

# Intelligente Camera Systemen en Biometrie

Mogelijkheden en onmogelijkheden

TNO | Kennis voor zaken



Trends zijn lastig te voorspellen!



## Enkele open deuren

- Maatschappij is complexer geworden
- Toegenomen anonimiteit
- Veiligheid is in toenemende mate een issue
  - Criminaliteit
  - Terrorisme
- Inzet van mensen is aan beperkingen gebonden
  - Financieel
  - Logistiek



## Maatschappelijke behoeften

- Aanwezigheid van surveillanten aanvullen met camerabewaking
- Waarneming, maar ook “bijsturing” (crowd control)
- Voorkomen is beter dan genezen
  - “Tegenhouden”
  - Vroegtijdig trends detecteren
  - Ruimtegebruik beïnvloeden (plaats, tijd)



## We zoeken een speld... .... maar creëren een hooiberg

- Beheersing van datastromen noodzakelijk
  - Voorkomen van overload van operators
  - Incidenten terug kunnen vinden
  - Omgaan met beperkingen in bandbreedte
- Door:
  - Data-compressie
  - Data-reductie (alleen beelden met inhoud)
  - Data-interpretatie (alleen beelden met betekenis)
- Helpt intelligentie in camera's ("videoanalyse") ons de speld te vinden?



## Taken voor intelligente camera's

- Bewegingsdetectie
  - Onderscheid wel/niet interessante gebieden
- Detectie van afwijkende situaties
- Druktemetingen
- Gedragsherkenning
- Identificatie op afstand
  - Gezichtsdetectie en -herkenning



# Video analyse systemen

## Motion detection

- "Er beweegt iets". Belangrijk ook vaststellen dat er juist niets gebeurt

## Motion analysis

- "Er beweegt iets kleins van links naar rechts"
- Bomen in de wind negeren
- Rekening houden met het perspectief in beeld
- Veelal beeldpunthoeveelheid gebruikt als maat voor alarmering

## Object detection/tracking

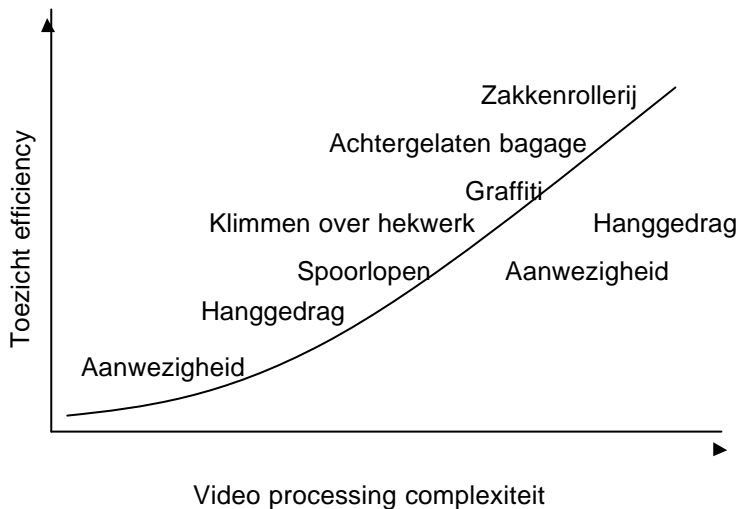
- Beeldpunten tot objecten geclusterd en geclassificeerd
- Volgen: tracking, tracing
- Personen, fietsers, personenvoertuigen en vrachtwagens. Volgen ook als er (korte tijd) occlusie plaatsvindt. Houdt rekening met het perspectief in beeld

## Behaviour analysis

- Kan gedrag van objecten herkennen, "een voertuig rijdt slingerend over de weg"



# De camera-intelligentie landkaart



## Hoe werkt videoanalyse?

- Achtergrondschatting is de eerste stap
  - 704 kolommen x 576 rijen x 3 bytes per pixel x 25 fps ~ 30 MB/sec.
- Leren achtergrond door uitmiddelen
  - Snelle update vs. langzame update
- Niet relevante gebieden worden aangegeven en genegeerd



9

woensdag 5 april 2006

## Mogelijke hinderpalen

- Veranderende buitenomstandigheden
  - Nederlandse situatie is een van de lastigste in de wereld door laaghangende bewolking en veel wind
- Grote drukte
- Reflecties
- Weer
  - zware regen, mist en sneeuw
- Trillende camera
- Beweging die niet relevant is
  - bomen, water, schaduwen, ...
- ...

10

woensdag 5 april 2006

## Voorbeelden van lastige situaties



11

woensdag 5 april 2006



## Conclusies (voorbeeld “stenengooiers”)

- Alleen detectie van globale bewegingen en geen detectie van subtiele handelingen
- Geen verwachting van verbeteringen op korte termijn m.b.t. de herkenning van subtiel gedrag
- Bij detectie van stilstand en rondhangen zal, bij een geoptimaliseerd systeem, naar schatting nog 20% gemist worden
- Een automatisch systeem is hierdoor slechts een filter
- Het aantal meldingen van stilstand kan op een druk object enkele tientallen per dag bedragen
- De inzet van automatische videoanalyse ter preventie is alleen zinvol als er voldoende tijd is om in te grijpen

12

woensdag 5 april 2006



## Haalbaar? Observatie op parkeerterreinen



13

woensdag 5 april 2006



## Niet haalbaar: detectie van zakkenrollers



14

woensdag 5 april 2006



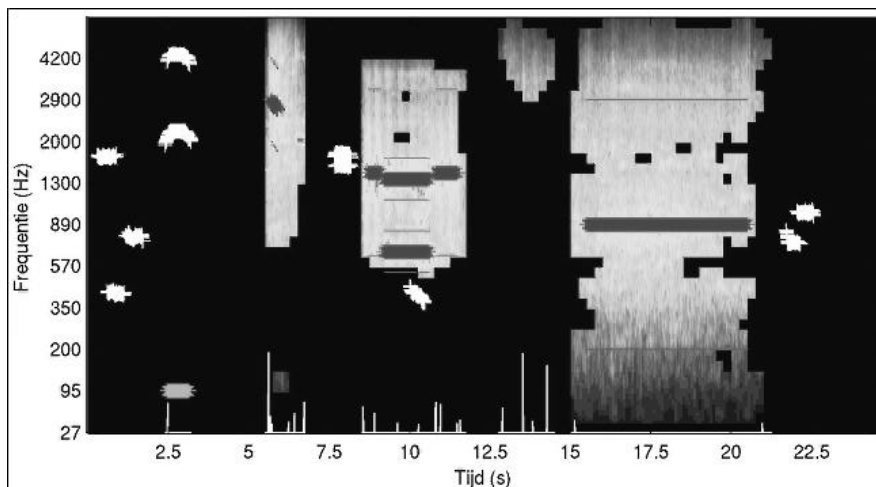
## Andere mogelijkheden bieden uitkomst

### Combineren van verschillende sensoren

- Primaire sensor: detectie / alarmering
- Secundaire sensor: verificatie van incident
- Voorbeeld:
  - Reductie valse alarmen bij politie door alarmcentrales al via video situatie te laten beoordelen
  - Politie wil incident kunnen verifiëren om prioriteit te kunnen geven
- Integraal gebruik van gegevensstromen
  - Multi-modaal (verschillende sensoren, beeld èn geluid)
  - Op verschillende plaatsen ("beelden samenvoegen")



## Multi-modaal: De rol van geluid





## Sensoren (multi-modaal)

Datareductie door niet continu video op te nemen maar pas n.a.v. trigger:

- Geluidsanalyse (gillen, glasgerinkel)
- Trillingssensor
- Apparaat status melding (vernietiging)
- (Mobiele) noodknop, hulpknop, telefoon
- Diverse andere sensoren (infrarood, radar)



## Huidige stand van zaken

- Objecten volgen onder rustige buitenomstandigheden
  - Nederlandse weerssituatie behoort tot de lastigste ter wereld
- Met name gericht op:
  - Verblijfstijd
  - Binnenkomen in gebied
  - Overschrijden 'tripwire' (evt. in combinaties)
- Beperkingen:
  - Relatief simpele analyse (geen modellen)
  - Verstoringen door reflecties, schaduwen, bewegingen in achtergrond
  - Combineren meerdere camera's staat in kinderschoenen, laat staan volgen over meerdere camera's
  - Rustige omgeving noodzakelijk anders te veel occlusie



## Ter overweging

- Zowel intelligente camerasystemen als biometrie zijn nog volop in ontwikkeling
- Toepassing intelligente camera's is beperkt tot filtering (geen echte gedragsherkenning)
- Cruciale rol operator
- Opnamekwaliteit is sleutel tot succes
  - Kwaliteit is taakafhankelijk
  - Overzicht vs. detail
- Hergebruik bestaande camerasystemen is beperkt
- Nu integrale visie op toekomst nodig om juiste keuzes te maken
  - Bijvoorbeeld: wóór het neerzetten van flitspalen bepalen of deze ook nog voor andere toepassingen gebruikt willen worden



## Biometrie



## Waarom biometrie?

- In theorie biometrie is:
  - Betrouwbaar want uniek
  - Niet te ontvreemden
  - Altijd beschikbaar
  - Comfortabel (geen PIN-code etc.)
- In werkelijkheid:
  - Beperkte nauwkeurigheid (FAR, FRR, ...)
  - Spoofing mogelijk
  - Lichamelijke beperkingen (handicap, ...)
  - Oncomfortabel (hygiëne, straling, afhankelijkheid van technologie, ...)



## De angst voor biometrie

- Vertrouwen in “ de andere kant”
  - Privacy
  - Identiteitsdiefstal
  - Gezondheidsrisicos
  - Persoonlijke informatie (gezondheid, ras, karakter, DNA, ...)

Daarom :

- Biometrie proportioneel en context afhankelijk invoeren
- Scholing van gebruikers: waarom is biometrie nodig, welke risico's zijn er, welke beveiligingsaspecten zijn er, ...



## Taken voor biometrie

- Identificatie
  - Voorkomen fraude
  - Beveiligen gegevens/bezittingen
- Anonieme biometrie
  - Gedragsdetectie



## Toepassingsvoorbeelden gezichtsherkenning

Paspoort	Verificatie Combinatie met vingerafdruk Opslag volledig gezicht in plaats van een template (standaardisatie!)
Toegangscontrole	Verificatie of identificatie met databases
Surveillance	Watchlist aanpak (identificatie) Anoniem (gedragsdetectie)
Tracking & tracing	Relaties tussen meerdere camera's Alleen betrouwbaar voor groepen? (statistisch: uitmiddeling van fouten)?



## Hoe werkt het?

### Enrolment – bekend maken bij het systeem



- Opnemen biometrisch kenmerk
- Segmentatie interessant gebied
- Detectie karakteristieke punten
- Analyse data
- Samenvatten in template
- Opslag template

### Verificatie

1-op-1 vergelijking



### Identificatie

1-op-N vergelijking



25

woensdag 5 april 2006



## Hoe goed werkt het?

### Effect op prestatie

- (Beeld) acquisitie
  - Ruis
  - Verlichting
  - Sensor
  - Resolutie
- Conditie biometrische kenmerken
  - Werken met handen
  - Zweet
  - Verwonding
  - Afvallen/aankomen
  - Make-up

26

woensdag 5 april 2006



## Hoe goed werkt het?

### Houding van Gebruiker

- Belang (wat krijg ik?)
- Vrijwillig of niet
- Bekendheid met het systeem
- Psychologische effecten (user psychology index)

### Toepassing

- Verificatie of identificatie
- Met of zonder medewerking
- Groot- of kleinschalig
- Toegang tot service of middel voor opsporing
- Proces vereenvoudigen of fraude beperken



## Mogelijke hinderpalen

- Biometrie is uniek maar niet geheim
- Gebruiker moet in de meeste gevallen meewerken
- Succes hangt af van vele componenten
  - Sensor (bij enrolment EN verificatie/identificatie)
  - Algoritme
  - Gebruiker
  - Toepassing

→ De hele beveiligingsketen



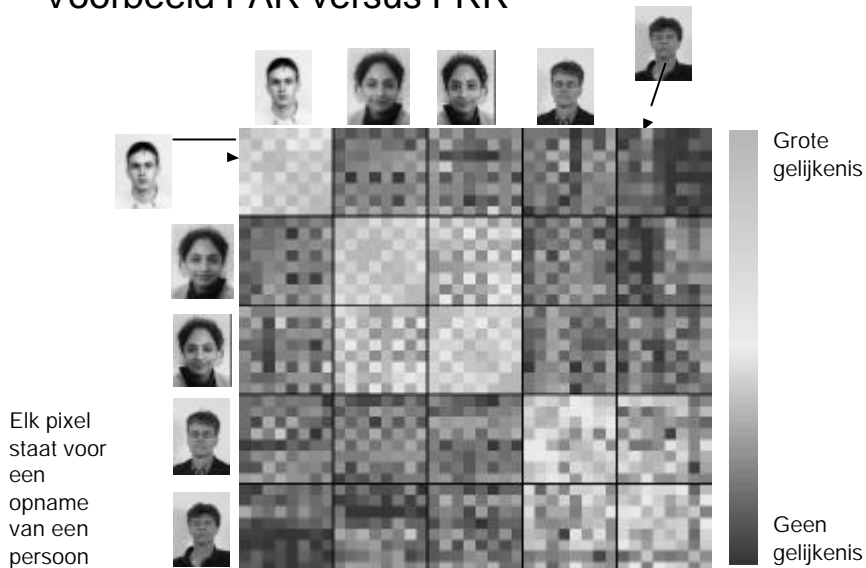
## Nauwkeurigheid

- Geen enkel biometrisch systeem is 100% nauwkeurig
- Nauwkeurigheid hangt af van drempelkeuze  
lage drempel → meer valse acceptaties  
hoge drempel → meer valse afwijzingen
- Drempelkeuze afhankelijk van applicatie

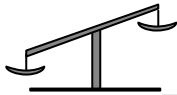
→ Dit maakt het bijna onmogelijk om systemen te vergelijken



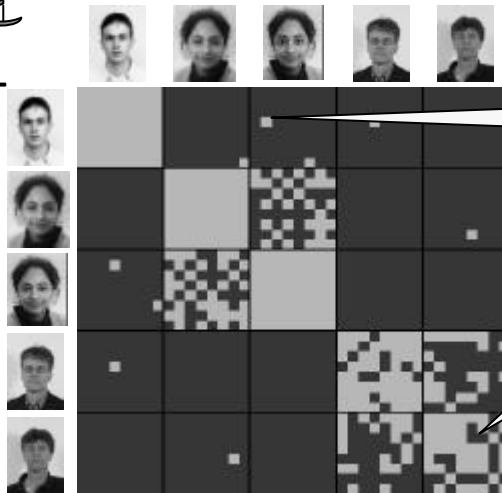
## Voorbeeld FAR versus FRR



## Voorbeeld FAR versus FRR



Minimaliseer  
valse  
afwijzing



False accepts

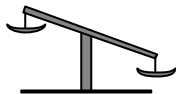
False rejects

31

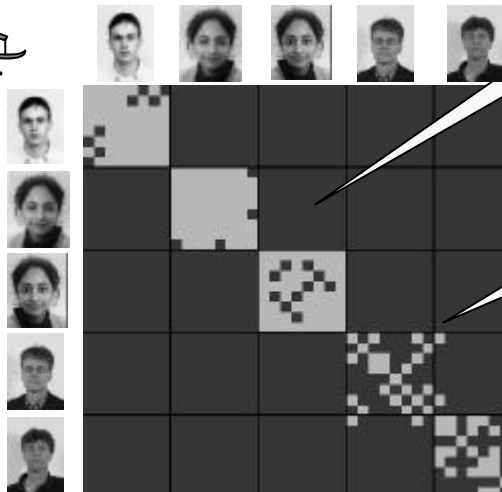
woensdag 5 april 2006



## Voorbeeld FAR versus FRR



Minimaliseer  
valse  
acceptatie



No false  
accepts

False accepts

False rejects

32

woensdag 5 april 2006





## Prestaties in een notendop

Biometrie	FTE %	FNMR ("FRR") %	FMR1 ("FAR") %	FMR2 ("FAR") %	FMR3 ("FAR") %
Gezicht	--	4	10	40	12
Vinger	4	2,5	<0,01	0,1	<0,1
Hand	2	1,5	1,5	--	--
Iris	7	6	<0,001	--	--
Stem	1	15	3	--	--

FMR1: verification; FMR2 & FMR3: large scale identification (1 million / 500)

Bron: A.K. Jain et al: Biometrics: A Grand Challenge (ICPR 2004, Cambridge UK)

33

woensdag 5 april 2006



## Biometrics enrolment trial (UK, mei 2005) UK Passport Service

Biometrics	Enrolment Success (Quota) %	Enrolment Success (Disabled) %	Verification Success (Quota) %	Verification Success (Disabled) %
Face	100	98	69	48
Finger	100	96	81	80
Iris	90	61	96	91

34

woensdag 5 april 2006



## Spoofting



(a) Live Finger

(b) Silicone Finger

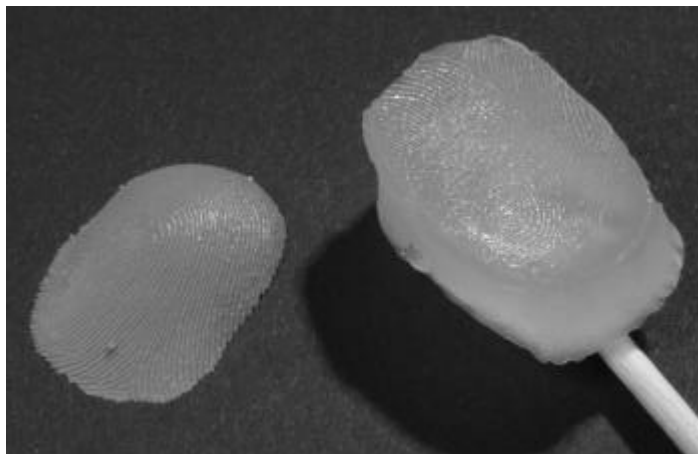
(c) Gummy Finger

**Figure 4.2** Fingerprint images of a live finger, a silicone finger and a *gummy* finger, which were displayed by the system with Device C (equipped with an optical scanner).

Bron: Tsutomu Matsumoto, "Impact of Artificial "Gummy" Fingers on Fingerprint Systems"



## Spoofting



# Testprotocollen biometrie

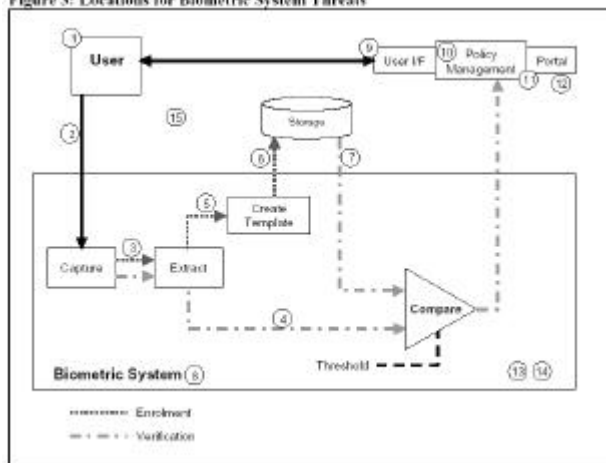
- Common Criteria
- Protection Profile
- Best Practices in Testing and Reporting Performance of Biometric Devices

Bron: <http://www.cesg.gov.uk/>



# Testprotocollen biometrie

Figure 3: Locations for Biometric System Threats



Bron: Common Criteria - Common Methodology for Information Technology Security Evaluation



## Ter overweging

Waarom biometrie toepassen?

- Biometrie is attractief als het iets toevoegt aan het totale proces
- Biometrie heeft invloed op de hele keten en kan daarom een combinatie van voordelen opleveren

→ Om biometrie in te voeren is kennis en inzicht in de hele beveiligingsketen noodzakelijk!

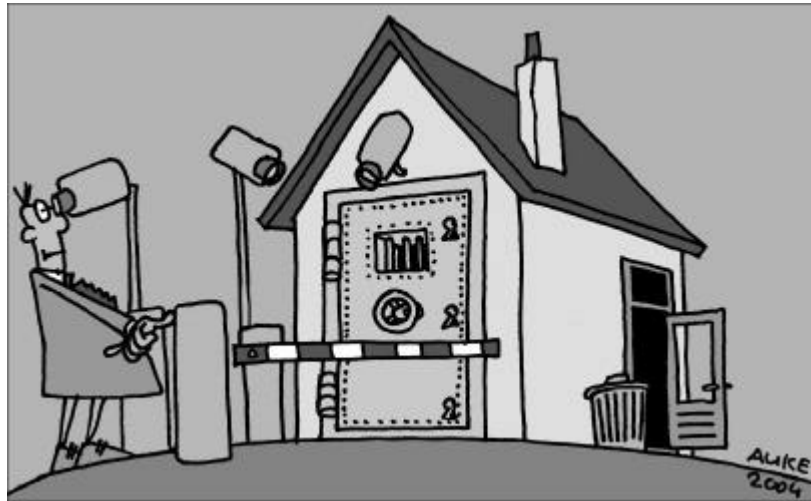


## Rol van TNO

- Kennispartner
- Strategische consultancy
- Roadmapping
- Benchmarking
- Ontwikkeling van vernieuwende concepten
- Ontwikkeling van prototypes binnen niches



Dank u voor uw aandacht!



E-mail: [stephanie.moro@tno.nl](mailto:stephanie.moro@tno.nl) or [ruud.vanmunster@tno.nl](mailto:ruud.vanmunster@tno.nl)

