

Ein biometrisches Bezahlsystem für Kaufhäuser

Herausforderungen für Entwickler und Datenschützer

Manfred Bromba

Biometrische Bezahlsysteme auf Identifikationsbasis stellen höchste Ansprüche an die biometrischen Algorithmen, den Fälschungsschutz, die Rechenleistung – und an den Datenschutz. Warum das so ist, soll hier an einem Beispielkonzept erläutert werden.

Einleitung

Biometrische Bezahlsysteme erfreuen sich immer höherer Akzeptanz und Beliebtheit. Hierbei bietet das Geschäft seinen Stammkunden die Möglichkeit, sich beim Einkauf allein auf Basis des Fingerabdrucks zu identifizieren und damit das Einverständnis für eine automatische Abbuchung des Kaufbetrags vom Konto des Kunden einzuleiten. Zusätzliche biometrische Überprüfungen von Gesicht und Unterschrift sollen einen extrem hohen Manipulationsschutz garantieren. Denn mehr noch als bei einer Verifikation, stellen Identifikationsanwendungen mit großer Nutzerzahl eine besondere Herausforderung für Datenschutz und Sicherheit dar. Dieser Artikel beschreibt eine mögliche Realisierung einer Kassenanwendung mit bis zu drei teilweise vom Kassenspersonal auszuwertenden biometrischen Merkmalen.

Warum Biometrie?

Eine freiwillig genutzte biometrische Anwendung wird sich nur dort durchsetzen, wo in Summe für Betreiber und Endanwender (besser: „Merkmalsträger“) ein konkreter Nutzen entsteht. Im Fall der Bezahlungen muss man nicht lange suchen:

Vorteile für den Kunden:

- ◆ Keine Karten oder Ausweise bei sich tragen müssen
- ◆ Schnellerer Einkauf
- ◆ Nutzung von Zusatzrabatten wie bei Kundenkarten
- ◆ Weniger Fälschungsmöglichkeiten

Vorteile für den Betreiber:

- ◆ Mehr Umsatz durch kundenfreundlichere Prozeduren
- ◆ Weniger Extern-Kosten als bei Kartentransaktionen
- ◆ Weniger Zeitbedarf als für Karten und Bargeld

- ◆ Wie bei Kundenkarten kein Bargeldverkehr
- ◆ Wie bei Kundenkarten Kundenbindungsprogramme möglich
- ◆ Geringeres Risiko durch Betrugsversuche

Es sollen aber auch die Nachteile nicht verschwiegen werden:

- ◆ Wie bei Kundenkarten ist keine Anonymität möglich
- ◆ Der Kunde muss seinem Geschäft vertrauen können (Datenschutz)

Es folgen zunächst einige Vorschläge, wie sich die optimale Performanz des Systems in Bezug auf biometrische Erkennungsleistung und Rechenleistung gewährleisten lässt. Die gewählten Beispiele entsprechen den Möglichkeiten am Markt verfügbarer qualitativ hochwertiger Hardware- und Software-Komponenten.

Biometrische Performanz

Definitionen

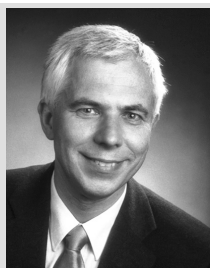
FAR „*Falschakzeptanzrate*“: Wahrscheinlichkeit, dass ein nicht registrierter Finger identifiziert wird

FRR „*Falschrückweisungsrate*“: Wahrscheinlichkeit, dass ein registrierter Finger nicht identifiziert wird

FIR „*Falschidentifikationsrate*“: Wahrscheinlichkeit, dass ein registrierter Finger identifiziert, aber einer falschen ID zugeordnet wird

Näherungen für große Kundenzahlen

Grundsätzlich hängen bei einer Identifikation die definierten Performanzwerte von der Zahl N der gespeicherten Referenz-Templates ab. Dies lässt sich sogar näh-



Dr. Manfred Bromba

Geschäftsführer der Bromba GmbH, Biometrics Consulting

Copyright Meinen Fotografie München Fotografin A. Hegner

<http://www.bromba.com/contactd.htm>

rungsweise im Voraus berechnen. Man beachte jedoch, dass die Performanzwerte stark vom gewählten Sensor abhängen und letztendlich für eine gewählte Konfiguration nur durch geeignete Messungen zu ermitteln sind! Auch ist zu beachten, dass insbesondere die FRR personenspezifisch ist. Üblicherweise wird jedoch über viele Personen gemittelt, so dass manche Aussagen und Berechnungen für den Individualfall nur begrenzte Gültigkeit haben.

Da bei einer Identifikation der Anfragefingerabdruck mit vielen gespeicherten Referenzfingerabdrücken verglichen wird, kann der Fall auftreten, dass die Ähnlichkeitswerte (Scores) für *mehrere* Referenzen die voreingestellte Schwelle überschreiten. Dies ist für einen registrierten Nutzer zwar unkritisch, wenn es um reine Zutrittsberechtigungen geht, führt aber zu großen Problemen, wenn wie bei einer Bezahllösung eine korrekte Zuordnung von Identitätsdaten zum biometrischen Merkmal unabdingbar ist. Man kann sich vorstellen, was passiert, wenn ein Käufer zwar als Kunde erkannt, das Geld aber von einem anderen Kundenkonto abgebucht wird.

Die Wahrscheinlichkeit dafür, dass unabhängig von der richtigen Referenz noch weitere (aber per Definition falsche) Kandidaten die Akzeptanzschwelle des biometrischen Systems überschreiten, lässt sich aus der FAR berechnen, da diese Kandidaten bei einer Verifikation eben eine Falschakzeptanz darstellen würden. Ihr Wert ist für große Referenzzahlen N durch

$\sim N \cdot FAR_1$ *Mehrfachakzeptanzrate*
gegeben, wobei FAR_1 die Falschakzeptanzrate (Verifikations-FAR) für ein System mit einer Referenz darstellt. Diese Näherung gilt nur für den Fall, dass die resultierende Mehrfachakzeptanzrate deutlich unter 1 liegt [FQ].

Mit obigen Definitionen ergeben sich unter idealisierten Bedingungen (statistische Unabhängigkeit, gleiche Fehlerraten für alle Personen, ...) folgende Formeln für große N :

$FAR_N \sim N \cdot FAR_1$ *Identifikations-Falschakzeptanzrate*

Damit steigt die FAR ungefähr linear mit der Zahl der Templates an.

$FRR_N \sim FRR_1$ *Identifikations-Falschrückweisungsrate*

Das heißt, die mittlere FRR hängt näherungsweise nicht von der Zahl der Templates und der FAR_1 ab.

$FIR_N \sim FRR_1 \cdot FAR_N$ *Falschidentifikationsrate*

Die Falschidentifikationsrate ist somit näherungsweise gleich der FAR_N , vermindert um die FRR_1 . Denn dieser Fehler kann mit der in [FQ] gewählten Definition nur auftreten, wenn eine Falschrückweisung vorliegt!

Beispiel 1: Es seien 100 000 Fingerabdrücke (von z.B. 50 000 Kunden) als Templates gespeichert. Die FAR_1 für eine Verifikation betrage 10^{-8} bei einer FRR_1 von 5% (derzeit nur mit Bildkorrelationsverfahren einfach zu erreichen). Dann ist
 $FAR_N \sim 0.1\%$ und $FIR_N \sim 0.005\%$

Enrollment- und Identifikationsstrategie

Bei der Berechnung der Zahl der fehlerhaften Transaktionen ist es wichtig, zwischen einem Fehler, der durch einen Kunden verursacht wurde und einem durch eine Attacke hervorgerufen Fehler zu unterscheiden. Im ersten Fall ist der Fingerabdruck bekannt und als Referenztemplate in der Datenbank abgespeichert. Im zweiten Fall handelt es sich um einen gänzlich unbekanntem Finger. Dieser kann von einem nicht registrierten Kunden oder von einem nicht registrierten Finger eines registrierten Kunden stammen. Fehler der ersten Art lassen sich durch folgende Strategie minimieren:

1. Beim Enrollment wird der neue Finger eines (neuen) Kunden gegen alle schon gespeicherten Finger geprüft. Es darf dann keine Falschakzeptanz gegen die Finger der übrigen Kunden erfolgen. Da mehrmaliges Auflegen des gleichen Fingers (große Sensorfläche vorausgesetzt) immer sehr ähnliche Bilder liefert, sollte auf diese Weise ausgeschlossen werden können, dass das System zwei registrierte unterschiedliche Finger als ähnlich erkennt. Sollte eine Falschakzeptanz beim Enrollment auftreten, darf man einen solchen Finger natürlich nicht in die Datenbank aufnehmen. Sicherheitshalber sollte man für diesen Check die Akzeptanzschwelle etwas niedriger einstellen. Umgekehrt könnte man für solche „biometrischen Zwillinge“ auch individuell die Schwellwerte während der Identifikation erhöhen.

2. Um auszuschließen, dass registrierte Kunden durch einen nicht registrierten Finger eine Falschakzeptanz bzw. Falschidentifikation erzeugen, sollte die Finger-Nummer grafisch ausgegeben und durch den Kassierer kontrolliert werden.

Zahl der fehlerhaften Transaktionen

Zur Ermittlung der Gesamtzahl der fehlerhaften Transaktionen pro Zeiteinheit unterscheiden wir wieder die beiden Fälle

1. Finger ist in Datenbank registriert
2. Finger ist nicht registriert
Wenn im ersten Fall die vorgeschlagene Enrollmentstrategie genutzt wurde, sollten eigentlich keine Falschidentifikationen auftreten, weil das Auflegen immer desselben Fingers stark korrelierte Daten erzeugt mit ähnlich niedrigen Scorewerten. Leider ist dieser Fall nicht rechnerisch quantifizierbar. (Man bräuchte dazu allerdings lediglich die mittlere (über alle Finger gemittelte) statistische Verteilung der Scorewerte bei Auflegen immer desselben Fingers und Vergleich gegen die Gesamtdatenbank!)

Der zweite Fall ist ein reiner Angriffsfall, der durch folgende Möglichkeiten entsteht:

2a. Ein registrierter Kunde legt nichtwissentlich oder wissentlich einen nichtregistrierten Finger auf („Lotto spielen und einen anderen Kunden bezahlen lassen!“)

2b. Ein nicht registrierter Kunde legt irgendeinen Finger auf, um das System zu „testen“.

Beide Fälle lassen sich wiederum dadurch deutlich entschärfen, dass der Kassierer die am Kassendisplay auszugebende Finger-Nummer vergleicht.

Um die Gesamtzahl der durch Attacken erfolgten Falschakzeptanzen zu ermitteln, genügt es wegen der statistischen Unabhängigkeit, die Zahl der unabhängigen (d.h. mit unterschiedlichen Fingern erfolgten) Attacken mit FAR_N zu multiplizieren.

Beispiel 2: Daten wie in Beispiel 1. Die Zahl der Schummelversuche betrage 100 pro Tag. Dann ist die Zahl der Falschakzeptanzen 1 pro 10 Tage!

Kombination mit weiteren Merkmalen

Um die Zahl der fehlerhaften Transaktionen weiter zu verringern, bietet sich eine Kombination von Fingerprint mit Displayausgabe eines Kundenfotos an. Der Verkäufer kann sich dann ein letztes Mal von der Richtigkeit der Kundenzuordnung überzeugen. Schlägt der Bildvergleich fehl, liegt offenbar ein FAR-Fall vor. Der Kunden kann dann entweder den Finger nochmals auflegen oder einen anderen registrierten Finger hernehmen. (Auf jeden Fall sollte

eine solche Situation eine Neuüberprüfung des Enrollments auslösen!

Diese Kombination hat folgende Auswirkung auf die Fehlerraten:

- ◆ 1. Die Gesamt-FRR steigt an, weil der Kassierer das Bild nicht immer sicher zuordnen kann.
- ◆ 2. Die Gesamt-FAR sinkt ungefähr um einen (geschätzten) Faktor 100.

Beispiel 3: Daten wie in Beispiel 2. Durch die manuelle Gesichtserkennung sinkt die Zahl der Falschakzeptanzen auf etwa 1 alle 3 Jahre!

Beweissicherung

Obwohl die Zahl der Falschakzeptanzen und -identifikationen sehr niedrig gehalten werden kann, mag es doch als störend empfunden werden, dass das Geschäft keinerlei Beweismittel für den Fall aller Fälle in der Hand behält. Denn wenn ein Kunde eine Transaktion nachträglich abstreitet und sich dabei auf die von null verschiedene FAR beruft, bleibt dem Geschäft nichts anderes übrig, als den Schaden zu ersetzen. Das ist bei kleinen Fehlerraten kein Problem. Sollte sich diese Form der Kulanz jedoch herumsprechen, werden sich viele echte Betrüger finden!

Als Vorschlag zur Lösung dieses Problem bietet sich der Einsatz der Unterschrift als drittem biometrischen Merkmal an. Die Unterschrift lässt sich genauso wie ein Gesichtsfoto beim Enrollment speichern und nach der Identifikation als Grafik am Kassendisplay ausgeben, so dass der Verkäufer die Möglichkeit hat, auch die Unterschrift in Echtzeit auf Echtheit zu überprüfen. Wird die Unterschrift auf Papier geleistet, ist sogar eine nachträgliche Prüfung möglich. Bei dieser Methode ist mit einer weiteren Reduktion der Gesamt-FAR um einen Faktor 100 zu rechnen. Zusätzlicher Vorteil: Die Unterschrift ist nur dem Kassierer in Anwesenheit des Käufers zugänglich. Damit entfällt die bei verlorengegangenen Kreditkarten kurzzeitig vorhandene Möglichkeit, die fremde Unterschrift zum Zwecke des Betruges „üben“ zu können.

Sicherheit

Besondere Vorteile bietet das zusammengesetzte „multimodale“ System mit Fingerprint-, Gesichts- und Unterschriftenkennung in Bezug auf Fälschungen. Da schon die Fingerabdruckererkennung unter den Augen des Kassierers stattfindet, sind hier Fälschungen mit schwer zu stehlenden aber

sonst vielleicht relativ einfach nachzumachenden Fingerabdrücken nur schwer realisierbar. Des Weiteren müsste ein „Angreifer“ sich noch eine Gesichtsmaske zulegen sowie die passende Unterschrift nachmachen können, um Erfolg zu haben. Insgesamt bietet das zusammen mit einer Kaufsummenbeschränkung so wenig Anreiz, dass sich niemand dieses Aufwands mit dem Ziel eines Betruges unterziehen wird. Außerdem wird man davon ausgehen können, dass die Sicherheit für den Kunden größer ist als bei Einsatz von EC-Karten, Kreditkarten oder Bargeld. Rechnet man nämlich für die Unterschriftenverifikation einen weiteren Faktor 100 hinzu, kommt man unter den Voraussetzungen von Beispiel 3 auf 1 Fehler alle 300 Jahre.

Falschrückweisungen

Falschrückweisungen sind in der Bezahlanwendung kaum ein Sicherheitsthema, sondern eher ein Problem der Transaktionszeiten. Es ist vergleichbar mit der Nichtakzeptanz von Kreditkarten, wenn z.B. die Übertragungsleitung gestört ist.

Es wird empfohlen, bis zu drei Identifikationsversuche mit einem Finger zuzulassen. Hat das System sinnvollerweise beim Enrollment „Ersatzfinger“ abgespeichert (was aber je nach Konzept den Identifikationsrechenaufwand erhöht), sollte zunächst dieser herangezogen werden. (Ersatzfinger erhöhen allerdings auch die FAR_N durch Erhöhung von N, was bei der Kalkulation zu berücksichtigen ist, siehe oben.)

Gibt das System als Fehlerursache eine schlechte Bildqualität aus, sollte der Verkäufer dem Kunden geeignete Abhilfemaßnahmen vorschlagen. Hierbei können mehr als 3 Versuche erlaubt sein.

Kunden mit erhöhter Falschrückweisung bei der Identifikation sind u. U. neu zu registrieren. Es ist allerdings auch bei den besten Fingerabdruckscannern immer mit einem gewissen Prozentsatz von zeitweise nicht identifizierbaren Personen zu rechnen. Für solche Fälle ist ein Rückfallverfahren ähnlich wie bei Kreditkarten vorzusehen.

Rechnerische Performanz

Welche Templategröße?

Beim Vergleich der Fingerprinttemplates kommt das gesamte Spektrum der in ISO/IEC 19794 vorgesehenen Methoden in

Frage. Die kleinsten Templates (einige 100 Bytes) erzielt man mit Minuzienverfahren, die größten (ca. 100 kB) bei den Bildkorrelationsverfahren, die im Prinzip mit vorverarbeiteten Rohbildern arbeiten. Verständlich, dass große Templates auch kleinere Identifikationsraten pro Prozessor erzielen:

- ◆ Große Templates: z.B. 1 000 pro s
- ◆ Kleine Templates: z.B. 10 000 pro s

Vorteil der Korrelation gegenüber dem Minuzienvergleich ist die mit zunehmendem Schwellwert des Entscheiders weit weniger stark ansteigende FRR. Das macht sich z.B. so bemerkbar, dass die kleinen Templates bei einer FRR von 10% nur eine FAR von 10⁻⁵ erreichen, während die großen 10⁻⁸ schaffen können.

In beiden Fällen steigt die Vergleichszeit ungefähr linear mit der Zahl der Referenztemplates an, vorausgesetzt, der Arbeitsspeicher ist groß genug, um alle Templates ohne Auslagerungsoperationen aufnehmen zu können.

Die kleinen Templates sind vor allem dann von Vorteil, wenn es um die Übertragungsrate zu anderen Systemen geht. Um 100 kB-Templates in 1 s zu übertragen, ist immerhin eine Rate von fast 1 Mbit/s erforderlich!

Erforderliche Rechenleistung

Wichtig ist die Skalierbarkeit des Identifikationssystems, um mit zunehmender Akzeptanz und/oder Geschäftsgröße eine problemlose Erweiterung durchführen zu können. Dabei ist insbesondere das Problem des mit der Kundenzahl annähernd quadratisch ansteigenden Rechenaufwands zu lösen. Verdoppelt sich nämlich die Zahl der registrierten Kunden, verdoppelt sich auch der Rechenaufwand für *eine* Identifikation. Gleichzeitig kann man jedoch davon ausgehen, dass auch doppelt so viele Kunden diesen Service nutzen werden, womit sich die Zahl der notwendigen Identifikationen ein weiteres Mal verdoppelt. Insgesamt haben wir also eine Vervielfachung des Rechenbedarfs! Zum Glück wächst die zur Verfügung stehende Prozessorrechenleistung gemäß dem Mooreschen Gesetz mit fortschreitender Entwicklung exponentiell, so dass man sich mit zunehmender Kundenzahl auf keinen aussichtslosen Wettlauf einlassen muss.

Beispiel 4: Ein Geschäft hat 1 000 Kunden mit je 2 registrierten Fingerprints und 1 Kasse, deren Prozessor auch zur Erkennung genutzt wird. In diesem Fall ist die Erkennung in ca. 2 s abgeschlossen, was schneller ist als jedes andere Zahlungsmittel. Für Bildüberprüfung und Unterschrift kommen nochmals ca. 5 s dazu. Pro Tag wären damit bei angenommenen 10s -Einkäufen max. 3 600 Bezahlvorgänge möglich.

Beispiel 5: Ein Geschäft hat 5 000 Kunden mit je 2 registrierten Fingerprints und 10 Kassen, deren Prozessor auch zur Erkennung genutzt wird. In jeder Kasse sind 1 000 unterschiedliche Referenztemplates (1 pro Finger) abgespeichert. Die Kassen sind untereinander mit 100 Mbit/s vernetzt. Jede Identifikationsanfrage wird von allen Kassen parallel verarbeitet. In diesem Fall ist die Erkennung unter Vernachlässigung der Kommunikation in ca. 1 s abgeschlossen, wenn in Summe nicht mehr als 1 Anfrage pro 10 s erfolgt. Damit wären pro Tag max. 3 600 Kunden bedienbar.

Beispiel 6: Ein Geschäft hat 50 000 Kunden mit je 2 Fingerprints und 100 Kassen mit einer jeweiligen maximalen Transaktionsrate von 1 Kunden pro 20 s. Das ergibt in Summe maximal 500 000 Vergleiche pro s. Daraus ergibt sich ein Bedarf von 500 Prozessoren. Es wären pro Tag max. 180 000 Bezahlvorgänge möglich.

Schnelle Identifikation

Vergleicht man bei der Identifikation nicht mit allen gespeicherten Referenztemplates, sondern hört auf, sobald der erste Vergleich einen Scorewert oberhalb der Schwelle liefert, sollte sich bei einer Gleichverteilung (alle Kunden kaufen gleich häufig ein) im Mittel eine Rechenzeitersparnis von einem Faktor 2 ergeben. (Wir vernachlässigen hier die Falschrückweisungsfälle und die Attacken mit nichtregistrierten Fingern, die immer die volle Suchzeit beanspruchen.)

Allerdings ist mit einer höheren Fehlerrate zu rechnen. Solch ein Fehler tritt grundsätzlich nur dann auf, wenn tatsächlich mehrere Referenztemplates die Schwelle überschreiten würden. Diese Fehlerrate entspricht der oben definierten Mehrfachakzeptanzrate und damit der N-fachen Verifikations-FAR, wenn dieser Wert deutlich unter 1 liegt. Unter genau dieser äußerst sinnvollen Bedingung dürfte sich die Fehlerrate deshalb *nicht* spürbar erhöhen!

Beispiel 7: Gleiche Bedingungen wie in Beispiel 6, jedoch wird mit Schneller Identifikation gearbeitet. Das ergibt im Mittel maximal 250 000 Vergleiche/ s und damit einen Bedarf von 250 statt 500 Prozessoren. Es wären pro Tag max. 180 000 Bezahlvorgänge möglich.

In der Praxis wird es große Unterschiede in der Einkaufshäufigkeit einzelner Kunden geben, das heißt, es gibt eine erhebliche Abweichung von der Gleichverteilung. Wenn man deshalb die Kunden-Referenztemplates nach ihrer Nutzungshäufigkeit so „anordnet“, dass die häufigsten Kunden zuerst überprüft werden, lässt sich eine weitere deutliche Reduktion der mittleren Rechenzeit erzielen, wobei der Mittelwert der geordneten Verteilung für das Maß der Einsparung entscheidend sein dürfte.

Schließlich lassen sich weitere Kriterien zur Reduktion der mittleren Rechenzeit heranziehen, wie z.B. den Ort einer Transaktion. Wenn Kunden bestimmte Kassen oder Geschäfte einer Kette bevorzugen, sollte man zuerst in den zugeordneten ortsabhängigen Datenbankteilen suchen.

Auch das Zeitverhalten könnte ein Kriterium sein, wenn sich z.B. herausstellt, dass ein Kunde nach einem Einkauf erst nach einer bestimmten „Totzeit“ zurückkehrt. Dabei ist auch zu berücksichtigen, dass bei einem Einkauf häufig mehrere Kassen aufgesucht werden.

Alles in allem kommt es darauf an, für die Betriebsart Schnelle Identifikation einen Ordnungsalgorithmus zu finden, der im Zusammenspiel mit zugehörigen Statistiken die Kundentemplates nach ihrer aktuellen Einkaufswahrscheinlichkeit anordnet. Dabei kommt einem zu Gute, dass sich alle Statistikwerte automatisch aus dem tatsächlichen Kundenverhalten ableiten lassen, weshalb man permanent auch auf Änderungen reagieren kann.

Minimierung der Transaktionszeit

Um die Transaktionszeiten für einen Kassenvorgang optimal zu nutzen, kann die Nutzung von *Pipelining* deutliche Vorteile bringen. Dabei geht es darum, durch parallele Abarbeitung von manuellen und automatisierten Prozessen die Gesamtzeit dadurch zu minimieren, dass alle Ressourcen möglichst ohne Leerzeiten arbeiten. So ist zu prüfen, ob man das Scannen des Fingerabdrucks nicht z.B. vor dem Einscannen der Kaufartikel durchführt. Die Rechenarbeit findet dann während des manuellen Scannens statt. Danach Bildprüfung, Ausdruck des Kassensons und Unterschrift. Mit der Unterschrift wird schließlich der Vorgang der Einverständniserklärung rechtlich abgesichert.

Alternative Konzepte

Minuzientemplates benötigen weniger Übertragungskapazität, Arbeitsspeicherplatz und Rechenleistung beim Vergleich, ermöglichen aber leider keine so gute Personentrennung (FAR). Abhilfe brächte hier die Identifikation zweier Finger oder das zweimalige Auflegen desselben Fingers. So ließe sich mit dem zweimaligen Auflegen desselben Fingers und einer ODER-Verknüpfung der Resultate bei gleichzeitiger Reduktion der Entscheidungsschwelle [MV] möglicherweise eine Verifikations-FAR von 10^{-8} bei einer FRR von 10% erreichen! (Wegen möglicher Korrelationen beim zweimaligen Auflegen desselben Fingers kann die FRR im theoretischen Worst-Case aber auch ca. 30% betragen!) Auf jeden Fall ist mit einem Rechenleistungsvorteil von einem Faktor 5 und einem Übertragungskapazitäts- und Arbeitsspeicherplatz-Vorteil von einem Faktor 200 zu rechnen.

Optionen

Der Entscheidungsschwellwert des biometrischen Systems lässt sich dem Wert eines Einkaufs individuell anpassen. Es ist dann allerdings bei höheren Werten mit einer höheren FRR zu rechnen. Dies wird ein Kunde aber aus Sicherheitsgründen gerne in Kauf nehmen (falls er es weiß!).

Sensorauswahl

Es dürfte inzwischen allgemein bekannt sein, dass sich bei einem biometrischen Erkennungssystem die Fehlerraten FRR und FAR gegenläufig mit dem Akzeptanzschwellwert ändern. Höhere Schwelle bedeutet höhere FRR bei kleinerer FAR und umgekehrt. Der Fingerprintsensor hat einen erheblichen Einfluss auf die FRR bei gleicher FAR. Je besser die Bildqualität und die Bedienbarkeit im Mittel über alle Kunden, desto besser wird auch die FRR bei konstanter FAR sein. Während die FRR insbesondere die Transaktionszeiten beeinflusst, ist die FAR eher für die Rate der fehlerhaften Kundenzuweisungen verantwortlich. Wie man beide Werte zueinander einstellt ist letztlich eine Frage der Optimierung der aus Kulanzkosten und Systemkosten (Prozessoranzahl) bestehenden Gesamtkosten.

Weitere Anforderungen an das Sensorgehäus sind

- ◆ Eignung für Multiuserbetrieb

- ◆ Schutz gegen elektrostatische Aufladungen (lässt sich auch durch Gestaltung der Kassenumgebung beeinflussen)
- ◆ Reinigungs- und Desinfektionsmöglichkeiten

Diese Anforderungen sind heute durch gute optische und kapazitive Sensoren problemlos erfüllbar. Aus der Anfangszeit der kapazitiven Sensoren weiß man noch, dass Multiusereignung nicht trivial ist, da jeder Nutzer unsichtbare Reste auf der Sensoroberfläche hinterlässt. So kann es bei älteren Sensoren durchaus noch passieren, dass Benutzer mit trockenen Fingern nicht die Hinterlassenschaften eines Vorgängers mit feuchteren Fingern „überschreiben“ können, was dann zu einer Abweisung wegen schlechter Bildqualität durch Überlagerung führen kann.

Beim der Aufstellung des Sensorgeräts auf dem Kassentisch ist darauf zu achten, dass die meisten Einzelgeräte für die sitzende und nicht für die stehende Nutzung konzipiert wurden. Hier kann man dem Kunden durch eine angeschrägte Aufstellung (45° Erhöhung zum Kunden hin) entgegenkommen. Anforderungen, die in dieser Anwendung weniger Bedeutung haben, sind Fälschungsschutz, Vandalismusschutz und Größe.

Normung

Angetrieben durch den Zeitdruck beim biometrischen Reisepass, gibt es seit kurzem erste Normen, die auf biometrische Systeme zugeschnitten sind. Bereits verfügbar ist die Standardisierung der Referenztemplates (ISO/IEC 19794), der Programmierschnittstellen für die Erkennungsalgorithmen (ISO/IEC 19784) und der Ermittlung der Fehlerraten (ISO/IEC 19795).

Aus Sicht des Betreibers ist das wichtigste Thema der Schutz der Referenztemplates gegen Ausfall des Systemanbieters. Zwar wird ein softwarebasiertes System nicht von heute auf morgen ausfallen, nur weil der Systemanbieter nicht mehr existiert. Muss man jedoch sein System ersetzen, ergibt sich bei nichtgenormten Templates das Problem, bei einem neuen System schlagartig alle Kunden neu registrieren zu müssen. Da ist die Wiederverwendbarkeit der alten Templates fast ein Muss! Aus Sicht des Verfassers ist die flexibelste Möglichkeit die Abspeicherung der Rohbilder, da sich aus diesen problemlos alle anderen, auch proprietären (und

damit in der Regel leistungsfähigeren) Templateformate ableiten lassen.

Zum Vergleich unterschiedliche Systeme in Hinblick auf ihre Leistungsfähigkeit ist eine Performanzbestimmung nach ISO/IEC 19795 essenziell. So werden von den Algorithmenanbietern auch heute noch FRRs im Bereich 0.001% angepriesen, was weit jenseits aller Machbarkeit liegt, legt man eine Bestimmungsmethode nach ISO/IEC zugrunde. Praxisnah sind Werte im einstelligen Prozentbereich, niedrige FAR-Werte vorausgesetzt!

Die Standardisierung der Programmierschnittstellen ist primär für den Systemanbieter von Bedeutung, wenn sich dieser gegen Ausfall des Algorithmenerstellers absichern will. Allerdings hat der Standard ISO/IEC 19784 („BioAPI 2.0“) bisher noch nicht nachgewiesen, dass der Einbau einer neuen proprietären Schnittstelle tatsächlich immer kostenträchtiger ist als das Auswechseln eines genormten Erkennungs-Moduls.

Datenschutz

Der Schutz der Kundendaten [DS] ist für das hier vorgestellte System von besonderer Bedeutung. Das gilt sowohl für die Kundenverkehrsdaten als auch für die biometrischen Daten, auf die wir uns hier beschränken wollen.

Warum ist der Schutz der biometrischen Daten wichtig? Es gibt zwei Aspekte, die hier besondere Beachtung finden müssen:

1. Das Bekanntwerden der biometrischen Daten kann ein Sicherheitsrisiko darstellen.
2. Insbesondere Fingerprintdaten lassen sich als (fast) eindeutige Identifikatoren zur Informationsgewinnung und –zusammenführung nutzen.

Punkt 1 ist relativ schnell abgehandelt. Geraten die Daten, und hier sind insbesondere unverschlüsselte und formatgenormte Daten ein Problem, in falsche Hände, könnte ein Betrüger versuchen, sich eine falsche Identität durch physikalische Nachbildung eines Fingerabdrucks, einer Unterschrift oder eines Gesichts zu verschaffen und dadurch den Systembetreiber oder Kunden schädigen. Wie aber bereits oben erläutert, ist durch die teilmanuelle Mehrfachüberprüfung das Risiko, das Bezahlsystem zu hintergehen, beliebig niedrig, besonders im Vergleich zu herkömmlichen Zahlmethoden. Anders sieht es aus, wenn die beschriebenen Rohdaten für die Überlistung fremder biometrischer Systeme genutzt

werden, die nicht über die hier vorgesehene Mehrfachabsicherung verfügen. Aber auch für die gilt der Grundsatz: Biometrische Merkmale sollten nur in einfachen Anwendungen mit niedrigem Gefahrenpotenzial als Geheimnisse betrachtet werden. Um trotzdem sicherzugehen, wird empfohlen, die „Betriebs-Templates“ im proprietären Format zu belassen und ausschließlich verschlüsselt zu speichern und zu verarbeiten. Für die genormten „Backup-Roh-Templates“ sind dagegen Hochsicherheitsvorkehrungen zu treffen.

Punkt 2 ist schon etwas kritischer und gleichzeitig diffuser, obwohl das Prinzip der Freiwilligkeit die Sache deutlich entschärft. Da es sich beim hier vorgestellten Bezahlsystem um ein *Identifikationssystem* handelt, sind auch „Nebenanwendungen“ denkbar, die nur dann keinen Schaden anrichten, wenn kein Missbrauch zu befürchten ist [DS]. So zeigt die Erfahrung, dass eine größere Ansammlung von Identitätsdaten Begehrlichkeiten weckt. Es sei nur an das Beispiel Mautdaten erinnert, die ursprünglich nicht zur Nutzung bei der Verbrechensaufklärung vorgesehen waren. In unserem Falle könnte es z.B. für Strafverfolger von Interesse sein, einen gesuchten Tatort-Fingerabdruck in einer großen Kaufhaussammlung wiederzufinden und auf diese Weise an weitere Informationen wie Namen etc. eines Ersttätters zu kommen. Selbst, wenn der Biometrieteil des Bezahlsystems aus Sicherheitsgründen keine Schnittstelle nach außen hat, ist doch durch Anfertigung eines Stempels [BS] relativ leicht eine Probe-Identifikation über den Sensor möglich. Wie schon beim Internet oder beim Handy, sind als Preis für die Bequemlichkeit auch hier Konflikte mit der informationellen Selbstbestimmung vorprogrammiert.

Literatur

- FQ M. Bromba, FAQ der Bioidentifikation, <http://www.bromba.com/faq/biofaqd.htm>
- DS M. Bromba, Datenschutz-FAQ, <http://www.bromba.com/faq/bprifaqd.htm>
- MV Wesemann-Schlegel, H.; Bromba, M., Combination of multiple fingers in fingerprint verification, 2001, <http://www.bromba.com/knownow/multiverification.htm>
- BS M. Bromba, Biometrie und Sicherheit, 2003, <http://www.bromba.com/knownow/biosich.htm>