

Sicherheit – eine traurige Notwendigkeit

Von Dipl.-Ing. Günther Konecny

Aus trauriger Aktualität sollen hier die Möglichkeiten der Sicherung von Gebäuden, Anlagen und selbstverständlich auch des persönlichen Schutzes der dort arbeitenden Menschen aufgezeigt werden. Heute vergeht leider kein Tag mehr, an dem uns nicht die Nachricht von Attentaten, Terroranschlägen, Geiselnahmen oder Überfällen erreicht. Waren in vergangenen Zeiten vorwiegend Banken das Ziel von Überfällen, so werden nunmehr auch öffentliche Gebäude und Veranstaltungsstätten Ziele krimineller oder terroristischer Aktionen. Denken wir nur an die fürchterlichen Szenen in einem Moskauer Theater vor nicht allzu langer Zeit. Vor diesem traurigen Szenarium gewinnt zuverlässiger materieller und personeller Schutz heute zunehmend an Bedeutung, weil er ganz einfach zur zwingenden Notwendigkeit geworden ist. Man darf Eigentum durch unzureichende Sicherheitsvorkehrungen nicht fremdem Zugriff aussetzen oder Menschen in Gefahr bringen.

Beim Gebäudeschutz sind zwei Sparten der Absicherung erforderlich:

- Gebäudeüberwachung (äußere und innere Überwachung) und
- Zutrittskontrolle

Gebäudeüberwachung:

Hier bieten sich elektronische Kameras an, mit deren Hilfe die Außenfront, die Eingänge, strategisch wichtige Punkte im Inneren sowie bestimmte Räume – im Theater beispielsweise Foyer, Kassenraum und Zuschauerraum – überwacht werden können. Auf

diesem Gebiet kommt die rasche Weiterentwicklung der Kameras voll zum Tragen. Die Kameras sind heute auf einem Entwicklungsstand, der es ihnen ermöglicht, sich selbst auf extrem wechselnde Lichtverhältnisse (direkte Sonneneinstrahlung oder Dämmerung) nachjustieren und so stets den größtmöglichen Kontrastumfang bei hoher Bildauflösung sicherzustellen. Koppelt man die Kameras mit Bewegungsmeldern, so schalten sie sich erst ein, wenn eine Person den zu überwachenden Bereich betritt, was den Vorteil hat, dass bei der Aufzeichnung des Kamerabildes (die Bilder sämtlicher Überwachungskameras werden aufgezeichnet) Speicherplatz gespart wird. Sinnvoll ist natürlich der Einsatz schwenkbarer Kameras, da mit diesen ein größerer Bereich erfasst werden kann. Die Kameras können mittels Joystick vom Kontrollraum aus gesteuert oder per Knopfdruck auf vorprogrammierte Positionen geschwenkt werden. Sie können aber auch selbstständig sich bewegende Objekte wahrnehmen und verfolgen. Früher wurden alle Kamerabilder auf Videorecordern aufgezeichnet, womit nur eine beschränkte Aufzeichnungsdauer bei relativ geringer Bildauflösung möglich war. Heutiger Stand der Technik ist das Harddisk-Recording mit einer Plattenspeicherkapazität von 250 GByte. Damit kann sehr lange mit höchster Bildauflösung aufgezeichnet werden. Um ein bestimmtes aufgezeichnetes Ereignis ansehen zu können, musste dieses früher zeitaufwendig auf dem Band gesucht werden. Heute ist es – zeitcodiert – auf der Harddisk blitzartig auffind-

bar. Diese Art der Kameraaufzeichnung kann quasi als Quantensprung in der Überwachungstechnik bezeichnet werden. Auf dem Sektor der Kamera-gestützten Gebäudeüberwachung hat sich die Firma Panasonic auf dem Weltmarkt eine Führungsposition gesichert.

Zutrittskontrolle:

Dafür sind üblicherweise Schlüsselpäne, Ausweise oder Magnetkarten sowie Codes und Passwörter bei elektronischen Anlagen in Verwendung. Sie alle weisen gravierende Nachteile auf:

Schlüssel können vergessen, verlegt oder gar verloren werden. Codes und Passwörter können vergessen werden (überhaupt dann, wenn sie aus Sicherheitsgründen turnusmäßig geändert werden). Das Ergebnis: Man steht in jedem Falle verzweifelt vor verschlossenen Türen. Bei Verlust von Schlüsseln muss oft ein komplettes Schlüsselsystem getauscht werden – eine teure Angelegenheit. Und eine verlorene oder gestohlene Magnetkarte öffnet Unbefugten im wahrsten Sinne des Wortes Tür und Tor. Damit ist jetzt aber Schluss. Das neue Zauberwort heißt „**Biometrie**“.

Die Zukunft: Ihre Finger und Ihre Augen werden zum Schlüssel

Diese Technik bietet eine sichere, vor allem aber auch äußerst bequeme Alternative zu Schlüsseln, Passwörtern, Zugangscodes etc. Ihr liegt die „Biometrie“ zu Grunde. Biometrie ist die Lehre von der Messung an Lebewesen. Durch Bestimmung geeigneter charakteristischer körperlicher Merkmale während des Identifizierungsvorgangs wird durch Vergleich mit den hinterlegten biometrischen Daten die Identität einer Person festgestellt. Die Biometrie als Lehre von der

Erfassung und Vermessung körperlicher Merkmale kennt inzwischen eine Vielzahl von Merkmalen, die sich ideal zur eindeutigen Identifizierung sogar von Zwillingen heranziehen lassen. Beispiele sind Fingerprint, Iris und Blutgefäßstrukturen. Um mit der Erkennungsleistung des menschlichen

Gehirns mithalten zu können (vorausgesetzt man beschränkt sich auf ein einziges biometrisches Erkennungsverfahren), sind allerdings gut 100 Millionen Rechenoperationen pro Sekunde zu leisten. Da Standard-PCs erst seit kurzem diese hohe Rechenleistung erreichen und andererseits geeignete Sensoren zur Aufnahme der menschlichen Körpermerkmale immer kostengünstiger werden, ist jetzt die Zeit gekommen, das Passwort flächendeckend durch eine benutzerfreundliche Alternative zu ersetzen, nämlich die biometrische Authentifikation (Oberbegriff für Identifikation und Verifikation). Bei der Entwicklung biometrischer Identifikationsverfahren geht es vor allem darum, Körper- und Verhaltensmerkmale zu finden und zur Erkennung zu nutzen,

- die möglichst eindeutig sind, d. h. sich bei keiner weiteren Person wiederholen,
- bei möglichst vielen Personen vorkommen,
- sich zeitlich möglichst wenig verändern,
- mit möglichst einfachen technischen Mitteln erfassbar sind oder
- deren Erfassung für den Anwender bequem durchführbar ist.

Die Kriterien sind also Eindeutigkeit, Universalität, Konstanz, Messbarkeit und Anwenderfreundlichkeit. Von den oben genannten biometrischen Merkmalen weist die Iris die höchste Konstanz auf. Auch in puncto Genauigkeit liegt die Iris an erster



Positionierbare 1/4 Zoll Dome-Kamera mit Auto-Tracking



Fernbedienung der Kamera mittels Joystick oder über Tasten

Fotos: Dipl.-Ing. Günther Konecny

Foto: Dipl.-Ing. Günther Konecny



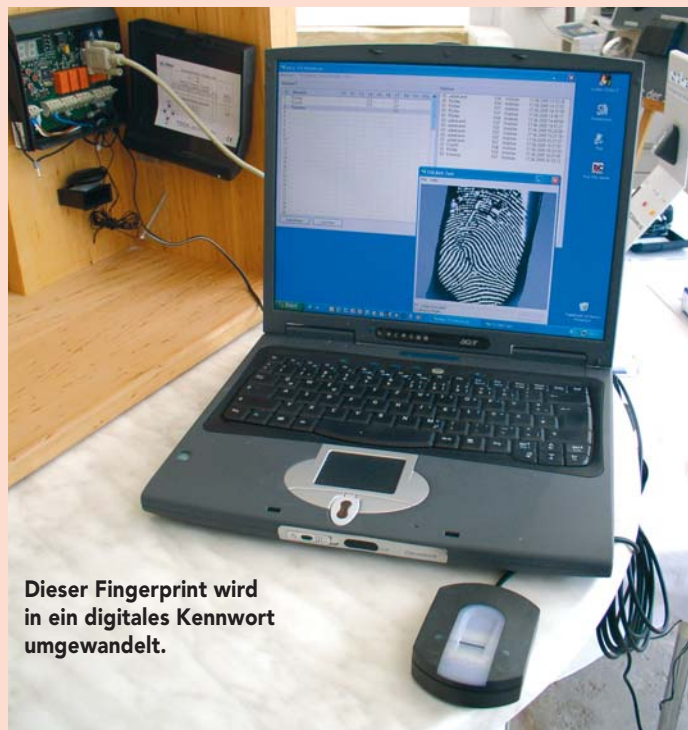
Zum Escannen wird der Finger vom Benutzer einfach über den Scanner gezogen.

Stelle, dann aber schon gefolgt vom Fingerprint, der die gleiche Genauigkeit wie die DNA-Analyse aufweist. Die bisher üblichen Mittel zur Identifikation wie Karten und Codes konnten in Wahrheit nicht nur vom Eigentümer benutzt werden, da ja eine mögliche Weitergabe an andere Personen jederzeit möglich war. Dies ist bei Einsatz der Biometrie mit Sicherheit ausgeschlossen.

Fingerprint

Hier wird nach einem von der Firma „ekey-biometric systems“ entwickelten Verfahren – es nennt sich TOCA – der Fingerabdruck als eindeutiges Merkmal zur Identifikation benutzt. Dabei wird der Fingerabdruck nicht als Bild gespeichert, sondern ein aus dem gescannten Bild erstelltes digitales Kennwort. Dadurch kann kein gespeichertes Bild eines Finger-

abdrucks kopiert und missbräuchlich verwendet werden. Zum Escannen wird der Finger vom Benutzer einfach über den Scanner gezogen. Das gescannte Bild wird – wie beschrieben – in ein digitales Kennwort umgewandelt, dieses mit den gespeicherten verglichen und bei Vorhandensein eines registrierten, identischen Kennwortes wird der elektrische Türöffner mittels Impuls geöffnet. Es ist dies ein äußerst sicheres Verfahren, bei dem Missbrauch ausgeschlossen ist. Allerdings muss sich der Benutzer merken, mit welchem seiner Finger er registriert worden ist! Selbstverständlich können die an den verschiedensten Eingängen angebrachten Erkennungs-Scanner miteinander vernetzt werden und soherart ein Zugangssystem auf rein elektronischer Basis erstellt werden.



Dieser Fingerprint wird in ein digitales Kennwort umgewandelt.

Foto: Dipl.-Ing. Günther Konecny

Iris-Erkennung

Zwischen der Iris (Regenbogenhaut) und der Hornhaut des menschlichen Auges liegen komplexe band- und kammartige Bindegewebsstrukturen. Diese Strukturen sind bei jedem Menschen unterschiedlich. Sie unterscheiden sich selbst bei eineiigen Zwillingen. Außerdem verändern sie sich in einem gesunden Auge während eines Lebens wenig. Das mit einer herkömmlichen Kamera (z. B. einer CCD-Kamera) von außen aufgenommene Bild der Iris lässt diese Strukturen erkennen und eignet sich damit als eindeutiges Erkennungsmerkmal. Bei Menschen mit dunkler Augenfärbung sind die Strukturen im sichtbaren Licht allerdings nur schwer zu erkennen. Biometrische Iris-Erkennungssysteme beleuchten daher die Iris aus einem Abstand von etwa einem Meter mit für das Auge nahezu unsichtbarem Licht im nahen Infrarotbereich. Dieses durchdringt den „Farbstoff“ des menschlichen Auges (Melanin) besser als sichtbares Licht. So kann eine Aufnahme der Irisstrukturen bei allen Menschen mit gesunden Augen angefertigt werden, ohne zu blenden. Aus den aufgenommenen

Bildern wird mit speziell für diesen Zweck entwickelten mathematischen Methoden ein eindeutiger Datensatz gebildet, der als so genanntes „Template“ für die biometrische Erkennung dient. Der erste einsatzfähige biometrische Algorithmus wurde Anfang der neunziger Jahre von John Daugman entwickelt und patentiert. Inzwischen gibt es eine Vielzahl von Algorithmen zur Iriserkennung, allerdings gelangte aus patentrechtlichen Gründen bisher nur der von Daugman zur weltweiten Praxisanwendung. Die entsprechenden Patente gelten in der EU noch bis Februar 2006. Bevor ein Template aus einem Bild der Iris erzeugt werden kann, muss die Iris im Auge erkannt werden und offensichtliche Störungen, wie z. B. Reflektionen, Abschattungen und verdeckte Teile entfernt werden. In Abb. 1 (Seite 30) ist dies veranschaulicht durch den von der feinen weißen Linie ausgewählten Bereich, der bei der Template-Erzeugung berücksichtigt wird.

Im Gegensatz zu allen anderen biometrischen Merkmalen hat die Iris einen hohen Grad an Symmetrie, die Merkmale befinden sich



Von der CCD-Kamera aufgenommene Iris-Bilder vor der Digitalisierung

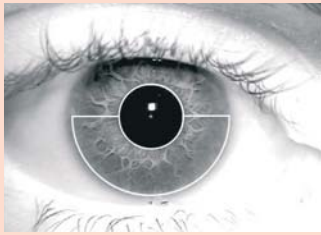


Abb. 1: Aufnahme einer Iris bei einer Wellenlänge von 850 nm (nahes Infrarot). Man erkennt die komplexen Strukturen in der Iris. Die feinen weißen Linien wurden von einem Auswertprogramm erzeugt, und deuten die Region an, die für die Erzeugung eines Templates verwendet wurde. Die innere schwarze Pupille wird nicht verwendet. Der weiße Fleck auf der Pupille wird durch die beleuchtende Infrarot-Diode erzeugt.

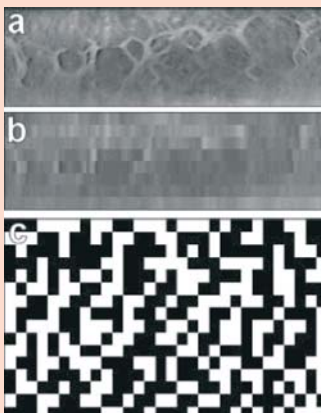


Abb. 2: Erzeugung eines Templates

in einem Kreissegment, das um die Pupille liegt (Abb. 1). Dies erleichtert die Erzeugung des Templates erheblich, da Verformungen der Iris (z. B. durch Kontraktion der Iris bei erhöhtem Lichteinfall) auf einfache Weise mathematisch korrigiert werden können. In einem ersten Schritt transformieren die meisten Verfahren einen Teil dieses Kreissegments in einen Streifen konstanter Breite (Abb. 2 a).

Dieser Streifen wird mit mathematischen Verfahren bearbeitet (Abb. 2 b) und dann in eine Abfolge von Nullen und Einsen gewandelt (Abb. 2 c).

Die Grundidee der Verfahren ist aber typischerweise die folgende: Die Abbildung der Iris wird in eine endliche Anzahl von Rechtecke geteilt. Die Helligkeit in jedem dieser Rechtecke wird gemittelt, indem Variationen über sowohl sehr kleine als auch sehr große Regionen entfernt werden. Nun werden zur Erstellung des Template-Datensatzes alle Rechtecke, die heller als der Mittelwert sind, gleich „1“ und diejenigen die dunkler als der Mittelwert sind, gleich „0“ gesetzt. Die typische Größe von Iris-Templates liegt im Bereich einiger hundert Bytes.

Panasonic verwendet für sein Iris-Erkennungsverfahren ein Gerät, welches mit zwei Kameras beide Augen erfasst. Die zu identifizie-



Foto: Dipl.-Ing. Günther Konecny

Panasonic-Erkennungsgerät mit zwei Kameras

rende Person muss sich dabei lediglich in einem Abstand von zirka 60 bis 90 cm vor die biometrische Sensoreinheit stellen, wobei die Einheit von selbst erkennt, dass jemand davor steht. Sodann werden zuerst das Gesicht und danach die Augen lokalisiert und Schwarzweißbilder der Irismuster aufgenommen. Daraus werden die digitalen Iris-Templates generiert und mit den biometrischen Referenzdaten der Datenbank verglichen. Stimmen die zu prüfenden Daten überein, so öffnet sich die Tür.

Vorbehalte gegen biometrische Verfahren

Oft werden von Mitarbeitern Bedenken gegen den Einsatz bio-

metrischer Schutzverfahren für zu schützende Betriebsbereiche geäußert und es wird in diesem Zusammenhang oft vom „Gläsernen Menschen“ gesprochen, zu dem die Mitarbeiter degradiert zu werden scheinen. Dabei wird aber übersehen, dass die auf Biometrie beruhenden Verfahren die größte Fälschungssicherheit und somit auch den größten Schutz für das Personal bieten. Darüber hinaus ist ihre Handhabung äußerst bequem, da für sie nur der eigene Körper zum „Sesam öffne dich“ vonnöten ist. Auf dem Sektor der Zutrittskontrolle werden daher komplizierte Schlösser und die dazugehörigen Schlüssel in absehbarer Zeit der Vergangenheit angehören.



ING. FRANZ TEUFEL Ges.m.b.H.
TRANSPORTGERÄTE
und FÖRDERANLAGEN

Rollo
Ing. Franz Teufel GesmbH.
Wolfholzgasse 27
2345 Brunn am Gebirge
Tel.: 02236/379580-13
Fax: 02236/379580-22
E-Mail: office@rollo-teufel.com
www.rollo-teufel.com