbe usw. Uns geht es hier jedoch um die automatische Prüfung solcher Merkmale. Von neueren, erst etwa in den vergangenen zehn Jahren diskutierten und auf den Markt gebrachten biometrischen Identifikationsverfahren sind bis jetzt folgende bekannt und praktisch eingesetzt:

- Stimmerkennung (Eigenschaft/Verhalten)
- Erkennung der Handgeometrie (Eigenschaft)
- Erkennung der Dynamik der Unterschrift (Verhalten)
- Erkennung des Netzhautmusters des Auges (Eigenschaft)
- Erkennung des Fingerabdruckmusters eines oder mehrerer Finger (Eigenschaft)

Noch gearbeitet wird an Verfahren zur Erkennung von Gesichtszügen (Eigenschaft), zur Identifikation mittels Tastenanschlag-Charakteristiken auf einer PC-Tastatur (Verhalten) und zur Erkennung der Irismuster des Auges (Eigenschaft) [1].

Gegenüber der elektrisch oder magnetisch lesbaren Karte haben alle diese Verfahren den Nachteil höherer Komplexität: Die Erkennung der Merkmale bereitet mehr Mühe, da sie nicht in maschinencodierter Form vorliegen, sondern zuerst über Erkennungsprozesse erfasst werden müssen, und da die meist grosse Zahl der Merkmale in geeigneter Weise auf ein leicht speicherbares *codiertes Muster* reduziert werden muss.

Nachstehend werden die bis heute kommerziell erhältlichen Verfahren der biometrischen Identifizierung beschrieben und deren Vor- und Nachteile kurz skizziert. Alle diese Verfahren können durch zwei Werte charakterisiert werden, die aber in den meisten Fällen nicht berechenbar sind, sondern durch umfangreiche Versuche statistisch erfasst werden müssen:

- die *falsche Rückweisung* berechtigter Personen (False reject rate, FRR, auch als Fehler Typ 1 bezeichnet)

Bild 2 Handgeometrie-Erkennungsgerät
Das Bild zeigt ein Gerät von Recognition Systems.

- die *falsche Zulassung* nicht berechtigter Personen (False acceptance rate, FAR, auch Fehler Typ 2 genannt)

Zu bemerken ist hier, dass bei den oft nicht sehr sachlichen Quervergleichen biometrischer Methoden mit konventionellen, wie Magnetkarte, Chipkarte und PIN, auch bei letzteren von FAR und FRR gesprochen werden sollte: Eine vergessene PIN kann zum Beispiel durchaus als falsche Rückweisung betrachtet werden! Wir werden im folgenden diese statistischen Werte, soweit sie durch unabhängige Tests [2, 3] bekanntgeworden sind, als Qualitätsmerkmal hinzuziehen.

Gemeinsam ist diesen biometrischen Verfahren auch, dass zunächst mit den Berechtigten ein Registrierprozess durchgeführt werden muss (das Gerät «lernt die Merkmale erkennen»), der mehrere Regi-

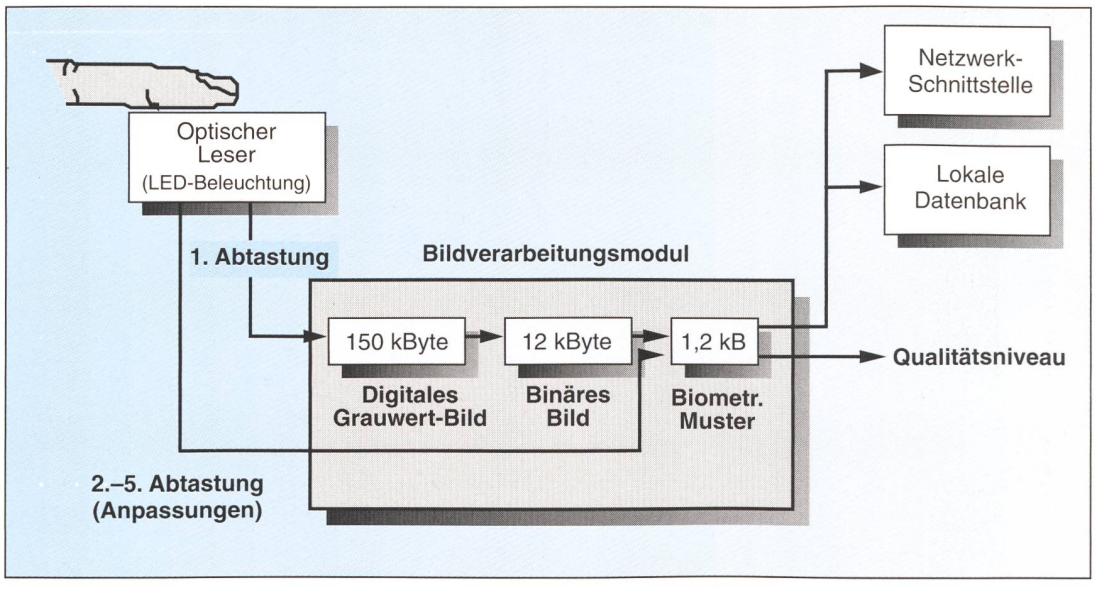
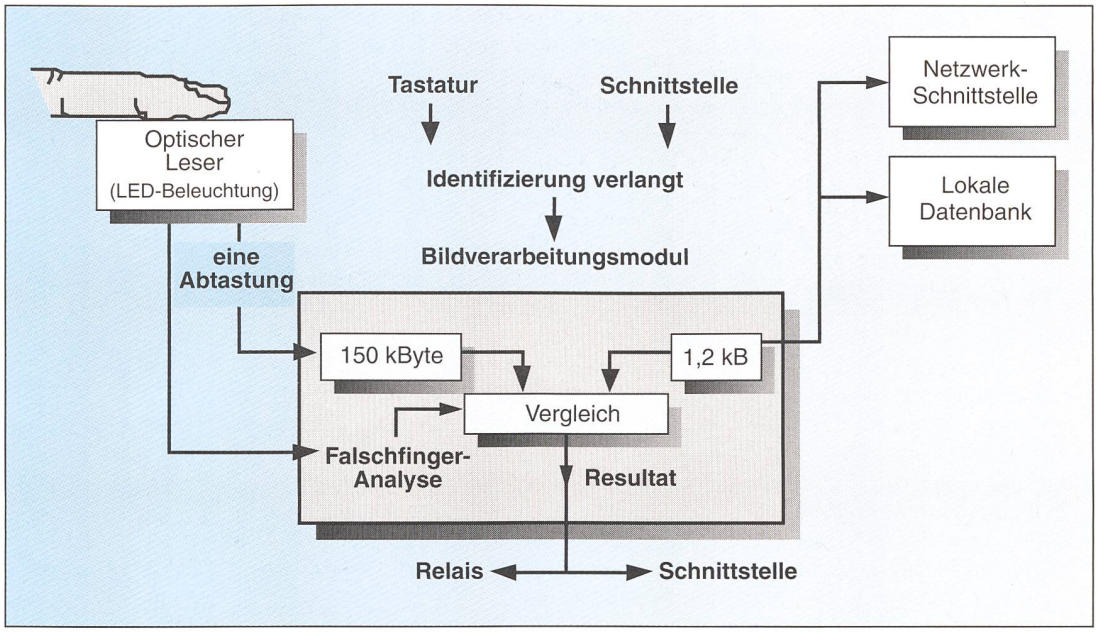


Bild 3 Diagramm der Registrierung eines Fingerabdrucks mit einem Fingerabdruck-Identifiziergerät

Bild 4 Diagramm der Personenidentifizierung mit einem Fingerabdruck-Identifiziergerät



strierungen umfasst und aufgrund dessen ein Muster (englisch: template) erstellt und abgespeichert wird. Im Identifizierungsprozess wird hernach dieses Muster mit den präsentierten Merkmalen verglichen und die mehr oder weniger gute Übereinstimmung als Zulassungskriterium verwendet. Schliesslich ist den meisten dieser Verfahren gemeinsam, dass sie die Identität einer Person nur feststellen können, wenn diese «sagt, wer sie ist». Mit andern Worten: Unbekannte Personen können mit diesen Mitteln nicht (oder nur sehr schwer) identifiziert werden. Dies jedoch ist die Aufgabe, die sich der Polizei stellt und die mit andern Mitteln gelöst wird (AFIS: Automatic Fingerprint Identification Systems).

Personenidentifikation aufgrund der Handgeometrie

Geräte zur Personenidentifikation aufgrund der Handgeometrie besitzen eine Öffnung, die das Hinlegen der flachen (rechten) Hand ermöglichen. Um eine einheitliche Positionierung zu erreichen, führen Stifte die einzelnen Finger der Hand an den richtigen Platz. Die Geräte messen die Dimensionen von vier Fingern (Länge, Breite, Fläche) sowie die Dicke der Hand aufgrund einer Abtastung mit einer CCD-Kamera und vergleichen die Daten mit einem bei der Registrierung gerechneten, 9 Byte umfassenden Vektor (Bild 2).

Dieses bezüglich der Erfassung nicht sehr komplexe Verfahren resultiert in einer Registrierung, die mit drei Wiederholungen auskommt, und in einer kurzen Identifikationszeit (etwa 2 Sekunden). Allerdings ist die Sicherheit nicht sehr hoch: FAR-Werte von 0,1 bis 1% sind, je nach Einstellung, übliche Resultate. Entsprechend liegen die Rückweisungsraten FRR in derselben Grössenordnung. Das nicht umfangreiche Muster lässt sich bequem auf einer Chipkarte oder sogar in einem Strichcode unterbringen; dementsprechend ist auch die Speicherfähigkeit von Einzelgeräten recht hoch (bis 20 000 Handmuster). Die Grösse der Geräte ist, gegeben durch die Abmessungen der grössten zu erwartenden Hand, nicht vernachlässigbar.

Unterschrifterkennung

Hier handelt es sich nicht um eine biologische Eigenschaft des zu Identifizierenden, sondern um ein Verhaltensmuster. Die Methode wirkt dadurch attraktiv, dass bis heute das Unterschreiben von Dokumenten als Identitätsbeweis in vielen Transaktionen Gültigkeit hat (Bankdokumente, Verträge usw.). Die automatischen Verfahren, die auf dem Markt sind, orientieren sich jedoch nicht am Unterschriftsbild, wie dies zum Beispiel ein Bankkassierer tut, sondern an der Dynamik der Handbewegungen beim Vorgang des Unterschreibens.

Die Geräte zur Unterschrifterkennung, von denen es verschiedene kommerzielle Ausführungen gibt, arbeiten mit einem mit dem Gerät elektrisch verbundenen Stift, mit einem druckempfindlichen Tablett oder mit beidem. Die Schwierigkeit der Erfassung und Berechnung des Musters besteht darin, die invarianten Teile der Unterschriftsdynamik von den variablen zu trennen und nur die ersteren für die Erkennung zu verwenden (dies ist das Grundproblem aller verhaltensorientierten Verfahren). Bis heute haben diese Geräte, im Vergleich zur konventionellen Unterschriftsprüfung auf visueller Basis, eine recht hohe Rückweisungsrate FRR von mehr als 10% gezeigt, was sie für Bankapplikationen nur schwer akzeptabel machte. Für physische Zutrittskontrollen sind sie wegen des Zeitbedarfs für die Identifizierung weniger geeignet. Hochsicherheitsanwendungen scheitern an der zu hohen FAR von ebenfalls etwa 10%.

Personenidentifikation durch Stimmerkennung

In allen sprachorientierten Anwendungen (z. B. Telefonnetze) ist die Erkennung eines Benutzers über die Charakteristiken seiner Stimme ein Mittel, das mit einem einfachen, überall verfügbaren Eingabegerät (Telefon) auskommt. Für die Stimmerkennung (nicht zu verwechseln mit der Spracherkennung, wo es um die Erkennung von Sprachinhalten geht) wird die zeitliche und spektrale Zusammensetzung sowie der Energieverlauf der Sprache analysiert und daraus ein charakteristisches Muster abgeleitet. Die Systeme sind relativ fälschungssicher, da auch ein Stimmenimitator nicht die einzelnen spektralen Komponenten seiner Stimme willentlich beeinflussen kann. Zu knacken ist das System jedoch mit einer Tonbandaufnahme der echten Stimme.

Die Systeme verlangen in der Regel, dass ein bestimmtes Wort gesprochen wird, das dann in seiner Zusammensetzung mit dem vorher aufgenommenen Muster verglichen wird. Nach unabhängigen Tests

liegt die FRR aber relativ hoch (10–30%), und auch die FAR erreicht eine ähnliche Grössenordnung. Für höhere Sicherheitsanforderungen sollten solche Systeme deshalb lediglich in Kombination mit andern Verfahren angewandt werden.

Das Auge als Träger von Erkennungsmustern

Eines der ersten kommerziell bekanntgewordenen biometrischen Verfahren war die Abtastung der Augennetzhaut. Die Blutgefässe der Netzhaut bilden ein Muster, das ähnlich wie der Fingerabdruck völlig individuell ist. Die vor etwa zehn Jahren eingeführten Geräte tasten deshalb mittels eines Infrarot-Laserstrahls die Netzhaut auf Merkmale ab und bilden damit ein Muster von etwa 250 Byte Länge, das zum Vergleich dient. Dazu ist nötig, dass der Benutzer in das betreffende Gerät hineinblickt – möglichst mit dem unbewaffneten Auge, um Verzerrungen zu vermeiden. Die Identifikation geschieht innert etwa einer Sekunde. Die Fälschungssicherheit ist sehr hoch, da die Netzhautstruktur mit konventionellen Mitteln nicht nachgeahmt werden kann, und die Eigenschaften-Varianz ist hoch genug, um die FAR auf 10^{-6} sinken zu lassen. Die FRR liegt bei etwa 1–2%. Problematisch ist das Gerät dadurch, dass die Benutzer schlecht akzeptieren, einen Laserstrahl (obwohl ungefährlich) in ihr Auge eindringen zu lassen. Ausserdem ist die Montagehöhe an einer Wand in Anbetracht der sehr verschiedenen Körpergrössen der Benutzer kritisch, da die Distanz des Geräts zum Auge nur etwa 2 cm betragen darf.

In neuer Zeit ist ein Gerät bekannt geworden, das die Iris des Auges erfasst und als Muster verwendet. Die Varianz der Merkmale ist etwa sechsmal grösser als bei Netzhaut und Fingerabdruck. Das Gerät ist aber noch nicht kommerziell erhältlich.

Fingerabdruck als Identifikationsmerkmal

In unabhängigen Tests hat sich neben der Netzhautprüfung die Fingermusterprüfung als weitaus sicherstes Verfahren erwiesen. Die Varianz der Merkmale ist bei diesen beiden Verfahren gross genug, um grosse Populationen zweifelsfrei unterscheiden zu können, und Doppelgänger sind zumindest bei der Fingermustererkennung – aufgrund der bald hundertjährigen Erfahrung der Polizei – bisher nicht bekannt geworden. Die heute bekannten Fingerabdruck-Erkennungsgeräte sind seit mehr als zehn Jahren in verschiedensten Applikationen im Einsatz, haben sich also praktisch bewährt.

Konzept eines Fingerabdruck-Erkennungsgerätes

Nachstehend sei das Konzept eines spezifischen Fingerabdruck-Identifiziergerätes, des Touch Lock von Identix, etwas genauer beschrieben [4]. Die Erfassung des Abdrucks geschieht durch Auflegen des Fingers auf ein Prisma. Dieses ist beleuchtet, und das Licht wird an allen Stellen, auf denen keine Haut aufliegt, totalreflektiert. Dadurch entsteht ein Bild des Fingerabdrucks nur, wenn der aufgelegte Finger eine dreidimensionale Struktur aufweist. Eine CCD-Kleinkamera nimmt das Grauwertbild auf, zusammen mit spektralen Informationen, welche bestätigen, dass ein lebender (d. h. blutdurchströmter) Finger aufliegt.

Erstmaliges Registrieren

Beim erstmaligen Registrieren wird das entstehende Graustufenbild, das etwa 150 kByte (500 Pixel pro Zoll, 8 Bit pro Pixel) enthält, gespeichert und danach in zwei Schritten zuerst in ein Schwarzweissbild mit etwa 15 kByte und dann mittels Algorithmen in ein mathematisches Muster von 1,2 kByte Länge reduziert (Bild 3). Dieses wird zusammen mit dem PIN-Code der registrierten Person und allfälligen weiteren Daten (biographische Angaben, Zutrittsberechtigungen, Gültigkeit) als endgültiges Erkennungsmuster gespeichert. Die Bildverarbeitung geschieht mit Hilfe einer kundenspezifischen integrierten Schaltung (Asic). Die Steuerung des Ablaufes erfolgt mit einem Prozessor von Motorola (68000 oder 68302), das Programm ist als Firmware in Eprom oder Flash Memory gespeichert.

Das komplette mathematische Fingerabdruckmuster besteht aus den Charakteristiken von neun geometrischen Bereichen. Diese werden während des Registrierprozesses aufgrund verschiedener Kriterien sorgfältig ausgewählt, wie zum Beispiel:

- Unterscheidbarkeit von den Nachbarbereichen (weisen die Bereiche Besonderheiten auf?)
- Schwärzungsgrad
- Überlappung mit bereits ausgewählten Feldern
- Wiedererkennbarkeit in nachfolgenden Fingerpräsentationen

Das Fingerabdruckmuster enthält ausserdem das Resultat des Lebendfingertests, die Software-Versionsnummer sowie eine Prüfsumme. Der mit dem Muster zusammen abgespeicherte PIN-Code ist – im Unterschied zu vielen anderen Erkennungsverfahren – nicht geheim, sondern dient bei der Verifikation lediglich zum Abrufen des richtigen Vergleichsmusters aus der Datenbank. Er kann deshalb trivial gewählt werden (Telefonnummer, Autokennzeichen, Geburtsdatum usw.).

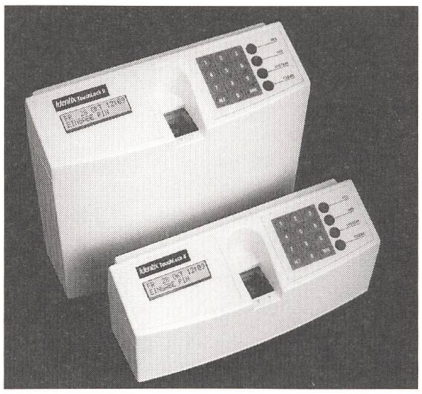


Bild 5 Fingerabdruck-Identifiziergeräte
Im Bild werden zwei Touch-Lock-II-Geräte von Identix gezeigt.

Die beschriebenen Geräte können mit erweitertem Speicher mehr als 1100 Fingerabdruckmuster speichern. Sie sind aber auch zur Kommunikation mit aussenliegenden Rechnern eingerichtet, auf denen die Anzahl Muster nur noch von der Speicherkapazität des Rechners begrenzt ist. Eine weitere Möglichkeit besteht in der Abspeicherung des Fingermusters in einer dem Benutzer abgegebenen Chipkarte.

Eigentliche Identifikation

Stellt sich die Person zur neuerlichen Identifikation an der Abtasteinheit ein, so ruft sie auf der Tastatur mit ihrem PIN-Code das entsprechende Muster aus dem Speicher ab und legt den passenden Finger auf die Abtasteinheit, worauf das neue Schwarzweissbild mit dem gespeicherten Muster verglichen wird (Bild 4). Bei diesem Vorgang werden aufgrund der im Muster gespeicherten Informationen die entsprechenden Felder des Lebendfingerbildes gesucht, allenfalls Rotationen und Translationen vorgenommen und danach die Korrelationswerte der Muster- und Fingerfelder gerechnet und einem Schwellwert gegenübergestellt, um ein Bild des Übereinstimmungsgrades zu erhalten. Der Vergleich dauert etwa 0,5 Sekunden.

Die Wahrscheinlichkeit für die Akzeptanz eines falschen (d. h. nicht vorher registrierten) Fingerabdrucks FAR liegt unter 10^{-6} und genügt damit allen praktischen Anforderungen. Voraussetzung ist eine korrekte Einstellung der Verifikationsschwellwerte, sowohl für das geometrische Muster wie auch für den Lebendfingertest. Die FRR beim ersten Versuch liegt mit etwa 1% noch durchaus in akzeptabler Grössenordnung; das Gerät kann für ein bis

drei Versuche eingestellt werden. Sowohl FAR wie FRR können beeinflusst werden durch die Einstellung der Verifikationsschwellwerte, allerdings immer unter gleichzeitiger Beeinflussung der Sicherheit.

Um Schwierigkeiten zu vermeiden, die sich vor allem bei extrem kalter und trockener Witterung ergeben können (zu trockene Haut verursacht auf der Glasplatte des Abtastgeräts einen schlechten Kontakt), wird mit einer speziellen Beschichtung auf der Platte der Kontakt zur Hautoberfläche verbessert. Für ausgesprochene «Problemfinger», die eine zu hohe Rückweisungsrate erzeugen, lässt sich die Verifikationsschwelle individuell tiefer stellen, ohne damit die Sicherheit des gesamten Systems zu beeinträchtigen. Rückweisungsraten sind im übrigen sehr von den äussern Umständen und vom Verhalten der Benutzer abhängig. Es empfiehlt sich (wie auch bei andern biometrischen Verfahren), die Benutzer genau zu instruieren.

In der vorstehend geschilderten Form sind die Geräte, die aus einer am Verifikationsort zu montierenden Abtasteinheit in robustem Gehäuse und einer geschützt anzubringenden Prozessoreinheit bestehen, aber auch als integrale Einheit verfügbar sind, bereits zahlreich im Einsatz für den Zutrittsschutz von Sicherheitsbereichen, zum Beispiel in Kernkraftwerken, Banken, militärischen Einrichtungen und anderem mehr (Bild 5). In bestimmten Fällen empfiehlt sich ihr Einsatz auch als Zeiterfassungs-Terminals. In entsprechend angepasster Form wird die Technik ferner zur Zugangssicherung eines Terminals oder Datennetzes verwendet.

Die beschriebenen Geräte können durch entsprechende Software ergänzt werden. Für alleinstehende Geräte besteht die Möglichkeit der Speichererweiterung mit einem einfachen PC. Anlagen mit mehreren Geräten können auf Basis von RS-422/485-Schnittstellen mit einem Rechner vernetzt werden. Dazu existiert voll funktionsfähige Zutrittskontroll-Software für die Betriebssysteme DOS, Windows oder OS/2, zum Teil auch für gemischten Einsatz von Kartenlesern und Fingerabdrucklesern. Für den Schutz von Computernetzwerken steht ebenfalls entsprechende Software (Windows, OS/2 mit der integrierten Möglichkeit der Verwaltung von Windows- und DOS-Maschinen) bereit.

Schlussbemerkungen

Biometrische Identifikationsgeräte sind seit über zehn Jahren auf dem Markt, kommen aber erst jetzt in Europa mehr und mehr auf. Die Eigenschaften dieser Anlagen sind in den vergangenen Jahren stark verbessert worden, so dass sie heute den Erwartungen an solche Geräte zu entsprechen vermögen. Zur Beurteilung sind folgende Kriterien bedeutsam:

- Sicherheit: Diese wird durch die FAR bestimmt, die je nach Anwendung einstellbar sein sollte zwischen etwa 1 Promille und 1/1000 Promille; schlechtere FAR lohnen den Aufwand zum Einsatz von biometrischen Identifikationssystemen nicht.
- Falsche Rückweisung: Der Wert ist stark vom Benutzerverhalten abhängig. Werte wesentlich über 1% sind jedoch für die meisten Anwendungen nicht akzeptabel.
- Geschwindigkeit: Für die Öffnung einer Tür wird eine Identifikationszeit von weniger als 1 Sekunde erwartet, obwohl gerade bei Schleusen und Drehkreuzen theoretisch auch höhere Werte den Personenfluss nicht wesentlich beeinträchtigen. In Büroumgebungen (Computersicherheit) können längere Zeiten zulässig sein.
- Akzeptanz des Verfahrens: Verschiedene Verfahren werden vom Benutzer schlecht akzeptiert, so alle jene, die mit dem Auge arbeiten, und – aus hygienischen Gründen – teilweise auch die auf der Handgeometrie basierenden Verfahren.
- Invarianz der registrierten Merkmale: In dieser Hinsicht bieten Verhaltensmerkmale (Unterschrift, Tastenanschlag, Stimme) mehr Schwierigkeiten als physiologische Merkmale.
- Grösse der Geräte: Diese spielt bei der Unterbringung in verschiedenen Umgebungen eine Rolle.
- Preis: Erste Geräte waren prohibitiv teuer und in keiner Weise mit konventionellen Anlagen (z.B. Magnetkartenleser) vergleichbar. Heutige Geräte bewegen sich in Grössenordnungen, die etwa beim 1,5- bis 2fachen eines intelligenten Chipkartenlesers liegen.

Der heute erreichte Stand der Technik führt zum Schluss, dass biometrische Identifikationsgeräte in Zukunft eine weitere Verbreitung in Applikationen finden werden, die in irgendeiner Form die Sicherstellung der Identität eines Benutzers verlangen.

Literatur

[1] *B. Miller:* Vital signs of identity. IEEE Spectrum, New York, Vol. 31, No. 2, February 1994.

[2] *J. R. Rodriguez* et al.: A Performance Evaluation of Biometric Identification Devices. Preliminary Draft. Sandia National Laboratories, Albuquerque, 1993.

[3] *J. P. Holmes* et al.: A Performance Evaluation of Biometric Identification Devices. Sandia National Laboratories, Albuquerque, 1990.

[4] US Patent No. 5 057 162 vom 19. 11. 1991.

Identification biométrique de personnes par moyens électroniques

L'identité d'une personne désirant avoir accès à un bâtiment ou à une prestation de service en prétendant «Je suis Jean Dupont», peut être déterminée de trois manières: par sa possession (clé, carte d'identité), par sa connaissance (PIN, mot de passe), par ses propriétés biologiques ou une combinaison de ces trois procédés (figure 1). Les propriétés biométriques constituent le plus sûr moyen d'identification comme démontré par la police depuis plus d'un siècle avec les empreintes digitales. Elles ont de plus l'avantage de ne pouvoir ni être perdues, ni volées.

Plusieurs procédés sont actuellement disponibles et mis en œuvre commercialement pour les contrôles d'accès à des bâtiments, mais également à des réseaux de données et pour d'autres moyens d'identification. Un procédé très simple mais exigeant un appareil quelque peu encombrant est la mesure de la géométrie de la main qui suffit dans les cas pas trop sévères contre les faux (figure 2). Une plus grande sécurité est offerte par la vérification de la structure de la rétine de même que celle des empreintes digitales. Avec ces deux procédés, on atteint un degré de sécurité contre une admission en infraction de 1 sur 1 million ou même supérieure. Tous les appareils du commerce reconnaissent une personne enregistrée en 0,5 à 2 secondes, ce qui est suffisant pour l'usage pratique. Un appareil pour identifier au moyen des empreintes digitales est décrit en détail et ses possibilités d'emploi sont illustrées (figures 3 à 5).

Des appareils d'identification biométrique sont évalués en fonction de divers critères. Par exemple, indépendamment du prix, le taux de refus de personnes enregistrées, la reconnaissance de personnes non enregistrées (sécurité contre admission en infraction), la vitesse de la reconnaissance, la stabilité de la caractéristique biométrique de même que l'acceptation par une large couche de la population entrent en ligne de compte.