Untersuchung der Möglichkeit eines biometrischen On-Pen Matching

Tobias Scheidat · Claus Vielhauer

Otto-von-Guericke Universität Magdeburg
{tobias.scheidat | claus.vielhauer}@iti.cs.uni-magdeburg.de

Zusammenfassung

In diesem Beitrag soll die Möglichkeit untersucht werden, ein On-Pen Matching mit dem biometrischen Merkmal der dynamischen Handschrift durchzuführen. Dabei soll ähnlich dem On-Card Matching bzw. On-Card Sensor der Vergleich zwischen den Authentifikations- und Referenzdaten auf demselben digitalen Stift erfolgen, mit dem die Authentifikationsdaten erfasst wurden. Da eine solche Hardware nach dem Wissen der Autoren derzeit nicht zur Verfügung steht, wird zunächst ein Stift zur reinen Erfassung von Notizen und Skizzen genutzt. Die aufgenommenen Daten werden dann auf einen Computer übertragen, der Referenz- und Testdaten miteinander vergleicht. Auf diese Weise kann konzeptionell überprüft werden, ob die erfassten und gespeicherten Daten für eine biometrische Erkennung ausreichen. Dabei konnte festgestellt werden, dass die Equal Error Rate ähnlich der für die bisher genutzte Hardware ist, in einem Großteil der untersuchten Fälle konnten sogar bessere Ergebnisse erzielt werden. In einem zweiten Schritt wird dann eine Untersuchung der Komplexität des genutzten Verifikationsalgorithmus durchgeführt, um eine Abschätzung für die erforderliche Hardware bei der künftigen Implementierung eines On-Pen Matchers zu erhalten.

1 Motivation

Neben den bisher weit verbreiteten Verfahren zur Benutzerauthentifikation, geheimes Wissen bzw. persönlicher Besitz, bietet sich die biometrische Benutzerauthentifikation als Ersatz oder Ergänzung an. Vorteil der Biometrie ist die Verbundenheit des genutzten Charakteristikums mit dem Körper des Inhabers. Bei der Authentifikation durch geheimes Wissen verfügt der Anwender über ein anderen Personen unbekanntes Wissen, welches den Zugang zu einem gesicherten Bereich ermöglicht. Dieses Verfahren ist sehr weit verbreitet, zum Beispiel in Form von Passwörtern beim Login von Betriebssystemen. Der persönliche Gegenstand ist ein physisches Objekt, mit dem die Berechtigung zum Zugang zu einem geschützten Bereich nachgewiesen wird. Beispielhaft ist hier die Verwendung eines Schlüssels oder einer SmartCard zu nennen. Große Nachteile beider Verfahren sind neben dem Verlieren bzw. Vergessen die beabsichtigte Weitergabe oder das Ausspähen des Wissens bzw. der Diebstahl des Gegenstandes. Dadurch kann eine dritte Person sich mit dem Authentifikationsobjekt eines berechtigten Nutzers Zugang verschaffen. Dieses Vorgehen kann durch die Kombination der Verfahren untereinander erschwert werden, beispielsweise durch die Verbindung einer geheimen Zahlenkombination mit einer SmartCard (z.B. PIN und EC-Karte im Bankverkehr). Dadurch kann zwar der Aufwand eines Angreifers vergrößert werden, aber falls er über die benötigten Merkmale verfügt, kann er sie für einen Missbrauch nutzen. Das ist möglich, da keine physische Verbindung zwischen geheimem Wissen bzw. persönlichem Gegenstand und dem Inha-

P. Horster (Hrsg.) · D•A•CH Security 2006 · syssec (2006) 392-404.

ber besteht. Anders verhält es sich bei der Verwendung eines oder mehrerer biometrischer Merkmale zur Benutzerauthentifikation. Diese Charakteristiken sind fest mit dem Körper (*statisch*) oder dem Verhalten (*dynamisch*) eines Menschen verbunden. Bekannte Beispiele sind hier die Nutzung des Fingerabdruckes, der Iris oder der Handschrift. Die biometrischen Verfahren basieren also auf der Tatsache des Vorhandenseins der berechtigten Person, wogegen bei den oben genannten Verfahren nur die Präsenz eines bestimmten Wissens oder Gegenstandes überprüft werden kann. Auch hier kann eine Verbesserung der Sicherheit erreicht werden, indem einzelne biometrische Modalitäten miteinander bzw. mit den Merkmalen geheimes Wissen und persönlicher Besitz kombiniert werden. Hier ist beispielsweise die Kombination des Fingerabdrucks (Biometrie) mit einer SmartCard (Besitz) zu nennen.

Die dieser Arbeit zugrunde liegenden Untersuchungen basieren auf der dynamischen Charakteristik der Handschrift. Dabei soll festgestellt werden, ob es möglich ist, eine Benutzerauthentifikation anhand der Datenaufzeichnung eines digitalen Stifts, am Beispiel des *Logitech io Personal Digital Pen* (io Pen) durchzuführen. Ist dies mit zufrieden stellender Genauigkeit möglich, sollen Überlegungen angestellt werden, ob analog zum On-Card Matching ein On-Pen Matching mit dieser oder einer ähnlichen Hardware möglich ist. Durch die Kombination von dynamischer Biometrie (Handschrift) und persönlichem Besitz (io Pen) kann sowohl eine Verbesserung der Sicherheit als auch der Akzeptanz von Seiten des Nutzers erwartet werden. Weiterhin wird untersucht, ob die zusätzliche Verwendung von geheimem Wissen, in Form einer Passphrase oder eines Symbols, zu einer weiteren Verbesserung führen kann. Auch die Unterschrift wird als weit verbreitetes und akzeptiertes Authentifikationsmerkmal mit in die Untersuchungen einbezogen.

Der Beitrag gliedert sich wie folgt: Zunächst werden zum besseren Verständnis einige Grundlagen der biometrischen Benutzerauthentifikation erläutert. Daran anschließend wird auf für diesen Beitrag relevante Hardware zur Erfassung von dynamischer Handschrift und auf das On-Card Matching eingegangen. Im dritten Abschnitt wird der Aufbau der dieser Arbeit zugrunde liegenden Tests beschrieben. Dabei wird auf die Zusammensetzung und Ermittlung der Testmenge eingegangen, aber auch auf die Durchführung der Tests. Der daran anschließende Abschnitt befasst sich mit der Performanz des io Pen bezüglich der Erkennungsgenauigkeit. Vergleichend wird dabei auch auf die Resultate früherer Test mit anderer Hardware eingegangen. Dabei handelt es sich um Tests mit Grafik-Tabletts und speziellen Signatur-Tabletts. Im fünften Abschnitt wird, basierend auf den Testergebnissen, nochmals die Möglichkeit der Verwendung von Stift basierter Aufnahme-Hardware und eines On-Pen Matching diskutiert. Eine Zusammenfassung des Beitrages und ein Ausblick auf zukünftige Arbeit im Bezug auf die ermittelten Ergebnisse werden im letzten Abschnitt gegeben.

2 Biometrische Benutzerauthentifikation

An dieser Stelle werden einige wichtige Grundlagen für die biometrische Benutzerauthentifikation vorgestellt. Außerdem wird auf ausgewählte Hardware zur Erfassung biometrischer Eigenschaften der Handschrift eingegangen. Die Selektion basiert dabei auf den für unsere Arbeit relevanten technischen Geräten. Zusätzlich werden anhand von Referenzen auf entsprechende Publikationen Möglichkeiten aufgezeigt, biometrische Merkmale und persönlichen Besitz miteinander zu kombinieren, um die Sicherheit zu verbessern.

2.1 Grundlagen biometrischer Benutzerauthentifikation

Als Benutzerauthentifikation wird der Vorgang bezeichnet, bei dem die Identität von Personen überprüft wird. Für diese Überprüfung werden zwei Arten von Daten benötigt, die Referenzdaten und die Daten deren Authentizität nachgewiesen werden sollen. Die Authentifikation gilt als erfolgreich, wenn beide Daten in ausreichendem Maß übereinstimmen. Bei der Authentifikation können zwei Arten der Bestätigung der Identität unterschieden werden. Unter einer *Identifikation* versteht man den Vergleich aller hinterlegten Referenzdaten mit den Authentifikationsdaten. Die Person gilt als identifiziert, wenn Referenzdaten gefunden werden können, die ausreichend mit den aktuell vorgewiesenen Daten übereinstimmen. Von *Verifikation* spricht man, wenn das System überprüft, ob die vorgewiesenen Authentifikationsdaten mit den Referenzdaten einer behaupteten Identität (z.B. Nutzername) innerhalb eines Variationsbereiches übereinstimmen. Die dieser Arbeit zugrunde liegenden Tests wurden grundsätzlich als Benutzerverifikation durchgeführt und werden im Folgenden auch vereinfachend als Authentifikation bezeichnet.

Die Abbildung 1 stellt den allgemeinen Prozess der biometrischen Verifikation schematisch dar. Grundlage der Verifikation sind die hinterlegten Referenzdaten im System bzw. auf der SmartCard oder dem Pen. Der Vorgang zur Generierung dieser Daten wird in der Biometrie als Referenzdatenerfassung (Enrollment) bezeichnet. Dabei werden die folgenden Prozesse des biometrischen Systems durchlaufen: die biologischen Daten werden durch den Sensor erfasst und die Merkmale extrahiert (Merkmalsextraktion). Liegen die Daten in ausreichender Qualität und Anzahl (die Mehrzahl der Systeme verlangt mehrere Authentifikationsdaten zur Erzeugung der Referenzdaten) vor, kann vom System ein Referenzdatensatz erzeugt werden, der dann gespeichert wird. Im ersten Schritt der Verifikation wird dann die vorgewiesene biometrische Eigenschaft (aktuelle Authentifizierungsdaten) vom Sensor erfasst und nach einer eventuellen Vorverarbeitung (in Abbildung 1 nicht berücksichtigt, da nicht Bestandteil unseres Systems) an den Merkmalsextraktor weitergegeben. Dieser extrahiert die erforderlichen Merkmale aus den Eingabedaten und erzeugt daraus einen Merkmalsvektor, der das Merkmal innerhalb des Systems repräsentiert. Dieser Vektor wird in einem Vergleichsprozess dem Featurevektor der Referenzdaten der behaupteten Identität gegenübergestellt. Der Ähnlichkeitswert stellt das Maß der Ähnlichkeit beider Vektoren zueinander dar. Dieser ist der Eingangswert für die Klassifizierung, die über das Ergebnis der Verifikation entscheidet. Entscheidet das System, dass der Nutzer derjenige ist, der er vorgibt zu sein, so wird *true* zurückgegeben, sonst *false*.

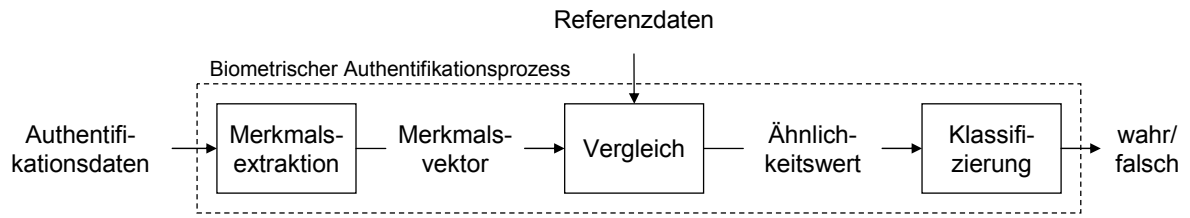


Abb. 1: schematische Darstellung eines biometrischen Verifikationsprozesses

Für die Untersuchung der Leistungsfähigkeit unseres Systems bezüglich der Benutzerauthentifikation haben wir die Betrachtung der Fehlerraten *False Non Match Rate* (FNMR) und *False Match Rate* (FMR) herangezogen. Diese haben wir aus einer Vielzahl (siehe [Lass02] und [Waym99]) von möglichen Fehlerraten für biometrische Systeme bzw. Algorithmen ausge-

wählt. Dabei gibt die FNMR an, wie viele berechtigte Nutzer vom biometrischen Algorithmus abgelehnt wurden sind. Wie viele nicht autorisierte Nutzer vom Algorithmus angenommen werden, wird von der FMR beschrieben. Ist der Wert von FNMR und FMR identisch, spricht man von der *Equal Error Rate* (EER). Diese Größe wird als Vergleichswert in den einzelnen Tests verwendet.

2.2 Hardware zur dynamischen Handschriftenerfassung

Die Hardware zur Computer gestützten Aufnahme von dynamischen Handschriftenmerkmalen kann in drei Gruppen unterteilt werden. Diese Aufteilung basiert dabei auf der Art und Wiese, wie die Schrift erfasst wird.

Unterschriftentabletts: Die erste Gruppe bilden Unterschriftentabletts, auf denen die Schrift mit einem normalen Schreibstift und einem Blatt Papier aufgezeichnet wird. Grundlage dafür sind hochempfindliche Druck- oder Ultraschallsensoren, die den Druck bzw. die Position des Stiftes erfassen. Aus den so gewonnenen Daten kann die digitale Repräsentation bestimmt werden. Hier liegt der Vorteil darin, dass beispielsweise bei der Unterzeichnung eines Vertrages die Unterschrift sowohl als Original als auch digitalisiert vorliegt. So ist in einem Streitfall eine forensische Überprüfung der Urheberschaft möglich. Natürlich ist es ebenfalls möglich, mit den erfassten Daten des Tabletts eine automatisierte Benutzerauthentifikation durchzuführen.

Grafik-Tabletts: Grafik-Tabletts stellen die zweite Gruppe der Hardware zur Erfassung von dynamischen Handschriftendaten dar. Dabei handelt es sich in den meisten Fällen um ein grafisches Tablett und einen Spezialstift. Die Verbindung zwischen dem Tablett und dem Stift kann beispielsweise durch elektromagnetische Resonanz hergestellt werden. Da der ursprüngliche Anwendungsbereich in der Unterstützung der Erstellung verschiedenartiger Computergrafik liegt, ist bei den Grafik-Tabletts eine höhere Auflösung der X-/Y-Koordinaten und auch des Druckes üblich. Dadurch lassen sich folglich auch genauere Daten für die Handschrift ableiten. Weiterhin ist bei vielen dieser Tabletts auch die Erfassung der Winkel Azimut (Stiftorientierung oder Seitenwinkel auf der Schreibebene) und Altitude (Stifthöhenwinkel) möglich.

Stifte: Die dritte Gruppe umfasst Stifte, die ohne weitere Hardware in der Lage sind, Handschriften zu erfassen und zu speichern bzw. an einen Computer weiterzugeben. Auch ist meistens neben der Erfassung der horizontalen und vertikalen Koordinaten eine Aufnahme des Druckes möglich. Auch in diesem Fall steht dem Schreiber das Original seiner Handschrift auf dem Papier zur Verfügung.

Zusammenfassend kann gesagt werden, dass heutige Sensor-Hardware, die zur biometrischen Erfassung von Handschriften genutzt werden kann, die folgenden physikalischen Größen in Abhängigkeit zur Zeit erfassen kann:

- x(t): horizontales Positionssignal des Stiftes,
- y(t): vertikales Positionssignal des Stiftes und
- p(t): Signal des Druckverlaufs, ausgeübt auf die Spitze des Stiftes.

Zudem ist es möglich, mit einigen Grafik-Tabletts folgende Winkel zeitabhängig zu erfassen:

- $\Phi(t)$: Höhenwinkel des Stiftes über dem Tablett und
- $\Theta(t)$: Seitenwinkel des Stiftes über dem Tablett.

Basierend auf diesen Messwerten können dann verschiedene statistische Größen berechnet werden. Beispiele für diese statistischen Werte sind die gesamte Schreibdauer, die Geschwindigkeit oder der Druckverlauf.

2.3 Logitech io Personal Digital Pen

Der in dieser Arbeit auf seine Performanz im Bereich der Nutzerauthentifikation und der Möglichkeit des On-Pen Matching hin untersuchte Stift ist, repräsentativ für diese Gerätekategorie, ein *Logitech io Personal Digital Pen* (io Pen, siehe [Logi05]). Dabei handelt es sich um einen Stift, der einem Kugelschreiber in der Handhabung sehr ähnlich ist. Dieser erlaubt dem Nutzer, handschriftliche Notizen und Skizzen zu erfassen und über eine USB-Dockingstation auf den Rechner zu übertragen. Dazu ist ein Spezialpapier erforderlich, welches ein für jede Seite Papier einzigartiges Raster (siehe Abbildung 2) aufweist. Die Punkte (Durchmesser ca. 0,1 mm) liegen in einem Abstand von ca. 0,3 mm beieinander. Das Raster und die notwendige Technik wurden von der schwedischen Firma Anoto ([Anot05]) entwickelt und der io Pen ist eines von mehreren Produkten verschiedener Hersteller, die auf Basis dieser Technik heute auf dem Markt erhältlich sind. Eine in die Stiftspitze des io Pen integrierte digitale Kamera erfasst die Punkte in einem 6 x 6 Raster.

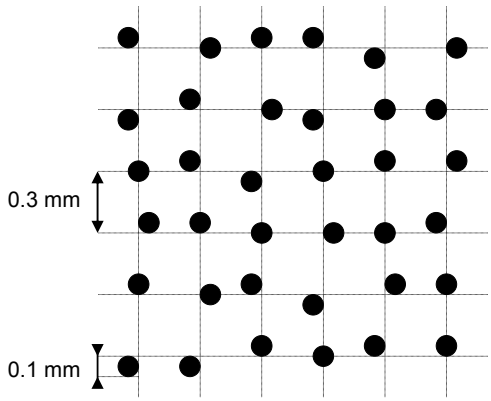


Abb. 2: Punktraster des Spezialpapiers – notwendig beim Logitech io Personal Digital Pen

Durch minimale Verschiebung der einzelnen Punkte im Raster ist eine eindeutige Erfassung der folgenden Daten möglich:

- horizontale und vertikale Stiftposition auf dem Blatt,
- Ursprung des verwendeten Papiers (ID von Seite, Schreiblock und Hersteller) und
- speziell gekennzeichnete Felder auf dem Blatt (z.B. Checkboxen zum Finalisieren der aktuellen Seite).

Weiterhin stellt der Stift den an der aktuellen Position ausgeübten Druck in 128 Stufen und das Datum und die Uhrzeit für jede erfasste Position zur Verfügung. Die so ermittelten Daten werden innerhalb des Stiftes abgelegt. Für die Übertragung an den PC wird eine USB-Dockingstation verwendet.

Die vom io Pen erfassten Daten bieten sich für die Bestimmung statistischer Daten zur biometrischen Benutzerauthentifikation mittel dynamischer Handschrift an. Im Kapitel 3 wird eine Testumgebung beschrieben, mit der eine systematische biometrische Handschriftenerfassung mit dem io Pen durchgeführt werden konnte. Die Auswertung der dabei ermittelten Daten ist dann in Kapitel 4 zu finden.

Wie bereits erwähnt, werden ähnliche Geräte auch von anderen Herstellern angeboten, zum Beispiel: Maxell Digital Pen DP-101 [Maxe05], Nokia Digital Pen SU-1B [Noki05] und Sony Ericson Chatpen [Sony05]. Die Technik der einzelnen Geräte ist vergleichbar, unterscheidet sich jedoch in Einzelheiten, wie beispielsweise der Möglichkeit der Datenübertragung via Bluetooth (Nokia Digital Pen SU-1B, Sony Ericson Chatpen), die die Verwendung mit z.B. Handys erleichtern soll.

2.4 Kombination von Biometrie und persönlichem Besitz

Im Folgenden wird auf Möglichkeiten der Kombination von biometrischen Merkmalen und persönlichem Besitz eingegangen. Dabei wird besonderer Wert auf Lösungen gelegt, die einen Vergleich der biometrischen Referenz- und Authentifikationsdaten unabhängig vom Rechner, der den Zugriff auf einen gesicherten Bereich überwacht, ermöglicht. In diesen Fällen wird das Matching auf einem persönlichen Gegenstand des Nutzers oder direkt auf der biometrischen Sensorhardware durchgeführt.

Beim On-Card Matching werden die Referenzdaten des Nutzers auf einer SmartCard gespeichert. Sollen diese nun mit aktuellen Authentifikationsdaten verglichen werden, wird die Karte mit einem Computer über ein entsprechendes Lesegerät verbunden. Dann werden die Authentifikationsdaten über diesem Computer aufgenommen und an die SmartCard weiter gegeben. Der auf der Karte integrierte Rechner vergleicht dann Referenz- und Authentifikationsdaten miteinander und gibt eine Meldung über den Erfolg oder Misserfolg zurück. Diese Vorgehensweise hat den Vorteil, dass die Referenzdaten des Nutzers nie die sichere Umgebung der SmartCard verlassen müssen. Sie befinden sich immer im Besitz des Nutzers und somit unter seiner Kontrolle. Dadurch ist ein Missbrauch oder eine Veränderung der Daten durch Dritte ausgeschlossen, sofern der Besitzer in ausreichendem Maße auf die Karte achtet. Eine Verbesserung dieses Verfahrens kann durch die Integration eines geeigneten biometrischen Sensors (z.B. Fingerprintsensor) auf der SmartCard erfolgen. Dabei können die biometrischen Authentifikationsdaten von der Karte selbst erfasst und an den internen Matcher übergeben werden. Nach dem Vergleich erhält der Rechner, der die Authentifikation angefordert hat, von der Karte die Meldung, ob diese erfolgreich war.

Die Firma Giesecke und Devrient bietet beispielsweise einen Fingerabdrucksensor in Form eines USB-Sticks an ([Gies2005]). Dieser vereint eine Chipkarte mit einem Fingerabdrucksensor und einem Bildverarbeitungs- und Verifikationsprozessor in einem handlichen Gehäuse. Vorteile liegen hier vor allem in der Aufnahme und Speicherung der Referenzdaten bzw. der Erfassung der Verifikationsdaten durch ein (persönliches) Gerät und im On-Card Matching von Referenz- und Verifikationsdaten mithilfe desselben Gerätes.

Eine ähnliche Lösung ist auch bei einigen USB-Speichersticks oder USB-Festplatten zu finden. Diese sichern die gespeicherten Daten durch einen in das Gerät integrierten Fingerprintsensor vor unautorisiertem Zugriff. Dabei befindet sich die zur Authentifikation benötigte Hard- und Software zum Teil ebenfalls in den Geräten. Die Authentifizierung des Nutzers erfolgt also unabhängig von dem Rechner, an dem die USB-Hardware angeschlossen ist. Auf diese Weise funktioniert beispielsweise der USB-Speicherstick *Cruzer Profile* der Firma SanDisk [Sand05].

Eine Kombination von Unterschrift und SmartCard wird von Henniger und Franke in [HeFr04] vorgestellt. Dabei werden die Referenzdaten ebenfalls auf der Karte gespeichert. Nach der Aufnahme der aktuellen Testdaten über ein Tablett, welches an den Authentifikati-

onsrechner angeschlossen ist, werden diese an die Karte übertragen. Die Referenz- und Testdaten werden dann durch den auf der Karte integrierten Rechner mit einander verglichen und das Ergebnis an den Authentifizierungsrechner zurückgegeben.

Dieser Arbeit liegt die Idee zugrunde, die Möglichkeit einer Handschrift basierten Nutzerauthentifikation auf dem biometrischen Sensor selbst, einem Stift (*On-Pen Matching*), zu untersuchen. Dazu wurde im ersten Schritt überprüft, ob eine Authentifikation mittels Handschrift mit den von einem solchen Stift (hier der Logitech io Personal Digital Pen) erfassten Daten überhaupt prinzipiell möglich ist. Dies ist erforderlich, da diese Hardware in erster Linie für die Erfassung und Übertragung von handschriftlichen Notizen und Skizzen auf den PC konzipiert wurde und bislang noch nicht auf Eignung für die Biometrie untersucht wurde. Im daran anschließenden Schritt wurden Untersuchungen angestellt, die den Aufwand bzw. die Komplexität des biometrischen Vergleichsprozesses betreffen. Da die Rechen- und Speicherkapazität mobiler Geräte beschränkt ist, sind auch die Größe der zu speichernden Referenz- und Testdaten und die Komplexität der Berechnungen zu berücksichtigen.

3 Testaufbau

Im Folgenden werden der Aufbau des Testsets und die Testmethodik erläutert. Dabei wird auf die Aufnahme von Enrollments, Verifikationen und Fälschungen, auf die verwendeten Semantikklassen und die Bewertungsmetrik anhand von biometrischen Fehlerraten eingegangen.

Die Semantiken beschreiben den Inhalt des Geschriebenen. Als Semantikklassen wurden in dieser Arbeit neben der eigenhändigen Unterschrift (Signatur) eine vorgegebene PIN (8710), ein selbst gewähltes Symbol und eine ebenfalls selbst gewählte Passphrase verwendet. Diese Auswahl dient dazu, die Eignung des io Pen in Kombination mit der Unterschrift bzw. geheimem Wissen zu überprüfen. Die Unterschrift wurde gewählt, da sie seit Jahrhunderten gesellschaftlich und juristisch als Authentifikationsmerkmal anerkannt ist und dadurch eine hohe Akzeptanz beim Nutzer genießt. Die anderen Semantiken wurden ausgesucht, um Abhängigkeiten zwischen geheimem und nicht geheimem Wissen untersuchen zu können.

Der Vorgehensweise von Zöbisch und Vielhauer [ZoVi03] folgend, wurden die aufgenommenen Daten in fünf verschiedenen Tests herangezogen, um die Erkennungsgenauigkeit des biometrischen Systems in verschiedenen Szenarien zu testen. Im ersten Schritt wird die *Verifikation* der Enrollmentdaten mit den Verifikationsdaten des dazu gehörenden Nutzers durchgeführt. Der nächste Schritt, der *zufällige Angriff*, ist ein Vergleich der Enrollmentdaten mit den Verifikationsdaten aller anderen im System registrierten Nutzer mit Ausnahme der Daten des Urhebers des momentan untersuchten Enrollments. Verbunden mit der Verifikation kann so die Erkennungsperformance eines Systems ermittelt werden, in dem nur registrierte Nutzer Zugang verlangen.

Die drei folgenden Angriffe sind echte Angriffe, bei denen andere Nutzer gezielte Fälschungen von bereits in der Datenbank gespeicherten Enrollments durchführen. Sie unterscheiden sich durch den Umfang des Wissens, das dem Fälscher zur Verfügung steht.

Beim *blinden Angriff* verfügt sie oder er nur über die Kenntnis der Semantik-Klasse, auf die der Angriff durchgeführt werden soll.

Die inhaltliche Information, was zu fälschen ist, sowie ein Bild des entsprechenden Schriftzuges kommen beim *Low Force Angriff* hinzu.

Kann der Fälscher auf alle verfügbaren Informationen zurückgreifen, also zusätzlich über die dynamischen Daten des Schreibvorgangs, sprechen wir von einem *Brute Force Angriff*.

Über die genannten drei Fälschungsstufen werden potentielle Angriffe auf das System mit unterschiedlicher Vorkenntnis des anzugreifenden Schriftzuges simuliert. An den bisherigen Tests haben sich neun Nutzer beteiligt. Bei der Aufnahme der Handschriften konnte festgestellt werden, dass es Vorbehalte der Versuchspersonen gegenüber der Speicherung ihrer Handschrift, vor allem der Unterschrift, in einer biometrischen Datenbank gibt. Hier ist eine Steigerung der Akzeptanz der Nutzer denkbar, wenn die Referenzdaten auf der eigenen Hardware (io Pen) gespeichert werden können. Würde das Matching zusätzlich auf dem Pen durchgeführt und die Entscheidung über die Authentizität des Nutzers über eine entsprechende Schnittstelle an den Rechner weitergegeben, der eine Authentifizierung verlangt, ist mit einer weiteren Steigerung der Akzeptanz zu rechnen. Durch die Tatsache, dass in diesem Fall weder die Referenz- noch die aktuellen Authentifizierungsdaten den Stift verlassen, könnte die Bereitschaft der Anwender, ein solches System zu nutzen, steigen. In Tabelle 1 sind die Mengen der jeweils durchgeführten Einzeltests pro Semantikklasse zusammengefasst.

Tab. 1: Einzeltests pro Semantikklasse

Aktion	Einzeltests/Semantiklasse
Verifikation	220
zufälliger Angriff	1760
blinder Angriff	3200
Low Force Angriff	1620
Brute Force Angriff	1380

Als Verifikationsalgorithmus wird der erstmalig von Vielhauer et. all in [ViSM02] vorgestellte und in [ViSt04] und [Viel05] weiterentwickelte Biometric Hash Algorithmus verwendet. Dieser wurde ursprünglich zur Berechnung biometrischer Haschwerte konzipiert, es hat sich aber gezeigt, dass der Algorithmus auch erfolgreich zur Merkmalsextraktion und zum Matching eingesetzt werden kann ([ViSS04], [ViSc05]). Dabei wird jeweils ein n-dimensionaler Vektor, bestehend aus n statistischen Merkmalen ($n=69$), für die Referenzdaten und die aktuellen Authentifikationsdaten berechnet und der Abstand zwischen beiden Vektoren über eine Distanzfunktion bestimmt Als Distanzmaß wird hier der Hamming Abstand verwendet. Liegt das Ergebnis dieser Funktion innerhalb eines festgelegten Toleranzbereiches, so gilt der Nutzer als verifiziert.

4 Erkennungsgenauigkeit des Logitech io Pen

Nach der Durchführung der in Kapitel 3 beschriebenen Tests können an dieser Stelle die Ergebnisse vorgestellt werden. Die Resultate des io Pen werden dann mit Ergebnissen von Tests aus früheren Arbeiten der Autoren [Viel05], welche auf einem Grafik-Tablett und einem Unterschriftentablett basieren, bezüglich ihrer Erkennungsgenauigkeit verglichen.

In Tabelle 2 werden die Equal Error Rates für den io Pen in Abhängigkeit von der Semantikklasse und dem Angriffstyp dargestellt. Die Equal Error Rate für die Verifikation liegt mit dem verwendeten Algorithmus zwischen 3,5% und 7,7% für die Passphrase, die Unterschrift und das Symbol. Dabei wird der günstigste Fall angenommen, dass das System keinen Angriffen ausgesetzt ist und nur zwischen den registrierten Nutzern unterscheiden muss. Werden

zusätzlich noch die unterschiedlichen Angriffe betrachtet, kann mit zunehmendem Wissen des Angreifers erwartungsgemäß ein Anstieg der EER beobachtet werden. Eine Ausnahme bildet hier die PIN (8710). Gründe hierfür liegen vermutlich in der einfachen Struktur von Zahlen, in der begrenzten Menge der verfügbaren Zeichen (0-9) und auch in der Tatsache, dass alle Testpersonen die gleiche Zahl geschrieben haben.

Tab. 2: EER in Abhängigkeit von der Semantikklasse und dem Angriffstyp für den *io Pen*

Semantikklasse	zufälliger Angriff	blinder Angriff	Low Force Angriff	Brute Force Angriff
8710	0,213	0,123	0,182	0,198
Passphrase	0,035	0,030	0,153	0,162
Signatur	0,077	0,047	0,173	0,199
Symbol	0,056	0,066	0,217	0,241

Tab. 3: EER in Abhängigkeit von der Semantikklasse und dem Angriffstyp für das *Cintiq15*

Semantikklasse	zufälliger Angriff	blinder Angriff	Low Force Angriff	Brute Force Angriff
8710	0,296	–	0,542	0,524
Passphrase	0,076	0,155	0,514	0,446
Signatur	0,092	0,110	0,279	0,301
Symbol	0,064	0,227	0,354	0,239

Tab. 4: EER in Abhängigkeit von der Semantikklasse und dem Angriffstyp für das *StepOver*

Semantikklasse	zufälliger Angriff	blinder Angriff	Low Force Angriff	Brute Force Angriff
8710	0,295	0,567	0,410	0,413
Passphrase	0,273	–	–	–
Signatur	0,084	0,360	–	0,351
Symbol	0,184	–	–	–

In Tabelle 3 und Tabelle 4 sind die EERs der untersuchten Semantikklassen und Angriffstypen für das Grafik-Tablett WACOM Cintiq15 bzw. eine Auswahl von StepOver Unterschriftentabletts dargestellt. Da für einige Semantiken der beiden Hardwaregruppen nicht ausreichend Daten für einen Test vorhanden waren, sind in den entsprechenden Tabellenzellen keine Werte angegeben. Im Vergleich mit den EERs des io Pen in Tabelle 2 sind alle Ergebnisse des io Pen bis auf einen leicht bis deutlich besser als bei den Tabletts. Dies kann einerseits an der natürlichen Handhabung des Stiftes in Verbindung mit dem Papier liegen. Auf der anderen Seite ist aber auch anzumerken, dass die teilnehmenden Testpersonen in den drei Hardware-Kategorien nur zu einem geringen Teil identisch waren. Dennoch können wir aufgrund der durchaus vergleichbaren und zum großen Teil besseren EERs davon ausgehen, dass eine Nutzung des io Pen zur Benutzerauthentifikation prinzipiell möglich ist.

5 On-Pen Matching

Eine zweite Kernfrage dieser Arbeit ist, ob ein On-Pen Matching generell möglich ist. Bisher wurde von uns bereits der Nachweis erbracht, dass es möglich ist, die von einem Logitech io Personal Digital Pen erfassten Daten zur biometrischen Benutzerauthentifikation heranzuziehen. Ziel dieses Kapitels ist, die Möglichkeit des On-Pen Matching bezüglich der erforderlichen Software und Hardware zu untersuchen. Im Folgenden soll nun die Komplexität der für

das On-Pen Matching notwendigen Berechnungen diskutiert werden. Eine solche theoretische Abschätzung ist wichtig, da ein Stift nur über begrenzten physischen Platz verfügt und die Rechenleistung bzw. Speicherkapazität entsprechend kleiner Hardware nicht beliebig groß ist.

Leider war es den Autoren nicht möglich, die genauen technischen Daten des Logitech io Personal Digital Pen in Erfahrung zu bringen. Aus diesem Grund soll die Abschätzung der technischen Machbarkeit des On-Pen Matching mittels Biometric Hash basierend auf heute verfügbarer, bekannter Hardware mit genügend kleinen Abmessungen durchgeführt werden. Daher wurde zum Komplexitätsvergleich das RSA-Verfahren zur Erzeugung von kryptografischen Schlüsseln herangezogen, welches häufig auf SmartCards für kryptografische und steganographische Anwendungen genutzt wird. Die SmartCards wurden an dieser Stelle als Vergleichsobjekt gewählt, da sie bereits für Zwecke der Authentifizierung eingesetzt werden. In unseren Arbeiten ist die Zyklomatische Komplexität nach McCabe [Mcca76] Grundlage zur Bestimmung der Komplexität, wobei zu erwähnen ist, dass im Bereich der Softwareanalyse eine Vielzahl alternativer Verfahren eingesetzt wird, aber speziell für dieses Verfahren heute Tools zur Verfügung stehen, welche automatisch die Komplexität eines vorgegebenen Quellcodes bestimmen können.

Dieses Komplexitätsmaß wird von uns auf die beiden zu untersuchenden Algorithmen angewendet, und die ermittelten Werte werden miteinander verglichen. Dabei wird davon ausgegangen, dass eine Umsetzung des Biometric Hash Algorithmus in eine Hardwareumgebung, die bzgl. der Rechenleistung und der Speicherkapazität begrenzt ist, möglich ist, wenn der ermittelte Komplexitätswert (wesentlich) geringer ist, als der bei dem in solcher Umgebung bewährten RSA-Schlüsselgenerierungsalgorithmus.

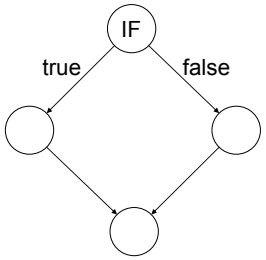
Mithilfe der zyklomatischen Komplexität nach McCabe kann die strukturelle Komplexität von Algorithmen bestimmt werden. Da das Verfahren aus der Graphentheorie stammt, basiert es auf der Interpretation der beteiligten Funktionen als Kontrollflussgraph. Der Komplexitätswert wird anhand des Graphen mit der folgenden Formel bestimmt:

$$M(G) = e - n + 2p.$$

Dabei gibt e die Anzahl der Kanten und n die Anzahl der Knoten im Graphen an. Mit p wird die Anzahl der Endpunkte der Funktion angegeben. Ist $p=1$ kann die Komplexität auch wie folgt berechnet werden:

$$M(G) = 1 + b.$$

In dieser Variante wird die Anzahl b aller Bedingungen und Schleifen (z.B. *IF*, *WHILE, FOR*) mit *1* addiert. Die Abbildung 3 zeigt die Vorgehensweise anhand einer einfachen IF-Schleife, beide Berechnungsmöglichkeiten sind ebenfalls angegeben.



$$M_1(G) = e - n + 2p \qquad M_2(G) = 1 + b$$
$$M_1(G) = 4 - 4 + 2 \qquad M_2(G) = 1 + 1$$
$$M_1(G) = 2 \qquad M_2(G) = 2$$

Abb. 3: Beispiel der Berechnung der zyklomatischen Komplexität nach McCabe

Auf die oben beschriebene Weise wurde die zyklomatische Komplexität für den Biometric Hash Algorithmus und das RSA-Schlüsselgenerierungsverfahren bestimmt. Für den Quellcode des Biometric Hash Algorithmus wurde ein Komplexitätswert von ca. 500 ermittelt, und für die RSA-Schlüsselerzeugung wurde ein Wert von ca. 4.500 bestimmt. Damit ist die mit diesem Verfahren bestimmte Komplexität für die Schlüsselgenerierung etwa neun Mal so groß wie die Komplexität für das von uns verwendete biometrische Authentifikationsverfahren. Von diesem Standpunkt aus scheint dessen Berechnung auf einer SmartCard theoretisch möglich zu sein.

Im Datenblatt der Smartcard ST19XT34 [Stmi05] wird die Laufzeit für die Erzeugung eines RSA-Schlüssels (1024 Bits) mit 3,2 Sekunden angeben. Wird die oben bestimmte Komplexität zur Grundlage genommen, die Laufzeit des Biometric Hash Algorithmus zu schätzen, kann eine ungefähre Ausführungsdauer von ca. 0,4 Sekunden angenommen werden. Nach unserer ersten Abschätzung kann in dieser Zeit eine einzelne Authentifizierung durch den Biometric Hash Algorithmus komplett durchgeführt werden.

Der physikalische Speicherplatz, der für die Speicherung der handschriftlichen Referenzdaten benötigt wird, beläuft sich auf ca. 500 Byte. Diese Größe ist unabhängig von der geschriebenen Menge, da sie sich aus den vom Algorithmus extrahierten 69 statistischen Merkmalen ableitet. Da laut Herstellerangaben auf dem Logitech io Personal Pen Speicherkapazität für ca. 40 A4 Seiten vorhanden ist, ist davon auszugehen, dass genügend Platz für die Referenzdaten vorhanden ist. Bei dieser Dimensionierung scheint auch die Unterbringung sowohl von alternativen Semantiken, z.B. für verschiedene User-Accounts oder unterschiedliche Berechtigungsstufen einer einzelnen Person, als auch von Referenzdaten verschiedener Personen durchaus machbar zu sein. Allerdings ist an dieser Stelle anzumerken, dass für eine Portierung des Biometric Hash Algorithmus von einer PC- auf eine Pen-Umgebung auch der verfügbare Arbeitsspeicher der mobilen Hardware berücksichtigt werden muss. Das bedeutet, dass große Datenstrukturen und rekursiv arbeitende Funktionen an die durch Speicher und Prozessor bedingten Einschränkungen angepasst werden müssen.

6 Zusammenfassung und Ausblick

Ziel unserer Arbeiten ist es, zu überprüfen ob eine biometrische Benutzerauthentifikation mithilfe des Logitech io Personal Digital Pen möglich ist und eine erste Abschätzung der Machbarkeit eines biometrischen On-Pen Matchings zu geben. Die Verifikation von Nutzern ist mit dem Logitech io Personal Digital Pen generell möglich. In allen Fällen bis auf einen liefert er sogar bessere Ergebnisse, als die von den Autoren bisher untersuchte Hardware. Dazu ist aber anzumerken, dass die Anzahl der User und damit auch der verwendeten Handschriftensamples viel geringer ausfiel, als in unseren Vorarbeiten. Die ermutigenden Ergebnisse bestätigen jedoch dennoch die Möglichkeit der Verwendung des io Pens zur Nutzerauthentifikation.

Leider war es nicht möglich, die genauen Hardwarekomponenten des Logitech io Personal Digital Pen zu erfahren. Daher wurde eine erste Abschätzung der Komplexität des Biometric Hash Algorithmus durchgeführt und mit der auf gleiche Weise bestimmten Komplexität eines auf biometrischen oder kryptografischen SmartCards oft eingesetzten Schlüsselgenerierungsalgorithmus (RSA) verglichen. Dabei konnte festgestellt werden, dass die Komplexität des Biometric Hash Verfahrens nur ein neuntel der Komplexität der Berechnung einer RSA-Schlüsselgenerierung beträgt. Damit kann die Umsetzung des Biometric Hash Algorithmus als möglich betrachtet werden.

Nach diesen viel versprechenden ersten Ergebnissen werden wir uns in unserer zukünftigen Arbeit im Bereich des On-Pen Matching mit der Untersuchung von Stift basierten Lösungen anderer Hersteller befassen. Dazu zählt natürlich auch die Erfassung weiterer Daten, um eine umfassendere Sammlung an Handschriftenproben für jeden zu untersuchenden Pen zu erhalten. Diese sollen in ihrer Zusammenstellung sehr ähnlich sein, um eine Vergleichbarkeit der Testergebnisse zu gewährleisten. Weiterhin soll die Implementierung unseres Algorithmus in einer entsprechenden Umgebung evaluiert werden, z.B. über einen Mikrocontroller- oder SmartCard-Simulator. Dadurch können die Abschätzungen der Hardware-Anforderungen überprüft bzw. ergänzt werden.

Ein weiterer wichtiger Punkt ist die Sicherheit der Referenzdaten. Da es sich bei dem Pen um persönlichen Besitz handelt, ist es natürlich prinzipiell möglich, dass dieser weitergegeben oder gestohlen werden kann. In diesem Fall sollten die Referenzdaten vor einem Auslesen bzw. einer Veränderung geschützt sein. Aus diesem Grund sind Vorkehrungen notwendig, die Daten auf dem Stift selbst aber auch die Übertragung des Verifikationsergebnisses zu sichern.

Weiteres Potenzial für künftige Anwendungen besteht in der Möglichkeit, bei der Verwendung von io Pen und Anoto-Papier bestimmte Papier spezifische Daten zu erfassen und zu speichern, da Papier abhängige Metadaten (z.B. Blatt-ID) im Anoto-Raster ([Anot05]) kodiert sind. So kann beispielsweise die Sicherheit erhöht werden, indem Referenzdaten nur auf speziellen Blättern aufgenommen werden, über die nur der Administrator des zu sichernden Bereiches verfügt. Dadurch kann u.a. sichergestellt werden, dass Enrollments und Verifikationen nur als vom System verwertbar betrachtet werden, wenn diese auf Blättern innerhalb eines vorher festgelegten Papier-ID-Bereiches angefertigt wurden. Diese Vorgehensweise erschwert die nachträgliche Veränderung oder die erneute Erzeugung und den Austausch der Referenzdaten bzw. eine Manipulation der Verifikationsdaten und erlaubt damit auch die Umsetzung von spezifischen Sicherheitspolitiken.

Danksagungen

Diese Veröffentlichung entstand unter Mithilfe der Europäischen Union (Informationen zum Projekt CultureTech unter http://amsl-smb.cs.uni-magdeburg.de/culturetech), sowie in Kooperation mit dem EU Network of Excellence, BioSecure (IST-2002-507634 BIOSECURE). Der Inhalt dieser Veröffentlichung steht in alleiniger Verantwortung der Autoren und widerspiegelt somit in keiner Weise die Meinung der Europäischen Union. Weiter danken wir Herrn Maik Schott für seine Arbeit bei der Erfassung der Handschriftendaten und der Implementierung einer Schnittstelle zwischen dem Logitech io Personal Digital Pen und unserer Software zur Erfassung und Evaluierung von dynamischen Handschriften.

Literatur

[Anot05] Anoto: http://www.anoto.com

[Gies05] Giesecke & Devrient GmbH: StarSign Bio Token. http://www.gi-de.com/pls/portal/maia.display_custom_items.DOWNLOAD_FILE_BLOB?p_ID=97296

[HeFr04] O. Henniger, K. Franke: Biometric User Authentication on Smart Cards by Means of Handwritten Signatures., 1st International Conference Biometric Authentication, ICBA 2004, LNCS 3072, Springer (2004), 547-554.

[Lass02] G. Laßmann: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, Kriterienkatalog V. 2.0, TeleTrusT, www.teletrust.de/down/kritkat_2-0.zip

[Logi05] Logitech Produkte > Digitales Schreiben mit Logitech® io™ > Das digitale Schreibsystem. http://www.logitech.com/index.cfm/products/features/digitalwritingtopics/CH/DE,CRID=2095

[Maxe05] maxell: Product Lineup: Products for companies: Digital Pens. www.maxell.co.jp/e/products/industrial/digitalpen/index.html

[Mcca76] T.J. McCabe: A complexity measurement, IEEE Transactions on Software Engineering, (2) (1976) 308-320.

[Noki05] Nokia Deutschland – Mobiltelefone – Zubehör - Digitalstift SU-1B. www.nokia.de/de/zubehoer/zubehoerteile/digitalstift_su1b/startseite/42070.html

[Sand05] SanDisk | Retail | Cruzer Profile. www.sandisk.com/retail/cruzer-profile. asp

[Sony05] Mobiltelefon – Sony Ericsson Chatpen™. www.sonyericsson.com/spg.jsp?cc=de&lc=de&ver=4000&template=pp1_1_1&zone=pp&lm=pp1&pid=9753

[Stmi05] STMicroelectronics | Smartcard Solutions | ST19 Multi-Application Smartcard ICs. http://www.st.com/stonline/products/families/smartcard/sc_sol_secure_ics_st19.htm, Download: 06.12.2005

[ViSc05] C. Vielhauer, T. Scheidat: Fusion von biometrischen Verfahren zur Benutzerauthentifikation. P. Horster (Hrsg.): D·A·CH Security 2005, syssec (2005) 82-97.

[ViSM02] C. Vielhauer, R. Steinmetz, A. Mayerhöfer: Biometric Hash based on Statistical Features of Online Signature. Proceedings International Conference on Pattern Recognition (ICPR), Vol 1 (2002) 123-126.

[ViSS04] C. Vielhauer, R. Steinmetz, T. Scheidat: Forensik und Biometrie zur Benutzererkennung. P. Horster (Hrsg.), D·A·CH Security 2004, syssec (2005) 192-205.

[ViSt04] C. Vielhauer, R. Steinmetz, Handwriting: Feature Correlation Analysis for Biometric Hashes. H. Bourlard, I. Pitas, K. Lam, Y. Wang (Eds.): EURASIP Journal on Applied Signal Processing, Special Issue on Biometric Signal Processing, Hindawi Publishing Corporation (2004) 542-558.

[Viel05] C. Vielhauer: Biometric User Authentication For IT Security: From Fundamentals to Handwriting, Springer Science+Business Media Inc. (2005).

[Waym99] J. L. Wayman, Technical Testing and Evaluation of Biometric Identification Devices. A. Jain, et al. (eds.): Biometrics – Personal Identification in a Networked Society, Kluwer Academic Press, 1999.

[ZoVi03] F. Zöbisch; C. Vielhauer: A Test Tool to support Brut-Force Online and Offline Signature Forgery Tests on Mobile Devices. Proceedings IEEE International Conference on Multimedia and Expo 2003 (ICME), Vol. 3 (2003) 225-228.