Technieken voor biometrische identificatie

Hoge eisen maken multi-modale biometrie noodzakelijk

Vanaf 26 oktober 2005 moeten bezoekers aan de Verenigde Staten een paspoort met biometrische kenmerken tonen, zelfs als men afkomstig is uit een land waarvoor geen visumplicht geldt. Voor identificatie-algoritmen zijn geschikte kenmerken nodig die maximaal onderscheid opleveren.

Asker M. Bazen

Biometrie is automatische herkenning van personen aan de hand van gemeten lichaamskenmerken of gedrag. De bekendste voorbeelden van biometrie zijn vingerafdrukherkenning, gezichtsherkenning en irisscan. Daarnaast worden ook handgeometrie, sprekerherkenning, schrift- of handtekeningherkenning en de manier van lopen (*gait*) gebruikt of onderzocht. Een andere, relatief nieuwe vorm van biometrie is herkenning van handdrukpatronen, die in prototypepistolen worden toegepast om deze op een transparante manier te beveiligen tegen ongeoorloofd gebruik.

Biometrie is een opkomende markt met een groot commercieel perspectief. De markt wordt gestuurd door de vraag naar meer veiligheid (alleen toegang voor de juiste personen), meer efficiëntie (automatische identificatie) en gebruiksgemak (minder pasjes en (pin)codes). De markt wordt voornamelijk gestimuleerd door internationale overheidsinitiatieven – het US-Visit-programma als reactie op de aanslagen van 11 september 2001, biometrische paspoorten, immigratie, et cetera, maar ook door andere sectoren. De International Biometric Group voorspelt dat de markt voor biometrie groeit van $ 719 miljoen in 2003 naar $ 4.6 miljard in 2008.[1]

Biometrie is nog niet uitontwikkeld. Voor veel toepassingen is de biometrische herkenningsprestatie nog niet goed genoeg, en is er nog veel onderzoek nodig om de prestaties te verbeteren.

Basisprincipes

Als er twee biometrische metingen aan een persoon worden gedaan, zullen deze nooit exact overeenkomen, terwijl biometrische metingen van verschillende personen sterk op elkaar kunnen lijken. Twee foto's van hetzelfde gezicht kunnen bijvoorbeeld verschillend zijn in belichting of gezichtsuitdrukking. Foto's van twee broers of zussen kunnen weer erg op elkaar lijken. Om personen toch te kunnen herkennen, moet een biometrisch systeem op een slimme manier bepalen of er voldoende overeenkomst is tussen twee metingen. Dit gebeurt door gebruik te maken van de karakteristieke kenmerken van een meting, de *featurevectoren*. De grote uitdaging bij de ontwikkeling van algoritmen voor biometrische herkenning is, geschikte featurevecto-

1. Zie www.biometricgroup.com/reports/public/market_report.html

Samenvatting

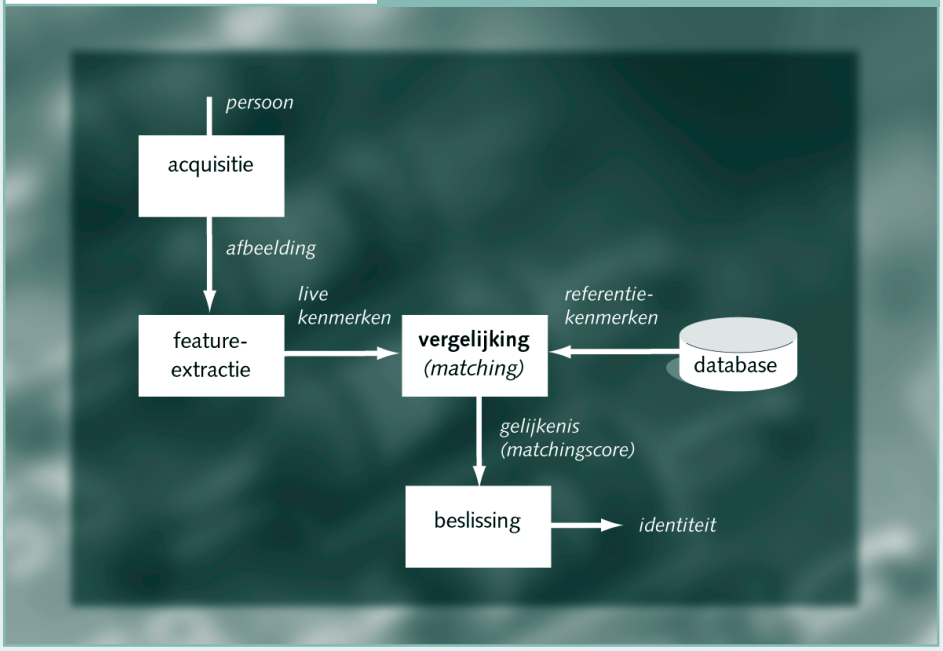
Een biometrisch systeem vergelijkt twee metingen van persoonskenmerken. Hierbij worden opgeslagen kenmerken gematcht met een *live* meting. Voor verificatie, identificatie en vergelijking met een zwarte lijst wordt biometrie ingezet bij beveiliging, verhoogde efficiëntie en groter gebruiksgemak. Metingen aan één persoon vertonen altijd variaties.

ren te vinden waarin de kenmerken vertegenwoordigd zijn die maximaal onderscheidend zijn. Het proces van biometrische herkenning is beschreven in figuur 1. De database is gevuld met biometrische referentiemetingen (sjablonen) die zijn opgeslagen tijdens een registratieprocedure (*enrollment*). Bij herkenning maakt een sensor (bijvoorbeeld een camera) een live meting van biometrische gegevens van een persoon. Hieruit worden de karakteristieke kenmerken bepaald (*feature-extractie*), die worden vergeleken met referentiekenmerken uit de database. De uitkomst van de vergelijking (matching) is een matchingscore, die de mate van overeenkomst weergeeft. Als de matchingscore boven een drempelwaarde ligt, wordt de persoon herkend, als die eronder ligt, niet.

Ondanks goede kenmerkenextractie kunnen de scores van echte gebruikers en indringers niet altijd door een drempel worden gescheiden. (Zie hierover ook het artikel van Bert Snel in dit nummer.) Twee featurevectoren van dezelfde persoon kunnen veel van elkaar afwijken, wat een lage matchingscore oplevert en tot een foute verwerping leidt (*false rejection rate*: frr). Ook kunnen metingen van verschillende personen veel op elkaar lijken, wat een hoge matchingscore geeft. De kans op foute acceptatie wordt *false acception rate* (far) genoemd.

Door de drempel in te stellen, kunnen foutkansen worden afgestemd op de toepassing. In een *high-securitytoepassing* wordt een hoge drempel gekozen. Hierdoor is een hoge mate van overeenkomst tussen de live meting en het in de database opgeslagen sjabloon nodig, wat een laag aantal foute acceptaties oplevert. Een nadeel is dat het aantal foute verwerpingen hierbij hoger wordt, oftewel de kans dat een rechtmatige gebruiker nogmaals moet proberen herkend te worden. Als gebruiksgemak een belangrijkere eis is dan hoge veiligheid, kan de keuze vallen op een lage drempel. Hierbij worden personen gemakkelijk her-

Stroomschema biometrie 1



kend, maar wordt de kans groter dat personen onterecht worden toegelaten.

Typen systemen

Biometrische systemen kunnen worden toegepast met verschillende doelen, die elk verschillende eisen stellen aan de biometrie.

- Als beveiliging het doel is, is het van belang de identiteit van een persoon met zekerheid vast te stellen. Een belangrijke eis is dan een laag aantal foute acceptaties.
- Als het doel verhoogde efficiëntie is, is het voornamelijk van belang een identiteitscontrole te automatiseren. Hierbij is een laag percentage valse afwijzingen een belangrijke eis.
- In geval van gebruiksgemak worden kaarten of wachtwoorden vervangen door biometrie. Als niet alleen het wachtwoord maar ook de kaart wordt vervangen, is het van belang zowel een extreem laag aantal foute acceptaties als een laag aantal foute verwerpingen te hebben.

Biometrie kan in verschillende *modes* werken: verificatie, identificatie en zwarte lijst (*watch list*). Bij alle modes wordt er eerst geregistreerd, waarbij referentie-opnamen van geregistreerde gebruikers worden gemaakt, en de hieruit geëxtraheerde sjablonen in een database worden opgeslagen.

Verificatie

Verificatie is de eenvoudigste vorm van biometrische herkenning. In dit verband spreekt men wel van één-tegen-éénmatching (1:1). De gebruiker geeft aan wie hij is, bijvoorbeeld door een *smart card* of gebruikersnaam in te voeren, en deze informatie wordt gebruikt om zijn referentiesjabloon uit de database te halen. Dan wordt er een nieuwe biometrische opname van de gebruiker gemaakt. Deze wordt gebruikt om de identiteit van de gebruiker te verifiëren door hem met het referentiesjabloon te vergelijken.
In een verificatiesysteem kan gekozen worden tussen een centrale database of een gedistribueerde database, bijvoorbeeld door de biometrische sjablonen op te slaan op smart cards die de gebruikers zelf meenemen. Uit privacy-overwegingen heeft deze laatste oplossing de voorkeur: de biometrische data zijn alleen beschikbaar wanneer de gebruiker dat zelf wil.

Identificatie

In een identificatiesysteem, ook wel één-tegen-veelmatching (1:n) genoemd, hoeft een gebruiker geen identiteit te claimen. In plaats daarvan maakt het systeem alleen een biometrische meting van de persoon en wordt deze meting vergeleken met alle entry's in de database. Zodra er een matchend sjabloon wordt gevonden, identificeert dit de gebruiker. Het voordeel van identificatie ligt vooral in de gebruiksvriendelijkheid. Gebruikers hoeven niet langer een kaart mee te nemen of een gebruikersnaam in te typen. Daar staat tegenover dat de herkenning voor het biometrische systeem veel moeilijker wordt. Door toenemende foutkansen en rekentijd is het doorzoeken van grote databases problematisch. Een algoritme dat 10 ms duurt en een percentage foute acceptaties heeft van 0,01%, kan bijvoorbeeld niet worden toegepast om een database met 10.000 entry's te doorzoeken. De zoektijd loopt dan namelijk op tot 100 seconden, en het percentage foute acceptaties loopt op tot 63%. Beide waarden zijn onacceptabel voor een toepassing zoals bijvoorbeeld toegangscontrole. Om databases van deze omvang betrouwbaar en snel te kunnen doorzoeken, zijn snellere en nauwkeurigere algoritmen nodig.

»Personen op een zwarte lijst werken niet mee aan een goede biometrische opname«

Zwarte lijst

Een zwartelijstsysteem bevat een lijst met biometrische kenmerken van personen die gedetecteerd moeten worden. Dit kunnen bijvoorbeeld personen zijn die geen toegang mogen krijgen tot een ruimte of dienst. Omdat deze personen niet zullen meewerken, moet gebruik worden gemaakt van identificatie. Daarnaast is het ook moeilijker om een goede biometrische opname te maken. Hierdoor is deze applicatie moeilijker dan identificatie vanuit een biometrisch standpunt. Daarnaast is ook de rol van de foutkansen omge-

draaid. Nu betekent een gemiste detectie een veiligheidsrisico, terwijl een vals alarm ongemak veroorzaakt. Er moet dus gefocust worden op een laag aantal gemiste detecties, terwijl gebruikers juist hun best doen om dit aantal te verhogen.
Een nog moeilijkere vorm van zwarte lijst is biometrische surveillance, waarbij de biometrische opname van een afstand wordt gemaakt. Hierbij kunnen alleen biometrieën zoals gezichtsherkenning worden gebruikt. Een andere vorm van biometrie in surveillancetoepassingen is anonieme biometrie: personen worden geregistreerd en geïdentificeerd uit surveillancebeelden, waardoor personen kunnen worden gevolgd zonder koppeling aan een identiteit. Biometrische surveillance is nog niet goed haalbaar, tenzij gebruik wordt gemaakt van uitermate goed geconditioneerde omstandigheden.

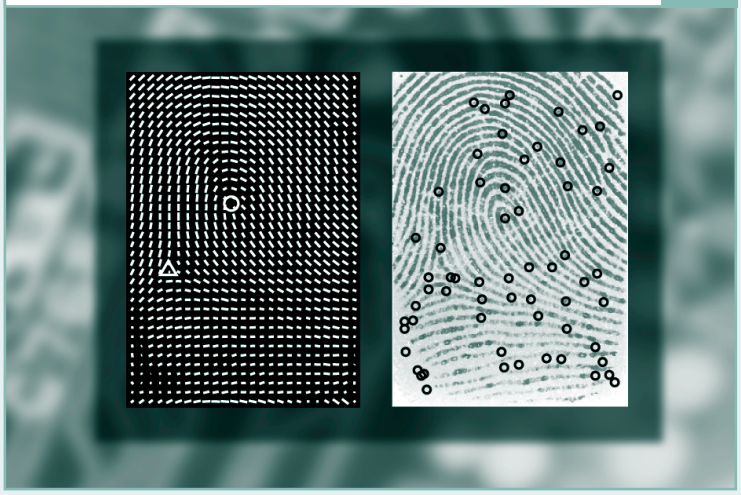
Gezichtsherkenning

Door het gebruiksgemak is gezichtsherkenning een aantrekkelijke kandidaat voor biometrische herkenning van personen. De herkenning zou zelfs transparant kunnen plaatsvinden, dat wil zeggen zonder expliciete actie van de gebruiker, zoals het geven van een vingerafdruk of het kijken in een iriscamera. In de praktijk is de techniek echter nog niet zo ver gevorderd dat dit echt mogelijk is.
Het grote probleem bij gezichtsherkenning vormen de variaties tussen verschillende afbeeldingen van hetzelfde gezicht, zoals expressie (gezichtsuitdrukking), haarstijl, baard, belichting, pose (houding), resolutie, occlusie (gedeeltelijke afdekking), enzovoorts.
Daarnaast kan veroudering een belangrijk probleem voor automatische gezichtsherkenning opleveren. Als een systeem dagelijks gebruikt wordt, kunnen de opgeslagen sjablonen eenvoudig worden bijgesteld om verschillen door veroudering te voorkomen. Maar bij gebruik in een biometrisch paspoort, dat vijf jaar meegaat zonder sjabloonbijstelling, kan de false rejection rate oplopen tot meer dan 50%.
Aan de andere kant kunnen afbeeldingen van verschillende gezichten juist erg op elkaar lijken. Het meest voor de hand liggende voorbeeld hiervan is een één-eïge tweeling (van wie juist wel de vingerafdrukken altijd verschillen). Maar ook andere familieleden of zelfs niet-verwante personen kunnen verbazingwekkend veel op elkaar lijken. Een voorbeeld hiervan is te zien in figuur 2. De vraag is hier: zijn dit drie verschillende dames, drie verschillende foto's van dezelfde dame of nog anders? Als je goed naar de details kijkt, is te zien dat de twee rechter foto's overeenkomen, terwijl de linker foto van een andere persoon afkomstig is.
Alle automatische gezichtsherkenningssystemen beginnen met de detectie van het gezicht. Hierbij wordt de positie en afmeting van het gezicht in de afbeelding gevonden. Daarna vindt registratie plaats, waarbij de afbeelding zo wordt verschoven, gedraaid en geschaald dat de gezichtskenmerken op exact de goede plek terechtkomen. Dan volgt de extractie van kenmerken die zo ongevoelig mogelijk zijn voor variaties tussen verschillende afbeeldingen van hetzelfde gezicht, maar tegelijkertijd onderscheid tussen verschillende gezichten versterken. Ten slotte worden de kenmerken vergeleken, wat leidt tot een herkenning.

Verschillende of gelijke dames? 2

Kenmerken van een gezicht: textuur en geometrie 3

Richtingsveld en minutiae van een vingerafdruk 4



Typen kenmerken

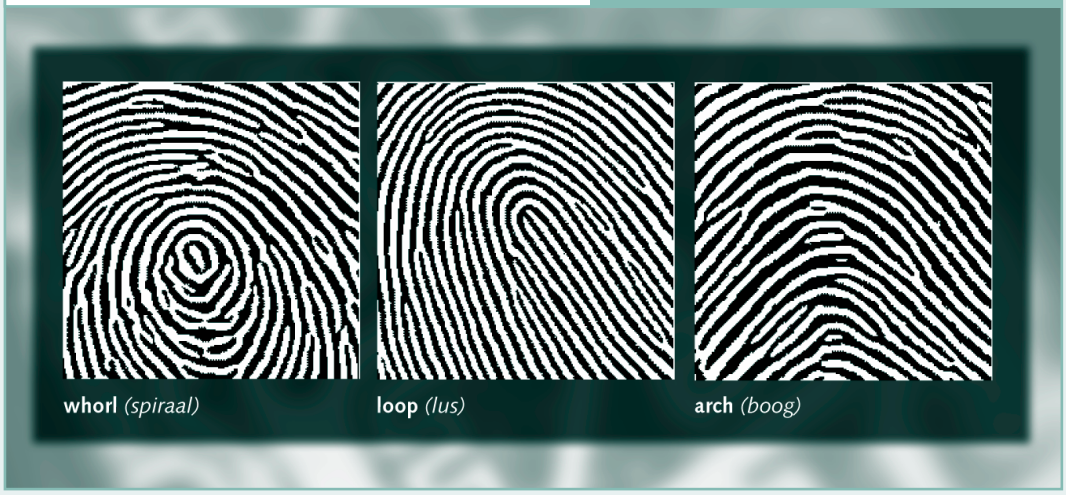
Er zijn twee typen kenmerken die gebruikt kunnen worden voor gezichtsherkenning. Het eerste type kenmerken maakt rechtstreeks gebruik van grijswaarden (textuur) in de afbeelding, zie de bovenste rij van figuur 3. De karakteristieke kenmerken worden hieruit gedestilleerd met Eigenfaces (Turk & Pentland, 1991) of Fisherfaces (Belhumeur e.a., 1997). Doordat dit meestal lineaire dimensiereductiemethoden zijn, is de matchingscore een soort gewogen som van het verschil in grijswaarden tussen de afbeeldingen. Het tweede type kenmerken is gebaseerd op de geometrie (vorm) van het gezicht, waarbij gebruik wordt gemaakt van de standaardgezichtskenmerken zoals de ogen, neus en mond (zie de onderste rij van figuur 3). Bij deze aanpak worden deze kenmerken eerst opgezocht, en wordt er een graaf van de kenmerken geconstrueerd. Een elastisch graafmatchingsalgoritme bepaalt daarna de overeenkomst tussen twee gezichten. Voor een betere herkenning is het ook mogelijk om beide typen kenmerken in een algoritme te combineren.

Driedimensionaal

Een nieuwe ontwikkeling in de gezichtsherkenning is het gebruik van driedimensionale scans. Deze worden opgenomen met stereovisie, laserscanners of *structured light*. Het voordeel van 3D-gezichtsherkenning is, dat het minder gevoelig is voor belichting en pose (Bowyer e.a.,2004). Het onderzoek naar optimale inzet van 3D-scans voor herkenning bevindt zich nog in een eerste fase.
De test die het beste overzicht van de huidige *state-of-the-art* in gezichtsherkenning geeft is de Face Recognition Vendor Test (FRVT) 2002 (Phillips e.a., 2003). FRVT 2002 was een uitgebreide evaluatie van technologie voor automatische gezichtsherkenning. Het belangrijkste doel van FRVT 2002 was prestatiematen te leveren die de mogelijkheden van automatische gezichtsherkenningssystemen meten om aan *real world* eisen te voldoen.
Uit FRVT 2002 kan een aantal conclusies worden getrokken. De huidige gezichtsherkenningssystemen presteren het best wanneer ze binnen worden gebruikt, onder gecontroleerde lichtomstandigheden. In FRVT 2002 had het best presterende systeem onder deze condities een false rejection rate van 10%, bij een false acceptance rate van 1%. Bij gebruik buiten neemt de false rejection rate toe tot 50%. Daarnaast blijkt dat gezichtsherkenningssystemen nog niet goed kunnen omgaan met een zwartelijsttaak. Wanneer de zwarte lijst groter wordt, daalt de prestatie. Het beste systeem had een false reject rate van 23% bij een false alarm rate van 1%, voor een zwarte lijst met 25 personen. Bij een zwarte lijst met 300 personen steeg de false reject rate naar 31%. Ten slotte stijgt de false reject rate met vijf procent per jaar wanneer een live opname vergeleken wordt met een eerder opgenomen sjabloon.
Een aantal bedrijven werkt serieus aan een degelijke technologie voor gezichtsherkenning. Er zijn echter ook partijen die de huidige stand van de techniek te positief voorspiegelen en gezichtsherkenning al te gemakkelijk als panacee voor alle problemen promoten. Doordat gezichtsherkenning nog niet voldoende robuust is voor betrouwbare grootschalige toepassing, liggen de haalbare toepassingen vooral in *low-security* toegangscontrole met kleine groepen gebruikers.

»Sommigen promoten gezichtsherkenning te gemakkelijk als panacee voor alle problemen«

Henry-klassen: whorl, right loop en arch 5



Vingerafdrukherkenning

Terwijl vingerafdrukken traditioneel met behulp van papier en inkt werden genomen en de vergelijking van twee afdrukken door forensische experts werd gedaan, kan dit nu ook automatisch gebeuren. Een vingerafdruk wordt digitaal opgenomen met een elektronische sensor die aan een computer is gekoppeld. Hiervoor wordt bijvoorbeeld een optische of capacitieve meting aan het oppervlak van de vingertop gedaan, wat over het algemeen leidt tot een 8-bits-grijswaardenplaatje van ongeveer 500 bij 500 pixels op een resolutie van 500 dpi. Sommige fabrikanten van moderne sensoren claimen daarnaast ook de mogelijkheid te bieden om te testen of er een echte, levende vinger wordt gebruikt. In de praktijk blijken deze methoden echter nog gemakkelijk te misleiden (Van der Putte & Keuning, 2000).

De top van de vinger bestaat uit zogenaamde *ridges* en *valleys*, ofwel berg- en dalstructuren. In een vingerafdruk zijn deze te zien als zwarte en witte lijnstructuren. Een vingerafdruk kan op verschillende niveaus van detail worden beschreven. Een globale beschrijving van de vorm van de afdruk wordt gegeven door het richtingsveld: de richting van de lijnen op elke plaats in de afdruk.

Het tweede niveau van detail wordt gegeven door de *minutiae*. Dit zijn de splitsingen en eindpunten van de lijnen die de lokale details van de vingerafdruk beschrijven. Deze worden het meest gebruikt in automatische vingerafdrukherkenning. Het meeste detail is te vinden in het oorspronkelijke grijswaardenplaatje. Het richtingsveld en de minutiae zijn te zien in figuur 4.

Gelijkenis

Net als bij elke andere biometrie, is ook bij vingerafdrukherkenning het grootste probleem dat twee afdrukken van dezelfde vinger nooit exact aan elkaar gelijk zijn. Een eerste oorzaak hiervan is samen te vatten in de beeldkwaliteit. Er kunnen vuil en (tijdelijke) krassen op de vinger zitten, er is meetruis in de sensor en de weersomstandigheden kunnen voor slechte afdrukken zorgen. Daarnaast hebben sommige personen hoe dan ook slechte afdrukken, bijvoorbeeld doordat ze afgesleten zijn door gebruik van de vingers, of doordat ze (genetisch veroorzaakte) ondiepe afdrukken hebben. In deze gevallen is het zelfs voor een expert nauwelijks mogelijk om aan te geven hoe de lijnen precies lopen.

Een tweede oorzaak is dat de vinger elke keer net iets anders op de sensor wordt gelegd, waardoor er een ander gedeelte van de afdruk wordt opgenomen. Hierdoor kunnen afdrukken slechts gedeeltelijk overlappen. Ten derde heeft het systeem te maken met rotaties, translaties en schaling van de afdrukken.

Het laatste probleem is de aanwezigheid van elastische niet-lineaire vervormingen tussen twee afdrukken. Deze worden veroorzaakt door het opnameproces zelf. Tijdens dit proces wordt het bolle, elastische, driedimensionale elastische oppervlak van de vinger platgedrukt op de sensor. Dit platdrukken gebeurt iedere keer anders, afhankelijk van bijvoorbeeld de druk en het schuiven en draaien van de vinger tijdens het maken van de opname. Dit komt vooral voor wanneer onwillige gebruikers expres veel kracht toepassen om herkenning te voorkomen.

Door deze problemen kunnen plaatjes van vin-

gerafdrukken niet rechtstreeks vergeleken worden, maar wordt er gebruikgemaakt van kenmerken die hier meer invariant voor zijn, zoals het richtingsveld en de minutiae.

Minutiae matchen

Zoals gezegd maken de meeste automatische systemen voor automatische vingerafdrukherkenning gebruik van minutiaematching. Eerst doorloopt het plaatje een zogenaamd *enhancementproces*, waarin de vingerafdruk wordt 'opgepoetst' met behulp van beeldbewerkingstechnieken. Het doel is het onderdrukken van ruis, het corrigeren van beschadigingen en het duidelijker maken van de ridge-valleystructuren. Daarna wordt het plaatje van grijswaarden omgezet in zwart-wit, waarna de minutiae eenvoudig kunnen worden gevonden.
Daarna volgt de daadwerkelijke minutiaematching. Eerst wordt de optimale registratie tussen de twee minutiaesets geschat. De meeste methoden maken hierbij gebruik van een rigide registratie die bestaat uit translatie, rotatie en schaling, maar het is ook mogelijk om een niet-lineaire registratie te gebruiken die compenseert voor elastische vervormingen. De tweede stap is bepaling van de matchingscore door het aantal overeenkomende minutiae te tellen. Door onvolkomenheden in de minutiae-extractie en de elastische vervormingen zullen gelijke minutiae niet precies op elkaar vallen. Daarom wordt er gekeken in een tolerantiegebied rond elke minutia. Er kunnen ook minutiae van niet-overeenkomstige afdrukken binnen deze gebieden vallen, waardoor sommige vingerafdrukken ten onrechte worden geaccepteerd. Een uitgebreide beschrijving van minutiaematchingalgoritmen is te vinden in Bazen & Gerez (2003).
Het is ook mogelijk om vingerafdrukken te vergelijken aan de hand van de globale vorm. Dit wordt vooral toegepast in identificatiesystemen, om het zoekproces wat efficiënter te laten verlopen. De vormen worden opgedeeld in Henry-klassen (Henry, 1900) (zie figuur 5) en alleen afdrukken met gelijke klasse worden vergeleken. Deze methode heeft twee nadelen. Ten eerste valt 90% van alle vingerafdrukken in slechts drie klassen, waardoor gemiddeld nog steeds 30% van de database wordt doorzocht. Ten tweede bestaat de kans op foute classificaties, waardoor de juiste afdruk zeker niet wordt gevonden.
Een alternatief is het vergelijken van vormen zonder deze in discrete klassen op te delen (Bazen & Veldhuis, 2004). Dit heeft twee voordelen ten opzichte van traditionele classificatie. Ten eerste komen er nu geen classificatiefouten voor doordat bepaalde vormen op klassengrenzen liggen. Ten tweede bestaat er, ook binnen een Henry-klasse, een maat die de overeenkomst in vorm aangeeft, waardoor niet alle afdrukken van dezelfde klasse ook geschikte kandidaten zijn. Identificatie kan nu worden gedaan door de afdrukken in de database eerst te sorteren op overeenkomst in vorm, en daarna de minutiae in deze volgorde te vergelijken, tot de juiste vingerafdruk is gevonden.
De foutkansen van vingerafdrukherkenning zijn veel lager dan die van gezichtsherkenning. Vooral een lage false acceptance rate is goed haalbaar. Het blijft een uitdaging om ook in slechte omstandigheden een lage false rejection rate te halen. De recentste grote test is de Fingerprint Vendor Technology Evaluation (FpVTE) 2003 (Wilson e.a., 2004). Deze test, die operationele data afkomstig van diverse Amerikaanse overheidsinstanties gebruikte, laat zien dat het best presterende systeem een percentage gemiste detecties van 0,6% haalt bij een percentage valse acceptaties van 0,01%.
Er zijn veel aanbieders van vingerafdrukherkenning actief op de markt. De grotere partijen richten zich met vooral op grote *afis*-systemen (*automatic fingerprint identification system*), waarbij forensische databases semi-automatisch worden doorzocht. Daarnaast worden ook veel vingerafdrukverificatiesystemen aangeboden voor toegangscontrole. Hierbij richten veel aanbieders zich op een combinatie van biometrie en smart cards.

Multi-modale biometrie

Om de biometrische herkenningsscores te verbeteren kan gebruik worden gemaakt van multimodale biometrie. Hierbij wordt de herkenning gedaan op basis van een combinatie van verschillende biometrische metingen. Er kunnen verschillende typen metingen worden gecombineerd:

- Verschillende typen kenmerken van één biometrie, bijvoorbeeld minutiae en vorm bij vingerafdrukherkenning.

• Verschillende gelijke biometrische modaliteiten, bijvoorbeeld twee verschillende vingerafdrukken, zoals gebruikt in het biometrische paspoort.
• Verschillende biometrische modaliteiten, bijvoorbeeld vingerafdruk en gezicht, zoals gebruikt in het biometrische paspoort.

Multi-modale biometrie kan ten eerste zorgen voor lagere foutkansen door combinatie van matchingscores: de kans dat zowel het gezicht als de vingerafdruk van een indringer voldoende lijkt, is veel lager dan de kans dat een van beide voldoende lijkt. Ten tweede is een multi-modaal systeem veel robuuster tegen false rejection. Als een vingerafdruk van onvoldoende kwaliteit is, zal deze ten onrechte worden afgewezen. Maar dan is er nog een tweede biometrie aanwezig als back-up. Ten derde kan multi-modale biometrie een belangrijke rol spelen bij identificatie en zwartelijstsystemen. Naast het grote belang van lage foutkansen kunnen de verschillende modaliteiten ook worden gebruikt om een database snel te doorzoeken. Naarmate de eisen aan biometrische herkenning hoger worden, zal multi-modale biometrie een steeds grotere rol spelen.

Literatuur

Bazen, A.M. & R.N.J. Veldhuis (2004). Likelihood ratio-based biometric verification. *IEEE Trans. Circuits and Systems for Video Technology*, 14(1):86–94, januari 2004.

Bazen, A.M. & S.H. Gerez (2003). *Fingerprint matching by thin-plate spline modelling of elastic deformations. Pattern Recognition*, 36(8):1859–1867, augustus 2003.

Belhumeur, P.N., J.P. Hespanha & D.J. Kriegman (1997). Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. *IEEE Trans. PAMI*, 19(7):711–720, juli 1997.

Bowyer, K.W., K. Chang & P.J. Flynn (2004). A survey of approaches to 3d and multi-modal 3d+2d face recognition. In: *Proc. ICPR 2004*. Cambridge, UK, augustus 2004.

Henry, E.R. (1900). *Classification and Uses of Finger Prints*. Londen: Routledge.

Maio, D., D. Maltoni, R. Cappelli, J.L. Wayman & A.K. Jain (2004). Fvc2004: Third fingerprint verification competition. In: *Proc. Int. Conf. on Biometric Authentication (ICBA04)*, pages 1–7, Hong Kong, juli 2004.

Phillips, P.J. et al. (2003). *FRVT 2002: Overview and summary. Technical report, March 2003*. Available from www.frvt.org.

Putte, T. van der, & J. Keuning (2000). Biometrical fingerprint recognition: Don't get your fingers burned. In: *Proc. CARDIS 2000*.

Turk, M. & A. Pentland (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1):71–86, 1991.

Wilson, C. et al. (2004). FpVTE 2003 summary of results. *Technical Report NISTIR 7123, NIST*, 2004. Available from fpvte.nist.gov.

Dr.ir. Asker M. Bazen
is post-doctoraal onderzoeker elektrotechniek aan de Universiteit Twente. E-mail: a.m.bazen@utwente.nl.