



LaCie SAFE-harddrive

Wat is biometrie?

De term heeft betrekking op het opkomende technologische vakgebied dat zich bezighoudt met de identificatie van individuen middels biologische kenmerken. Biometrisch geautomatiseerde herkenningmethoden meten fysieke of gedragsmatige kenmerken van individuen. Algemene biometrische lichaamskenmerken zijn onder meer vingerafdrukken, hand- of handpalmgeometrie en netvlies-, iris- of gezichtskenmerken. Gedragskenmerken zijn onder meer de handtekening, de stem (die tevens een fysieke component omvat), toetsaanslagpatronen en manier van lopen. Binnen dit type biometrie zijn de technologieën voor handtekening en stem het verst ontwikkeld.



Biometrie gebaseerd op vingerafdrukken zoekt naar minutiae, de punten van een vingerafdruk waar een richel eindigt of zich splitst.

Wat is vingerafdrukherkenning?

Vergelijken van vingerafdrukken is verreweg de succesvolste biometrische technologie vanwege het gebruiksgemak, het non-invasieve karakter en de betrouwbaarheid ervan. Vingerafdrukken bestaan uit richels en dalen in een complex patroon dat voor elke persoon uniek is. Hierdoor bieden zij een optimale verificatiemethode. Niet elke richel wordt gescand. Bij de biometrie van vingerafdrukken wordt gekeken naar 'minutiae': de punten in een vingerafdruk waar een richel eindigt of zich splitst. Een algoritme haalt de meest veelbelovende minutiaepunten uit een beeld en maakt vervolgens een sjabloon aan, meestal ongeveer 250 tot 1000 bytes groot.

Bij de registratie (inschrijving) wordt de plaats van de minutiaepunten bepaald en wordt hun positie ten opzichte van elkaar en hun richting opgeslagen. Deze gegevens vormen het sjabloon - de informatie die later gebruikt wordt om een persoon te herkennen. In het matchingstadium wordt het binnenkomende vingerafdrukbeeld voorbehandeld en worden de minutiaepunten geëxtraheerd. De minutiaepunten worden vergeleken met het geregistreerde sjabloon en er wordt geprobeerd (binnen bepaalde grenzen) zoveel mogelijk gelijke punten te lokaliseren. De uitslag van het matchen is meestal het aantal overeenkomende minutia. Vervolgens wordt een drempel toegepast waarmee bepaald wordt hoe groot dit aantal moet zijn om een match te hebben tussen de vingerafdruk en het sjabloon.

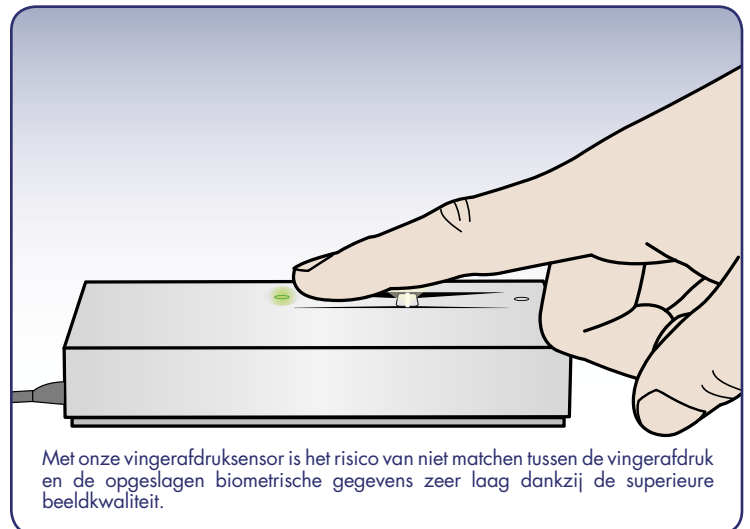
Vingerafdrukverificatie is heel geschikt voor apparaten met toegangsregeling. Deze biometrietechnologie is gebruiksvriendelijk en zeer geaccepteerd vergeleken met andere identificatietechnologieën. Vingerafdrukverificatie heeft ook een lagere foutincidentie vergeleken met andere biometrische oplossingen.

Welk type biometrische technologie wordt er gebruikt in de SAFE-drive?

De LaCie SAFE Mobile Harddisk bevat actieve vingerafdrukdetectietechnologie. Elke sensorcel (pixel) bevat een actieve capacitieve feedbackschakeling waarvan de effectieve feedbackcapaciteit gemoduleerd wordt door de aanwezigheid van levende huid dichtbij het oppervlak van de sensor. De sensor kan bijvoorbeeld geen vingerafdruk van een overleden persoon matchen. In tegenstelling tot optische sensors met panelen zijn capacitieve sensors - ook wel 'solid state' genoemd - moeilijk te imiteren. 'Solid state'-technologie maakt het mogelijk de verandering in elektrische huidcapaciteit van een vinger te meten. Als u bijvoorbeeld op uw vingertop met inkt een lijn zou tekenen, dan is deze lijn in het 'solid state'-beeld niet te zien. 'Solid state'-technologie is gebaseerd op het meten van de vinger - niet het er naar kijken zoals dat bij optische detectie gaat.

De siliciumvingerafdruksensor geïntegreerd in de LaCie SAFE-drive produceert een volledig, schoon beeld rondom alle delen van de vinger die in contact komen met de sensor. Optische oplossingen kunnen beeldranden produceren die niet scherp zijn omdat sensors zich slechts op een klein gebied kunnen scherpstellen. Met onze vingerafdruksensor is het risico van niet matchen tussen de vingerafdruk en de opgeslagen biometrische gegevens zeer laag dankzij de superieure beeldkwaliteit.

De integratie van een langshaal-vingerafdruksensor beperkt het risico van fraude tot een minimum. Het is voor eindgebruikers zeer moeilijk om een vingerafdruk te kopiëren omdat de beweging van de vinger eventueel achtergelaten sporen ogenblikkelijk elimineert. Veel goedkope oplossingen kunnen worden omzeild door een eenvoudige fotokopie van een vingerafdruk. Sommige goedkope optische oplossingen hebben ook problemen met vingerafdrukken die achterblijven op de sensor door vette handen. Door het integreren van de vingerafdrukmatching-technologie in de hardware is de LaCie SAFE-harddrive een volledig op zichzelf staande drive die niet afhankelijk is van de hostcomputer om het vingerafdrukmatchen uit te voeren. Dit zorgt voor volledige draagbaarheid voor de gebruiker doordat het niet nodig is voor het gebruik stuurprogramma's te installeren op de hostcomputer.



Met onze vingerafdruksensor is het risico van niet matchen tussen de vingerafdruk en de opgeslagen biometrische gegevens zeer laag dankzij de superieure beeldkwaliteit.

Wat zijn de huidige toepassingen van biometrie?

Biometrische technologieën zijn bezig de basis te vormen voor een uitgebreid assortiment aan sterk beveiligde oplossingen voor identificatie en persoonsverificatie. Veel technologische apparatuur en systemen worden op dit moment uitgerust met biometrische oplossingen voor regeling van de toegang tot ruimtes, werkstations, netwerken en bepaalde softwaretoepassingen. Op zichzelf gebruikt of geïntegreerd met andere technologieën zoals smartcards, gecodeerde sleutels en digitale handtekeningen zal de biometrische technologie in de nabije toekomst zijn intrede doen in veel aspecten van de economie en ons dagelijks leven. Steeds meer consumentenelektronica producten bevatten biometrische identificatie, zoals sommige laptops, PDA's, mobiele telefoons en MP3-spelers.

Bronnen:

<http://www.biometrics.org/html/introduction.html>

<http://csrc.nist.gov/cryptval/des/tripledesval.html>

Zijn biometrische oplossingen echt nodig?

Tegenwoordig verzetten mensen zich over het algemeen niet tegen het gebruik van hun biologische kenmerken in plaats van een wachtwoord voor identificatie. In het dagelijks leven moeten mensen zoveel wachtwoorden onthouden (creditcards, toegangspoorten, regeling van de boordcomputer van de auto...) dat zij het makkelijker en sneller vinden om hun vingers over een paneel te halen dan een nieuw wachtwoord in te voeren en te onthouden. Het gebruik van biometrie voor persoonslegitimatie wordt steeds gemakkelijker in het gebruik ten opzicht van andere methoden (zoals wachtwoorden of smartcards).

Er is een trend in de richting van het centraliseren van identiteitsbeheer - het inzetten van een combinatie van zowel fysieke als logische toegangsparemeters voor het verkrijgen van toegang tot verschillende soorten hulpmiddelen. Veel bedrijven zijn tegenwoordig op zoek naar dit soort oplossingen voor identiteitsbeheer, waarvoor het gebruik van biometrie nodig is. Naarmate het aantal beveiligingsschendingen en zaken van transactiefraude toeneemt, wordt de noodzaak van sterk beveiligde identificatie en persoonslegitimatie steeds groter. Een behoefte aan biometrie bestaat bij landelijke zowel als plaatselijke overheden, in het leger en bij bedrijven. Bedrijfsoverkoepelende infrastructures van netwerkbeveiliging, overheidslegitimatie, veilig elektronisch bankieren, beleggen en andere financiële transacties, detailhandel, ordehandhaving, gezondheidszorg en sociale voorzieningen hebben op dit moment reeds baat bij deze technologie.

Is identificatie van biologische eigenschappen veilig en betrouwbaar?

In de beveiliging worden drie verschillende soorten legitimatie gebruikt: iets dat u weet (een wachtwoord, PIN), iets dat u bezit (een kaartsleutel, smartcard) of iets dat u bent (een biometrische eigenschap). Van deze voorbeelden is de biometrische eigenschapsidentiteit het veiligste en het makkelijkste legitimatiehulpmiddel. Hij kan niet geleend, gestolen of vergeten worden en namaken is praktisch onmogelijk. Ieder mens heeft zijn/haar eigen biologische identiteit die anders is dan die van alle anderen, wat de reden is waarom het moeilijk is dit soort gegevens te vervalsen. De betrouwbaarheid van biometrie wordt geïllustreerd door het feit dat veel staten ervoor kiezen om vingerafdrukken en gezichtsdigitalisering te gebruiken voor legitimatiebewijzen en visa om mensen zo beter te kunnen identificeren. Door gebruik van biometrische identificatie wordt het risico van vergeten wachtwoorden of omzeilen van gegevensstoe-gangscontrole uitgeschakeld.

LaCie, gevestigd in de Verenigde Staten, Europa en Azië, is de wereldleidende producent van met pc en Macintosh compatibele randapparatuur voor opslag. Via een gespecialiseerd dealernetwerk biedt LaCie innovatieve oplossingen voor professionals bij vele toepassingen (afbeeldingen, audio, video, webdesign, digitale fotografie, etc.) Wat LaCie onderscheidt is de kwaliteit en het ontwerp van de producten - originele creaties door ontwerpers zoals Philippe Starck, Porsche Design GmbH en Neil Poulton. LaCie is genoteerd aan de Nouveau Marché Parijs (code 5431).

