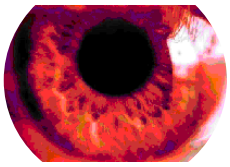
Seminar “Verfahren der BioSignaturen”
Sommersemester 2003

Iris- und Retinaerkennung



Aamer Qadeer Mahmood
Zeitreisender@aamer.de

4. Semester BioInformatik

Johann Wolfgang Goethe-Universität
Frankfurt am Main

12. Juni 2003

Diese Ausarbeitung demonstriert Verfahren der biosignaturgestützten Authifizierung mit speziellem Augenmerk auf die Klassifizierung anhand der Iris- und Retinaerkennung. Nach einer allgemeinen Einführung in die Welt der Biometrie werden die Verfahren zur Erkennung am Auge näher betrachtet. Vertieft werden hierbei die mathematischen und biologischen Grundlagen. Auf dem Verständnis dieser Elemente aufbauend werden dann sicherheitsrelevante Überlegungen und moralische Auswirkungen sowie die Vor und Nachteile der beiden Technologien untersucht. Zum Abschluß folgt die Präsentation einiger erfolgreich implementierten Verfahren und Systeme die einen Einblick in die praktische Realität geben.

Inhalt :

1. Einführung

In unserem globalen Zeitalter, in dem die Welt täglich weiter zusammenwächst, wird die Identifizierung von berechtigten Personen stetig wichtiger. Immer schnellere und effektivere Verfahren werden in einer computergestützten multimedialen Gesellschaft erforderlich. Einfache Objekte wie ein Türschlüssel reichen längst nicht mehr, zu groß sind die Fehlerquellen und zu gering die sich damit ergebende Sicherheit. So ist es heute unabdingbar die Identität einer Person ohne menschliche Zuhilfenahme eindeutig festzustellen, sei es für das bloße öffnen einer Tür oder für vertrauliche Bankgeschäfte.

Die folgende Betrachtung diskutiert konventionelle, also klassische, Methoden und stellt Ihnen die Verfahren der Iris- und Retinaerkennung, die biologische Merkmalesinformationen – demnach die Biometrie eines Menschen – zur eindeutigen Identfizierung nutzen, gegenüber.

1. konventionelle Authifizierungsmethoden in unserem Alltag

a) Objektgestützt :

Hier erfolgt eine bestätigte Erlaubnis, die Authifizierung, durch den Besitz eines Objektes. Nur wer autorisiert ist, demnach eine Authifizierung erhalten hat, erhält beispielsweise eine Karte aus Pappe oder einen Schlüssel. Die Einfachheit des Objektes und die Verantwortung seitens der Person birgt Fehlerquellen in sich :

- Eine solches Zugangsobjekt ist leicht zu kopieren. (z.B: Kopiergerät)
- Bei Verlust ist die Gefahr des Mißbrauches zu hoch und zieht meist viel Aufwand (z.B.: das Erkennen einer nicht mehr erlaubten Zugangskarte) nach sich.

b) Gedächtnisgestützt :

Hierbei wird die Zugangsbestätigung nach der erfolgreicher Eingabe eines Kennwortes erteilt. Durch eine computergestützte Überprüfung wird eine bessere Identifikation ermöglicht. Dennoch ergeben sich auch hier Probleme :

- Das System stützt sich auf die Wiedergabe von alphanumerischen Begriffen, die im Gedächntis der autorisierten Person verweilen müssen. Bei steigender Anzahl dieser 'Passwörter' nimmt die Fehlerquote aufgrund der meist hohen Ausfallsrate des menschlichen Gehirns durch Vergesslichkeit zu.
- Das Passwort kann mithilfe geeigneter Programme leicht abgehört oder durch Probieralgorithmen (automatische Anwendungen die verschiedene Kennwörter ausprobieren) entschlüsselt werden.

2. Verfahren der Biosignaturen, eine Alternative ?

a) Biometrische Verfahren

Die Qualität eines Authifizierungsverfahrens wird an der effizienten Zeitnutzung und der Intraklassenvariabilität, sprich einer guten Unterscheidungsfähigkeit der Identifizierungssmerkmale untereinander, gemessen. Eine andere Möglichkeit gegenüber den konventionellen (die Standartverfahren) bieten die Verfahren der Biosignaturen. Diese nutzen kaum veränderliche Merkmale des menschlichen Körpers (die Biometrie) zur Identifizierung, auch ihre Intraklassenvariablität ist sehr hoch da sich jeder Mensch durch individuelle Ausprägungen unterscheidet[1]. Im folgenden eine kurze Beschreibung zweier dieser Verfahren :

- Iriserkennung:
  Dieses Vefahren nutzt einen von außen sichtbaren aber geschützten Bereich[1] des menschlichen Auges. Nach Auffinden der Iris wird ein repräsentativer IrisCode erstellt, der dann mit einem gespeicherten verglichen wird, wodurch die Identifikation geschieht. Ein Vorteil dabei ist das diese

berührungslose Methode auf Entfernungen schnell und eindeutig, auch unbemerkt und aus einem nicht gegenwärtigen Bild angewendet werden kann[1].

- Retinaerkennung:
  Diese Methode beruht auf einem spezifischem Merkmal bei der Blutzufuhr des Auges. Es benötigt aber eine recht aufwendige Erfassung des Augeninneren mithilfe von IR-Licht. Die geringe Fern-erkennungsfähigkeit und der Umstand dass, das Auge gescannt, sprich durchleuchtet werden muss machen dieses Vefahren weniger Nutzerfreundlich, aber es besticht dennoch mit sehr guten Erkennungsergebnissen.

b) Eine Alternative ?

Der Vorteil der beiden biosignatorischen Systeme liegt auf der Hand, sie sind vergleichbar mit einem optimalen konventionellen Vefahren, in dem der Schlüssel immer und eindeutig mit sich geführt wird. Auch die benötigte Rechenzeit ist bei den heutigen Rechnerfähigkeiten ausgewogen[1,2]. In den folgenden Teilen dieser Ausarbeitung wird nach der aneignung der Grundlagen genauer auf die Methodik und die Leistungen dieser biometrischen Verfahren Einsicht genommen.

2. Grundlagen

Das Auge ist wohl das bemerkenswerteste Sinnesorgan des Menschens. Da es eine zentrale Rolle in unserem Alltag spielt erfordert dieses hochkomplexe Organ eine gut sichtbare aber auch geschützte Platzierung im Gesicht[1]. Dadurch ist das Auge gut geeignet für eine biometriespezifische Identifikation. Die Verfahren der Iris und Retinaerkennung stützen sich hierbei auf grundlegende Merkmale des Auges die im nächsten Abschnitt erklärt werden. Diese müssen auch in geeigneter Form digital erfasst werden um ihre Nutzung als biologische Signatur zu ermöglichen. Mit den dafür benötigten mathematischen Überlegungen befasst sich dann der zweite Teil.

1. Das Auge, ein sonderbares Organ

a) Iris

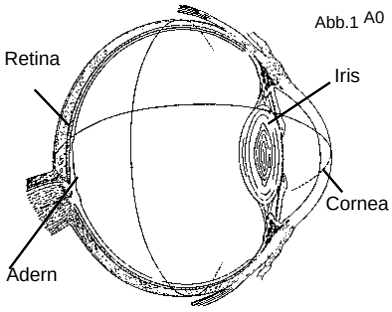


Abb.1 A0

Die Iris (Regenbogenhaut), ein ringförmiger Muskel, sitzt in der vorderen Augenkammer hinter einer transparenten Hornhaut, der Cornea (Abb 1). Dadurch geschützt von äußeren Einflüssen stellt sie mit ihrer gut strukturierten Oberfläche ein effektiv verwertbares biometrisches Merkmal dar. Die Regenbogenhaut ist bis zum 8. Schwangerschaftsmonat weitgehend ausgebildet[1] und enthält ein komplexes Muster. Die Farbe wird dabei durch die Anlagerung des Melaninpigmentes (biologischer Farbstoff) bestimmt. Ist es nicht vorhanden so ist die Irisfarbe blau, weil das Licht frei bis zum Pigmentepithel (Pigmenthaut) durchdringen kann und von dort teils gestreut, teils reflektiert wird. Die im sichtbaren Lichtwellenbereich reflektierten Strukturen der Regenbogenhaut sind meist Muster der oberflächligen Zonen des Auges. Nimmt man stattdessen Wellenlängen nahe des Infrarotbereiches (NIR) so erscheinen Muster die eher vom Augengrundgewebe stammen, sogar auch wenn die Iris dunkelpigmentiert ist[1]. Dieses Muster ist für jeden Menschen mit einer Wahrscheinlichkeit von nahezu 100% individuell da schon die beiden Augen eines Menschens dadurch das unterschiedliche Einflüsse auf sie wirken, verschiedene Irismuster besitzen[1].

b) Retina

Die Retina, auch als Netzhaut bezeichnet, ist der Teil des Auges in dem die eigentliche Aufgabe des Organes stattfindet. Sie wird bei Säugetieren auch als inverse Retina bezeichnet, da sie, wie in Abb 1 dargestellt hinter den Adern die für ihre Durchblutung sorgen, liegt. Dieser Umstand ermöglicht es sie als biometrisches Objekt zu nutzen. Das Licht muss erst die Aderschicht passieren und macht sie somit sichtbar. Das individuelle und eindeutige Muster[2] (Die Wahrscheinlichkeit zweier Übereinstimmungen

ist nicht gegeben da sich die beiden Augen einer einzigen Person sogar unterscheiden.) der Netzhautadern ermöglicht eine eindeutige Identifizierung. Noch dazu liegt dieser Bereich gut geschützt im Augapfel und ist von außen durch die Pupille hindurch einsehbar.

2. Mathematisch algorithmisches Erkennen

Die Erkennung an der Iris erfordert eine Vielzahl von mathematischen Vorüberlegungen. Einen wichtigen Teil bilden die Waveletfunktionen. Sie dienen dem Erstellen des eindeutigen Iriscodes. Einer der Pioniere dieser Verfahren, Phd Daughman, war in der Lage mit einem von ihm entwickelten Erkennungsalgorithmus (eine für einen Computer verarbeitbare abarbeitbare Anweisung) die eine Gaborfunktion, deren Herkunft wir im Folgendem auch behandeln, enthält diesen Iriscode in nur 2048 Bit darzustellen.

a) Fourier

Die Fourier-Theorie dient als Grundidee auf der die der Wavelets aufbaut. Sie wurde 1807 von Jean Baptise Fourier entwickelt und besagt dass, jede periodische (sich wiederholende) Funktion durch eine Summe von Sinus und Cosinusfunktionen beschrieben werden kann[3]. Die daraus hergeleitete Formel erlaubt die Zerlegung eines Signals in seine Frequenzanteile. Darauf stützen sich unter anderem Bildkompressionsverfahren beispielweise das JPEG-Verfahren (Joint Photographic Experts Group)[3].

b) Wavelet

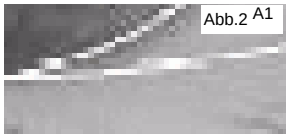


Abb.2 A1

Das Wavelettheorie ist die Weiterentwickelung der Fourierüberlegung, die zwei Nachteile hatte. Erstens, harte Übergänge wie Ecken sind sehr schwer darzustellen. Wie bei dem JPEG Format bekannt, enstehen hier Unschärfen (Abb 2) und der zweite mathematischer Natur seiende Nachteil; es wird mit einer periodischen sich unendlich fortsetzenden Sinuswelle gerechnet. Das aber ist nicht nötig da die meisten zu komprimierenden (verpackenden) Bereiche aus einem abgeschlossenen Intervall (Bereich) bestehen. Die Nachteile werden durch die von Jean Morlet und Alex Gossman entwickelten Wavelet-Theorie ausgebessert[3]. Dabei wird eine Hauptfunktion, auch Mutterwavelet genannt, gewählt die eine Funktionsfamilie aus mehreren Funktionen gleicher Art enthält (s.Formel 1). Ψ ist eine spezifische Funktion der Funktionsfamilie die sich aus dem Mutterwavelet (Ψ) ergeben. Dabei sind, s die Skalierungs- und d die Verschiebungs-Parameter. Ein Signal wird bei anwenden des Verfahrens solange geteilt bis sie durch die Funktionen der Familie dargestellt werden können. Sie sind somit durch ein Mutterwavelet mit geeigneten Parametern (Eingaben) abbildbar.

Formel 1

$$\Psi_{s,d}(t) = \frac{1}{\sqrt{s}}\Psi\left(\frac{t-d}{s}\right)$$

Für kontinuierliche Funktionen ist eine Krücke notwendig, da sonst das Aufteilen in die Funktionen der Familie unendlich verlaufen würde[3]. Es wird deshalb nur ein bestimter Integralbereich gewählt (s.Formel 2). Eine Waveletfunktion kann nun dazu dienen exakt alle Details wiederzugeben, dann ist sie Aufgrund ihrer Größe nicht mehr wirklich komprimierend. Sie kann aber auch bei hoher Verpackung ein Signal in ihrer Hauptinformation wiedergeben was wiederum eine sehr schlechte Detailwiedergabe zur Folge hat.

Formel 2

$$\Theta_{s,d}(t) = \int_{-\infty}^{\infty} x(t)\Psi_{s,d}(t)dt$$

b) Gabor Funktion

Die um 1946 von Gabor entwickelte Gaborfunktion ist eine bestimmte Waveletfunktionsart die Detail und Kompressionsgrad im Gleichtgewicht hält[1]. Sie wird zu der Codierung des Irismusters durch die Algorithmen von Daughman benötigt. Eine Darstellung der Funktion ist in Formel 3 (Seite 7) gezeigt und gilt für die Komprimierung einer zweidimensionalen Eingabe. Der Parameter $\bar{\sigma}$ gibt die Form einer Glockenkurve an die, die Funktion beschränkt. Die Frequenz wird durch ω gesetzt, die Parameter x und y werden durch folgende Terme mit Einbeziehung der Skalierungsvariablen s_x, s_y (s.Waveletskalierung) bestimmt : $x' = s_x((x-x_0)cos\theta - (y-y_0)sin\theta)$ $y' = s_y((x-x_0)sin\theta + (y-y_0)cos\theta)$

3. Die Iris Erkennung

1. Erfassen der Iris

a) Auffinden & Codieren

Zum Finden der Iris wird zuallererst eine geeignete Apparatur benötigt die das Auge als Bildinformation wiedergibt. Bewährt haben sich hier CCD Kameras bei NIR-Beleuchtung, die eine Auflösung von 100 – 140 Pixel im Irisbereich liefern[1]. Auf die verschiedenen Methoden zum Finden des Auges wird hier nicht weiter eingegangen. Wir begnügen uns mit einem schon gefundenen Augenbild in dem nur noch die Iris erkannt werden muss. Hier tritt das Daughmanverfahren wie folgend in Aktion. Da die Iris ein unsymetrisches Objekt ist und einen nicht exakten Radius aufweist und zudem auch ihre Form ändert, muss die Bereichsbestimmung durch drei Parametern erfolgen, dabei wird natürlich das auch dynamische Pupillensegment ausgenommen. Ein sehr effektiver Algorithmus[1] ist in Formel 4 dargestellt. Hier werden die drei benötigten Begrenzungsparameter in einem Polarkoordinatensystem zurückgegeben . I(x,y) ist die Bildquelle. Mit einer Funktion G, zur Glättung (hier Gauß-Funktion mit Skalierung σ) und einer Faltung * wird, entlang des Kreisbogens ds von dem BildMittelpunkt aus der Bereich mit zunehmedem Radius, der Irisbereich bestimmt. Die damit gefundene Iris ist in Abb 4 zu sehen. Nun werden die Merkmalsmuster erkannt. Dazu lässt man Sinus und Cosinus Funktionen , ergebend aus der in der Formel 3 gezeigten Gaborfunktion, mit verschiedenen Frequenzen über das Bild laufen. Wenn ein Hell-Dunkel-Übergang auf die Nullstelle der Funktion passt wird ein Bit gesetzt. Dieser Vorgang wird nach dem Verfahren von Daughman[1] mithilfe des in Formel 5 gezeigten Terms umgesetzt. Daraus ergibt sich ein dreidimensionaler Phasenquadrant-Demodulationscode. Dabei ist $h_{\{Re,Im\}}$ ein spezielles Bit das den Quadranten in einem Polarkoordinatensystem der komplexen Zahlen angibt in das dann das aktuelle Hell- Dunkel-Muster (Phasen) projeziert wird. Der ganze Vorgang wird mehrmals mit verschiedener Orientierung und Frequenzen zu unterschiedlichen Wavelets wiederholt. Um einen eindeutigen 2048 Bit Code (Abb 4 o.l.) zu erhalten wird jeder Quadrant des Demodulationscodes in zwei Bits interpretiert.

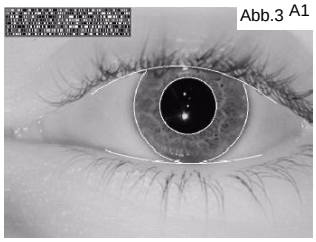


Abb.3 A1

Formel 3

$$g_{\sigma,\omega}(x,y) = e^{-\frac{x^2}{\sigma_x{}^2}} \cdot e^{-\frac{y^2}{\sigma_y{}^2}} \cdot \cos 2\pi\omega x$$

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|$$

Formel 5

$$h_{\{Re,Im\}} = \operatorname{sgn}_{\{Re,Im\}} \int_\rho \int_\phi I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} e^{-\frac{(r_0-\rho)^2}{\alpha^2}} e^{-\frac{(\theta_0-\rho)^2}{\beta^2}} \rho d\rho d\phi$$

b) Fehlerbeseitigung

Vorteile dieses komprimierten Codes sind unter anderen, dass, erstens zwischen zwei Phasenbereichen nur ein einzelnes Bit verändert und dadurch Fehlertoleranz erhöht ist, zweitens das Nebeninformationen Reflextionen, Augenbrauen, Augenlider gleichsam wiedergegeben werden können[2]. Wichtig für die Vermeidung möglicher Fehlerquellen ist das der IrisCode hauptsächlich Informationen verwertet die nicht von umweltabhängigen Veränderungen wie Bildkontrast etc. abhängen und damit ziemlich Aussagekräfig ist[1].

2. Auswertung der Iris-Daten

a) Auswertungsmethoden

Der Iriscode kann nun als Biosignatur verwendet werden. Die Identifizierung einer Person erfolgt durch einfaches Vergleichen mit gespeicherten Iriscodes. Die Autorisation und somit die Verifikation (Bestätigung) erfolgt bei einem gewissen Maß an Ähnlichkeit. Zu dem Berechnen der Ähnlichkeit zweier Iriscodes wird die Hammingdistanz (h) der Bits berechnet. Diese ergibt sich aus Formel 6. Es handelt sich hierbei um einen einfachen aber dadurch

Formel 6

$$h = \frac{\|(iriscode_A \otimes iriscode_B) \cap maske_A \cap maske_B\|}{\|maske_A \cap maske_B\|}$$

schnell arbeitenden booleschen Ausdruck. Die beiden Masken enthalten Bitmuster die Augenbrauen etc. ausblenden. Ist die Hammingdistanz (HD) genügend klein, ähneln sich der Iriscode ausreichend, Ist sie gleich einem variablen Schwellenwerten so gilt die Person als eindeutig verifiziert. Hierbei ist der Schwellenwert der gewählt wird ausschlaggebend. Ist der nähmlich zu hoch gesetzt, werden die meisten Unterscheidbarkeiten unterschlagen und es kann vor kommen das unterschieliche Irismuster als ähnliche erkannt werden. Wird der Wert zu gering gewählt führt das womöglich dazu das keine Iris mehr den Anforderungen entspricht da minimale Änderungen wie die der Augenbrauen etc. zu einem Nichterkennen führen. Die geeignete Wahl des Schwellenwertes, in der Iristechnik HD-Kriterium genannt bestimmt wie sehr sich die hohen Intraklassenvariablität (s. 2.1.a) der Iris im Erkennungsvorgang äußert. Dies wurde mit statistischer Mathematik überprüft und man erhält ein sehr gutes HD-Kriterium bei HD < oder = 0,33[1], bei dem eine Wahrscheinlichkeit für eine falsche Übereinstimmung, auch kurz FAR genannt (False Accept Rates), bei 1 / 127 000 000 liegt.

b) Effizienz

Die Gesamteffizenz der Iriserkennung kann mittels eines Testcomputers ermittelt werden. Der ganze Vorgang wurde auf einer 300Mhz SunWorkstation mit einer optimierten Implementierung berechnet. Die Erkennungszeit betrug 446ms[1](Milisekunden). Ein Vergleich zweier Codes dauert 10ms[1]. Damit ist die hohe Geschwindigkeit auch bei großen Datenbanken (Mit erfassten Personen) gewährleistet. Ein weiterer Vorteil ist dass der Algorithmus auf parallel laufenden System umgesetzt werden kann, was eine weitere Steigerung mit sich bringt[1].

Ein Effizienzverlust tritt ein wenn das System zu unwidrigen Lichtverhältnissen genutzt wird. Das erfordert vom Verfahren ansich eine erhörte Erkennungsqualität um zu vermeiden das eine autorisierte Person abgewiesen wird. Hierfür wurde eine etwas Leistungsverbrauchende Erweiterung gefunden. Die Iris wird zu verschiedenen Rotationsstufen gespeichert damit wird die eindeutige Erkennung erleichtert denn der IrisCode wird nun mit mehreren Orientierungen des Musters verglichen[1].

4. Die Retina Erkennung

1. Erfassung

a) Erfassungstechnik

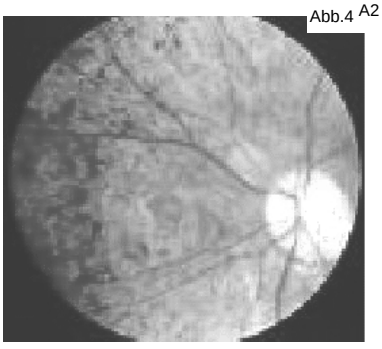


Abb.4 A2

Die Identifizierung anhand der Retina ist eins der ältestesten Biometrische Verfahren das bekannt ist. Ersten Überlegungen im Jahre 1930 nach, war schon bekannt das die Aderschicht oberhalb der Retina einzigartig von Person zu Person ist[6]. Diese Annahme wurde mittlerweile von weiteren Untersuchungen weitgehend Bestätigt[6]. Außer durch irreparabelen Schäden am Auge kann diese Aderschicht nicht zerstört werden. Um nun dieses Biometrische Merkmal zu nutzen wird bei der Retinaerkennung mithilfe eines Infrarot-Laserscanner ein Bild der Retina (s.2.2.b) gemacht. Wahlweise kann auch ein grüner Laser genutzt werden[6]. Aufgrund der Lichtbrechenden Cornea muss dabei das Auge in einer sehr kurzen Entfernung gescannt werden[2]. Die Erkennung erfolgt am Adermuster der Netzhaut, dieses wird in einzelnen Musterpunkten gespeichert. Das Muster entsteht durch die Abstandsmessung der Aderschicht durch den Laser. Das heißt dickere Adern sind näher an Laserlampe und reflektieren daher eher als dünne die weiter hinten liegen[6]. Die hauptsächliche Information wird wie zum Beispiel bei der Erkennung von Fingerabdrücken in eine Mustermatrize übertragen. Dieser wird dann zum Vergleich genutzt.[2] Dieses Muster hat auch eine hohe Intraklassenvariablität und ist dadurch sehr Aussagekräftig[2].

Ein Problem bei der Retinaerkennung ist das die Cornea meist die Form verändert um den Fokus zu ändern. Um dies zu vermeiden muss die zu verifizierende Person für den Zeitraum des Scanvorganges

einen bestimmten Punkt fixieren. Das Auge reagiert auch höchst sensibel auf Lichteinwirkung, um diesem zu entgegnen wird meist ein Infrarotlaser gebraucht. Dieser verhindert solche Irritationen[2]. Zudem lässt sich unter IR-Beleuchtung die Aderschicht deutlich besser erfassen[2].

2. Auswertung

a) Effizienz

Der gesamte Vorgang dauert ca. 45 Sekunden und bietet ein höchst scharfes Bild das dann weiterverarbeitet wird. Die FAR ist mit einer Warscheinlichkeit von 1 / 1 000 000[6] auch relativ gut und somit ist auf die Retinaerkennung ein gutes Erkennungssystem.
Trotzdem wird dieses System noch nicht in allzuvielen Anwendungen umgesetzt, denn der hohe Aufwand bringt Probleme mit denen wir uns später noch befassen werden. Auschlaggebend ist hier wohl die schlechte Wahrscheinlichkeit von dem System angenommen zu werden trotz das man autorisiert ist. Etwa 5-10% (FRR) werden durch die heute umgesetzten Verfahren nicht verifiziert (FRR Wert = False Reject Rate) und es erfordert einen erneuten Authifizierungsversuch[6].

5. Sicherheitsfaktoren

Nachdem uns nun die technischen Vorgehensweisen der beiden System bekannt sind, werden wir uns jetzt mit den sicherheitsrelevanten Überlegungen beschäftigen. Denn die Nutzung von biometrischen Merkmalen muss die Eindeutigkeit dieser voraussetzen. Diese dürfen durch Umweltfaktoren nicht verfälscht werden, auch die Frage nach der möglichen Täuschung erfordert unsere Aufmerksamkeit. Die Sicherheit der Benutzerinformation ist bei einem solchen System hinzu-kommend ein höchst sensibles Thema. Die folgende Betrachtung zu all diesen Aspekten soll einen Einblick in die Komplexität der praktischen Umsetzung vermitteln.

- Einfluß von Umweltbedingungen :
  Bei dem Verfahren der Retinaerkennung ist die Gefahr der Informationsverfälschung aufgrund von äußeren Einflüssen eher gering, da das System vom Anwender verlangt das er sich am Erkennungsgerät fixiert scannen lässt. Hier wirken mögliche Beeinflußungen durch das Reflexverhalten des Auges die wie in 4.2.a beschrieben, ausgeglichen werden. Trotzdem entsteht ein FRR Wert (False Reject Rate) von bis zu 10%, der nicht vermeidbar ist.
  In der Iriserkennung erfordert der Umwelteinfluß weiterer Überlegung, den selbst Veränderungen der Augenbrauen müssen berücksichtig werden. Wie in 3.2.a beschrieben enhält die Auswertungsformel (s.Formel 6) Masken die Iriscodes für reine Umweltfaktoren ausblenden. Ein großes Problem stellen die Lichtbedingungen dar, denn soll das System erfolgreich sein, muss es solche miteinbeziehen. Weitgehend wird das Problem dadurch umgangen, das das Irismuster unter IR-Licht aufgenommen wird und hinzukommend alle Muster, seien sie noch so unscheinbar oder stark ausgeprägt, gleichermaßen abgebildet werden[1]. Um die Qualität und die Wahl des HD-Kriteriums zu rechtfertigen wurden 7070 Vergleiche mit jeweils verschiedenen Bildern der gleichen Iris durchgeführt. Wurden die Bilder unter idealen Bedingungen aufgenommen war die HD = 0,0 unter widrigeren Bedingungen (die Iris war noch erkennbar) nahm sie höchstens den Wert von HD = 0,327 an[1]. Dies unterstützt die mathematischen Überlegungen (s. 3.2.a) zur Wahl des HD-Kriteriums. Um noch bessere Ergebnisse zu erzielen wurden Rotationen in der Iriscodierung hinzugefügt[1]. Das Ergebnis ist ein erkennungssicheres Verfahren mit einem recht kleinen FRR[1].

- Ist das System täuschungsicher ? :
  Auch hier schneidet der Retinascan sehr gut ab, denn es basiert auf dem Erkennen von Abstandsunterschieden (s. 4.1.a). Eine Retina nachzubilden mit all ihren Höhenunterschieden erfordert einen beträchtlichen Aufwand, hinzu kommt das die Aderschicht auf den IR-Laserstrahl dynamisch (unterschiedlich) reagiert da sie organisch ist[2]. Die Echtheit des Auges kann mit einem kurzen Lichtreiz überprüft werden, denn ist es echt so wird es im Reflex (ähnlich dem Kniereflex der auch unkontroliert ausgelöst wird) reagieren[2].
  Bei dem Irissystem ist die Gefahr wesentlich größer einem Scheinbild den Durchgang zu

gewähren, da es auf dem erkennen einer nicht dreidimensionalen Abbildung basiert. Die Nutzung von mehreren zusammengeschalteten Iriserkennern ist hilfreich doch auch dementsprechend Kostenaufwendig[1]. Eine andere Idee ist es die Augenbewegung zu überprüfen. Da das menschliche Auge in ständiger unbewußter Bewegung ist[1]. Doch auch dieses kann leicht mithilfe einer Videoaufnahme überbrückt werden. Erst wenn an das Auge aktive Licht-Signale gesendet werden und ihre Resonanz (Antwort) getestet wird ist dieses wirklich sicher, erfordert aber natürlich weitere Sensoren. Eine Überlegung meinerseits ist hier die Kopplung mit einem Bewegungssensorischen (Sensor = Erkenner) System. Mit einem Wärmesonar (Elektrikfachgeschäft ca. 40,-) ist eine Person mit ihrer Entfernung messbar, enspricht das Augenbild dieser Entfernung von der relativen Größe und Schärfe (mathematisch sicherlich umsetzbar) kann es als echtes Augenbild angenommen werden. Durch die Temperatursensibilität kann der Sonar nur ein lebendes Objekt anvisieren (Fokussieren).
Ein großer und leider nicht vermeidbarer Täuschungsfaktor ist durch das Abfangen der digitalen Information gegeben (IrisCode, Retinamuster). Dabei ist die Auswirkung schlimmer als bei dem Verlust einer Bankkarte oder Ähnlichem, denn ein Auge gehört immer nur einer Person die damit eindeutig identifizierbar ist und kann im Laufe des Lebens nicht verändert werden. Eine mögliche Lösung ist das verschlüsseln der übertragenen IrisCodes bzw. des Retinamusters. Genutzt werden hierbei häufig konventionelle Kryptverfahren (Verschlüsselungstechniken)[5]. Möglich wäre meiner Meinung nach sogar ein einfaches aber relativ sicheres optisches Verschlüsselungsverfahren. Optisch deshalb weil die Informationen der Iris[1] oder der Retina[2] in einem begrenzten Bitcode gespeichert sind und dadurch als ein Block von Bits abgebildet werden können. Ich würde hierbei die Farben Grün für ein gesetzte Bits und die Rot für nicht gesetzte Bits verwenden, nun könnte man mithilfe einer beliebigen Funktion die Vertauschungen der Bits untereinander vornehmen (z.B.: Vertausche Bit 1-100 mit 1948-2048). Dabei ist zu beachten das kein Bit überschrieben wird und dadurch keinerlei Verlust an der Qualität des IrisCodes auftritt. Wird eine Iris gescannt und muss verglichen werden, wird die Funktion auf den gerade erkannten Iriscode angewandt. Beide nun verschlüsselte IrisCodes werden ganz normal anhand der HD auf ihre Ähnlichkeit überprüft, dies kann ohne weiteres gemacht werden da der IrisCode noch den selben Informationsgehalt enthält. Da auf jedem Erkennungsterminal eine eigene Datenbank der Iriscodes vorhanden ist[5], kann die Funktion von Terminal zu Terminal unterschiedlich gewählt werden. Kommt der IrisCode abhanden ist es für den Dieb nicht ohne großen Aufwand möglich an die Funktion zu kommen die benötigt wird um den Code zu identifizieren (Es wäre einfacher sich mit einer Panzerfaust Eintritt zu verschaffen).

- Moralische Überlegungen :
Der wohl enscheidenste Punkt für Umsetzbarkeit eines Verfahrens ist die Akzeptanz durch die Gesellschaft. Wie eben erwähnt ist die Gefahr des Diebstahls der Augeninformation höchst bedrohlich, denn ist es erstmal geschehen gibt es keinerlei Maßnahmen die einen vor den Kosequenzen schützen könnten[6]. Aber auch ohne falschen Hintergedanken kommen Fragen und Ängste auf. Durch seine Biosignatur ist ein Mensch weitgehend individuell identifizierbar[1]. Es erlaubt ihm natürlich die gewisse Freiheit das er wie in 1.2.b beschrieben einen Schlüssel mit sich trägt der immer und überall nutzbar ist, den man nicht vergessen kann. Es treten dabei aber auch Überlegungen auf die die Privatspähre des Menschens betreffen. So ist es heute schon theoretisch möglich anhand der Kontobewegungen einer Person ihr ganz privates Kaufverhalten festzustellen. Jeder der eine EC-Karte nutzt teilt neben dem einfachen Geldtransfer auch die Information mit was er wo kauft, wie leicht auf dem Kontoauszug erkennbar ist. Übertragen auf die Retinaerkennung ist keine große Unterscheidung feststellbar da dies auch nur mit Zutun der Person geschehen kann. Doch die Iriserkennung ist da anders denn wenn es auch mit den heutigen technischen Möglichkeiten noch nicht umsetzbar ist, kann ein Irisscan auf einem einfachen Kaufhausbild in Echtzeit geschehen. Mal vom Kaufverhalten abgesehen wäre es sogar möglich Personen zu verfolgen, wenn genügend Kameras zur Vefügung stehen. Schon heute wird das Irisscanverfahren in den USA genutzt um Strafgefangene eindeutig zu identifizieren[9]. Das System ist portabel und über-

A3

all einsetzbar. Sicherlich kann es von Vorteil sein einen Sträfling durch automatische System ausfindig machen zu können. Doch die Gefahr des Missbrauches und das mögliche verkomme zum Überwachungstaates ist viel zu hoch. Eine weitere Überlegung ist die wirtschaftliche Nutzung des Erkennungssystemes, hier bieten SciFi Filme schon einen Ausblick auf mögliche Ausartungen. Beispielsweise in dem Streifen 'Minority Report', in einer Szene läuft die Hauptperson vor einer mutmaßlichen Gefahr weg. Dabei durchläuft er einen U-Bahnschacht mit futuristischen Werbeplakaten die mit Hilfe des Irisscans für ihn abgestimmte Werbung zeigen und ihn sogar mit Namen ansprechen. Doch auch andere Aspekte sind aufgeführt, z.B.: die Nutzung der U-Bahn wird simpel über den Scan verrechnet.
Wie zu erkennen ist erfordert diese neue Technologien noch eine rege gesellschaftlichen Diskussion bevor sie im großen Maßstab umgesetzt werden kann.

6. Vorteile und Nachteile beider Systeme im Überblick

a) Iriserkennung[5]

Vorteile :

- Benutzerfreundlichkeit

Da es eine Berührungslose Methode ist verlangt sie vom Benutzer keinerlei speziellen Kenntnisse und ist einfach zu bedienen.

- Hohe Genauigkeit und Aussagekraft

Die Iris ist ein gut geschütztes Teil des Auges der kaum Beinflussungen durch Verletztung oder ähnlichem unterliegt. Damit ist es höchst Aussagekräftig da es das eindeutige Muster über den Lebenszeitraum hinweg mit sich führt. Die FAR und FRR Werte liegen bei 1 zu 1,2 Millionen. So eindeutig ist kein anderes Verfahren. Diese Genauigkeit bleibt auch bei Benutzung von Kontaktlinsen, Brillen und Sonnenbrillen bestehen, da das System auf IR-Licht aufbaut.

- Hohe Erkennungsgeschwindigkeit

Der Eigentliche Scan dauert ca. 446 Millisekunden, ein Vergleich ca. 10ms. Diese Schnelligkeit erreicht kein anderes Verfahren.

Nachteile :

- Hohe Kosten

Die Umsetzung eines solchen Systems ist noch mit hohen Kosten verbunden da solche Systeme nur in geringer Stückzahl produziert werden.

- Moralische Vorbehalte

Vielen Menschen ist es zuwider ihr Auge durchleuchten zu lassen, da sie Schäden des wertvollen Organes befürchten. Nicht nur diese Bedenken sind Grund des Unmutes auch die Furcht vor Mißbrauch der Informationen führen dazu.

- Technische Schwierigkeiten

Die Iriserkennung steckt noch in den Kinderschuhen und hat noch vielerlei kleinere Probleme, die mehr mit der Interaktion (Zusammenarbeit) der verschiedenen Elemente als mit der Erkennung an sich zu tun haben. Trotz der hohen Auflösungsmöglichkeiten heutzutage, ist das Finden des Auges noch immer ein Hinderniss für die erfolgreiche Erkennung.

- Betrugsmöglichkeiten

Es ist möglich den IrisCode abzufangen und andersweitig zu nutzen. Mögliche Gegenmaßnahme ist die Verschlüsselung des Codes.

b) Retinaerkennung[6]

Vorteile :

- Hohe Genauigkeit und Aussagekraft

Der FAR Rate liegt kleiner als 0,0001 %. Auch hier ist die Verletzungsgefahr der Netzhaut und der darüberliegenden Aderschicht sehr gering.

- relative Betrugssicherheit

Im Moment ist die künstliche Herstellung einer Organisch reagierenden Retina nicht möglich. Das Verfahren unterliegt Effekten die nur bei einer echten Netzhaut vorkommen.

- kleiner Identifizierungscode

Bei der Retinaerkennung wird ein eindeutiger Code der nur 768 Bit umfasst erstellt.

Nachteile :

- Komplizierter Vorgang

Die Erkennung erfordert ein komplizierte Apparatur und verlangt von dem Benutzer einiges ab. z.B.: Muss ein Punkt fixiert werden um das Fukossieren des Auges zu vermeiden. Auch ein Scan über eine größere Entfernung hinweg ist, aufgrund der Augeneigenschaften, nicht machbar.

- Moralische Vorbehalte

Auch hier dieselben wie bei der Iriserkennung.

- Kosten und Technische Grenzen

Die hohen Kosten für die Technik die notwendig ist betragen zwischen 2000 - 2500$, die Technik ist hinzukommend auch an physikalische Grenzen gebunden das die Verbesserung erschwert.

7. Die Verfahren in der Praxis und ihre Zukunft

a) Iriserkennung

Abb.5 A4

Eine Praktische Umsetzung befindet sich auf dem Frankfurter Flughafen. Das dort eingesetzte EyeTicket System ist von der gleichnamigen Firma entwickelt worden und ist schon seit längerem am Londoner Flughafen Heathrow in Benutzung (Abb. 5). Es dient der automatischen Abfertigung von Einreiseformalitäten. Zum benutzen des Systemes muss eine Anmeldung mit gültigem Reisepass am Abflugsort erfolgen, dort wird die Iris das erste Mal zur Datenerfassung gescannt. Nach einer Überprüfung des Reiseapasses wird die Person in die Datenbank aufgenommen. Ist das geschehen wird der eindeutige IrisCode der Person dem Pass und den damit ver

bundenen Tickets zugeordnet. Diese Erfassung kann derzeit nur an den Flughäfen geschehen die das EyeTicket System anbieten. Bei der Ankunft wird der Benutzer einmalig gescannt und in der Datenbank gesucht, konnte er nicht verifiziert werden wird er an einen Zollbeamten überwiesen. Ansonsten erhält er sein Einreisevisum ausgedruckt und ist damit erfolgreich abgefertig, ganz ohne menschliches Zutun. Die schnelligkeit und einfachheit des Systems für den Benutzer ist das Hauptverkaufsargument der Firma. Weitere Informationen zu diesem System sind unter
'http://www.eyeticket.com' verfügbar.

a) Retinaerkennung

Die Retinaerkennung hat noch mit Anlaufschwierigkeiten durch die mangelnde Akzeptanz zu kämpfen. Es gibt ein einziges Modell das den Retinascan erfolgreich nutzt, das Icam 2001 (Abb 6). Dieses System ist recht kompakt und kann als Türerkennungsystem verwendet werden. Die Kosten für ein solches Gerät betragen ca. 2000 bis 2500 $. Der Ablauf der Erkennung ist wie folgt :


Abb.6 [6]

Nach Anmeldung am ICam mit Namen und Nummer, kann die Erkennung erfolgen, hierzu verlangt der ICam das ein bestimmter Punkt der im Blickfeld der Kamera erscheint mit den Augen fixiert wird. Danach erfolgt die eigentliche Retinaerkennung, der Vorgang kann Aufgrund der hohen Fehleranfälligkeit mehrmals wiederholt werden.

Es wird hier sogar von der Herstellerfirma darauf hingewiesen das das Verfahren mehrmalige Versuche erfordert also nicht gerade Benutzerfreundlich ist, und wird mit dem Argument das es ja kein System für den Heimgebrauch ist, kommentiert.
Weitere Informationen sind unter
'http://http://www.retina-scan.com/retina_scan_vendors_and_products.htm' verfügbar.

8. Zusammenfassung

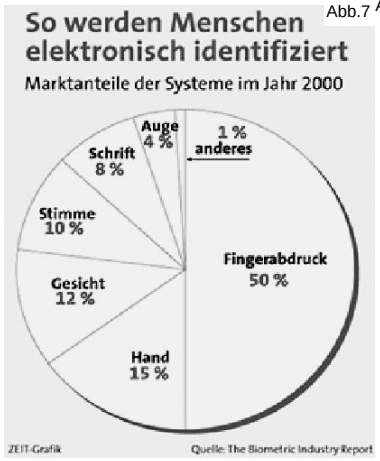


Abb.7 [A5]

Abschließend kann gesagt werden das beide Systeme ein hohes Potential besitzen, doch ihre technische Umsetzung befindet sich noch stark in der Entwicklungsphase. Vor 3 Jahren umfasst die Authifizierung anhand des Auges einen Marktanteil (Abb 7) von ca. nur 4% unter den gesamten Biosignatorischen Verfahren. Möglicherweise liegt die Ursache darin das beide Methoden auf Merkmale aufbauen die dem Menschen lieb und heilig sind und stößt daher auf Unmut. Dazu kommen diverse ungeklärte Fragen in der Sicherheit der Informationen und in der rechtmäßigen Nutzung dieser. Der Retinascan ist ein Verfahren das an seiner Komplexität scheitert, aber doch auch gute Werte in der Qualität bietet. Das Iriserkennungsverfahren ist hingegen dazu ein sehr viel besser umsetzbares biosignatorisches System mit ähnlichen Leistungen. Hier ist eine Umsetzung in weitere Bereiche unseres täglichen Lebens denkbar. Schon heute sind wie in dem Beispiel am Flughafen einfache Abfertigungsarbeiten durch den Irisscan erfolgreich zu meistern. Nimmt das Verfahren an Popularität zu, ist die weitere Nutzung in Bereichen der Bankgeschäfte denkbar. Aber das Werbeplakate mit einem solchen System arbeiten können ist wohl noch Science Fiction. Eine weitere nutzbringende Verwendung könnte in der Polizeiarbeit gefunden werden. Es könnten, wie heutzutage in den USA schon Gesichtserkennungssysteme die Gesichter von Strafverfolgten[10] am Flughafen in Überwachungsaufnahmen scannen, zur sicheren Erfassung von Straftäter hierzulande mit Hilfe der Iriserkennung umgesetzt werden. Hier ist die politische Durchsetzungsfähigkeit gefragt. Kurzum beide Verfahren sind weit genug entwickelt um Aufmerksamkeit zu erregen aber die Iriserkennung hat in den nächsten Jahren eine Möglichkeit wenn die System noch kompakter und Umweltunabhängiger werden. Die Retinaerkennung muss hier noch mehr bieten und wird wohl zweite Wahl bleiben.

9. Referenzen

a) Referenzliste

[1] Iriserkennung, (2001), J.Daughman: in: Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven, Michael Behrens, Richard Roth (Hrsg.), Vieweg-Verlag, S.129-158

[2] 07.05.03 : http://www.informatik.uni-stuttgart.de/ipvr/vs/de/teaching/ws0102/seminars/security/ausarbeitungen/biometrie-andreas_boronas.pdf; Seite 8+9

[3] 09.06.2003 : http://www.dgsys.de/rgsys/info/wavelet-introduction.pdf

[4] 10.06.2003 : http://ini.cs.tu-berlin.de/~schoener/sem-biometry/scheuermann00_biometrics_esignatures_eu.pdf

[5] 07.05.2003 : www.prip.tuwien.ac.at/~sab/papers/Biometrie.pdf; Seiten 36-52

[6] 10.06.2003 : http://www.retina-scan.com/

[7] 10.06.2003 : http://archiv.quintessenz.at/archiv/msg01133.html

[8] 10.06.2003 : http://www.eyeticket.com/de/releases2000.php?date=01172001.htm&about=hq

[9] 10.06.2003 : http://www.prosieben.de/

[10] 10.06.2003 : http://www.novosec.com/documents/Biometrie_030328.pdf

b) Abbildungen

[A0] Daughman;2001, http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html

[A1] Daughman; 2001, http://www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf

[A2] 10.06.2003 : http://www.axamedia.de/pdf/bio.pdf

[A3] 07.05.2003 : www.channel4.com/science/microsites/R/robots/images/science/ssv3a.gif

[A4] 10.06.03 : http://www.eyeticket.com/de/index.php?section=products&body=immigration

[A5] 10.06.03 : http://www.retina-scan.com

[Titel] 07.05.03 : http://www.forensic-evidence.com/site/ID/Iris1.gif