Biometrie *in* perspectief

Ruud van Munster studeerde af in de Technische Natuurkunde in Delft en werkt sinds 1970 bij TNO. Hij ontwikkelde onder andere TCL-Image dat wereldwijd als ontwikkelomgeving voor beeldverwerkingstoepassingen is gebruikt.

Met de vinger aan de pols, het gezicht op oneindig en het oog op de toekomst?
Biometrie staat flink in de belangstelling. Zo is recent in Nederland en een aantal andere Europese landen gezichtsherkenning opgenomen in het paspoort. Andere toepassingsgebieden zijn het veiliger maken van evenementen, zoals voetbalwedstrijden, winkels, zwembaden en discotheken. Alle experts zijn het erover eens: biometrie is een veelbelovende techniek om de maatschappij veiliger te maken.

Een greep uit het nieuws van de laatste tijd laat zien dat tal van organisaties bezig zijn met biometrische technieken om de veiligheid te verbeteren. Op Schiphol kun je tegenwoordig snel door de grenscontrole op basis van een irisscan. De KNVB is een proef gestart met het gebruik van vingerherkenning om ongewenste personen te weren. ADO Den Haag krijgt, dankzij een veiligheidsconcept op basis van biometrie en slimme camera's één van de modernste stadions van Europa. Andere voorbeelden zijn de invoering van handgeometrie bij Europoort en onderzoek in de bankwereld naar de toepassing van stemherkenning in combinatie met een gesproken pincode.

Identiteit vaststellen
Wat verstaan we onder biometrie? Biometrie is een manier om automatisch de identiteit vast te stellen van een (levend) persoon of dier. Biometrie doet dit op basis van lichaamskenmerken of gedragskenmerken. Grofweg zijn er drie manieren om iemands identiteit vast te stellen:

- Kennis; wat je weet, zoals een password of een andere geheime code;
- Bezit; wat je hebt, zoals een identiteitskaart of pinpas;
- Biometrie; wie je bent, zoals je gezicht, vinger, de manier waarop je loopt of hoe je schrijft.

Bij veel toepassingen worden combinaties van methoden

Biometrie is gebaseerd op de aanname dat de natuur zich nooit herhaalt en ieder mens daardoor een aantal unieke kenmerken bezit. De uitdaging is de vaststelling en vergelijking van die unieke kenmerken. Dat gebeurt door van een lichaamsdeel een (beeld-) opname te maken, zoals een gezichtfoto of vingerafdruk. Met beeldverwerkingtechnieken worden kenmerken uit het beeld berekend en vergeleken met een referentiedatabase. Deze referentiedatabase wordt opgebouwd tijdens de aanmeldprocedure, de enrollment.

Werking van biometrie
Tijdens **enrollment** worden referentieopnames gemaakt. Doorgaans wordt niet de volledige opname ('het beeld') in de database opgeslagen, maar een reeks uit het beeld afgeleide kenmerken die het beeld uniek beschrijven. Een beeld van vele beeldpunten ('pixels') wordt daarmee teruggebracht tot een beperkte set getallen: de template. De template wordt in de database opgeslagen. Voorbeelden van kenmerken zijn de afstand tussen de ogen en de posities van vertakkingen van lijnen in de vingerafdruk. De kwaliteit van enrollment speelt een belangrijke rol in het succes van een biometrieoplossing.
Tijdens **herkenning** wordt op vergelijkbare wijze een opname gemaakt en een template met kenmerken uit het opgenomen beeld bepaald. Vervolgens wordt deze template vergeleken met de templates in de database.

Aanpak afhankelijk van toepassing
Afhankelijk van de toepassing wordt bij biometrische systemen een verschillende aanpak gevolgd.
Bij **verificatie** wordt het systeem gevraagd of een geclaimde identiteit (zoals die bijvoorbeeld op een pas staat) klopt. Het systeem vergelijkt dan de actuele template met de template in de database die bij de geclaimde identiteit hoort. We noemen dit een één-op-één vergelijking.
Bij **identificatie** heeft het systeem geen voorkennis over de geclaimde identiteit. Het systeem vergelijkt dan de actuele template met alle templates in de database en geeft een lijst van de meest gelijkende identiteiten.
Een bijzondere vorm van identificatie is de **watchlist** toepassing. Hierbij wordt gecheckt of iemand op een lijst met bijzondere personen staat.
De toepassing bepaalt of er sprake is van verificatie of identificatie. Daarbij dient men zich bewust te zijn van de verschillen:

- Verificatie verloopt sneller omdat minder vergelijkingen nodig zijn (alleen de aangeboden template en de template van de geclaimde identiteit worden vergeleken);
- Verificatie is doorgaans nauwkeuriger omdat er gebruik wordt gemaakt van voorkennis;

- Identificatie heeft de voorkeur bij toepassingen waarbij geen medewerking wordt verwacht.

Toegepaste technieken
Gezichtsherkenning is misschien wel de bekendste biometrische techniek. Voordeel is dat het zonder veel medewerking kan worden gebruikt en daardoor geschikt is als observatietechniek. Mogelijke toepassingen zijn: signaleren van bezoekers die op een "watchlist" staan en het signaleren van mensen die vaak terugkomen. In vergelijking met vinger- en irisherkenning is gezichtsherkenning minder geschikt voor toepassingen waarbij hoge nauwkeurigheid wordt verwacht.
Gezichtsherkenning doet het momenteel binnen, onder geconditioneerde belichting, beter dan buiten, waar de invloed van zonlicht de meting kan verstoren. Hoewel het geen medewerking vraagt, is het wel erg gevoelig voor tegenwerking. Als de persoon in kwestie onvoldoende recht de camera in kijkt of een grimas maakt, nemen de prestaties snel af. Bekende toepassingen zijn de beveiliging van evenementen en preventie van winkeldiefstal.

Vingerafdrukken liggen qua nauwkeurigheid tussen de gezichtsherkenning en de irisscan. Voor beveiliging en toegangscontrole is de vingerafdruk vaak nauwkeurig genoeg, zeker als het in combinatie met een chipcard wordt gebruikt. De KNVB experimenteert bijvoorbeeld met het handhaven van stadionverboden. Van iedere toeschouwer wordt een vingerafdruk afgenomen, die wordt gecontroleerd tegen een watchlist met vingerafdrukken.
Bij gebruik van vingerafdrukken moet men alert zijn op het gebruik van nepvingers. Vrijwel alle scanners zijn op dat punt zwak. Bij toepassing zonder begeleiding moet men hierop extra alert zijn.
De irisscan is een van de meest nauwkeurige technieken. Deze techniek heeft wel als nadeel dat het percentage mensen dat zich vanwege een handicap niet kan aanmelden, groter is dan bij de andere technieken. Irisscan gold lang als een erg dure techniek voor de bovenkant van de markt. Mede door het aflopen van patenten en dankzij technologische voortgang komt ook deze techniek snel binnen bereik.

Minder bekende technieken zijn herkenning van handgeometrie, stem en het aderpatroon in de hand of vinger.
Handgeometrie is populair bij toepassingen onder wat moeilijker omgevingscondities, zoals in de Rotterdamse haven. De prestaties liggen in het middengebied tussen iris en gezichtsherkenning.
Stemherkenning levert in theorie niet de meest nauwkeurige resultaten op. Toch claimen diverse banken dat herkenning van de klant door deze techniek in combinatie met (het uitspreken van) een pincode (of een ander "geheim") met hoge betrouwbaarheid gebeurt. Wij hebben nog onvoldoende informatie om dit te kunnen beoordelen.

Het scannen van **aderpatronen** in hand of vinger is in opkomst. De eerste berichten spreken van een nauwkeurigheid vergelijkbaar met de irisscan. De methode neemt een grote vlucht in de Aziatische landen. Vooral het feit dat geen fysiek contact met de sensor nodig is, wordt daar bijzonder gewaardeerd.

Beperkingen
In theorie is biometrie een ideale identificatiemethode. Je kunt je lichaam niet vergeten mee te nemen, je lichaamskenmerken zitten onvervreemdbaar aan je vast en je hoeft geen pincodes te onthouden.
Helaas is de praktijk wat minder ideaal. Vervalsing is altijd mogelijk, en daarop is biometrie geen uitzondering. Bekend is het gebruik van de kopie van de vinger die met een gietafdruk van latex wordt gemaakt. Sommige systemen zijn in staat dergelijke fraude te detecteren, sommige niet. Het is van belang hier aandacht aan te geven. Aan de andere kant kunnen gewone sleutels ook worden nagemaakt. In die zin is er niets nieuws onder de zon.
Een aandachtspunt is ook dat sommige mensen niet in staat zijn, bijvoorbeeld door lichamelijke gebreken, om de biometrische techniek te gebruiken.
Biometrie is gebaseerd op het vergelijken van kenmerken. Doordat de omstandigheden tijdens enrollment en herkenning altijd verschillen, moet de vergelijking met een zekere tolerantie plaatshebben. Deze tolerantie is een factor van betekenis bij biometrie. Afhankelijk van de toepassing moet men kiezen tussen maximaal comfort (hoge tolerantie) en maximale veiligheid (lage tolerantie).
In de literatuur over biometrie wordt dit besproken in termen van **"false match rate"** (FMR), het onterecht herkennen en **"false non-match rate"** (FNMR), het onterecht afwijzen. In de praktijk worden voor deze twee begrippen nog vaak de vroegere termen **"false accept rate"** (FAR) en **"false reject rate"** (FRR) gebruikt.
De FMR beschrijft het percentage onterechte positieve detecties bij een gekozen FNMR; terwijl de FNMR omgekeerd het percentage onterechte negatieve detecties beschrijft bij een gekozen FMR. FMR en FNMR zijn onderling gekoppeld en hangen af van de ingestelde tolerantie. Een lagere FMR betekent een hogere FNMR en omgekeerd.

Overwegingen
Biometrie kan uiteraard een bijdrage leveren aan meer veiligheid. Maar ook comfort speelt een voorname rol, zoals het niet hoeven onthouden van een paswoord of pincode of het sneller langs de grenspassage kunnen. Je hebt je lichaam altijd bij je, terwijl je een sleutel kunt vergeten. Bij veel succesvolle toepassingen van biometrie spelen de beide aspecten veiligheid en comfort een belangrijke rol. Het is dan ook aan te raden daar goed over na te denken. Te meer omdat er een relatie is geconstateerd tussen de prestaties van een biometriesysteem en de mate van medewerking van de gebruikers. Belangrijk is dat men zich realiseert dat bij biometrie altijd een zekere foutkans aanwezig is. Bij toepassing van biometrie is dan ook aandacht nodig voor zowel de techniek als het proces waarin het wordt toegepast. Zo kan de kans dat iemand ten onrechte niet wordt herkend het noodzakelijk maken een fallback procedure in te richten. Die fallback procedure mag uiteraard niet minder betrouwbaar zijn dan het biometriesysteem zelf.

Biometrie in perspectief
Wie denkt dat biometrie iets van de laatste jaren is, vergist zich een beetje. Al in het oude Egypte werden de bouwers van de piramides mede geïdentificeerd op basis van

lichaamsafmetingen, gezichtsvorm, gezichtshuid en andere opvallende kenmerken zoals littekens. In 1858 kreeg de Engelsman William Herschell (1833-1917), hoofdambtenaar in het Indiase Hooghly district, het idee om vingerafdrukken te gebruiken op loonzakjes van de plaatselijke arbeiders. Dit omdat het nog al eens voorkwam dat de arbeider, na het in ontvangst nemen van zijn eigen loonzak nogmaals aansloot in de rij om een tweede te halen. In 1883 zorgde Alphonse Bertillon voor een doorbraak door het opmeten van mensen (antropometrie) te gebruiken om misdadigers te identificeren. De opkomst van de computertechnologie zorgde voor de grote vlucht die biometrie kon maken. Dit begon met de automatisering van het proces van de vergelijking van vingerafdrukken voor de politie.
Bij veel vormen van biometrie (zoals gezichtsherkenning, irisscan en vingerafdruk) spelen de disciplines beeldverwerking en patroonherkenning een belangrijke rol. Beeldverwerking is een rekenintensief proces, dat ook nog eens de beschikbaarheid van grote hoeveelheden computergeheugen vraagt. De onstuimige groei van het vak beeldverwerking wordt op twee fronten gesteund. Voor één à tweeduizend euro beschikken wij tegenwoordig over een rekenkracht die 20 jaar geleden was voorbehouden aan systemen met een prijs van 100 à 200 duizend euro. De enorm toegenomen rekenkracht maakt dat wij ons rekenmethoden (algoritmen) kunnen permitteren die complex zijn en toch binnen enkele minuten of zelfs seconden kunnen worden uitgevoerd. Tegelijkertijd heeft tientallen jaren van onderzoek ook werkelijk die complexere algoritmen opgeleverd die snelle en effectieve beeldinterpretatie dichterbij brengen. Waardoor de complexe beeldinterpretatie inderdaad “klaar is terwijl u wacht”, zodat u bij de grenspassage met biometrie ook echt tijdwinst boekt.
De ontwikkeling van computernetwerken maakt het ten slotte mogelijk dat systemen vanuit centrale databases met biometrische gegevens up to date worden gehouden, gesignaleerde incidenten kunnen worden doorgegeven.

Stand van zaken
Biometrie wordt voor uiteenlopende toepassingen waar de identiteit een rol speelt, gebruikt. Het meest bekend zijn wellicht de invoering van biometrie in het paspoort en de snelle grenspassage op Schiphol (“Privium”). Biometrie wordt gebruikt voor toegangscontrole, zoals bij beveiligde ruimtes. Attractieparken, zwembaden, sportscholen en dierenparken gebruiken soms biometrie om te voorkomen dat bezoekers toegang krijgen op het abonnement van een ander. Soms is ook de overweging om de bezoekers “uit de anonimiteit te halen”. Door de bezoekers uit de anonimiteit te halen, wordt ongewenst gedrag tegengegaan. In winkelcentra wordt met gezichtsherkenning geëxperimenteerd om winkelverboden te handhaven. Een moderne variant van de portier die je begroet als je in Londen een warenhuis binnengaat.
Sommige overheden gebruiken biometrie om dubbele aanmeldingen binnen hun databases op te sporen. Zo is in de Verenigde Staten met behulp van vergelijking van de pasfoto’s een groot aantal dubbele aanvragen van rijbewijzen opgespoord, waarmee grootschalige fraude met uitkeringen kon worden aangepakt. In Europa wordt vingerafdrukvergelijking gebruikt om dubbele asielaanvragen te voorkomen.
Na de grootschalige toepassingen, zoals in het paspoort, breken nu de kleinschalige toepassingen in bedrijven, zorginstellingen en zelfs bij particulieren door. Zo koop je nu voor enkele tientjes een met vingerafdruk beveiligde USB geheugenstick. En voor pakweg 100 Euro koop je een apparaatje dat op basis van je vingerafdruk het elektronische deurslot bedient. Een waarschuwing is hierbij wel op zijn plaats. De kans dat je onterecht de toegang tot je eigen huis wordt geweigerd, is zeker niet denkbeeldig. Het is altijd verstandig voor een goed alternatief te zorgen. Dus, gooi uw sleutel niet weg, zodat u om 2 uur ’s nachts niet voor uw eigen gesloten voordeur staat!

Niet alleen voor mensen
Hoewel biometrie vooral bij mensen wordt toegepast, kunnen sommige technieken ook voor dieren een rol spelen. Zo worden voorbeelden beschreven van het herkennen van koeien op basis van herkenning van hun netvlies. Een techniek om in de toekomst wellicht fraude met dieren te voorkomen. Ook wordt biometrie toegepast om het individuele gedrag van bedreigde dieren te bestuderen. Daarbij kan gebruik worden gemaakt van speciale technieken, zoals het vlekkenpatroon op de huid bij bepaalde haaiensoorten.

Toekomstblik
De ontwikkelingen gaan hard en het einde is nog niet in zicht. Een belangrijke nieuwe ontwikkeling is de driedimensionale gezichtsherkenning. Omdat een meer ruimtelijk plaatje van het gezicht wordt opgenomen, wordt gezichtsherkenning nu minder afhankelijk van toevallige belichtingsverschillen, zoals schaduwen op het gezicht. De verwachtingen van deze nieuwe techniek zijn hoog gespannen. De systemen die momenteel verkrijgbaar zijn hebben nog zo hun beperkingen, zoals overgevoeligheid voor brillen, baarden en snorren.
Een andere aanpak om gezichtsherkenning nauwkeuriger te maken is het inzoomen op details, zoals de textuur van de huid. Mede door deze laatste aanpak worden de laatste tijd aanmerkelijke verbeteringen in de prestaties bereikt.

Bij vingerafdruksystemen tekent zich een trend af om niet alleen naar het oppervlak van de vinger te kijken, maar ook een stukje dieper, zodat technieken om vingers na te maken geen kans meer krijgen. Ook deze trend is nog in volle gang. De eerste systemen met een dergelijke aanpak zijn op de markt verschenen.
Wij noemden al eerder het gebruik van aderpatronen in vinger of hand. Ook binnen het netvlies (retina) is een dergelijk aderpatroon waar te nemen. Retinascan heeft lang gegolden als een methode voor James Bond achtige toepassingen, maar ook op dit gebied is weer enige ontwikkeling te zien.
Spectaculair is de trend om irisscan vanaf enkele meters afstand te kunnen toepassen, waardoor ook de film Minority Report meer waarheidsgehalte krijgt.
En om een sciencefictionachtige blik op de toekomst te werpen: mogelijke kandidaten zijn “herkenning op basis van loopgedrag”, “geur” en DNA. Waarbij de eerste twee nog vooral een technische uitdaging zijn en de laatste om een extra bezinning over privacy aspecten vraagt.

Slotwoord
Iedereen krijgt zonder twijfel op grote schaal te maken met de toepassing van biometrie in de dagelijkse praktijk, zowel in de zakelijke markt als in (de top van) de consumentenmarkt.
Voor de beveiliging van bedrijven, zorginstellingen en zelfs woningen zal biometrie de komende jaren een steeds grotere rol gaan spelen. Dat is dan waarschijnlijk als onderdeel van steeds intelligentere systemen voor alarmverificatie en toegangsbeheer, in combinatie met intelligente camera's en RFID (radio frequency identification – identificatie met behulp van radiogolven, red). Aanvankelijk gaat het vooral om beveiliging via vingerafdrukherkenning, bij een komende prijsdaling ook de irisscan.
In winkelcentra en op bedrijfsterreinen wordt steeds vaker met gezichtsherkenning geëxperimenteerd. Deze techniek moet echter voor een grootschalige toepassing nog beduidend betrouwbaarder worden. Wellicht dat sommige bedrijven die veel last hebben van diefstal en hinder van ongewenste personen, hun toevlucht gaan zoeken in toegang op basis van (biometrische) identiteit.
In de privé-sfeer heeft beveiliging van elektronische transacties een grote potentie, mits systemen voldoende kunnen worden beveiligd en werken met nagemaakte vingers kan worden uitgesloten. Ook biometrische sloten lijken kansrijk als de sensoren nog betrouwbaarder worden.
Binnen Nederland is het Nederlands Biometrie Forum (NBF) actief. Het NBF is een netwerk organisatie voor zowel de afnemers als de gebruikers van biometrie. Participanten worden geïnformeerd tijdens strategische bijeenkomsten en op de website (www.biometrieforum.nl) Recent heeft het NBF een brochure uitgegeven over verantwoorde toepassing van biometrie.
Nadere informatie is te verkrijgen via de website.

Nieuw lid van bestuur

Pieter Arends

Mijn naam is Pieter Arends en sinds juni (!) 2006 ben ik lid van (het bestuur van) VIAS
Ik werk al erg lang (sinds 1986) bij het ministerie van LNV in diverse functies bij verschillende onderdelen. Sinds november 2004 werk ik bij de dienst ICT-uitvoering als hoofd van de afdeling Projectmanagement, Consultancy en Testservices en als lid van het MT. Ik ben 56 jaar en zit ondanks mijn opleiding Werktuigbouwkunde (HTS) nagenoeg mijn hele loopbaan al in de ICT. ICT is dan ook een rode draad door al mijn functies bij LNV en dan vooral het *gebruik* van ICT.
Door dat feit werd geleidelijk ook mijn belangstelling voor ICT-toepassingen in de agrarische sector gewekt. Toen het VIAS-bestuur met de vraag kwam of LNV zich ook op VIAS-bestuursniveau zou kunnen inzetten, heb ik na enig nadenken met plezier bedacht dat ik dat zelf wel wilde. En tot dusverre met plezier. Een interessant symposium meegemaakt en een veelheid aan thema's die ik binnen LNV tot dusverre nog niet tegenkwam. Een verrijking dus.
En wie weet wat ik zelf nog kan inbrengen!

Pieter Arends
Hoofd Projectmanagement, Consultancy & Testservices
Dienst ICT-Uitvoering
Laan van Nieuw Oost Indie 125
Postbus 20401
2500 EK Den Haag
tel 070-3785385