Biometrische identificatie: alle mensen zijn ongelijk!

R.L. van Renesse
TNO Technisch Physische Dienst, Postbus 155, 2600 AD Delft

Introduction
Alle mensen zijn ongelijk en dat is maar goed ook, want hoe zouden wij elkaar anders herkennen? Dagelijks identificeren wij elkaar vele malen, meestal visueel, middels de gelaatstrekken of vocaal middels de stem ("Hallo, met mij!") of zelfs aan de gestalte of aan een typisch loopje. Maar wanneer wij elkaar niet reeds kennen, is dat natuurlijk niet mogelijk en kan identificatie alleen plaats vinden door middel van iets wat we hebben afgesproken, zoals bijvoorbeeld een wachtwoord. Hoe identificeren wij elkaar? En, kan een apparaat ons identificeren en hoe veilig is dat?

Kennis, bezit, persoonskenmerk
In feite kan identificatie (en toegangscontrole) op drie principieel verschillende manieren plaats vinden, namelijk m.b.v.:

1. Kennis (wachtwoord, cijfercode, PIN, etc.)
2. Bezit (Paspoort, identificatiekaart, sleutel, etc.)
3. Persoonlijke (biometrische) kenmerken (gelaatstrekken, stem, vingerlijnenpatroon, etc.)

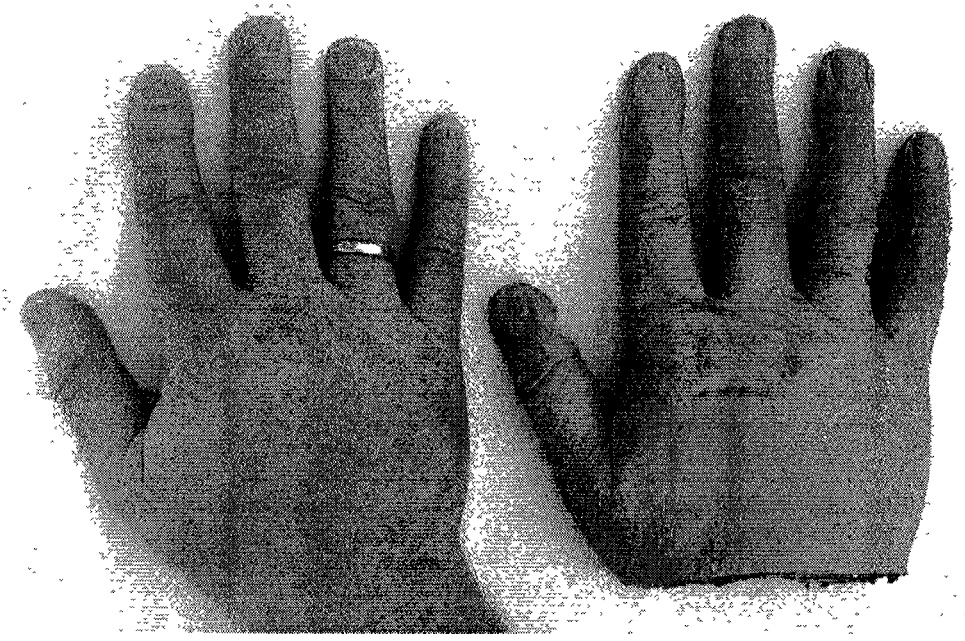
Soms vinden identificatie en toegangscontrole plaats op basis van een combinatie ervan zoals credit card + PIN; paspoort + pasfoto; cijfercode + brandkastsleutel.

De toepassing van persoonlijke eigendommen als sleutels en persoonlijke kennis als wachtwoorden zijn ons vanouds bekend. Gelaats- en stemherkenning zijn biometrische processen die waarschijnlijk vanaf het ontstaan van de mensheid gebruikt worden. Dactyloscopie, de eerste wetenschappelijke identificatiemethode, gebaseerd op het patroon van vingerlijnen, bestaat sinds ongeveer een eeuw. De toepassing van vingerafdrukken heeft een veel oudere oorsprong; vingerafdrukken werden al gebruikt in het oude Babylonië onder koning Hammoerabi, omstreeks 1800 vC. Sedert 300 vC werden hand- en vingerafdrukken in het oude China gebruikt als bevestiging van officiële contracten. Handtekening en pasfoto zijn recentere voorbeelden van biometrische attributen. Nieuwe toepassingen van biometrie zijn momenteel sterk in opkomst en zij beloven "James Bond-achtige" mogelijkheden. Voorbeelden zijn de automatische herkenning van gelaatstrekken, van patronen in het oog (netvlies of iris) of van de stem.

Maar aan de beide eerste methoden, kennis en bezit, kleven een paar besliste nadelen. Die geheime kennis is vaak iets wat je juist bent vergeten of iets wat je wellicht hebt opgeschreven om dat te voorkomen. Zo, of op een andere arglistige manier, komt een onverlaat mogelijk onze PIN te weten. Wachtwoorden liggen vaak voor de hand en worden dan gebroken. Iets wat je bezit kan worden verloren, gestolen of geroofd. Het kan worden nagemaakt en vervalst. Kennis noch bezit zijn kennelijk onverbrekelijk aan de rechtmatige persoon gebonden en verzekeren dus geen echt betrouwbare identificatie.

Biometrie
Anders is dit met de biometrische kenmer-

Verschenen in: Beveiliging, 9e jaargang, nummer 3, maart 1996



Biometrische apparatuur moet onderscheiden of een levend kenmerk wordt aangeboden

ken van een *levend* persoon, dit kunnen fysieke kenmerken of gedragskenmerken zijn. Het is natuurlijk van belang dat een persoonlijk fysiek- of gedragskenmerk onvervreemdbaar is, d.w.z. niet door een andere persoon kan worden gebruikt of geïmiteerd. In het algemeen is het daarom noodzakelijk dat de biometrische identificatie of verificatie tevens de controle inhoudt of het gepresenteerde kenmerk afkomstig is van een levend persoon. Biometrie wordt als volgt gedefinieerd: "*De automatische **identificatie** of **verificatie** van de identiteit van een levend individu door middel van de meting van een fysiek of gedragskenmerk*".

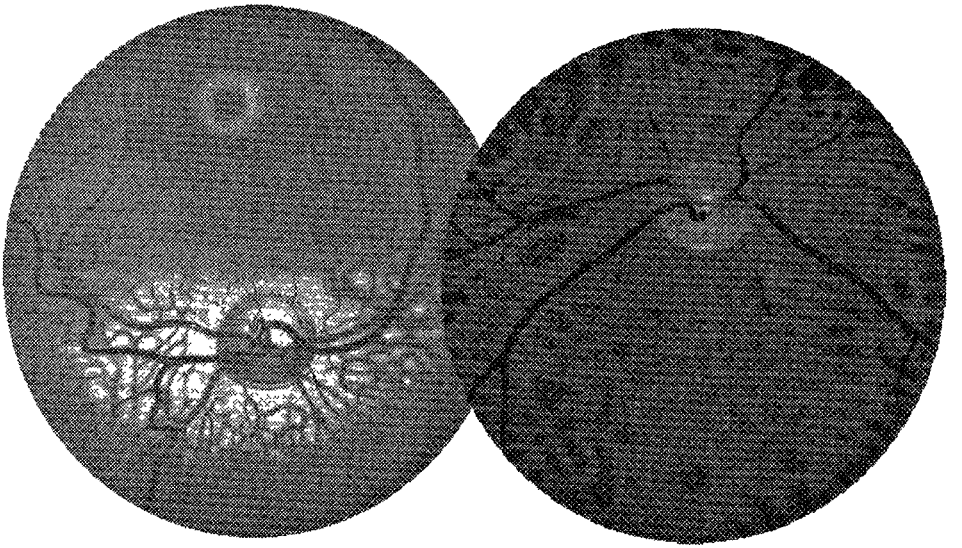
Onder ***identificatie*** wordt de "search & find" methode verstaan, waarbij één persoon in een bestand van vele personen wordt opgezocht. Een persoon meldt zich met een bepaald, uniek biometrisch kenmerk (vingerlijnenpatroon, stemkarakteristiek, etc.) bij het systeem en dit zoekt vervolgens in het bestand van geregistreerde personen, wie het meest overeenkomt met de persoon die zich aanmeldt. Bij voldoende overeenkomst met een geregistreerd persoon, neemt het systeem aan dat de aangemelde inderdaad overeenkomt met de in het bestand gevonden geregistreerde persoon. Het voordeel van deze methode is, dat noch het bezit van bewijsstukken (ID-kaart, paspoort) noch het kennen van codes (PIN-code, wachtwoord) noodzakelijk is, en deze dus ook niet kunnen worden vergeten, verloren, gestolen of nagemaakt. Nadelen van de methode zijn, dat het doorzoeken van een groot bestand veelal tijdrovend is en dat identiteiten kunnen worden verwisseld. Zo'n verwisseling van identiteit is altijd pijnlijk, of de vergissing nu een mens of door een machine wordt gemaakt.

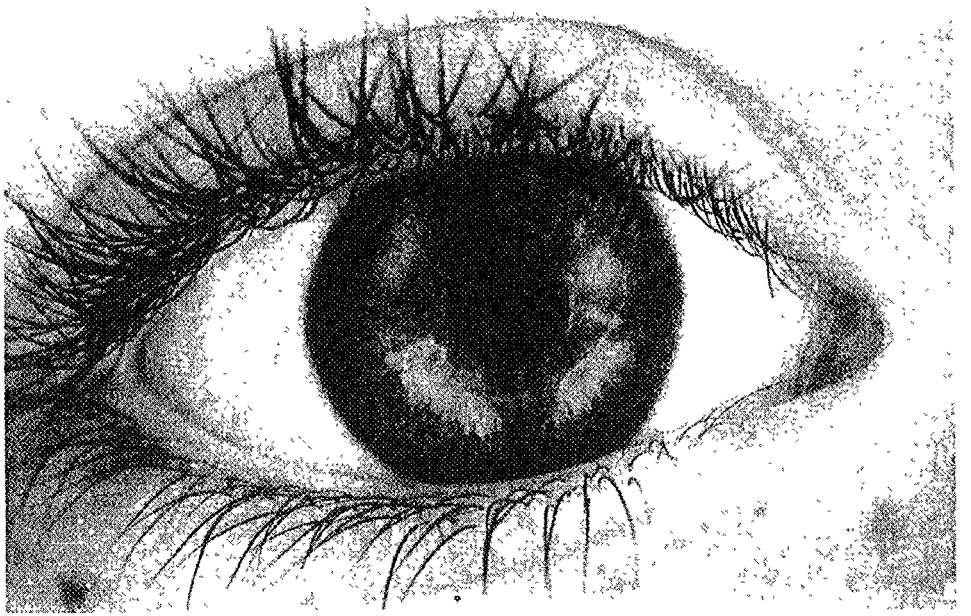
Onder ***verificatie*** wordt de "claim-

challenge-response" methode verstaan, waarbij de te verifiëren persoon een bewijs of code aanvoert. De gang van zaken is als volgt: de persoon in kwestie beweert P. te zijn (claim), het systeem vraagt vervolgens om een bewijs (challenge), waarna P. een identiteitsbewijs produceert (response). Voordelen van de methode zijn, dat ze relatief snel is, omdat een groot bestand niet behoeft te worden doorzocht, en dat identiteiten niet kunnen worden verwisseld. Nadeel is, dat bewijsstukken kunnen worden verloren, gestolen, geroofd en nagemaakt, terwijl persoonlijke codes als PIN-codes en wachtwoorden kunnen worden vergeten en slinks kunnen worden ontfutseld of gekraakt. Eventueel kan een tussengebied van twijfel worden toegestaan, waarin het systeem beslist tot het verzoek om nadere informatie (bijvoorbeeld: verificatieproces herhalen of verwijzen naar een balie).

De definitie van biometrie betreft ***automatische*** identificatie en verificatie, hoewel onder biometrie eveneens menselijke identificatie en verificatie zou kunnen worden verstaan. Menselijke inspectie is in veel opzichten superieur aan machine-inspectie. De mens is bijvoorbeeld de huidige stemherkennings- en gelaatsherkennings-apparatuur nog verre de baas. Nadeel van menselijke inspectie is, dat deze onderhevig is aan fysiologische en psychologische factoren. De mens wordt op een gegeven moment moe, terwijl stress, onzekerheid en verlegenheid het resultaat van de inspectie ongunstig kunnen beïnvloeden. Machine-inspectie daarentegen is betrouwbaar en constant van kwaliteit binnen de beperkte mogelijkheden van de beschikbare apparatuur. Er treedt geen vermoeidheid op en psychologische remmingen kent het apparaat niet. Wanneer het apparaat bovendien

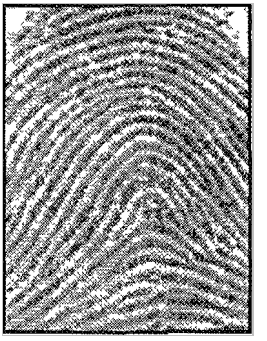
De *vingerlijnpatronen* van de eeneiige tweeling Eva en Anouk zijn duidelijk verschillend. Als voorbeeld zijn de patronen van beide linkerwijsvingers afgedrukt.





Het aderpatroon in de *retina* en het patroon van de *iris* zijn voor ieder mens uniek.

controleert of een kenmerk van een levend individu wordt aangeboden en het niet wordt beduveld met een geroofd of imitatielichaamsdeel, wordt de betrouwbaarheid van biometrische identificatie zeer hoog. Wij hoeven dan ook niet het pijnlijke onheil te vrezen dat een onverlaat biometrische kenmerken als handen of ogen van ons rooft Zo'n controle op "leven en welzijn" kan, afhankelijk van het biometrische kenmerk, op verschillende wijzen geschieden (bijv. hartslag, lichaamswarmte, typerende onwillekeurige bewegingen en bepaalde eigenschappen van de levende huid)



Empirische basis van biometrie

De empirische basis van biometrie is:

1. dat de natuur zich nooit herhaalt, en
2. dat bepaalde fysieke- en gedragskenmerken van de mens uniek zijn voor ieder mens.

Het volgende is bijvoorbeeld bekend van het vingerlijnenpatroon en van het patroon van de iris in het oog:

- De patronen zijn niet identiek voor eeneiige tweelingen.
- Geen wezenlijk deel van het patroon wordt binnen één persoon herhaald. Dat wil zeggen dat bijvoorbeeld een bepaald vingerlijnenpatroon niet nogmaals op een ander deel van dezelfde of een andere vinger wordt aangetroffen.
- Geen twee personen zijn ooit gevonden met identieke patronen.
- De patronen zijn in essentie onveranderlijk gedurende het leven. Hiermee wordt bedoeld dat kenmerken weliswaar kunnen veranderen op ondergeschikte punten, maar dat de unieke persoonlijke kenmerken behouden blijven. Een vingerlijnenpatroon kan bijvoorbeeld slijten, er kunnen littekens zijn ontstaan en het aantal poriën kan veranderen, maar het lijnenpatroon zelf blijft zijn unieke kenmerken behouden.

Het is waarschijnlijk dat een dergelijke uniciteit voor veel andere fysieke- en gedragskenmerken geldt, zoals weergegeven in tabel I. Een exact bewijs hiervoor is nooit te leveren, de biometrische praktijk moet in de loop van de tijd de overtuiging bieden.

Tabel I - Biometrische kenmerken

Fysieke karakteristieken	*Gedragskarakteristieken*
Gelaatstrekken*)	Stem*)
Gelaatsaderpatroon	Dynamiek handtekening*)
Vingerlijnen*)	Toetsaanslag dynamiek*)
Handpalmlijnen	
Hand- en vinger geometrie*)	
Hand aderpatroon	
Iris patroon	
Retina aderpatroon*)	
Oor verificatie	
Geuridentificatie	

*) Commercieel verkrijgbaar

Sommige van de in tabel I genoemde technieken staan nog in de kinderschoenen, andere zijn deze reeds ontgroeid en hebben succesvolle commerciële toepassingen gevonden. Dat veel fysieke en gedragskarakteristieken als identificatiekenmerk kunnen dienen, behoeft nauwelijks betoog Dieven die hun oor te luisteren leggen aan een potentieel project dienen erop bedacht te zijn dat de politie tegenwoordig ook oorafdrukken registreert. Nieuw is ook de geuridentificatie met een 'electronische neus' die een aantal sensoren bevat die gevoelig zijn voor de mate van aanwezigheid van specifieke geurstoffen. Uit de geurstofregistratie wordt een persoonlijk 'odourgram' afgeleid, dat niet te vervalsen is door het gebruik van parfums, deodorants, etc. Een 'snufje' van uw hand is voor het apparaat voldoende om u te herkennen! De stem is niet eenvoudig middels een magnetisch bandje te imiteren, want het biometrische apparaat vraagt degeen die zich identificeert, de geregistreerde trefwoorden in een willekeurige, door het apparaat te bepalen volgorde, uit te spreken. Ook dynamische gedragskarakteristieken als identificatiemiddel zijn iets nieuws. Een handtekening kan eenvoudig worden nagemaakt zonder dat de namaak opvalt, maar de dynamiek van het plaatsen van een handtekening, zoals de variatie in schrijfsnelheid, de totale schrijftijd, het schrijfritme, het tijdstip en het aantal malen dat de pen van papier wordt genomen, etc. is echter vrijwel onnavolgbaar voor de bedrieger.

Pennen en schrijftabletten die dergelijke dynamische kenmerken registreren zijn ontwikkeld en commercieel verkrijgbaar. Evenzeer vormt de dynamiek van de toetsaanslag tijdens het typen een persoonlijk kenmerk. Software bestaat die deze dynamiek registreert, waardoor controle mogelijk is op de identiteit van degeen die de computer bedient.

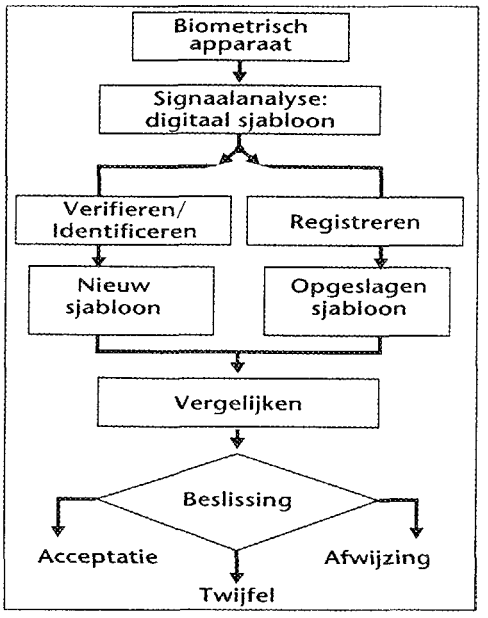
Een belangrijk aspect van biometrische apparatuur is de publieke acceptatie. Optische scanners van bloedvaten in het netvlies worden door sommigen bijvoorbeeld als opdringerig of bedreigend ervaren, vingerlijnpatroonlezers worden geassocieerd met criminaliteit en het wordt daarom verwacht dat ze niet algemeen zullen worden aanvaard. Hierbij moet echter worden bedacht dat wat nu sociaal onaanvaardbaar lijkt, te zijner tijd acceptabel kan worden, bijvoorbeeld onder de aanhoudende druk van bankinstellingen die de voortdurend toenemende schade van fraude wensen in te perken. Er is reden om aan te nemen dat, binnen de komende tien jaar, biometrie een integraal deel van ons dagelijks leven zal gaan uitmaken.

Registratie

De werking van biometrische apparatuur wordt schematisch in de figuur geïllustreerd. In eerste instantie wordt een persoon door het systeem geregistreerd. De betreffende biometrische karakteristiek wordt door het apparaat gelezen en het signaal wordt middels signaalanalyse omgezet in een digitaal sjabloon. Dit sjabloon bevat slechts de hoogstnoodzakelijke karakteristieken en vergt daardoor een relatief geringe geheugencapaciteit. Het sjabloon wordt vervolgens opgeslagen in een database register. Dit register kan zich bevinden in een chip of op een chip card, in een off-line computer verbonden met het biometrische systeem of in een centraal computersysteem. Aan het biometrische sjabloon worden de noodzakelijke persoonsgegevens van de registrant gekoppeld.

Verificatie/Identificatie

Bij een volgende gelegenheid kan de betreffende persoon zich aanmelden bij het biometrische inspectiepunt, waarna een verificatie of identificatie wordt uitgevoerd. Het nieuw berekende sjabloon wordt vergeleken met het in het geheugen geregistreerde sjabloon. Zelden zal de overeenkomst tussen beide sjablonen volledig zijn, een biometrisch kenmerk is namelijk voortdurend aan geringe veranderingen onderhevig. Biometrische apparatuur laat daarom een drempelinstelling toe, waarbij

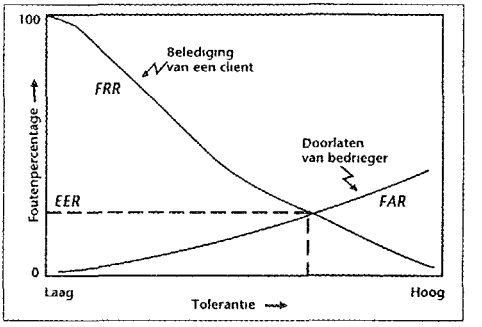


De werking van een systeem voor biometrische identificatie

de strengheid van de controle kan worden gevarieerd tussen 'strikt' en 'los'. Wanneer de gevonden correlatie de ingestelde drempel overschrijdt, wordt besloten tot acceptatie, bij onderschrijding tot afwijzing. Het is soms mogelijk een derde beslissing in te voegen, in geval van onderschrijding nabij de drempelwaarde: het systeem kan in dat geval de registrant om nadere informatie of identificatie vragen, bijvoorbeeld door de registrant voor verdere afhandeling naar een balie te verwijzen.

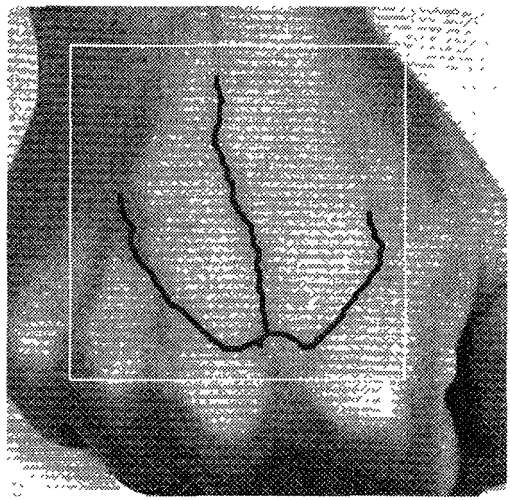
Foutenpercentages

Doordat de biometrische vergelijking nooit tot een exact resultaat kan leiden, treden onvermijdelijk fouten op in de biometrische beoordeling. Er worden twee types fout onderscheiden (1) de kans op het ten onrechte afwijzen van een persoon ('belediging van de cliënt') en (2) de kans op het ten onrechte toelaten van een persoon ('het binnendringen van een bedrieger'). Klantbelediging wordt aangeduid met de Engelse term *False Rejection Rate (**FRR**)*, het binnendringen van een bedrieger met *False Acceptance Rate (**FAR**)*. Bij een strikte drempelinstelling (lage tolerantie) zal het ten onrechte toelaten van een persoon niet gemakkelijk voorkomen en zal de *FAR* dus minimaal zijn. Het ten onrechte weigeren van een persoon zal dan echter vaker voorkomen en de *FRR* zal dan dus relatief hoog zijn Een hoge tolerantie leidt tot een tegengestelde situatie, belediging van cliënten wordt zo goed mogelijk voorkomen, op gevaar af bedriegers een grotere kans te geven. De volgende figuur illustreert deze verhoudingen.



Relatie tussen hoge en lage tolerantie en de gevolgen voor de organisatie

Het ligt voor de hand een instelling te kiezen, waarbij *FAR* en *FRR* beide klein zijn. Bij deze drempelinstelling wordt de *Equal Error Rate (EER)* gevonden: *FAR = FRR*. De *FAR*, de *FRR* en de *EER* zijn belangrijke functieparameters van biometrische apparatuur. De *EER*-instelling zal niet altijd worden gekozen. Voor high security toepassingen zal bijvoorbeeld gestreefd worden naar een *FAR* die praktisch nihil is, terwijl de *FRR* een matig hoge waarde zal mogen hebben (bijvoorbeeld *FRR* = 5%) Voor bankinstellingen zal de zaak eerder omgekeerd zijn. Het ten onrechte afwijzen van een cliënt mag slechts zeer sporadisch voorkomen, terwijl het voldoende is om de kans op het doordringen van een bedrieger te beperken tot een matige waarde (bij-



Het aderpatroon op de *rug van de hand* heeft onder infrarode verlichting een hoger contrast. Met beeldbewerkingstechnieken worden vervolgens de aderen gelocaliseerd

voorbeeld *FAR* = 5%). De foutenpercentages van de bestaande biometrische apparatuur verschillen aanzienlijk en variëren van een geringe fractie van een procent tot enkele procenten.

De Praktijk

Acceptabele foutenpercentages zijn een belangrijke voorwaarde voor biometrische apparatuur; wat acceptabel is, zal van de apparatuur en de specifieke toepassing daarvan afhangen. De *FRR* (kans op belediging van de bonafide gebruiker) kan bepaald worden door de apparatuur in de praktijk, met een grote testgroep, te onderzoeken. De *FAR* (de kans dat een geregistreerde voor een ander kan doorgaan) kan op deze wijze vanzelfsprekend niet worden bepaald. Dat gebeurt achteraf door, voor alle drempelinstellingen, de geregistreerde sjablonen met elkaar te vergelijken. Zo wordt de *FAR*-curve gevonden. Deze berekende curve geeft de kans weer dat de bedrieger in spé zondermeer binnendringt: in feite de kans op het slagen van 'bedrog zonder inspanning'. In de werkelijkheid, waar vastbesloten en vakkundige bedriegers bestaan, is de *FAR* mogelijk aanzienlijk hoger. Een exacte waarde van de *FAR* bij zulk een 'vastbesloten aanval' is uiteraard niet te geven. Een terzake kundige evaluator kan echter veelal meer licht werpen op de kans dat criminelen, in hun opzet de biometrische apparatuur te bedriegen, zullen slagen. Een dergelijke evaluatie van biometrische apparatuur is één van de taken van TNO. Een andere taak, elders in TNO, is het ontwerpen en bouwen van biometrische apparatuur, de hardware en de software en het adviseren daarbij.

Naast de genoemde publieke acceptatie (gebruikersgemak, etc.), de foutenpercentages en de weerstand tegen criminele aanvallen, zijn voor de beoordeling van biometrische apparatuur de kosten, de verificatietijd, de voor de sjablonen benodigde geheugenruimte en de robuustheid van belang.

Literatuur

Biometric Technology Today, S.J.B. Services, PO Box 20, Somerton, Somerset, England TA11 7YY; tel. +44 1458274444, fax +44 1458274495. BTT komt tienmaal per jaar uit.