

Mit freundlicher Genehmigung von
www.gitverlag.de

BIOMETRIE

Authentischer Zugang aus erster Hand

Handvenenmuster-Erkennung: komfortabel, hochsicher,
einfach in der Anwendung (Teil 1)

Für die eindeutige Identifizierung von Personen, sei es der physische Zutritt zu Gebäuden und Räumen oder der Zugang zu Automaten oder Rechensystemen, setzen sich zunehmend biometrische Authentifizierungs-Systeme durch. Neben einem maximalen Sicherheitsniveau ist auch die Ergonomie von Bedeutung, damit solche Systeme vom Anwender akzeptiert werden. Zu den sichersten und komfortabelsten Verfahren zählt die Handvenen-Erkennung, bei der das Muster des Verlaufs der Handvenen per Infrarotaufnahme erfasst wird. Ein Artikel von Werner Störmer in zwei Teilen.



Abb. 1

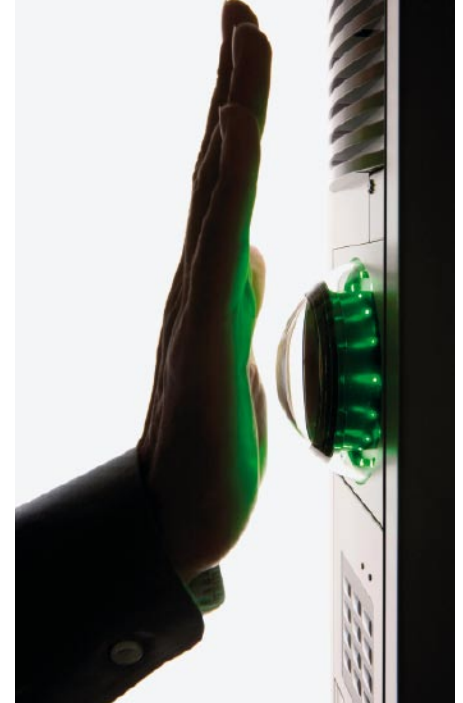
Bei niedrigen bis mittleren Sicherheitsanforderungen innerhalb der Zutritts- und Zugangskontrolle ist zur Zeit das gängigste Verfahren zur Personenerkennung die Ausweiserfassung. Solche codierten Karten werden aber nicht nur zur Personenidentifikation, sondern auch als elektronischer Datenträger und als Zahlungsmittel eingesetzt. Als multifunktional nutzbares Medium hat sich hier die RFID-basierende kontaktlose Chipkarte durchgesetzt.

Biometrische Identifikation oder Verifikation – warum und wie?

Für sicherheitsrelevante Anwendungen, wie der Zutrittskontrolle zu Hochsicherheitsbereichen, der Zugriffskontrolle zu sensiblen Daten oder der Zugangskontrolle zu Automaten, werden zunehmend biometrische Authentifizierungs-Systeme eingesetzt. Hierbei werden Personen anhand ihrer physiologischen oder verhaltensbedingten Merkmale eindeutig erkannt. Diese biometrischen Merkmale sollen die Schwächen anderer Identifikationsarten, wie vergessener PIN oder verlorener bzw. beschädigter Ausweis, eliminieren.

Es können statische physiologische Attribute (z. B. Fingerabdrücke, Handgeometrie, Iris- oder Netzhautmuster) oder variable physiologische Attribute (z. B. Gesichtsmimik, Stimme) und verhaltensabhängige Attribute, wie der Schreibrhythmus auf einer Computertastatur oder eine Unterschriftserkennung, herangezogen werden.

Alle Verfahren haben eine Gemeinsamkeit: zuerst muss eine Personalisierung oder Registrierung des Nutzers im System erfolgen, was als Enrollment bezeichnet wird. Dazu wird ein Referenzmuster bzw. ein Template angelegt, mit der Identität verbunden und in einer Datenbank oder Chipkarte abgespeichert. Meistens werden mehrere Messwerte aufgenommen. Aus diesen wird entweder der Mittelwert gebildet oder die unterschiedlichen Varianten werden als Referenzmuster im Speicher abgelegt. Da nur wenige spezifi-



sche Merkmale aus den Messdaten extrahiert und für den Vergleich benutzt werden, kann die Größe des Templates bis auf wenige Bytes reduziert werden. Der spätere Vergleich der aktuell ermittelten mit den zuvor abgespeicherten biometrischen Daten wird als Matching bezeichnet. Eine sinnvolle Ergänzung zur biometrischen Identifikation bietet die Verifikation. Hierfür werden die biometrischen Referenzdaten auf einer Chipkarte gespeichert. Diese Angaben werden verifiziert, indem die aktuell erfassten biometrischen Daten einer Person mit dem entsprechenden gespeicherten Referenzmuster verglichen werden.

Da solche – meist vorhandene und für andere kartengesteuerte Anwendungen genutzte – Ausweise sich im Besitz der Mitarbeiter befinden, können die personenbezogenen Daten nicht von Dritten zu anderen Zwecken missbraucht werden. Durch diese Kombination wird nicht nur die Sicherheit, sondern auch die Akzeptanz erhöht.

Außerdem fallen je nach Verfahren große Referenzdatenmengen an. Werden diese Daten zentral abgelegt, wird bei einer hohen Nutzerzahl nicht nur viel Speicherplatz benötigt, sondern die Suchzeiten für das Auffinden der jeweiligen Referenzdaten verlängern sich. Durch die Kombination eines biometrischen Verfahrens mit einem Kartensystem lässt sich die Suchzeit verringern, weil nur noch gezielt auf den Datensatz auf der jeweiligen Karte zugegriffen werden muss.

Vielfalt der biometrischen Erkennungssysteme

Fingerabdruck-, Gesichts- und Iriserkennung sind die gegenwärtig am meisten bekannten Verfahren, wobei der Fingerprint mit einem Marktanteil von über 50% unangefochtener Spitzenreiter ist. Diese Technologie hat aufgrund ihrer mittlerweile hohen Verbreitung ein attraktives Preisniveau erreicht und zeichnet sich insbesondere durch die Integrationsfähigkeit des Sensormoduls in Zutrittskontrollgeräten, Tastaturen und PC-Mäusen aus.

Abbildung 1 zeigt ein Beispiel für einen Zutrittsleser mit Fingerprint, RFID-Leser und Tastatur für PIN-Eingabe. Dass sich andere Technologien so schwer tun, sich gegen Fingerabdruckererkennung durchzusetzen, liegt nicht zuletzt an den verschiedenen Nachteilen, die diese Techniken bisweilen mit sich bringen, kombiniert mit einem hohen technischen Aufwand und damit hohen Preis, der nur in Ausnahmefällen gezahlt wird. Bei der Vielfalt der unterschiedlichen Sicherheitsanforderungen, Einsatzbedingungen und Unternehmenstypen muss folgendes berücksichtigt werden:

Systeme, bei denen eine Berührung mit dem Erkennungssystem stattfindet, wie beim Fingerabdruck oder der Vermessung der Handgeometrie, wird Verschmutzung oder die Problematik Hygiene nachgesagt. Dagegen erfolgt die Gesichtserkennung kontaktlos. Mittels Kamera wird automatisch ein Bild der zu identifizierenden Person aufgenommen und mit einem vorher abgespeicherten und ähnlich produzierten Bild verglichen. Hierbei muss die Integration der Kamera, oft kombiniert mit Spiegel als Positionierungshilfe und die Umgebungsbedingungen beachtet werden. Es muss mit Problemen bei wechselnden Lichtverhältnissen und bei der zuverlässigen Erkennung von Personen mit Brillen zumindest gerechnet werden.

Bei der Augenhintergrund- oder der Iris-Erkennung erfolgt oft die emotionale Ablehnung, weil viele Menschen überzeugt sind, ihr Auge würde von – gefährlichen – Laserstrahlen abgescannt, auch wenn es sich quasi nur um eine Art von Fotoaufnahme handelt, und Laser schon lange nicht mehr eingesetzt werden. Diese Vorbehalte, die zum Teil auch kulturell sehr unterschiedlich gesehen werden, müssen ernst genommen werden.

Dass negative Assoziationen im Laufe der Zeit auch neutralisiert werden können, zeigt die Fingerabdruckererkennung, die in der Anfangszeit viele Anwender zu sehr an polizeiliche Erkennungsmaßnahmen erinnerte. Anwender, die ein System innerlich ablehnen, finden im täglichen Betrieb tausend Gründe, dass ein biometrisches Verfahren nicht funktioniert oder dass das System fehlerhaft läuft. Je einfacher eine biometrische Identifikation ist, desto größer ist die Chance, ein Projekt erfolgreich durchzuführen.

Fortsetzung im nächsten Heft: Basiswissen um die Handvenenerkennung

► KONTAKT

Werner Störmer

PCS Systemtechnik GmbH, Essen

Tel.: 0201/89416-30 · Fax: 0201/89416-10

wstoermer@pcs.com · www.pcs.com