

Holographisch beschreibbare Polymere

Hochsicherer Speicher in Ausweisen für Biometrie-Anwendungen

Torsten Hupe

Biometrische Systeme verändern die Sicherheitswelt. Doch die Möglichkeiten elektronischer Chipkarten sind begrenzt. Das neue Kunststoff-Speichermedium PhenoStor® könnte bestehende Probleme lösen.

Einleitung

Zeige mir deinen Finger und ich sage dir, wer du bist: Biometrie erobert den Alltag. Wer sich am Flughafen, am Arbeitsplatz oder Geldautomaten identifizieren will, wird künftig nicht mehr nur gemustert, sondern auch vermessen.

Die Palette der mehr oder weniger erfolgreich erprobten Systeme, die auf Identifikation durch Körpermerkmale setzen, reicht vom Fingerabdruckvergleich über Iris-Scans bis zu Venenmuster- und Gesichtserkennung.

1 Forderung nach sicheren, dezentralen Datenspeichern

Eine zentrale Sammlung der Vergleichsdaten verursacht jedoch nicht nur Datenschützern Bauchschmerzen. Sie ist auch zeitaufwändig und benötigt bei jeder Überprüfung einen Kontakt zur Datenbank. Dezentrale Lösungen scheinen daher erstrebenswerter zu sein: Biometrische Daten werden auf einem Dokument (z.B. auf einem Ausweis) gespeichert, das die zu identifizierende Person bei sich trägt. Bei einer Abfrage wird die Übereinstimmung der persönlichen Merkmale mit den auf dem Dokument abgelegten Daten geprüft.

Die Anforderungen an Technik und Sicherheit sind hoch. Ob Reisepass, Firmenausweis oder Fußball-Saisonticket: Je detaillierter und umfangreicher biometrische Daten eingesetzt werden, desto mehr Speicherkapazität braucht das transportable Medium, auf dem diese Informationen abgelegt werden. Es muss fälschungssicher sein und die Daten gegen unberechtigtes Kopieren und Manipulieren schützen, aber auch Unbefugten den Zugang zu den Daten verwehren.

Datenschutzrechtliche Bedenken und Akzeptanzprobleme bei Ausweisnutzern ergeben sich dementsprechend nicht nur aus dem potenziellen Risiko des Missbrauchs oder der Weitergabe biometrischer Informationen durch die prüfberechtigten Stellen, sondern auch aus mangelndem Vertrauen in die Sicherheitstechnik. „Die Versprechen über Vorteile und Sicherheit der biometrischen Systeme werden mit der heute verfügbaren Technik nur bedingt gehalten“, schreibt der Bundesdatenschutzbeauftragte auf seiner Internet-Seite.¹

2 Steigender Bedarf nach Speicherkapazität

Bei den bisherigen Projekten kommen üblicherweise elektronische Chips zum Einsatz. Diese sind in ihrer Kapazität beschränkt: So ist das gleichzeitige Abspeichern mehrerer biometrischer Daten nur möglich, wenn Abstriche bei Auflösung oder Anzahl der erfassten Merkmale gemacht werden. Die dabei entstehenden Ungenauigkeiten führen bislang oft zu hohen ‚Falsch-Akzeptanzraten‘ bzw. ‚Falsch-Abweisungsraten‘. Die Folge: Das Kontrollsystem legitimiert eine falsche Person oder weist eine richtige zurück. Gleichermaßen verhält es sich mit der Verwendung so genannter Templates, bei denen die biometrischen Merkmale nicht als Bild, sondern bereits in codierter Form vorliegen: Je höher der Informationsgehalt eines Templates, desto besser die erzielten Akzeptanzraten, bzw. desto mehr Kapazität wird für die Speicherung der Daten abverlangt.



Dipl.-Ing.
Torsten Hupe

Projekt Manager
Bayer-Innovation
Storage&Security

torsten.hupe@bayer-innovation.de

3 Holographie als Basis für sichere und hoch-kapazitive Speicher

Der Einsatz neuer Kunststoffe in Verbindung mit der Holographie bietet nun zu den konventionellen, Chip-basierten Systemen eine konzeptionelle Alternative, bedingt durch die deutlich höhere Speicherkapazität, durch die Robustheit als auch aufgrund der zusätzlichen Sicherheit gegen Datenmanipulation und Datendiebstahl.

Wie funktioniert der Speichervorgang, bei dem Informationen in lichtempfindliche Polymere eingeschrieben werden? Durch Lichtstrahlen werden die Moleküle des Materials ausgerichtet und verursachen die lokale Änderung des Brechungsindex' [Abb.1]. Auf diese Weise lassen sich Daten-Hologramme in das Material einschreiben, wodurch z.B. biometrische Informationen festgehalten und später ausgelesen werden können. Je nach Einsatz erlaubt das Medium sowohl den einmaligen Einschreibevorgang („write once“) als auch alternativ das mehrmalige Beschreiben („re-write“).

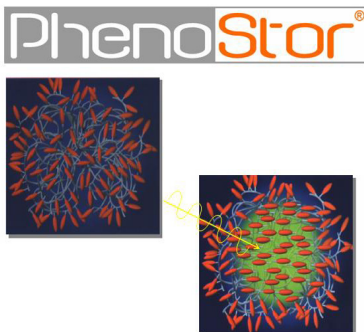


Abb. 1: Ausrichtung des Polymers durch Licht

Der praktische Ablauf: Informationen, z.B. ein Fingerabdruck, werden zunächst digital kodiert, ggf. digital verschlüsselt und anschließend einer optischen Maske zugeführt. Zwei Lichtstrahlen, bezeichnet als Objektstrahl und Referenzstrahl, projizieren die Informationen mit Hilfe der Maske auf das Speichermedium, wobei im Material durch Überlagerung der Lichtstrahlen ein Interferenzmuster entsteht. Die Moleküle richten sich nach dem gewonnenen Muster aus. Der Ausleseprozess erfordert später genau den Referenzstrahl, wie er beim Schreiben der Daten verwendet wurde –

ansonsten ist die Ordnung der Moleküle nicht zu erkennen, auch nicht unter einem Mikroskop [Hari06].

Dieser Umstand lässt sich aus Sicherheitsüberlegungen heraus nutzen: In dem der Referenzstrahl beim Einschreibevorgang eine optische Maske durchleuchtet, kann partiell die Phase des Lichtes verändert werden, was die Möglichkeit bietet, die zu speichernden Daten optisch zu codieren. Damit ist gewährleistet, dass das Auslesen der Daten ohne ein entsprechend codiertes Lesegerät nicht möglich ist [Voe05].

Auf diese Weise wird verhindert, dass neben der Manipulation und dem Kopieren der Daten auch der unberechtigte Zugriff auf die Hologramm-Daten für Unbefugte nicht möglich ist.

4 Vorteile der Holographie

Im Vergleich zur konventionellen Chip-Technologie ist zunächst die Speicherdichte der holographisch beschreibbaren Polymere herauszustellen: Sie beträgt ca. 3,5 Mbit/mm². Damit lassen sich umgerechnet auf die Fläche eines Chip-Speichermoduls etwa 10 MByte Daten unterbringen, wobei der Speicher als Laminat-Beschichtung in Form und Größe grundsätzlich frei wählbar ist.

Das Polymer ist zudem temperatur- und feuchtigkeitsresistent sowie unempfindlich gegenüber elektromagnetischer Strahlung. Zur Robustheit trägt auch eine Eigenschaft bei, die Hologramme per se besitzen: Ist ein Teil durch Schmutz oder Kratzer nicht mehr optisch erreichbar, bleibt die Information insgesamt verfügbar, wenn auch mit einem reduzierten Kontrast. Darüber hinaus ist den Daten eine selbstkorrigierende Codierung mitgegeben, die Fehler in einem gewissen Maße beheben kann [Voe06].

Durch die flexible Verwendbarkeit des Materials eignet sich der neue Speicher für kombinierte Dokumente, die sowohl auf Biometrie als auch auf klassischen Identifizierungskriterien (Foto, Unterschrift) beruhen. Dazu zählen Reisepässe, Personalausweise, Führerscheine oder Zugangskarten für den Arbeitsplatz [Henn06], [Abb. 2].



Abb. 2: PhenoStor®-Kartenrohlinge

Die holographisch beschreibbaren Polymere weisen in diesen Bereichen einige Vorteile auf:

- Während vor dem Hintergrund einer langen Lebensdauer große Anstrengungen unternommen werden, Chips in diese Dokumente zu integrieren, ist der Polymer-Speicher typischerweise bereits ein inhärenter Bestandteil einer Ausweiskarte.
- Hierbei braucht beim Auslesen nicht auf die RFID-Technologie zurückgegriffen werden, sondern der Vorgang erfolgt verschleißfrei durch einen Einsteckvorgang in das Lesegerät: Das ungewollte Auslesen eines z.B. in einer Tasche befindlichen Dokuments ist damit prinzipiell nicht möglich.
- Die Dokumente sind in ihrer Funktionalität beliebig erweiterbar: Sollten sich im Laufe des Lebenszyklus weitere Anwendungen ergeben, können die hierfür benötigten Informationen zu einem späteren Zeitpunkt hinzugefügt werden.
- Bedingt durch die optische Codierung erlaubt der Polymer-Speicher, als Multi-Applikationskarte mehrere Daten physikalisch getrennt auf demselben Medium zu speichern, indem verschiedene Bereiche voneinander unabhängig beschrieben werden.
- Quasi als Nebeneffekt ermöglicht schließlich die analoge, holographische Datenspeicherung, Kopien von Originalen zu unterscheiden: Während Chips grundsätzlich digitale Daten verarbeiten, bei denen die Unterscheidung zwischen Original und Kopie nur mittels aufwändiger elektronischer Signaturen möglich ist, lassen sich Kopien von analogen Daten anhand von Kopierverlusten ohne größeren Aufwand feststellen.

5 Ein neues Medium für neue Anwendungen

Die am weitesten fortgeschrittene Umsetzung der holographisch beschreibbaren Polymere als Datenspeicher stellt derzeit PhenoStor[®] dar. Die möglichen Einsatzfelder beschränken sich nicht auf den ID-Check, also der Authentisierung oder Identifizierung von Personen [Bund05], [Icao03]. Auch die Gesundheits- oder übergreifende Bankkarte werden als nahe liegende Anwendungen betrachtet. Umfassende Patienten- bzw. Kundendaten lassen sich, wirksam gegen Datenmissbrauch oder -diebstahl geschützt, auf einer PhenoStor[®]-Speicherkarte ablegen und autorisierten Benutzergruppen zur Verfügung stellen: Das Röntgenbild für den Radiologen, die Blutdruckwerte für den Internisten, Adresse und Geburtsort für die Krankenkasse können getrennt gespeichert und abgefragt werden. [Bmgs05]. Ähnlich verhält es sich beim Stand des Girokontos bei Bank A gegenüber den Informationen über die Sparbucheinlagen bei Bank B, die voneinander getrennt sein müssen.



Abb. 3: PhenoStor[®]-Kartenlese-Einheit

Aktuell befindet sich das PhenoStor[®]-System im Zertifizierungsprozess, der in diesem Jahr ein Sicherheitszertifikat nach ‚Common Criteria‘ mit der Vertrauenswürdigkeitsstufe EAL 3 vorsieht, welches für 2007 auf EAL 4+ erweitert wird. Zeitgleich befinden sich PhenoStor[®]-Anwendungen derzeit bei mehreren Pilotkunden im Testbetrieb, um die Voraussetzungen für ein ausgereiftes System zu schaffen [Abb.3].

Fazit

Insgesamt verspricht der Einsatz holographisch beschreibbaren Polymere wie z.B. PhenoStor[®] eine Vielzahl neuer Anwendungen: Die größere Speicherkapazität gegenüber heutigen Systemen, gepaart mit den optischen Sicherheitseigenschaften, erlauben neue Lösungsansätze im Bereich Identitätsmanagement, wobei hier Perspektiven insbesondere in Kombination mit der Biometrie aufgezeigt werden, die in der Vergangenheit – nicht zuletzt aus Datenschutzaspekten – kaum umsetzbar waren.

Bayer Innovation GmbH hat in Kooperation mit einer Reihe von Firmen und Forschungseinrichtungen mit Expertise in Optik, Kryptographie und Sicherheitstechnik das alternative Speichermedium PhenoStor[®] entwickelt: Es basiert auf einem speziellen Polymer, das es erlaubt, auf molekularer Ebene Informationen in sehr hoher Dichte zu speichern, und zugleich Schutz gegenüber Datenmanipulation und -diebstahl bietet. Die Technologie umfasst nicht nur das Medium, sondern auch die Schreib- und Lese-Einheiten.

Literatur

- [Bfdi05] Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit: http://www.bfdi.bund.de/nm_533592/DE/Schwerpunkte/Biometrie/Artikel/BiometrieVorDemDurchbruch.html
- [Bmgs05] Bundesministerium für Gesundheit: Informationen zur elektronischen Gesundheitskarte: <http://www.bmgs.bund.de/download/broschueren/a415.pdf>
- [Bund05] Informationen der Bundesdruckerei zum Personalausweis / Reisepass: http://www.bundesdruckerei.de/de/iddok/2_1/index.html
- [Hari02] P. Hariharan: Basics of Holography, University Press Cambridge (2002) 1-2
- [Henn06] O. Henninger, D. Scheuermann, U. Waldmann: Usability of holographic data storage technology for biometric data in governmental ID documents, Fraunhofer SIT Darmstadt (2006)
- [Icao03] ICAO TAG MRTD/NTWG Technical Report Version 2.0: Development and Specification of Globally Interoperable Biometric Standards for Machine Assisted Identity Confirmation using Machine Readable Travel Documents: <http://www.icao.int/mrtd/biometrics/recommendation.cfm>
- [Voe04] Völkening / Jüngermann / Hupe: Security Applications based on Memory Intelligent Polymers, Publication for D-A-CH Security (2004)
- [Voe05] Völkening / Jüngermann / Hupe: ‚Light sensitive polymers – a solution for the storage of large sensitive data on plastic cards/plastified cards‘, Publication for 9. Deutscher IT-Sicherheitskongress des BSI (2005)

Anmerkung / Remark

This article is also available in English on our web page ‘www.phenostor.com’.