Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DBI Biometrie

Versie 1.0
31 maart 2022

Inhoud

1 Soorten Biometrie

Dit document is een bijlage bij het *Onderzoeksrapport Digitale Bronidentiteit*.

Er zijn verschillende biometrische modaliteiten beschikbaar, waarmee individuen kunnen worden onderscheiden. In het algemeen vallen biometrische modaliteiten in twee hoofdcategorieën:

- biologische kenmerken, bijvoorbeeld vingerafdruk, gezicht, iris, handpalm, hand (geometrie), oor (vorm), netvlies (aderpatroon), DNA, enz.
- aan gedrag gerelateerde kenmerken, bijvoorbeeld een toetsaanslagdynamiek, manier van lopen, handtekening, stem, enz. [3, p.123].

De relevantie van een biometrische modaliteit voor een specifieke toepassing (use-case) hangt af van de:

- eigenschappen van de biometrische modaliteit;
- onderliggende technologie.

Vanwege de uiteenlopende aard van biometrische toepassingen, voldoet waarschijnlijk geen enkele biometrische modaliteit optimaal aan de vereisten van alle use cases.

In veel gevallen kan een multimodaal biometrisch systeem dat meerdere biometrische kenmerken combineert of versmelt vereist zijn om het gewenste prestatieniveau te bereiken. Een voorbeeld hiervan is het zeer grootschalige Aadhaar-biometrische project in India dat alle 10 vingerafdrukken, beide irissen en gezicht gebruikt voor deduplicatie – en identificatiedoeleinden [2, p.8].

2 Voordelen en nadelen van biometrische modaliteiten

Op basis van de analyse uit de literatuur, is om uiteenlopende en specifieke redenen het merendeel van de biometrische modaliteiten niet geschikt voor implementatie in DBI:

1. te hoge implementatiekosten voor de handafdruk-modaliteit;
2. beperkt onderscheidend vermogen voor handgeometrie en oor;
3. vervuiling, gevoeligheid, snelheid, gegevensbescherming en privacy kwesties voor DNA;
4. gebruikersacceptatie, gegevensbescherming en privacy-kwesties voor netvlies modaliteit; en
5. beperkt onderscheidend vermogen en gevoeligheid voor omgevingsomstandigheden voor een spraak-modaliteit [2, p.8].

De inzetbare modaliteiten kunnen zijn: vingerafdruk, gezicht en iris (zie Tabel 1) [1, p.80-105 en 6]. De vingerafdruk, gezicht en irismodaliteiten worden grotendeels toegepast in een aantal soorten civiele, reis, wetshandhavings- en beveiligingstoepassingen vanwege hun eigenschappen [2, p.8].

Tabel 1:

Eigenschappen van een modaliteit	Vingerafdruk	Gezicht	Iris
Onderscheidend vermogen	Extreem	Groot	Extreem
Permanentie	Extreem	Beperkt	Extreem
Universaliteit	Zeer groot	Extreem	Zeer groot
Verzamelbaarheid	Zeer groot	Extreem	Zeer groot
Prestaties	Extreem	Groot	Extreem
Aanvaarding door de gebruiker	Zeer groot	Zeer groot	Groot
Robuustheid tegen presentation attack	Groot	Groot	Groot

2.1 Vingerafdruk-modaliteit

De vingerafdrukmodaliteit is zeer onderscheidend, het is zelfs mogelijk tweelingen te onderscheiden. Het is een robuuste tegenmaatregel voor *look-a-like* fraude. Vingerafdrukken zijn permanent, schaalbaar, interoperabel en breed geïmplementeerd maar ze zijn niet universeel.

Vingerafdrukken kunnen bij bepaalde groepen slecht of beschadigd zijn en kunnen leiden tot het niet vastleggen (*failure to capture*) van een steekproef of zelfs geen registratie (*failure to enroll*). Mensen die fysiek geen vingerafdrukken kunnen verstrekken zijn bijvoorbeeld geamputeerden en overlevenden van lepra. Er zijn ook mensen bij wie het moeilijk is betrouwbare vingerafdrukken af te nemen, bijvoorbeeld handarbeiders, ouderen, kinderen [1, 2, 5].

2.2 Gezichts-modaliteit

De gezichtsmodaliteit heeft een hoge gebruikersacceptatie, is universeel en het betreft een snel contactloos proces. Nadeel is dat er een regelmatige herregistratie moet plaatsvinden na verloop van tijd om het betrouwbaarheidsniveau te kunnen vasthouden. Ook de schaalbaarheid is beperkt waardoor deduplicatie in grote datasets moeilijk wordt.

Een cruciale uitdaging die blijft bestaan, is de stabiliteit en uniformiteit van prestaties, in onbeperkte omstandigheden, tussen alle personen van een referentiedatabase.

Ook de intrinsieke beperking van het onderscheidend vermogen van het gezicht als gevolg van genetische factoren, die fysieke gelijkenissen (etnische achtergrond en familierelaties) veroorzaken, blijft een beperking.

Vooral de prevalentie van monozygotische tweelingen bij de menselijke bevolking heeft belangrijke gevolgen voor de prestaties van de gezichtsmodaliteit [1, 2, 5].

2.3 Irismodaliteit

De irismodaliteit is onderscheidend, permanent, schaalbaar en bijna universeel, maar is niet interoperabel vanwege het ontbreken van beschikbare databases.

De kenmerken van de iris zijn meer permanent dan die van het gezicht waardoor de noodzaak van regelmatige herregistratie wordt beperkt.

Het onderscheidend vermogen van de iris is uniform vanwege de epigenetische aard van de gegevens en de technologie presteert zeer goed. De iris is ook minder kwetsbaar voor aanvallen dan het gezicht en de vingerafdruk. De implementatie van de irismodaliteit is echter om verschillende redenen vertraagd, waaronder een beperkte acceptatie door de gebruikers en de kosten van gepatenteerde technologie [1, 2, p.11, 5].

3 Samenvatting

Samenvattend kan worden gezegd dat de modaliteiten niet ideaal en onfeilbaar zijn. Bij alle modaliteiten is er sprake van specifieke tekortkomingen en beperkingen. Dit pleit vanzelfsprekend voor een multimodale aanpak.

Bijvoorbeeld in alle bestudeerde onderzoeken hebben de prestaties van vingerafdruk- en gezichtsmodaliteit in combinatie systematisch de prestaties van elke modaliteit vervangen bij onafhankelijk gebruik.

Hetzelfde fenomeen wordt waargenomen voor onkwetsbaarheid: de weerstand tegen de presentatie-aanval van de combinatie van de vingerafdruk en de gezichtsmodus vervangt de prestaties van elke modaliteit die voor zichzelf wordt beschouwd.

De toegevoegde waarde in het combineren van het gezicht en de iris modaliteit zit in het feit dat beide modaliteiten in dezelfde instantie en met dezelfde sensor kunnen worden verzameld, namelijk met behulp van een camera. Het gezicht kan dan worden gebruikt voor authenticatie- en iris voor deduplicatie- en identificatiedoeleinde, als irisdatabases beschikbaar zijn.

Het combineren van meerdere modaliteiten betekent dat er moet worden geïnvesteerd in meerdere biometrische technologieën en in het realiseren van databases met als resultaat een complexer en duurder systeem, waarvoor meer gekwalificeerd personeel nodig is om het te ontwikkelen, onderhouden en om het uit te voeren [2, p.9].

Het gebruik van meerdere verificatiefactoren verhoogt de mate van zekerheid bij een transactie (bijvoorbeeld veiligheid en betrouwbaarheid):

- meer gegevens zorgen voor statistische uniciteit met een hogere mate van nauwkeurigheid. Biometrische ontdubbeling is wellicht de beste oplossing om het unieke karakter van een grote populatie vast te stellen. Echter, niet alle biometrische modi bieden dezelfde nauwkeurigheid.
- verbeterde inclusie- en fouttolerantie: (meer) verschillende modi kunnen de kans vergroten dat alle leden van de bevolking een biometrisch monster kunnen verstrekken. Bepaalde biometrie kan voor sommige mensen moeilijk of onmogelijk zijn om betrouwbaar af te geven waardoor multimodale biometrie en / of passende technische en procedurele maatregelen nodig zijn om uitsluiting te verminderen.[1]
- mensen met criminele bedoelingen, kunnen zich richten op het bedreigen van iemands biometrisch kenmerk. Dat zal mislukken als ook een tweede biometrische kenmerk is geverifieerd. Het is een enorme uitdaging voor criminelen om twee monsters van biometrische gegevens van dezelfde persoon te krijgen;

[1] Het risico van uitsluiting: de systemen werken niet altijd en sommige mensen zullen minder snel herkend worden met als risico dat een persoon ten onrechte wordt buitengesloten. Zeker als de modellen niet goed om kunnen gaan met verschillende etniciteit, afwijkingen of seksen kan dit een gestigmatiseerd effect hebben. Ook hier is het daarom van belang dat er altijd een terugval mogelijkheid is om personen bijvoorbeeld bij falende gezichtsherkenningstechnologie alsnog te registreren. Voor mensen die vaak niet worden herkend door de systemen, kan dit een belemmering zijn en kan leiden tot stigmatisering. Het foutief herkennen van mensen kan leiden tot uitsluiting, discriminatie en sociaal ongemakkelijke omstandigheden.

- maakt het mogelijk verschillende biometrie (fusie) te zien voor ontdubbelen en verificatie. Bepaalde biometrische modaliteiten kunnen optimaal zijn voor het uitvoeren van dubbele biometrische registraties (vingerafdrukken voor 1:N- of N:N-matching[2]), terwijl andere mogelijk optimaal of voldoende zijn voor gebruik tijdens verificatie (gezichtsherkenning voor 1:1-matching[3]) [5].

Biometrie is geen wondermiddel. Met behulp van biometrische matching moeten de algoritmen op bepaalde toleranties worden ingesteld om de veiligheid te kunnen garanderen. Biometrie werkt in de rijken van risico's en waarschijnlijkheden. Uiteindelijk moet het gebruik van biometrie worden gezien als één tool. Zoals alle technologieën kunnen worden ondermijnd, is dat ook mogelijk met biometrie. Bijvoorbeeld: een persoon kan unieke frauduleuze identiteiten hebben in meerdere staten omdat de biometrische informatie wordt niet gecombineerde met andere (bestaande) identiteitssystemen.

Opgeslagen biometrische gegevens moeten naar behoren worden beschermd. Het zou niet mogelijk moeten zijn dat elke ongeautoriseerde organisatie /persoon gebruik maakt van verzamelde biometrische gegevens, ze verder deelt en/of bewaart.[4]

Biometrische gegevens moeten overeenkomstig met de nationale wet worden ingezet, waar deze het meest effectief en gepast is en in overeenstemming met de principes van doel, specificatie, noodzaak en evenredigheid. Het publiek moet proactief geïnformeerd worden over datagebruik om vertrouwen te winnen in zowel het systeem als het gebruik en toezicht [4].

[2] Identificatie (1-to-many matching). Identificatie wordt gebruikt om de identiteit van een persoon te achterhalen wanneer de identiteit is onbekend, of wanneer de autoriteit probeert het biometrisch te bevestigen wie de aanvrager is. Is die uniek en nog niet bekend in het systeem onder een andere identiteit. In tegenstelling tot verificatie, het identificatieproces vereist een centrale database. Zonder een databank met records is het proces van identificatie niet mogelijk. Voor een identificatieproces levert de persoon een live biometrie monster (d.w.z. er wordt een foto of vingerafdruk genomen). De gegevens worden verwerkt en het biometrische template wordt met alle geregistreerde templates in de database vergeleken om een match te vinden (of een lijst met mogelijke kandidaten). Het onderhoud van de integriteit van de database is essentieel om individuen te beschermen van identiteitsdiefstal.

[3] Verificatie (1-op-1 matching). Verificatie (1-op-1 matching) is om ervoor te zorgen dat een persoon overeenkomt met het bekende biometrische kenmerk. Er zijn twee soorten verificatie mogelijk: met gecentraliseerde opslag en decentraliseerde opslag. Als er een gecentraliseerde database bestaat, wordt deze eenmaal aangemaakt bij inschrijving en bijgewerkt met elke aanvraag, waar alle biometrische gegevens en de bijbehorende identiteiten worden opgeslagen. Het biometrische monster van de geclaimde identiteit wordt opgehaald uit de database (d.w.z. door te zoeken voor uniek documentnummer). Dit wordt dan vergeleken met het leven monster, wat vervolgens resulteert in een match of een non-match.

[4] Voor het verwerken van biometrische gegevens geldt een 'nee-tenzij 'regime, in tegenstelling tot de verwerking van gewone, niet-bijzondere persoonsgegevens, waarvoor een 'ja-mits 'regime geldt. Gelet op artikel 9, tweede lid, onderdeel g, van de AVG, is het verbod om biometrische gegevens met het oog op de unieke identificatie van een persoon te verwerken niet van toepassing, indien de verwerking noodzakelijk is van zwaarwegend algemeen belang (authenticatie of beveiligingsdoeleinden). Nog steeds moet men uitgaan van de redenering van noodzakelijkheid, proportionaliteit en subsidiariteit.

4 Referenties

[1] Anil K. Jain, Karthik Nandakumar, Arun Ross (2016). *50 years of biometric research: Accomplishments, challenges, and opportunities.* DOI: 10.1016/j.patrec.2015.12.013

[2] Didier Meuwly, Nigel Baker (2020). *Biometrics in the aliens' identity chain.* A literature study. Universiteit Twente. Wetenschappelijk Onderzoek- en Documentatiecentrum. Project 2965.

[3] Digital Identity Guidelines: *Enrollment and Identity Proofing* (June 2017). NIST 800-63A:2017

[4] Esther Keymolen, Merel Noorman, Bart van der Sloot, Colette Cuijpers, Bert-Jaap Koops, Bo Zhao (2020). *Op het eerste gezicht. Een verkenning van gezichtsherkenning en privacyrisico's in horizontale relaties*. Universiteit van Tilburg. Wetenschappelijk Onderzoek- en Documentatiecentrum.

[5] ID4D Practitioner's Guide: Version 1.0 (October 2019). Washington, DC: World Bank Group. World Bank Document

[6] Didier Meuwly (2 oktober 2018). *Biometrics in ID Documents. Potential and Limits of the Facial and Fingerprint Modes*. [PowerPoint slides]. European Parliament, Strasbourg, France.

Dit is een uitgave van:

Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Postbus 10451 | 2501 HL Den Haag

December 2022