Biometrie als Bindeglied zwischen Person und Identität : Teil 1

Autor(en): **Müller, Lorenz**

Objekttyp: **Article**

Zeitschrift: **Bulletin.ch : Fachzeitschrift und Verbandsinformationen von Electrosuisse, VSE = revue spécialisée et informations des associations Electrosuisse, AES**

Band (Jahr): **94 (2003)**

Heft 19

PDF erstellt am: **08.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-857597

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Biometrie als Bindeglied zwischen Person und Identität – Teil 1

Neben herkömmlichen Methoden wie etwa Fingerabdruck oder Unterschrift finden heute für die Identifizierung physischer Personen zunehmend neue biometrische Verfahren wie beispielsweise Gesichts- und Stimmerkennung oder genetische Fingerabdrücke Anwendung, wobei komplexere Sicherheitssysteme gleichzeitig mehrere Kennzeichen erfassen und auswerten. In der Regel müssen bei biometrischen Sicherheitssystemen die Personaldaten allerdings in einer zentralen Datenbank abgespeichert werden, was unter anderem auch Fragen des Datenschutzes aufwirft. Ein an der Hochschule für Technik und Architektur Biel entwickeltes Authentifizierungskonzept erlaubt die Überprüfung von Berechtigungen mittels einer Smart-Card, welche über eine biometrische Schnittstelle zu der zu authentifizierenden Person verfügt. Der vorliegende erste Teil gibt eine Übersicht über die verschiedenen Verfahren zur Überprüfung der Identifikation. Im zweiten Teil wird das neu entwickelte Authentifizierungskonzept vorgestellt.

Wer erinnert sich nicht an Chaplins genialen Film «The Great Dictator»? Das Problem der falschen Identitätszuordnung wird darin meisterhaft illustriert. Am Schluss findet sich der verfolgte Barbier in der Rolle des Diktators, nur weil er als physische Person genau gleich aussieht wie der Tyrann – beide Personen werden dabei natürlich von Chaplin selbst gespielt. Die falsche Zuordnung

Lorenz Müller

einer physischen Person zu einer sozialen Identität ist ein Thema, das die Menschen seit jeher beschäftigt und in Theater, Literatur und Mythen immer wieder thematisiert wird.

Besitz, Status, Zugehörigkeit zu Gemeinschaften und Existenz als Staatsbürger sind ausschliesslich durch die soziale Identität definiert. Verbunden wird diese Identität mit einer physischen Person durch die Wahrnehmung anderer Individuen, die eine Person erkennen und die richtige soziale Identität zuordnen können. Unser Gehirn ist speziell für die Erkennung von feinsten Unterscheidungsmerkmalen in Gesicht und Verhalten von anderen Personen optimiert. Allerdings wird eine eindeutige Zuordnung auf Grund der ständig wachsenden Zahl von Leuten, denen wir im täglichen Leben begegnen, immer schwieriger. Grössere Gemeinschaften wie Staaten, Armeen oder andere Organisationen rüsten deshalb ihre Mitglieder mit Ausweisen und Erkennungszeichen aus, über die sich eine Person authentifizieren kann. Eine andere Möglichkeit besteht darin, die Identität mit einem Geheimnis zu verbinden, das nur die richtige Person kennt. Beides sind seit jeher gebräuchliche Methoden, die weiterhin wichtige Faktoren für die Authentifizierung bleiben.

Mit dem Aufkommen des wissenschaftlichen Denkens kam aber auch der Wunsch, die Zuordnung der physischen Person zu ihrer Identität durch objektive Messungen und rational nachvollziehbare Methoden zu verbessern. Die 1880 in der Fachzeitschrift *Nature* publizierte Absicht des schottischen Arztes Henry Faulds und der Versuch des englischen Beamten William Herschel (1878), Personen anhand ihres Fingerabdrucks zu identifizieren, nachdem Anatomen das spezielle Furchenmuster der Handflächen schon zwei Jahrhunderte früher beschrieben hatten, kann wohl als Geburtsstunde der Biometrie bezeichnet werden. Seither sind eine Reihe von weiteren physiologischen Merkmalen oder Verhaltensmuster entdeckt worden, die für ein Individuum charakteristisch und einzigartig sind. So stehen heute mit dem Ausweis, dem Geheimnis und der biometrischen Messung drei unabhängige Konzepte für die Identifizierung oder Authentifizierung (Überprüfung einer behaupteten Identität) einer Person zur Verfügung. Je nachdem, wie viele der drei Konzepte in einem Prüfprozess einbezogen werden, spricht man dann von Ein-, Zwei- oder Dreifaktor-Authentifizierung.

Identifizierung
Unter Identifizierung versteht man das Feststellen der Identität, also die Zuordnung einer physischen Person zu den sie beschreibenden Daten. Dabei werden die vorgelegten oder gemessenen Identifikationsmerkmale – z.B. Name und Pass – mit hinterlegten Sollwerten – z.B. in einer Datenbank abgespeicherte Zugehörigkeit von Namen und Passnummer – verglichen.

Authentifizierung
Unter Authentifizierung versteht man die Überprüfung einer vorgegebenen Identität. Nach der Identifizierung – beispielsweise durch Angabe eines Namens – wird die angegebene Identität zusätzlich durch Überprüfung von Testfaktoren verifiziert, die nur die tatsächlich berechtigte Person erbringen kann. Es gibt drei Kategorien von solchen Testfaktoren für die Authentifizierung:
- etwas, das man besitzt: Pass, Karte, Schlüssel usw.
- etwas, das man weiss: PIN-Code, Passwort, Nummernkombination usw.
- etwas, das man ist: biometrische Eigenschaft.

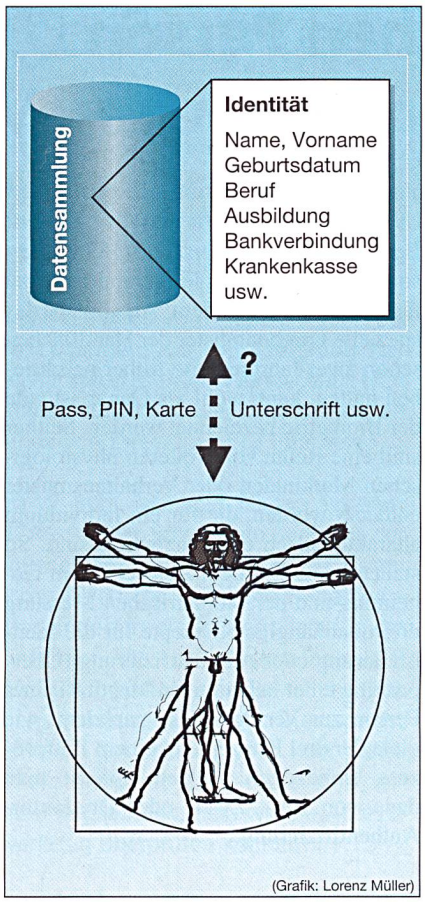


Bild 1 Die Verbindung zwischen Person und Identität ist eine notorische Schwachstelle in vielen Sicherheitskonzepten

Biometrie

Als Biometrie bezeichnet man die Anwendung naturwissenschaftlicher Messmethodik für die Bestimmung von Eigenschaften eines lebenden Organismus. Dabei unterscheidet man grob zwei Kategorien von Observablen: Passive, physiologisch bedingte Eigenschaften eines Körpers – beispielsweise Fingerabdruck, Gesichtsform oder Irismuster – und aktive, verhaltensbasierte Eigenschaften eines Individuums wie etwa Handschrift, Stimme oder Bewegungsdynamik.

Für die biometrische Authentifizierung eines Individuums muss vorerst eine möglichst gute Messung der Merkmale durchgeführt und diese dem Individuum eindeutig zugewiesen werden (Enrollment). Dieses Basismuster (Template) dient dann als Sollwert, mit dem alle späteren Messungen (Query) verglichen werden. Die spätere Identifizierung eines Individuums erfolgt durch den Vergleich einer weiteren Messung mit den abgespeicherten Sollwerten. Bei der Authentifizierung wird die neue Messung nur mit dem Sollwert der angeblichen Identität verglichen. Entspricht die Messung innerhalb von vorgegebenen Toleranzgrenzen dem Sollwert, wird die Messung als ein authentifizierender Faktor akzeptiert. Für eine sichere Authentifizierung überprüft man meistens mehrere Faktoren aus unterschiedlichen Kategorien (siehe Kasten). Die Qualität eines solchen Zuordnungsprozesses wird durch die Fehlerraten erster und zweiter Art charakterisiert: Die False Acceptance Rate (FAR, Fehlerraten erster Art) bezeichnet die relative Häufigkeit der akzeptierten Anfragen eines falschen Nutzers, und die False Rejection Rate (FRR, Fehlerraten zweiter Art) bezeichnet die relative Häufigkeit der nicht akzeptierten Anfragen eines richtigen Nutzers. Die beiden Qualitätsparameter hängen sehr stark von der Messmethodik, der Observablen und den eingebauten Toleranzen im Erkennungsalgorithmus ab und korrelieren deswegen im Allgemeinen negativ[1].

Warum Biometrie?

Der technologische Fortschritt, der schnelle Messungen von Merkmalen und deren Auswertung mit vertretbarem Aufwand und hoher Qualität erlaubt, hat zu einem stark wachsenden Interesse für biometrische Methoden geführt. Dem steht aber das ungelöste Problem aller Sicherheitskonzepte gegenüber: Wie verbindet man Identitätsdaten mit den richtigen physischen Personen, die der Identität entsprechen?

Bei allem Fortschritt, der in der Sicherheitstechnologie gemacht wurde, ist und bleibt die Authentifizierung von Personen ein Schwachpunkt (Bild 1). Pässe mit einer wenig aussagekräftigen Fotographie, durch eine nur oberflächlich verifizierbare Unterschrift, nur rudimentär gesicherte Kreditkarten oder leicht zu erratende Passwörter machen es leicht, eine Identität zu stehlen[2].

Diese Problematik ist bekannt und kann nicht allein durch Verbesserungen im digitalen Sicherheitssystem gelöst werden. Die Schwachstelle zwischen physischer Person und ihrer digitalen erfassten Identität ist mit konventionellen Methoden kaum zu eliminieren. Biometrische Methoden sind hier ein viel versprechender Ansatz, da mit ihnen ein direkter, nur schwierig zu manipulierender Bezug zwischen Daten und Person geschaffen wird.

Biometrie im täglichen Leben

Der heutige Boom in der Sicherheitstechnologie als Folge der Terroranschläge in den USA hat der Biometrie enormen Auftrieb verschafft. Dies, obschon das Gebiet nicht überall den besten Ruf geniesst. Gewisse Bedenken sind durchaus begründet, sind doch mit sehr ähnlichen Methoden unter dem Begriff Physiognomik noch bis weit ins letzte Jahrhundert hinein rassistische und diskriminierende Ideologien auf eine pseudo-wissenschaftliche Basis gestellt worden. Auch neueste, in das weite Gebiet der Biometrie fallende Methoden wie zum Beispiel die DNA-Analyse[3], verbunden mit der Suche nach problematischen Genen, können begründete und

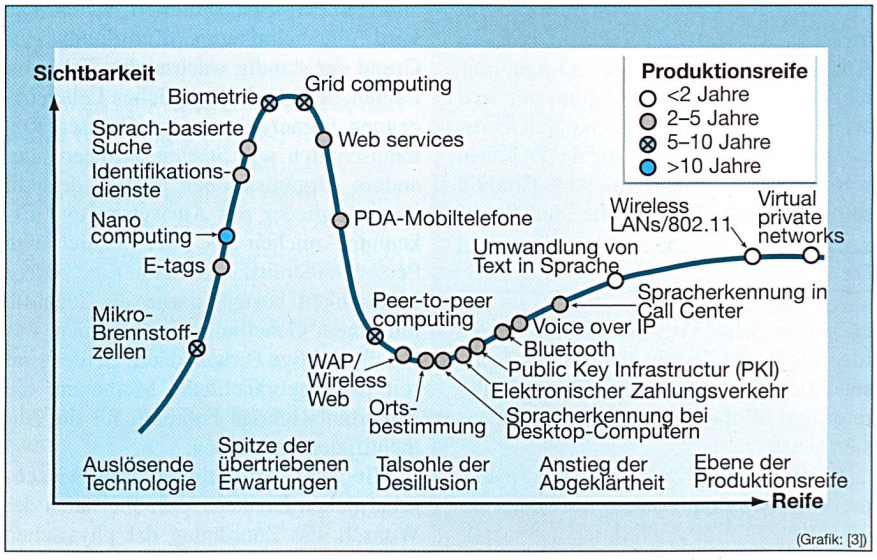


Bild 2 Sichtbarkeit biometrischer Technologien

Gemäss der Gartner Research Group haben biometrische Technologien heute eine hohe Sichtbarkeit, wirtschaftlich wirklich relevant werden sie aber erst in einigen Jahren. So werden heute z.B. rund 260 Mio. $ für die am weitesten verbreitete Methode – die Fingerabdruckerkennung – umgesetzt, was jedoch nur etwa 2,5% des gesamten Sicherheitsmarktes entspricht. In der neuesten Kompilation des Hype Cycles [4] wird Biometrie deshalb bereits in der Nähe der «Talsohle der Desillusion» positioniert, von wo an es aber stetig aufwärts geht.

manchmal auch unbegründete Ängste schüren. Breit anerkannt ist die Methodik in der Kriminalistik. Schon seit über 100 Jahren nutzt die Polizei z.B. Fingerabdrücke als Beweismittel bei der Suche und Überführung von Verbrechern[4].

Trotz aller Bedenken verlangen immer mehr Staaten und Organisationen eine zusätzlich biometrisch abgesicherte Authentifizierung von Personen, um Zugangsrechte zu gewähren. In ihren strategischen Berichten zur Sicherheit betont die US-Regierung die Wichtigkeit von biometrischen Methoden zur Identifizierung und Authentifizierung von Personen[5], und in einzelnen Staaten werden bereits biometrisch gesicherte Identitätsausweise eingeführt[6]. Obschon biometrische Technologien heute bereits eine hohe Sichtbarkeit (hohe Präsenz in den Medien, in Fachpublikationen und in der Wahrnehmung der Spezialisten) haben, dürfte der volle wirtschaftliche Durchbruch noch einige Jahre auf sich warten lassen (Bild 2).

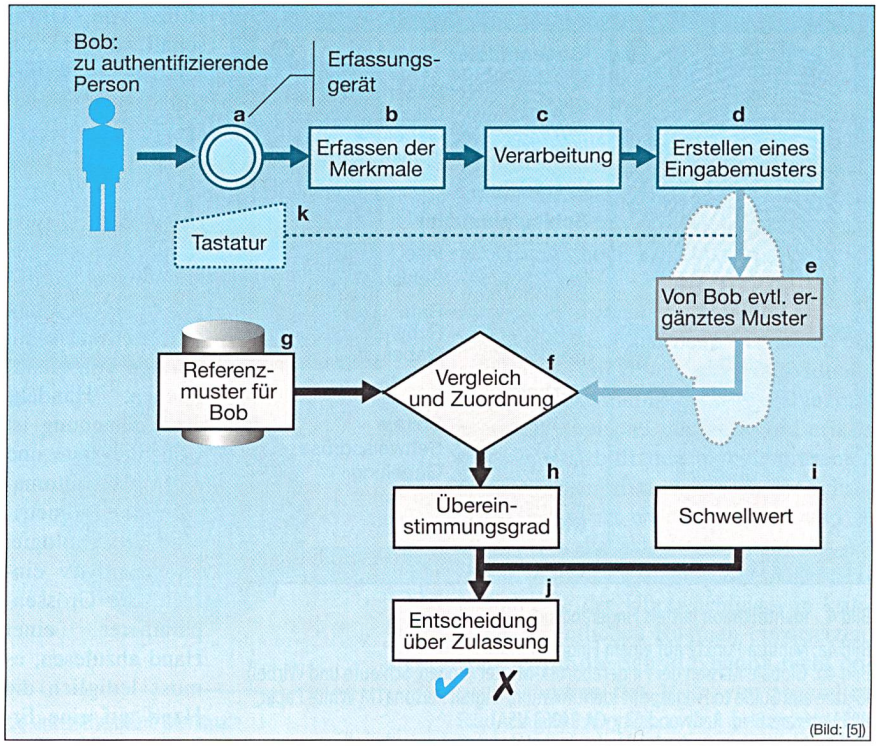


Bild 3 Ablaufdiagramm einer biometrischen Authentifizierung mit vorgängig in einem Muster (Template) abgespeicherten Merkmalen

Die Merkmale der zu authentifizierenden Person werden erfasst (a) und daraus ein Eingabemuster (b–d) erstellt, das ggf. noch mit Eingaben der Person versehen wird (k, e). Dieses Muster wird mit einem auf eindeutigen Merkmalen erstellten Referenzmuster (g) verglichen (f). Der Grad der Übereinstimmung (h) wird mit einem Schwellwert (i) verglichen, woraus die Entscheidung – nicht als übliches Ja/Nein wie bei einem Passwort – über Zulassung oder Zurückweisung hergeleitet wird (j).

Biometrische Methoden

Wie Biometrie funktionieren könnte, wurde kürzlich in Spielbergs Film «Minority Report» ziemlich drastisch dargestellt. Obschon die Anwendung durch den totalen Überwachungsstaat Science-Fiction ist – und hoffentlich auch bleibt –, ist die gezeigte Technologie nicht weit von der Realität entfernt. Biometrische Identifikation basiert auf der Tatsache, dass gewisse physiologische Eigenschaften eines Individuums einzigartig sind und sich lebenslang kaum verändern oder dass jede Person unbewusst individuelle Verhaltensmuster entwickelt, die sie von anderen Leuten unterscheidet. In der Biometrie geht es darum, solche geeigneten Merkmale und Verhaltensmuster zu identifizieren, diese messtechnisch zu erfassen, die Resultate zu parametrisieren und durch eine entsprechende Eichung zu standardisieren. In allen Methoden ist der Messablauf für eine Identifizierung oder Authentifizierung vom Prinzip her gleich. Bild 3 gibt das Ablaufdiagramm eines Authentifizierungsprozesses wieder.

Die wichtigsten Technologien – gruppiert in die beiden Hauptkategorien «physiologische» und «verhaltensbasierte» Merkmale – sollen nachfolgend kurz beleuchtet werden.

Physiologische Biometrie

Die physiologische Biometrie nutzt die Tatsache aus, dass gewisse Körpermerkmale sich im fötalen Stadium sogar bei eineiigen Zwillingen unterschiedlich ausprägen und ein Leben lang gleich bleiben. Bekannt und für biometrische Messungen genutzt wird das Rillenmuster der Fingerspitzen (Fingerabdruck), das Bindegewebemuster der Iris, das Muster der Adern in der Retina, die Geometrie der Gesichtszüge und der Handfläche. Nicht alle diese Merkmale haben das gleiche Unterscheidungspotenzial: die beiden letztgenannten Merkmale sind auch nicht ein Leben lang konstant, sondern entwickeln sich. Eine ganze Klasse von neuen biochemischen Merkmalstypen wird sich durch verbesserte Biosensoren erschliessen lassen. Bis heute ist lediglich die DNA-Analyse gebräuchlich. Diese funktioniert aber wegen der zeitverzögerten Messprozedur nur im Offline-Modus und verlangt das Vorhandensein einer Stoffprobe mit DNA-Material des zu identifizierenden Individuums.

Fingerabdruck

Allgemein bekannt ist die Einzigartigkeit des Fingerabdrucks jedes einzelnen Fingers. Die Methodik, einen Fingerabdruck in standardisierter Form zu erfassen und abzulegen, ist weltweit erprobt und in der Personenauthentifikation gebräuchlich[7]. Neuestes Beispiel ist die Datenbank Eurodac im Rahmen des Dubliner Abkommens[8]. Wie man an sich selbst leicht feststellen kann, bilden die Hautrillen ein Muster von parallel verlaufenden gekurvten Linien, die im äusseren Bereich der Fingerkuppen meist offene Schlaufen bilden. Im zentralen Bereich sind die Rillen zum Teil geschlossen, abrupt endend und können Wirbel bilden. Dieser zentrale Bereich ist besonders reich an charakteristischen Merkmalen. Das globale Muster wird nach bestimmten Kriterien zentriert, orientiert und in Klassen eingeteilt (Bild 4). Dazu kommen so genannte lokale Merkmale, die man als «Minutia»-Punkte bezeichnet. Diese charakterisieren und definieren die Lage und Art von Verzweigungen, Endungen, Einschlüssen, Divergenzen, lokale Rillendichte usw. Heutige Systeme für Fingerabdruckerkennung identifizieren rund 50 bis 70 solche Minutia-Punkte, je mit bis zu 7 charakteristischen Merkmalen und ihrer relativen Positionierung zu den anderen Punkten. Die Wahrscheinlichkeit, dass zwei Fingerabdrücke gleich klassiert werden, ist damit auch unter Berücksichtigung von gewissen Messfehlern sehr klein.

Technisch besteht ein Fingerabdruckerkennungssystem aus einem Sensor, der das Rillenmuster erfasst, einem Bildver-

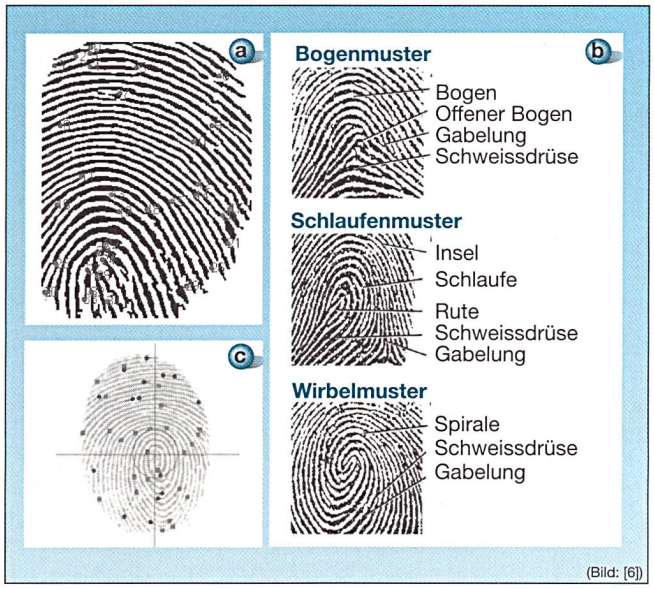


Bild 4 Identifikation mittels Fingerabdruck

Bild 4a: Minutia-Punkte auf einem Fingerabdruck.
Bild 4b: Globale Klassen der Fingerabdruck-Muster (Bogen, Schlaufe und Wirbel) (Skizze aus Guide to Fingerprint Identifikation; Digital PersonaTM White Paper; 805 Veterans Blvd. Redwood City, CA 94063 USA).
Bild 4c: Positionierung der Punkte in einem lokal definierten Koordinatensystem (Nullpunkt: Position eines Minutia-Punktes; X-Achse: Richtung der Tangente an lokale Rillen beim Minutia-Punkt).

arbeitungsteil, der die relevanten Merkmale herausfiltert, einem Erkennungsalgorithmus, der die globalen Merkmale bzw. die Minutia-Punkte nach Lage und Eigenschaften identifiziert und einem Matchingsystem, welches das aufgenommene Muster mit dem abgespeicherten Template vergleicht und über Akzeptanz bzw. Ablehnung entscheidet. Die gebräuchlichen Sensortechnologien basieren dabei entweder auf optischer oder kapazitiver Erkennung der Rillenmuster. Rein optische Systeme sind natürlich anfällig auf Replay-Angriffe (Präsentation von kopierten Fingerabdrücken) und müssen mit zusätzlichen Sensoren die Echtheit des präsentierten Bildes nachprüfen. Kapazitive Sensoren messen die unterschiedlichen elektrischen oder thermischen Eigenschaften zwischen den direkt am Sensor aufliegenden Rillenbergen und den Tälern mit etwas Luft dazwischen. Die Überlistung solcher Sensoren mit gefälschten Fingern ist zwar schwierig, aber nicht unmöglich[9]. Nachteil der kapazitiven Sensoren ist ihre Empfindlichkeit gegenüber elektrostatischen Entladungen und ihr Preis (grossflächige Halbleiterchips). Sowohl optische als auch kapazitive Sensoren werden heute in Erkennungssystemen eingesetzt und können teilweise sogar in Smart-Cards implementiert werden. Vielversprechend, aber noch wenig erprobt ist eine neue Sensortechnologie, die mit Hilfe von Ultraschall direkt ein dreidimensionales Bild des Rillenmusters eines Fingers erfasst.

Handabdruck

Eine weitere Erkennungstechnologie basiert auf den unterschiedlichen Formen von Handflächen. Handabdruckerkennung ist wohl die erste und einfachste automatisierte biometrische Technologie. Es ist relativ einfach, die Grössenparameter einer Hand abzulesen, es muss lediglich die Hand auf eine Erkennungsfläche gelegt werden. Handerkennung ist eine robuste Technologie und wird noch oft in Hochsicherheitsumgebungen – jedoch meist in Kombination mit einem Passwort oder PIN-Code – angewendet. Die Einzigartigkeit ist aber nicht im gleichen Mass gesichert, wie diejenige der anderen genannten Methoden.

Gesichtserkennung

Die wohl umstrittenste Technologie ist die Gesichtserkennung. Sie erlaubt es, Personen ohne deren Einverständnis und von ihnen sogar unbemerkt biometrisch zu erfassen, was aus Sicht des Daten- und Persönlichkeitsschutzes sicherlich fragwürdig ist. Die Erkennung erfolgt durch die Messung der relativen Positionen und Grössen von Augen, Nase, Mund und anderen Charakteristika. Aufnahmen werden mit optischen oder Infrarotkameras gemacht, die auch im Dunkeln noch ein Gesichtsbild ergeben. Die Auswertung der Bilder ist jedoch sehr anspruchsvoll, und es werden neueste Methoden der Bild- und Objekterkennung sowie der künstlichen Intelligenz (z.B. neuronale Netze) eingesetzt, da die Aufnahmen ja aus verschiedensten Blickwinkeln und Distanzen erfolgen[10]. Da die Gesichtserkennung auch ohne direkten Einbezug der erfassten Personen abläuft, ist das Resultat nicht eine Zuordnung von biometrischen Daten zu einer digitalen Identität, sondern nur eine Übereinstimmungswahrscheinlichkeit mit bereits erfassten Personendaten. Gesichtserkennungssysteme werden heute in sicherheitskritischen öffentlichen Räumen wie etwa Flugplätzen, Stadien oder Schalterräumen eingesetzt, obschon ihr Nutzen in der Terrorismusbekämpfung sehr zweifelhaft ist[11]. Die Technologie eignet sich aber für die Authentifikation von berechtigten Personen in Zugangskontrollsystemen.

Iris und Retina

Das Auge ist das auffälligste individuelle Merkmale, und es ist wohl kein Zufall, dass sich Menschen, die einander begegnen, zur Erkennung in die Augen schauen. Biometrisch interessant sind sowohl das Äussere der Augen (Iris) wie auch der Augenhintergrund (Retina) (Bild 5).

Erst vor wenigen Jahren ist die Individualität der Iris mit ihrer Struktur und Farbe[12] entdeckt und patentiert worden. Länger bekannt – aber auch erst in den letzten Jahren systematisch genutzt – ist das individuelle Muster des Aderngeflechts der Retina im Augenhintergrund[13] (Bild 5b). Die erstgenannte Technologie basiert auf der individuellen Struktur und dem Muster der Filamente in der Iris (Bild 5d). Diese werden durch Gabor-Wavelets[14] beschrieben und in einem 2048-Bit-Vektor dargestellt. Bei der Retinaerkennung wird das Muster der Adern erfasst und parametrisiert. Beide Methoden sind biometrisch ausserordentlich sicher, das heisst, die False Acceptance Rate (FAR) liegt im Bereich von $1:10^6$ und die False Rejection Rate (FRR) ist vernachlässigbar. In beiden Fällen braucht es aber aufwändige und teure Technologien für die Datenerfassung, und insbesondere die Retinaerkennung wird von den erfassten Personen als invasiv und unangenehm empfunden. Ausserdem gelingt die Messung nur, wenn die Personen stillhalten und direkt in die Detektoren hineinschauen. Die Methoden werden deshalb hauptsächlich in speziellen Anwendungsnischen zum Einsatz kommen.

DNA und verwandte Methoden

Mit der rasanten Entwicklung in der Biotechnologie sind bereits heute völlig neue biochemisch basierte Identifikationssysteme absehbar. Vorläufer dieser Entwicklung ist die DNA-Analyse, die geringste Mengen von Zellmaterial eindeutig einem Individuum zuordnen kann. Es ist absehbar, dass bald weitere biochemische individualisierende Markersysteme gefunden werden. Vorläufig sind diese Methoden für die unmittelbare Authentifikation noch nicht geeignet, da die Messung nur offline im Labor durchge-

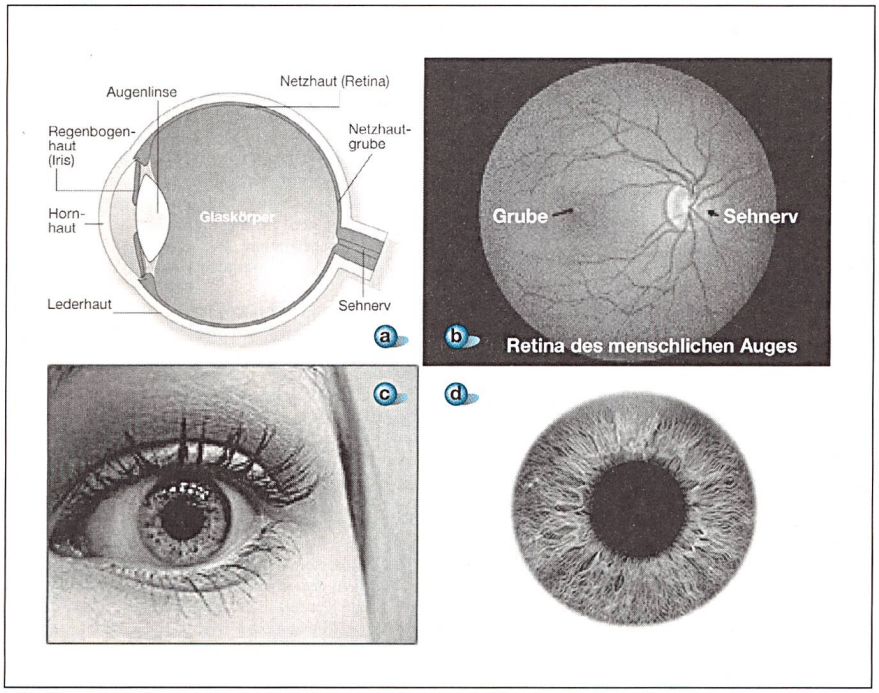


Bild 5 Iris und Retina haben bei jedem Menschen eindeutig unterscheidbare Merkmale
5a: Schematischer Querschnitt durch das Auge; 5b: Retina; 5c: Gesamtansicht des menschlichen Auges; 5d: Iris.

führt werden kann. Biochips haben jedoch das Potenzial, diesen Mangel bald zu beheben. Die Entwicklung von biochemisch basierten, kaum mehr angreifbaren Authentifizierungssystemen ist wohl nur eine Frage der Zeit.

Verhaltensbasierte Biometrie

Verhaltensbasierte Biometrie wird oft auch als aktive oder dynamische Biometrie bezeichnet. Der Grund liegt darin, dass immer eine Tätigkeit als Basis für die Merkmalsextraktion dient. Das Individuum muss somit bewusst oder unbewusst mit dem biometrischen Erkennungssystem zusammenarbeiten und sich um möglichst normales Verhalten bemühen. Allgemein sind diese Verfahren weniger genau, da das Verhalten einer Person von Situation zu Situation signifikant variieren und sich im Lauf eines Lebens in relativ kurzen Zeitabschnitten ändern kann. Oft werden deshalb verhaltensbasierte Verfahren nur zusätzlich zu anderen Identifikations- oder Authentifikationsprotokollen eingesetzt.

Stimmerkennung

Ein grösseres und breiteres Anwendungspotenzial hat die Stimmerkennung. Im Erkennungsprozess wird die Person aufgefordert, eine bestimmte Passphrase zu sprechen, die vorher nicht bekannt ist. Dies soll die natürlich nahe liegenden Replay-Angriffe durch aufgenommene Stimmen erschweren. Das Frequenzmuster der Stimme wird dann in einem Voice-Print in Funktion der Zeit aufgetragen und mit abgespeicherten Lautmustern der Person verglichen. Stimmerkennung ist eine komplementäre Technologie zur Spracherkennung. Im ersten Fall versucht man möglichst genau ein Stimmmuster zu erfassen, im zweiten Fall wird versucht, gemeinsame Phonemmuster[15] aus möglichst vielen unterschiedlichen Stimmen zu identifizieren. Für die beiden unterschiedlichen Probleme sind deshalb nicht die gleichen Erkennungstechnologien anwendbar. Wie alle verhaltensbasierten Methoden muss die Stimmerkennung situationsabhängige Variationen in der Stimmlage ausgleichen können. Das heisst natürlich, dass die Vergleichsmessungen mit grösseren Toleranzschwellen interpretiert werden und sich die Sicherheit der Authentifikation dadurch reduziert.

Unterschrift

Seit Jahrhunderten ist das Unterschreiben die Standardmethode, um zwischen einem Dokument und einer Person einen verpflichtenden Bezug zu schaffen. Die digitale Erfassung von Unterschriften gehört deshalb zu den Basistechniken der Biometrie. Unterschriftsdetektoren erfassen nicht nur das Schriftbild, sondern auch die Dynamik der Schreibstiftführung. Trotzdem ist die Unterschriftserkennung wie alle verhaltensbasierten Methoden nicht sehr sicher, da die natürlichen Schwankungen bei der Unterschriftsabgabe berücksichtigt und damit die Akzeptanzbandbreiten für die Merkmale zu gross gewählt werden müssen. Unterschriftserkennung ist trotz dieser Schwäche in fast allen Geldtransaktionen eine immer noch gebräuchliche Technik.

Bewegungsdynamik

Jeder Mensch hat beim Verrichten bestimmter Tätigkeiten eine individuelle Bewegungsdynamik. Diese Dynamik kann zum Beispiel via Keyboard erfasst werden und hilft den aktuell präsenten Nutzer zu identifizieren. Auch der Schritt einer Person ist charakteristisch, und es ist geplant, die Schritterkennung als Alternative bzw. Ergänzung zur Gesichtserkennung in der Überwachung von kritischen öffentlichen Räumen einzusetzen. Dabei wird die Schrittdynamik nicht optisch, sondern mit Hilfe von speziellen Radarsignalen erfasst, was es erlaubt, den störenden Einfluss der Kleider weit gehend zu eliminieren.

Wichtig für alle biometrischen Verfahren ist die Akzeptanz der Personen, die sich einem Erkennungsprotokoll unterziehen müssen. Die Gartner Research Group hat die verschiedenen biometrischen Techniken miteinander verglichen und unter den Aspekten «nicht invasiv», «sicher», «preiswert» und «einfach» beurteilt. Das Resultat dieser Beurteilung ist in Bild 6 dargestellt.

Anwendung und Trends in der Biometrie

Biometrie hat sich in den letzten Jahren zu einer wahren Boombranche entwickelt. Dutzende von Start-Ups bieten biometrische Sicherheitstechnologien an. Es hat sich jedoch gezeigt, dass fast alle heute gebräuchlichen Systeme die hochgesteckten Erwartungen punkto Sicherheit nicht vollständig erfüllen können. Zwar ist die Hürde für biometrische Fälschungen deutlich höher als für das Stehlen von Ausweisen oder digitalen Geheimnissen wie PIN-Codes oder Passwörter, doch können die Erfassungssysteme mit etwas Insiderkenntnissen oft ohne grossen Aufwand überlistet werden. Ein biometrischer Angriff verlangt jedoch direkt eine physische Präsenz am Ort des Detektors. Obschon dies eine beträchtliche Hürde darstellt, ist das Risiko eines erfolgreichen Angriffs auf einen biometrischen Detektor kaum kalkulierbar. Ein Ausweg aus diesem Problem sind komplexere Sensorsysteme, die gleichzeitig mehrere Merkmale erfassen,

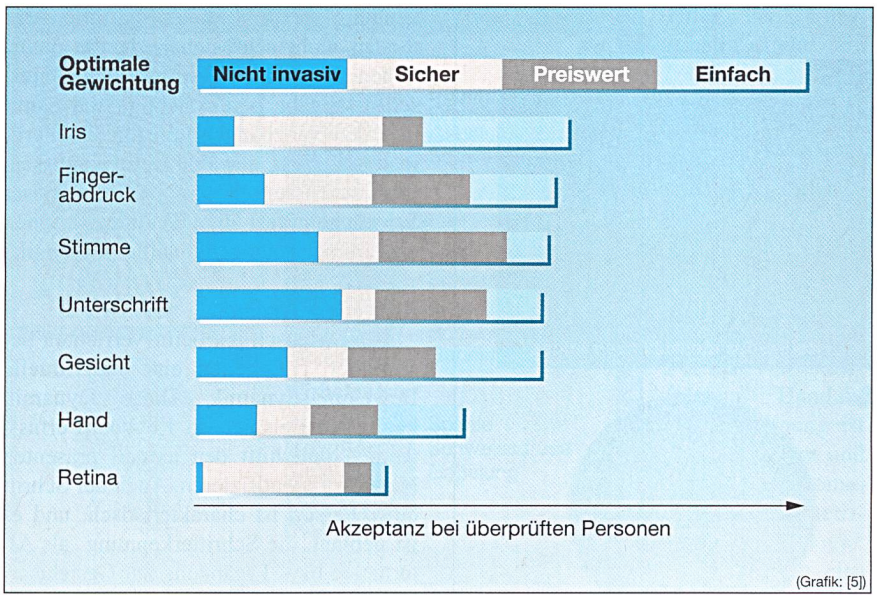


Bild 6 Vergleich der biometrischen Methoden unter dem Aspekt der Nutzerakzeptanz

wie zum Beispiel Fingerabdruckdetektoren, die gleichzeitig auch Puls, Hautimpedanz und weitere Eigenschaften messen. Dies führt jedoch zu teuren und störanfälligen Systemen. Einfacher und nahe liegend ist der hybride Ansatz mit einer Kombination von biometrischen und passwortbasierten Identifikationskriterien. Ein erfolgreicher Angriff, der gleichzeitig mehrere Prüffaktoren erfüllen muss, wird dann sehr unwahrscheinlich.

Referenzen

[1] *T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino:* Impact of artificial «gummy» fingers on fingerprint systems. Optical Security and Counterfeit Deterrence Techniques IV, Bellingham, Washington, 2002-01-23/25, Vol. 4677, The International Society for Optical Engineering, p. 275/288, 2002.

[2] *H. W. Kramer:* Improvement of Fingerprint Verification Algorithms. Diplomarbeit B29.11, Software-Schule Schweiz, Bern, 2003.

[3] *J. Fenn, A. Linden:* Gartner's Emerging Technology Hype Cycle for 2002. IGG-06122002-2.

[4] *V. Wheatman et al.:* Hype Cycle for Information Security. Gartner Research R-19-9974, 2003.

[5] *A. Allan:* Technology Overview. Gartner Research Report, DPRO-95808; 19.7.2002.

[6] *M. D. Garris et al.:* User's Guide to NIST Fingerprint Image Software. (NFIS) NISTIR 6813, National Institute of Standards and Technology, Gaithersburg, MD 20899-8940, mgarris@nist.gov.

Angaben zum Autor

Prof. Dr. **Lorenz Müller** hat Mathematik und Physik studiert und war danach längere Zeit in der Forschung tätig (Hochenergiephysik am CERN und am Stanford Linear Accelerator Center). Nach der Rückkehr in die Schweiz leitete er vorerst die Neuroinformatikgruppe an der Uni Bern, führte dann längere Zeit die Nachdiplomausbildung Eduswiss und ist heute Leiter der Dienststelle für angewandte Forschung, Entwicklung und Technologietransfer an der Hochschule für Technik und Informatik der Berner Fachhochschule. Kryptographie, Datensicherheit und Biometrie gehören seit längerem zu seinen Interessengebieten und stehen auch im Mittelpunkt der Aktivitäten seiner kürzlich mit Kollegen gegründeten Firma AXSionics.

Hochschule für Technik und Informatik, Biel, lorenz.mueller@hta-bi.bfh.ch

[1] Bei einem gleich bleibenden System kann die FRR durch Erhöhung der Toleranzgrenzen reduziert werden, gleichzeitig erhöht sich aber die FAR und umgekehrt. Die absolute Fehlerquote, bei der beide Fehlerraten gleich sind (EER: Equal Error Rate), ist ein Mass für die Qualität eines biometrischen Systems.

[2] Identity theft bzw. Identitätsdiebstahl ist heute eine der Hauptbedrohungen für IT-Grosssysteme. Die in Boston ansässige Aberdeen Group prognostiziert, dass sich die durch Identitätsraub verursachten Kosten von heute 8,75 Mrd. US-Dollar auf 24 Mrd. verdreifachen werden (Quelle: www.aberdeen.com, 12. März 2003)

[3] DNA: Desoxyribonukleinsäure. Molekül, das die Erbinformation trägt.

[4] Scotland Yard nutzt Fingerabdrücke nach dem Galton-Klassifikationssystem offiziell schon seit 1901.

[5] In den zwei Berichten *National Strategy to Secure Cyberspace* und *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* setzt die US-Regierung Standards für die Umsetzung von Sicherheitsmassnahmen, die biometrische Methoden für die Personenidentifizierung und -authentifizierung einbeziehen müssen. (Department of Homeland Security, DHS).

[6] In Macao und Brunei sind bereits heute in Deutschland hergestellte biometrische (Fingerabdruck-)Identitätskarten im Gebrauch (http://www.heise.de/; Meldung vom 13.02.2003)

[7] Bereits im 19. Jahrhundert wurden die grundlegenden Fingerabdruckmuster beschrieben und klassifiziert. Das von Sir Francis Galton (Britischer Anthropologe) 1892 eingeführte Klassifizierungssystem mit «Minutiae Punkten» ist immer noch die Basis der Fingerabdruckerkennung.

[8] Suchabfrage auf der Web-Seite http://europa.eu.int/scadplus/scad_de.htm

[9] T. Matsumoto, ein japanischer Professor, konnte kürzlich zeigen, dass ein Grossteil der Fingerprint-Sensoren gefälschte Finger nicht zurückweisen (False Acceptance). Im Rahmen einer Diplomarbeit an der Software-Schule Schweiz wurden diese Experimente verifiziert und Gegenmassnahmen für die Verbesserung der Erkennungsalgorithmen gesucht [1, 2].

[10] Auf der Homepage der Firma Cognitec Systems findet man Illustrationen zu den einzelnen Auswertungsschritten vom Rohbild bis zum Merkmalsvektor (www.cognitec-systems.de/technology-description.htm, 7. August 2003)

[11] www.findbiometrics.com/Pages/face_articles/face_2.html; 12.7.2003

[12] Basierend auf Dr. John Daughman's Arbeit, Cambridge University, und patentiert von Leonard Flom, Aran Safir, 1987

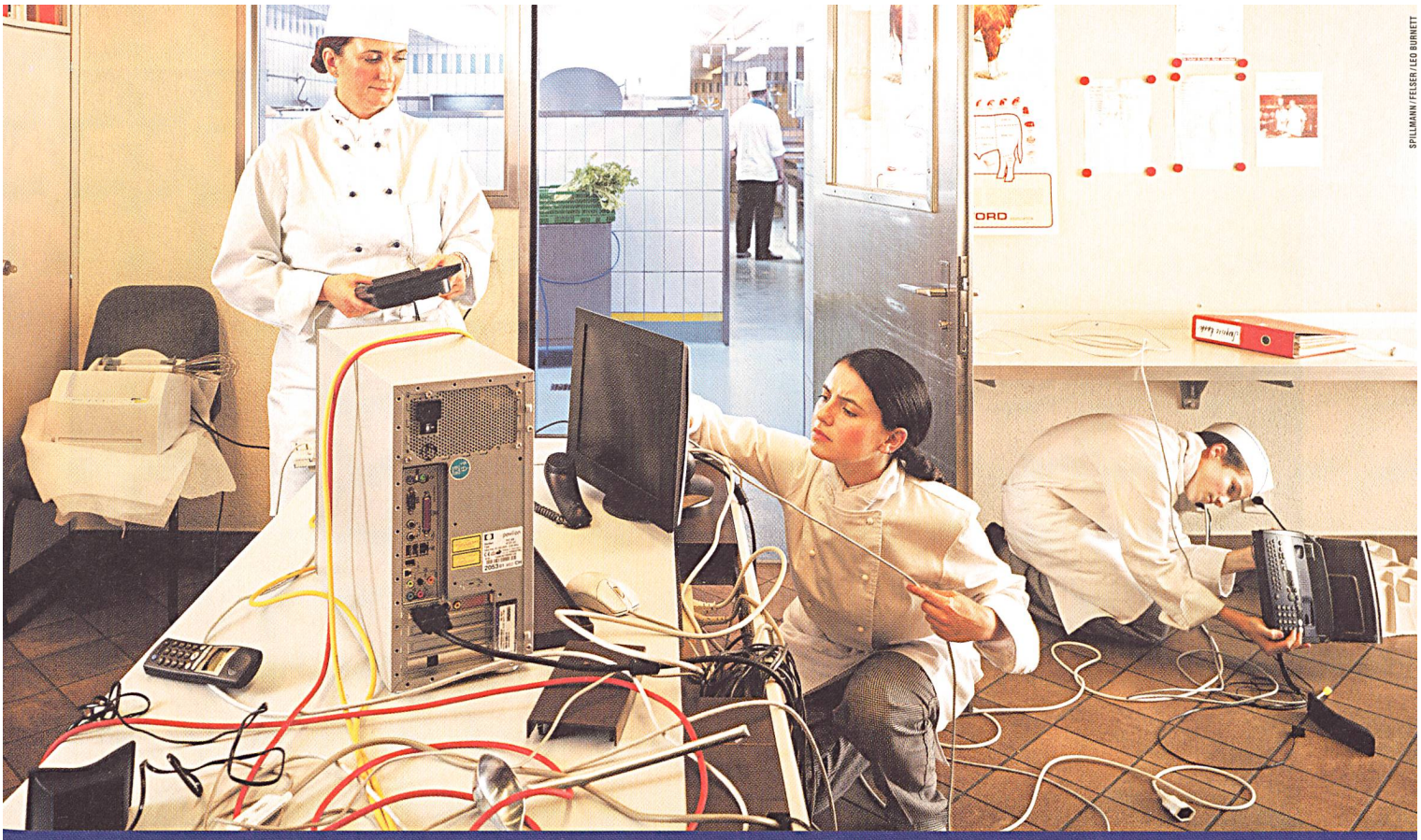
[13] Nebenprodukt der Augenlaserchirurgie. Dr. John Marshall, Augenarzt in London, hat die Nutzung der Einzigartigkeit patentiert, das Grundpatent ist inzwischen aber abgelaufen.

[14] Gabor-Wavelets: Transformationsverfahren, das sich für die Erkennung von Linien und Kanten eignet. Eine der Eigenschaften von Gabor-Wavelets ist die Fähigkeit, Lücken in Linien zu schliessen.

[15] Phonem: Phoneme einer Sprache sind deren kürzeste bedeutungsunterscheidende lautliche Elemente. So unterscheiden sich beispielsweise Miete und Mitte oder Miete Mine jeweils in nur einem Phonem.

La biométrie – trait d'union entre la personne et son identité – Première partie

A côté des méthodes conventionnelles comme les empreintes digitales ou la signature, on a de plus en plus souvent recours à des procédés biométriques d'identification des personnes physiques, par exemple par les traits du visage et la voix ou encore par les empreintes digitales génétiques, les systèmes complexes saisissant et évaluant simultanément plusieurs caractéristiques. En général, les systèmes biométriques nécessitent l'enregistrement des données personnelles à une base de données centralisée, ce qui pose également des problèmes de protection des données. Un concept d'authentification développé à la haute école spécialisée de technique et d'architecture de Bienne permet le contrôle d'autorisation au moyen d'une Smart-Card équipée d'une interface biométrique vers la personne à authentifier. La première partie de l'article donne un aperçu des différents procédés utilisés dans le contrôle d'identification. La seconde partie présentera le nouveau concept d'authentification.



SPILLMANN/FELSER/LEO BURNETT

Ganz gleich welche Kommunikationsbedürfnisse Sie in Ihrem KMU haben, wir bieten Ihnen die entsprechenden Lösungen. Bei uns erhalten Sie nebst den neusten Telefonapparaten, Faxgeräten und Telefonzentralen eine fachkundige Installation der Geräte, Zugriff auf das flächendeckende Netz von Swisscom Mobile und Internetzugang via Bluewin mit dem neuen noch schnelleren und leistungsfähigeren ADSL-Anschluss. Und dazu eine fachkundige Beratung und einen Service, die beide auch nach dem Kauf weitergehen. Damit Sie noch mehr Zeit für Ihre Kunden haben. Zürich 01 294 88 27, Luzern 041 207 71 70, St. Gallen 071 499 20 30, Olten 062 286 44 80, Lausanne 021 344 24 40. www.swisscom-fixnet.ch/kmu

Gut, dass einer von 3857 Fachhändlern aus dem Swisscom Partner-Netz in Ihrer Nähe ist.

Für alle KMU.

VSEI USIE

ELITE ELECTRO-PARTNER

swisscom Partner

swisscom fixnet

Einfach verbunden.

Sie können Strahlen –
unsere Transformatoren nicht!

VA TECH ELIN
Transformator Typ SR

Strahlungsreduziert
Stark reduzierte elektromagnetische Strahlung (unter 1 μT).

Niedriger Wärmeverlust und kaum wahrnehmbares Betriebsgeräusch.

Wirtschaftlich
Die Investitionskosten für eine Neuanschaffung sind geringer als die Kosten für den Umbau Ihrer bestehenden Anlage.

IBA Elektro AG
Binzmattweg 2 • 5035 Unterentfelden
Telefon 062 835 03 70 • Telefax 062 835 03 80
servicebetriebe@iba-aarau.ch

IBA

Zählerfernauslesung, Energiedaten erfassen, analysieren, visualisieren...

Für die Energieverrechnung benötigen Sie zuverlässige Energiedaten.

Wir liefern die gesamte Lösung von der mobilen Zählerdatenerfassung, dem Zählerfernauslese-System über das Energiedatenmanagement bis zur Internet-Visualisierung.

www.optimatik.ch

Generalvertretung für
- **Zählerfernauslese-System ITF-EDV Fröschl**
- **Energiedatenmanagement-System BelVis von Kisters AG**

OPTIMATIK xamax

Optimatik AG, GZS Strahlholz, 9056 Gais, Tel. 071 793 30 30, Fax 071 793 18 18, info@optimatik.ch
Xamax AG, Hardhofstrasse 17, 8424 Embrach, Tel. 01 866 70 80, Fax 01 866 70 90, info@xamax-ag.ch