AI IN DE ZORG

dwengo

AI OP SCHOOL

INFOFICHES

DIT PROJECT WERD GEREALISEERD MET DE STEUN VAN
DE KONING BOUDEWIJNSTICHTING, DE NATIONALE LOTERIJ EN ENKELE PARTNERS.

Kaart	Relevante infofiches
1	Encryptie, Databanken. Hashing, Authenticatie, Anonimiseren
2	Encryptie, Databanken, Hashing, Anonimiseren, Taalverwerking
3	Encryptie, Datacommunicatie, Sensoren, Authenticatie, IoT
4	Encryptie, Datacommunicatie, Sensoren, Authenticatie, IoT
5	Digitale beelden, Beeldherkenning, Sensoren, Sociale robots
6	Sociale robots, Biomimicry
7	Sensoren, Sociale robots, Taalverwerking, Spraak, Biomimicry
8	Beslissingen, Sociale robots, Taalverwerking, Spraak
9	Digitale beelden, Beeldherkenning, Sensoren, Sociale robots, Spraak
10	Digitale beelden, Beeldherkenning, Sensoren, Sociale robots, Spraak
11	Beslissingen, Taalverwerking, Chatbots
12	Encryptie, Datacommunicatie, Sensoren, Authenticatie, IoT
13	Datacommunicatie, Sensoren
14	Digitale beelden, Beeldherkenning, Sensoren, Sociale robots, Spraak
15	Digitale beelden, Beeldherkenning, Beslissingen, Sociale robots,Spraak
16	Encryptie, Hashing, Beslissingen, Taalverwerking, Chatbots
17	Encryptie, Hashing, Taalverwerking, Chatbots, Spraak
18	Databanken, Datacommunicatie, IoT, Sociale robots
19	Digitale beelden, Beeldherkenning, Sensoren, Sociale robots, Spraak
20	Sensoren, Sociale robots, Spraak, Biomimicry
21	Databanken, Digitale beelden, Beeldherkenning
22	Sociale robots, Taalverwerking, Spraak
23	Digitale beelden, Sociale robots, Taalverwerking, Spraak
24	Digitale beelden, Beeldherkenning, Sociale robots, Spraak
25	Databanken, Beslissingen, Tracking
26	Beslissingen, Taalverwerking, Chatbots
27	Anonimiseren, Taalverwerking, Spraak
28	Encryptie, Databanken, Hashing, Authenticatie, Beslissingen
29	Beeldherkenning, Beslissingen, Sociale robots, Spraak
30	Digitale beelden, Beeldherkenning, Sensoren, Biomimicry
31	Digitale beelden, Beeldherkenning, Sensoren, Sociale robots, Biomimicry
32	Beeldherkenning, Sensoren, Beslissingen, Taalverwerking, Spraak
33	Sensoren, Sociale robots, Biomimicry

Anonimiseren van gegevens

Je kent misschien wel iemand die al deelgenomen heeft aan een medische studie. Zulke studies zijn er om de effectiviteit van een geneesmiddel of vaccin te testen. Tijdens de studie wordt er meestal gevraagd naar je ***persoonsgegevens***. Dit zijn ***gegevens waarmee je geïdentificeerd kan worden***. Je geeft bijvoorbeeld je ***naam en e-mailadres*** door zodat de onderzoekers je kunnen contacteren met informatie gerelateerd aan de studie. Naast deze contactgegevens zullen de onderzoekers ook vaak ***gegevens verzamelen die nodig zijn voor het onderzoek***. Dit is vaak heel persoonlijke informatie, bv. ***lengte, gewicht, bloedgroep, allergieën*** … Om ervoor te zorgen dat jouw privacy beschermd is, moeten de onderzoekers ervoor zorgen dat deze gegevens niet aan jou gelinkt kunnen worden. Je contactgegevens zoals e-mailadres, naam, telefoonnummer, adres … mogen dus niet samen met de gegevens voor het onderzoek opgeslagen worden, m.a.w. ***de onderzoeksgegevens worden geanonimiseerd***.

Waarom moet je dit leren? Bedrijven en scholen hebben gegevens van jou nodig, bijvoorbeeld om pakjes te bezorgen of rekeningen te sturen. Door te begrijpen hoe anonimiseren werkt, snap je hoe ze ervoor zorgen dat jouw informatie veilig blijft en leer je hoe je je eigen privacy kunt beschermen.

Uitdaging: Het is niet altijd even gemakkelijk om gegevens op een goede manier te anonimiseren. Op de volgende pagina zie je twee tabellen. Deze bevatten de gegevens van deelnemers aan een effectiviteitsstudie van een vaccin. De ene tabel bevat de contactgegevens van de deelnemers. De andere de anonieme gegevens die nodig zijn voor de studie.
Kan jij de personen linken met hun gegevens voor de studie?

De contactgegevens

Voor-naam	Naam	Telefoon-nummer	Adres	E-mailadres	Minder-jarig	E-mailadres voogd
Emma	De Vries	555123456	Mechelsesteenweg 10, Antwerpen	emma.devries@mail.com	Nee	
Finn	Janssen	555123457	Brusselsestraat 15, Leuven	finn.janssen@mail.com	Ja	jan.janssen@mail.com
Sophie	Vermeulen	555123458	Kerkstraat 25, Gent	sophie.vermeulen@mail.com	Ja	karel.vermeulen@mail.com
Gustaaf	Peters	555123459	Woonzorgcentrum Regina Celi, Rijlaan 21, Hasselt, Kamer 67	Gustaaf.peters@mail.com	Nee	
Finn	Bosch	555123461	Lange Munt 30, Gent	finn.bosch@mail.com	Nee	
Ginette	Smits	555123462	Zeedijk 12, bus 20, Oostende	ginette.smits@mail.com	Nee	

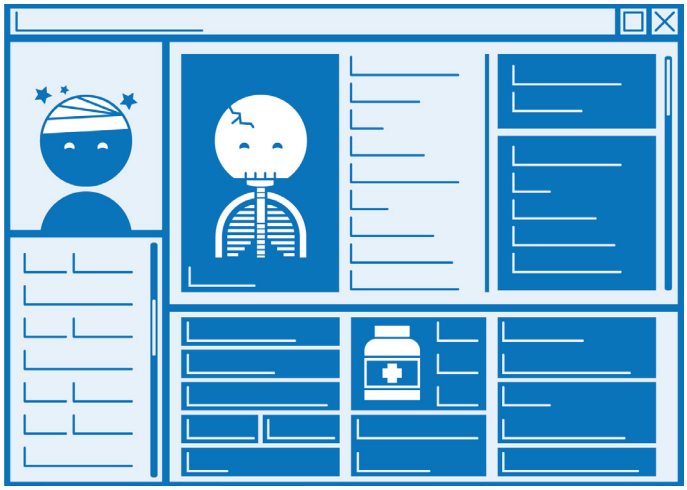
Gegevens voor de studie

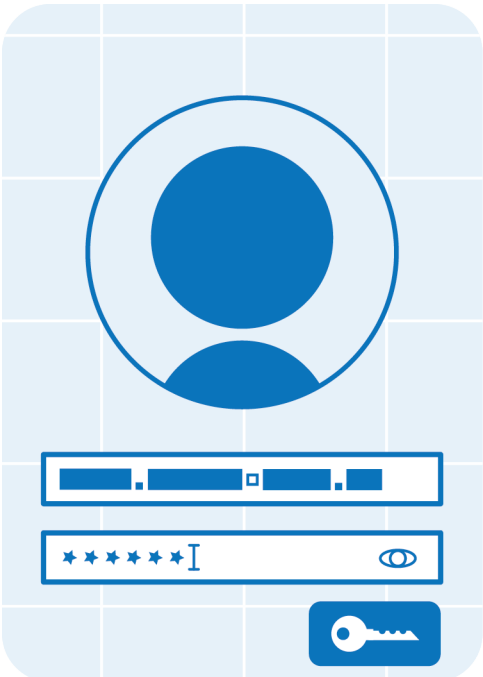
Leeftijd	Gender	Bloedgroep	Allergieën	Aandoeningen
12	Vrouw	O+	Geen	Bedplassen
13	Man	B+	Geen	Geen
19	Man	O-	Geen	Diabetes Type 2
33	Vrouw	A+	Pollen	Ziekte van Crohn
79	Vrouw	B-	Geen	Geen
82	Man	AB+	Noten	Incontinentie

Authenticatie en autorisatie

Je logt dagelijks in op verschillende platformen zoals Smartschool, Instagram, TikTok, OneDrive … Maar heb je je al eens afgevraagd waarom het nodig is om in te loggen op die platformen?
Er zijn twee belangrijke redenen waarom inloggen noodzakelijk kan zijn: authenticatie en autorisatie. ***Authenticatie is nodig zodat het platform waarop je inlogt weet wie jij bent***.
Wanneer het platform weet wie jij bent, geeft het je toegang tot bepaalde gegevens (bv. de informatie op je Facebookprofiel). ***De beslissing tot welke gegevens jij toegang krijgt noemt men autorisatie***. Autorisatie is nodig omdat je geen toegang zou krijgen tot gegevens die jij niet mag zien, zoals de gegevens op een Facebookprofiel van een persoon waar je niet mee bevriend bent.

Authenticatie kan op verschillende manieren, bijvoorbeeld, door een combinatie van een gebruikersnaam met een uniek wachtwoord, aan de hand van een document dat enkel jij hebt (bv. je elektronische identiteitskaart) of via een authenticatie-applicatie (bv. itsme).
Autorisatie kan gebeuren doordat er bijvoorbeeld in een tabel werd opgeslagen wie toegang heeft tot welk bestand.





In de ***zorgsector*** zijn authenticatie en autorisatie van groot belang. Meer en meer ***informatie over patiënten*** wordt digitaal opgeslagen, bijvoorbeeld in een gedeeld medisch dossier. Op jouw vraag bewaart je huisarts al jouw medische gegevens in een Globaal Medisch Dossier (GMD). Dat GMD bevat een overzicht van al je medische gegevens. Een deel van die gegevens kan uitgewisseld worden via een gedeeld medisch dossier. Dat gedeeld medisch dossier kan door verschillende zorgverleners geraadpleegd of aangepast worden. Toch wil je niet dat elke zorgverlener zomaar alle

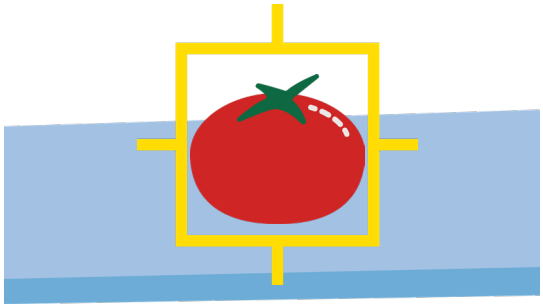
informatie uit je gedeeld medisch dossier kan lezen. Het is dus heel belangrijk dat enkel personen die toegang moeten hebben tot deze persoonlijke informatie, effectief toegang krijgen. Het is dus noodzakelijk dat de applicatie van het gedeeld medisch dossier kan achterhalen wie bepaalde info opvraagt (***authenticatie***) en deze personen enkel toegang geeft tot de gegevens die ze nodig hebben om hun medische taak te kunnen uitvoeren (***autorisatie***). Zo zal je kinesist informatie over een behandeling kunnen toevoegen, maar niet zomaar toegang hebben tot de resultaten van een bloedonderzoek.

Uitdaging: Maak een bestand aan op Google Drive, Microsoft OneDrive of een ander gelijksoortig platform. Deel dat bestand met twee personen. De ene persoon mag het bestand kunnen lezen maar niet bewerken, de andere kan het bestand wel bewerken.

*Authenticatie en autorisatie komen vaak voor in combinatie met **encryptie** en **hashing**. Encryptie wordt gebruikt om de gegevens van een gebruiker te beschermen. Hashing kan worden gebruikt om de identiteit van een gebruiker te verifiëren. Bekijk de fiches van encryptie en hashing om meer te weten te komen over deze technieken.*

Beeldherkenning

Je kan er niet meer onderuit, systemen met beeldherkenning (***computer vision***) zijn overal: zo geeft Facebook suggesties om personen in je foto's te taggen, een auto waarschuwt de bestuurder wanneer die slaperig begint te worden of een slimme deurbel zegt wie er aan de deur staat.
Beeldherkenning is heel krachtig, maar ook complex. Om een ***computer een object te laten detecteren in een afbeelding moeten er duidelijke regels zijn die die computer kan volgen***. En laat nu net het opstellen van zulke regels heel moeilijk zijn, niet in het minst omdat een afbeelding voor een computer een raster van pixels is. Via technieken van machinaal leren kunnen deze regels met behulp van de computer opgesteld worden. Op die manier worden er ***algoritmes*** ontwikkeld waarmee de computer kan 'zien'.



Om bijvoorbeeld een tomaat te herkennen in een afbeelding zou je kunnen kijken naar de kleur van de pixels. Is deze overwegend rood, dan heb je al een indicatie dat het over een tomaat gaat. Je zou ook de vorm kunnen bekijken: is deze min of meer rond, dan is het nog waarschijnlijker dat er een tomaat te zien is op de afbeelding. Verder zou je kunnen kijken of er bovenaan een groen kroontje te zien is. Door meer en meer regels te verzinnen, word je beter in het herkennen van een tomaat. Krijg je echter een afbeelding van een gele tomaat te zien, dan zal je er met deze regels niet in slagen om de tomaat te herkennen. De detectieregels zullen in dat geval niet werken.

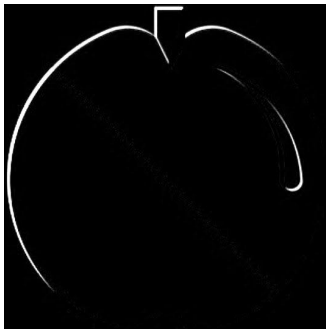
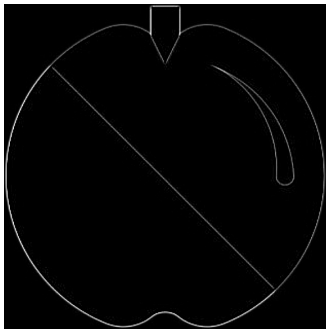
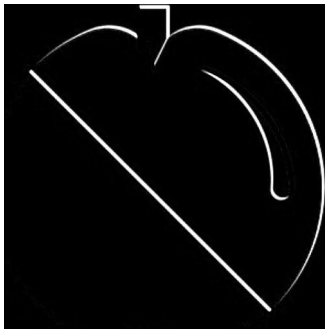
Omdat het praktisch onmogelijk is om voor elke afbeelding van elke soort tomaat zelf detectieregels op te stellen, bedachten computerwetenschappers algoritmes om een computer deze regels automatisch te laten leren op basis van voorbeelden. Dit noemen ze ***machinaal leren***.
Beeldherkenning is belangrijk ***in de zorg***. In onderzoek naar autismespectrumstoornissen worden soms sociale robots ingezet die met kinderen met autisme communiceren. Onderzoek heeft immers aangetoond dat sociale robots een positief effect kunnen hebben op het sociaal functioneren van kinderen met autisme[1]. Het kunnen herkennen van de emoties van de kinderen is daarbij zeer belangrijk. Door de emoties correct te kunnen herkennen, kan het systeem op een correcte manier interageren met het kind.

1: Kouroupa A, Laws KR, Irvine K, Mengoni SE, Baird A, Sharma S. The use of social robots with children and young people on the autism spectrum: A systematic review and meta-analysis. PLoS One. 2022 Jun 22;17(6):e0269800. doi: 10.1371/journal.pone.0269800. PMID: 35731805; PMCID: PMC9216612.

Uitdaging: Wil je te weten komen hoe je een computer kan leren om emoties te detecteren? Scan dan de QR-code of surf naar de webpagina met onderstaande link. Je kan voor de opdracht best een computer of tablet gebruiken.

https://dwengo.org/basics_ai/emoties

Succesvolle beeldherkenning verloopt via convolutionele diepe neurale netwerken. Via filters op de afbeeldingen zal de computer kenmerken van objecten detecteren in de afbeeldingen. Vanuit die kenmerken zal het systeem dan beslissen welke objecten het detecteert en met welke zekerheid. Je kan daar meer over lezen op de Dwengo-website.

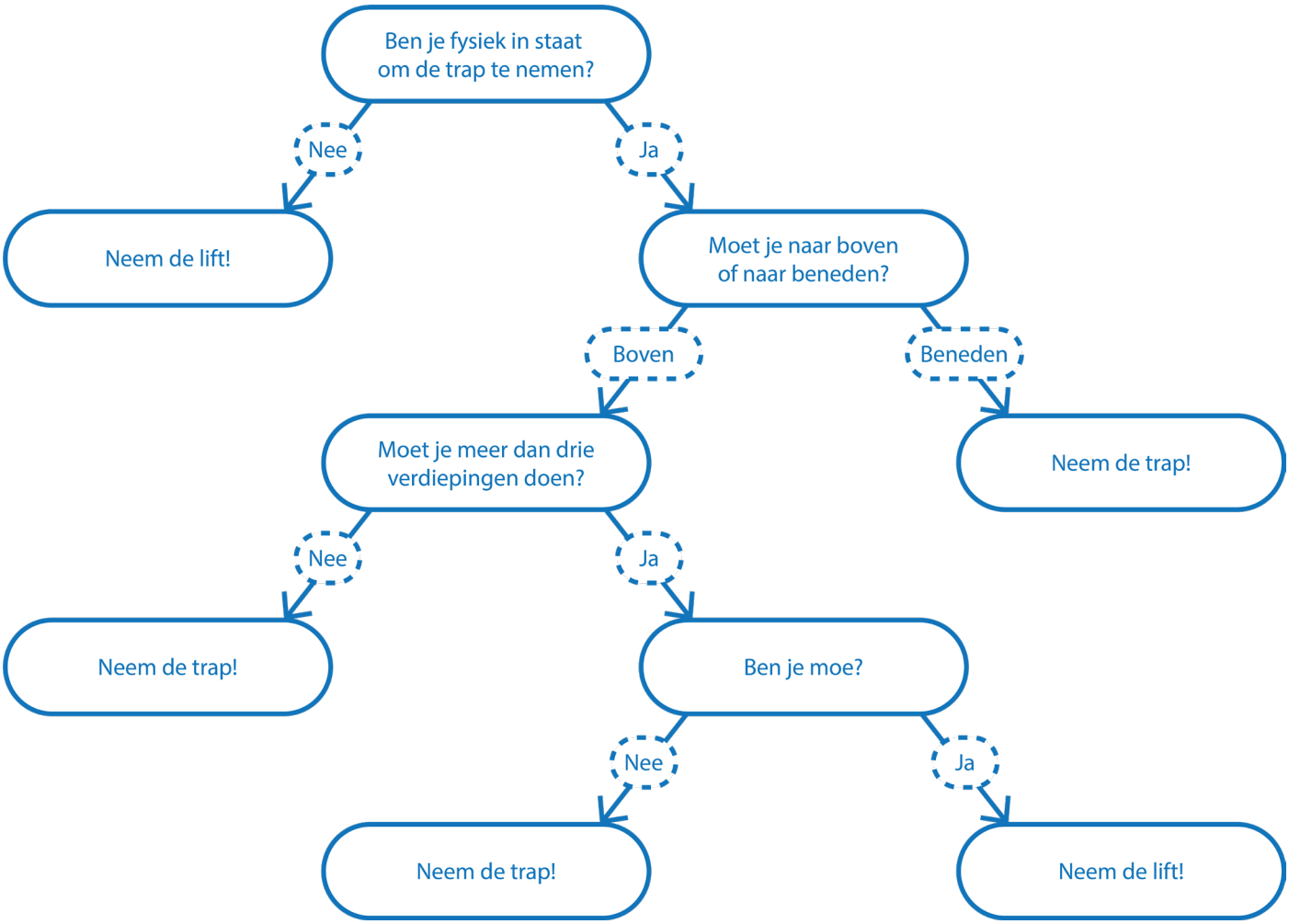





Beslissingen nemen

Iedereen neemt dagelijks honderden beslissingen. Je beslist wat je zal eten, welke schoenen je zal dragen en of je een regenjas aandoet. Voor deze beslissingen baseer je je op informatie uit je omgeving. Je beslissing om een regenjas aan te doen zal bijvoorbeeld afhangen van de weersvoorspellingen, maar ook van de manier waarop je je zal verplaatsen (bus, fiets, auto …). ***Wanneer computers beslissingen kunnen nemen, kunnen ze bepaalde taken van ons overnemen.*** Hiervoor ***moet een programmeur de regels die de computer moet volgen om de beslissing te nemen, heel nauwkeurig en ondubbelzinnig noteren in een programma***, bijvoorbeeld aan de hand van een ***beslissingsboom***.

Moderne ***insulinepompen*** beslissen, bijvoorbeeld, om insuline toe te dienen op basis van de gemeten bloedsuikerspiegel, de tijd sinds en de hoeveelheid van de vorige dosis. Om de computer deze beslissingen te laten nemen, moet hij beschikken over de regels die hij moet volgen.

Hieronder zie je een voorbeeld van een beslissingsboom om te beslissen of je de trap neemt of niet.



Bij beslissingsbomen worden de regels vaak opgesteld door experten in een bepaald vakgebied, bijvoorbeeld dokters, waarna een programmeur deze regels invoert in de computer door te programmeren. De programmeur draagt hierin dus een grote verantwoordelijkheid. Zo'n computersystemen worden ***regelgebaseerde, kennisgebaseerde of expertsystemen*** genoemd en kunnen het werk van de expert verlichten.

In de ***gezondheidszorg*** worden beslissingsbomen bijvoorbeeld gebruikt als hulp om een diagnose te stellen of een behandelingsplan te bepalen. Er is bijvoorbeeld ook een app gemaakt om migrainepatiënten te waarschuwen dat er een migraineaanval zit aan te komen en dat ze dus best preventief medicatie nemen. Beslissingsbomen zijn er heel populair omwille van transparantie: als je de beslissing van de computer krijgt, dan kan je immers in principe weten hoe de computer tot die beslissing is gekomen.

Uitdaging: Verken de applicatie 'Moet ik naar de dokter?'.

Maar soms is het zelfs voor een expert moeilijk om alle regels te bedenken die noodzakelijk zijn om een probleem op te lossen. Voor zulke problemen kunnen technieken van machinaal leren gebruikt worden.

Databanken

In 2024 worden wereldwijd meer dan ***50 zettabyte*** (ZB) aan gegevens opgeslagen. Eén zettabyte is gelijk aan 10^{21} bytes. Dat betekent dat ***per persoon op aarde gemiddeld 6,25 terrabyte*** (TB) aan data wordt opgeslagen. Deze hoeveelheid data groeit elk jaar zeer snel. Er wordt geschat dat de hoeveelheid data die wordt opgeslagen ongeveer elke twee jaar zal verdubbelen.

Om met deze enorme hoeveelheden data te kunnen omgaan, is er nood aan technieken om gegevens op een ***compacte*** en ***efficiënt doorzoekbare*** manier op te slaan. Computerwetenschappers bedachten verschillende van deze technieken en brachten ze samen in de vorm van een ***databanksysteem***. Een databanksysteem of kortweg ***databank*** is dus een verzameling van technieken die ons toelaat om gegevens compact en efficiënt doorzoekbaar op te slaan.

Een aantal voorbeelden van deze technieken zijn: verwijderen van overbodige gegevens, sorteren van gegevens en binair doorzoeken van gegevens.

Een belangrijke techniek binnen databanksystemen is het ***indexeren*** van gegevens. Het indexeren van gegevens zorgt ervoor dat je informatie sneller kan terugvinden. Je zou dit kunnen vergelijken met een index voor- of achteraan in een boek, waardoor je gemakkelijk kan achterhalen op welke pagina's een begrip voorkomt.

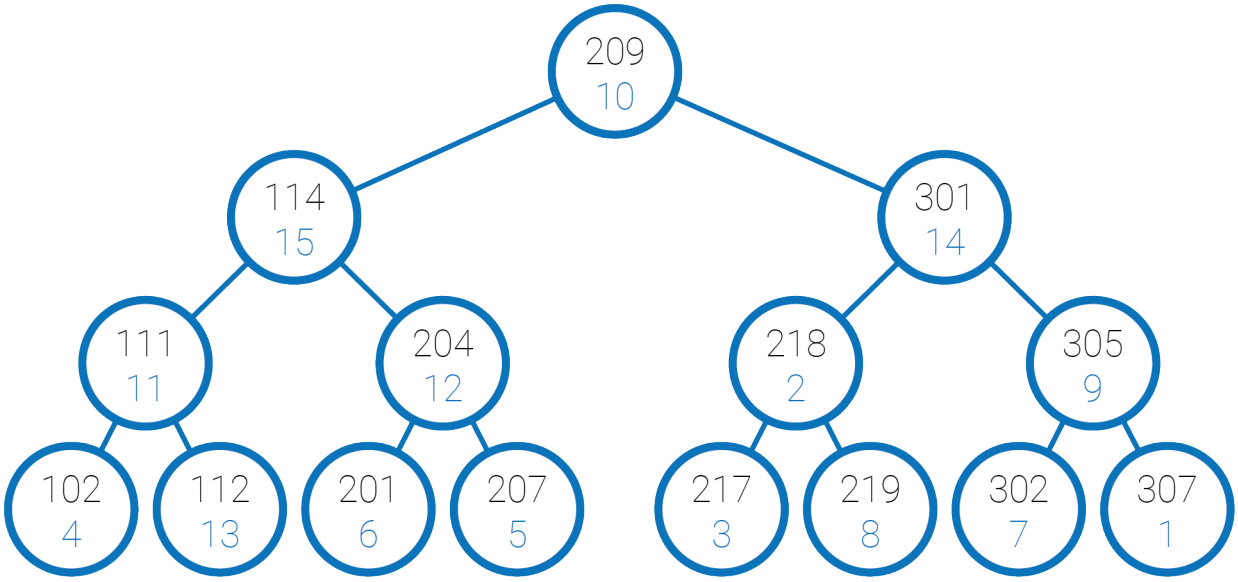
De tabel bevat de kamer-nummers en patiënten van een ziekenhuis. Bekijk de tabel. Welke patiënt is 66 jaar oud?

Nr.	Naam	Voornaam	Leeftijd	Kamer
1	Berendzen	Douwe	40	307
2	Burckhard	Karl	41	218
3	Claussen	Lies	62	217
4	De Ronde	Huib	31	102
5	Eyman	Eelco	64	207
6	Halle	Teun	32	201
7	Henneke	Arnoldus	44	302
8	Hinken	Marie	51	219
9	Jagers	Wim	70	305
10	Koen	Felix	58	209
11	Roode	Klaus	37	111
12	Rooth	Wijnand	66	204
13	Rosh	Amira	41	112
14	Robrecht	Rein	51	301
15	Veerkamp	Lukas	41	114

Hieronder zie je een index, voorgesteld als een binaire boom. Dankzij deze boom kan je de lijst snel doorzoeken. Deze boom maakt het makkelijk om terug te vinden welke patiënt er in een bepaalde kamer ligt, zonder dat je die lijst met patiënten volledig moet overlopen.

De boom bestaat uit cirkels (knopen) en verbindingen tussen deze cirkels (bogen). In een ***knoop*** staat het ***nummer van de kamer*** met daaronder het ***nummer van de patiënt***. Je kan terugvinden welke patiënt er in een kamer ligt door te vertrekken in de bovenste knoop van de boom (de wortel). In die knoop zijn er drie mogelijke acties.

1) Het kamernummer dat je zoekt ***komt overeen*** met het kamernummer in deze knoop. Dan staat het nummer van de patiënt die je zoekt ook in deze knoop. Je hoeft dus niet verder te zoeken.
2 Het kamernummer dat je zoekt is ***kleiner*** dan het kamernummer in deze knoop. Ga via de linkse boog naar een volgende knoop. Herbekijk deze drie acties voor die knoop.
3) Het kamernummer dat je zoekt is groter dan het kamernummer in deze knoop. Ga via de rechterboog naar de volgende knoop. Herbekijk deze drie acties voor die knoop.



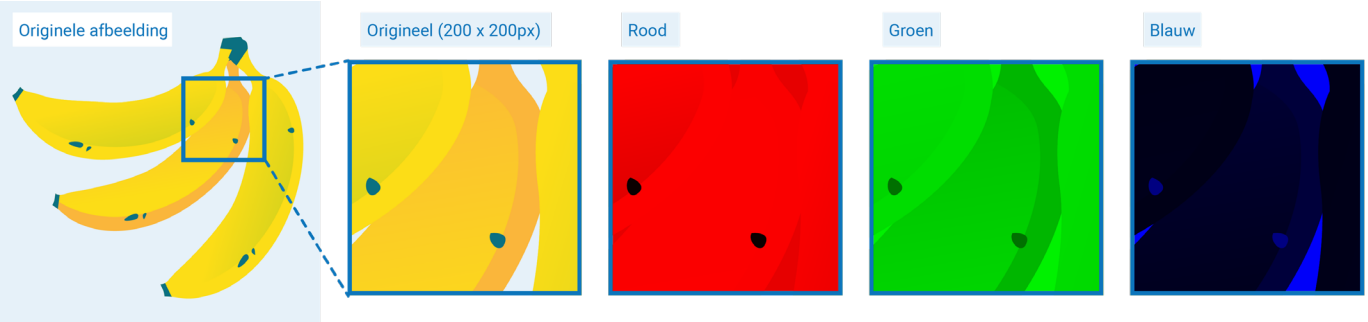
Uitdaging: Gebruik de binaire boom om op te zoeken ***welke patiënt in kamer 204 ligt***. Hoeveel kamernummers heb je moeten bekijken voor je de naam van de patiënt gevonden hebt? Hoeveel had je er moeten bekijken wanneer je de tabel rij per rij had overlopen? Stel je voor dat de lijst 1024 namen bevat, hoeveel kamernummers had je dan maximaal moeten overlopen in de binaire boom?

Wist-je-datje:
Om deze boom op te stellen werd het concept van binair zoeken toegepast. Alle kamers worden geordend van links naar rechts: 102, 111, 112, 114, 201, 204, …, 219, 301, …, 307. De middelste kamer wordt als wortel van de boom gekozen. Vervolgens worden voor de volgende knopen de middelste kamer van het linkerdeel en van het rechterdeel gekozen, enz.

Digitale beelden

Digitale beelden worden door de computer voorgesteld als een ***raster van pixels***. Het woord ***pixel*** komt van de beschrijving ***picture element***, wat je kan vertalen als onderdeel van een afbeelding. Elke pixel heeft een bepaalde ***kleur***, deze wordt ***voorgesteld door een combinatie van tinten rood, groen en blauw (RGB)***. De computer stelt een pixel meestal voor door drie getallen van 0 tot en met 255, een getal voor elke kleur.

Op onderstaande afbeeldingen zie je links telkens een afbeelding van bananen. Daarin is aan de hand van een blauw vakje een regio aangeduid. Van die regio zie je rechts de RGB-waarden.



Wanneer je genoeg inzoomt op de afbeelding zie je de individuele pixels, waarbij de kleur van een pixel bepaald wordt door drie getallen.

Een computer kan - veel beter dan een mens - heel kleine veranderingen op een foto detecteren. Een computer kan immers elke pixel afzonderlijk 'zien'. Daarom kunnen radiologen een beroep doen op AI-systemen om hen te helpen om ***medische beelden*** meer in detail te bekijken en te interpreteren.

Uitdaging: Pixels spotten! Elk scherm gebruikt pixels om beelden voor te stellen. Neem met de camera van een smartphone een foto van je computerscherm. Doe dit zo dicht mogelijk bij het scherm, maar zorg dat de inhoud van het scherm in focus is. Zoom daarna met de smartphone in op de foto. Zie je de pixels?

ENCRYPTIE

Elke dag slaan we persoonlijke gegevens op, zowel op onze eigen computer als in de cloud.

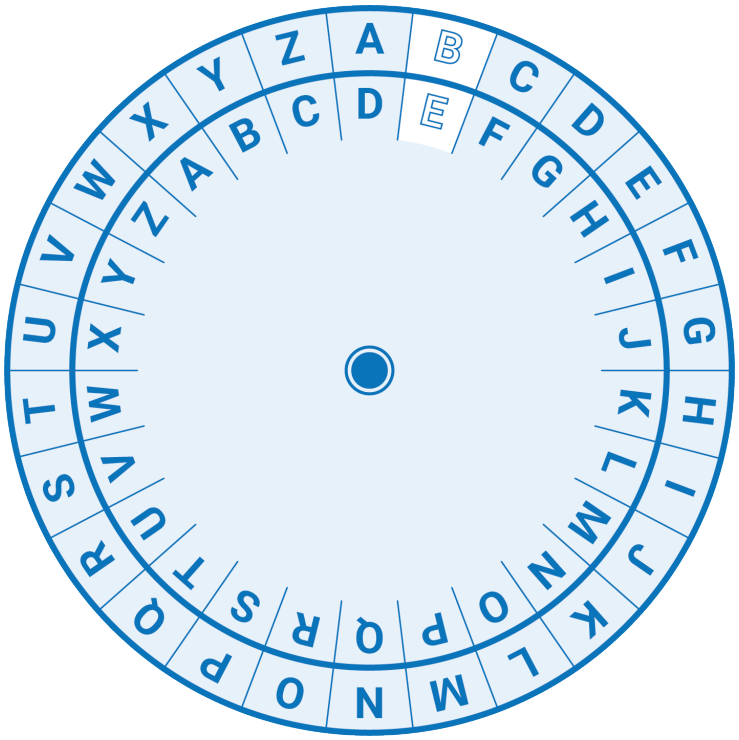
Hoe kan je zeker zijn dat jouw persoonlijke gegevens niet door anderen gelezen kunnen worden? Hoe bescherm je jezelf tegen het oneigenlijk gebruik van jouw gegevens?

Computerwetenschappers bedachten technieken om ervoor te zorgen dat enkel jij, of een partij die jij vertrouwt, de mogelijkheid hebben om je gegevens te lezen. Deze technieken om gegevens op een veilige manier op te slaan, noemen ze ***encryptie-*** of ***versleutelingstechnieken***.

Wanneer je gegevens ***versleutelt***, vorm je ze via een formule om naar een voorstelling die moeilijk te lezen is. Enkel wanneer je de formule volledig kent, kan je het bericht ***ontsleutelen*** en dus terug leesbaar maken.

Een eenvoudig voorbeeld van encryptie is het ***Caesarcijfer***, ook wel Caesarrotatie genoemd.
Het is een versleutelingstechniek die al door Julius Caesar gebruikt werd om in geheimschrift met zijn veldheren te communiceren. Het Caesarcijfer geeft aan met hoeveel letters in het alfabet je elke letter in de boodschap opschuift.

Hiernaast zie je bijvoorbeeld een versleuteling met Caesarcijfer 4.



Uitdaging: kan je de volgende boodschap ontcijferen?

Ot utfk jomozgrk ckxkrj oy ktixevzok bgt rkbktyhkrgtm!

Tip: deze boodschap werd versleuteld met Caesarcijfer 6

Bij het Caesarcijfer kan je op een relatief eenvoudige manier achterhalen hoe de versleuteling werkt. Moderne versleutelingstechnieken zijn zodanig ontworpen dat het zo goed als onmogelijk is om te achterhalen met welke tekst een versleutelde boodschap overeenkomt.
Dergelijke technieken maken gebruik van een ***encryptiesleutel***. Deze sleutel heb je nodig om de boodschap te versleutelen maar ook om die terug leesbaar te maken. De encryptiesleutel is een onderdeel van de wiskundige formule die de gegevens onleesbaar maakt. Zolang enkel jij deze sleutel kent, kan niemand anders de versleutelde boodschap lezen.

*Een van de bekendste en meest gebruikte versleutelingstechnieken is het **AES algoritme**, ook wel het **Rijndael algoritme** genoemd. AES staat voor **Advanced Encryption Standard**.*
Het is een internationale standaard en wordt onder meer gebruikt door de Amerikaanse National Security Agency (NSA) om de meest gevoelige informatie van de Amerikaanse overheid te versleutelen.
Het AES algoritme werd uitgevonden door twee Belgische computerwetenschappers, Joan Daemen en Vincent Rijmen. Zij ontwikkelden het algoritme tussen 1997 en 2000 en namen ermee deel aan een wedstrijd van het Amerikaans Nationaal Instituut voor Standaardisatie en Technologie. De twee Belgen wonnen de wedstrijd waardoor hun algoritme nu een internationale standaard is en de persoonlijke informatie van miljarden mensen beveiligt.

Hashing

Hashing is nuttig wanneer je bijvoorbeeld een wachtwoord wilt opslaan en wilt voorkomen dat anderen het kunnen lezen. Hashing zal de tekst, dus het wachtwoord, omvormen naar een ***groot getal***. Dat getal wordt opgeslagen in de plaats van het wachtwoord zelf. Bovendien kan het gehashte getal niet terug omgevormd worden naar de oorspronkelijke tekst.

Je weet waarschijnlijk dat het een slecht idee is om een wachtwoord neer te schrijven. Op het moment dat je een wachtwoord fysiek of digitaal neerschrijft, is er een kans dat mensen je wachtwoord kunnen lezen. Dit wil je niet, dus kan je je wachtwoorden best onthouden. Dit roept natuurlijk de vraag op: hoe kunnen websites en applicaties jouw wachtwoord opslaan zonder het gewoon ergens (digitaal) te noteren? Het antwoord op deze vraag is ***hashing***.

Hashing is een techniek waarmee je een ***stuk tekst***, bijvoorbeeld een wachtwoord, via een ***algoritme*** omvormt naar een ***groot getal***. Het is - in tegenstelling tot encryptie - echter onmogelijk om het getal terug om te vormen naar de originele tekst. Door niet het wachtwoord, maar wel het gehashte getal op te slaan, is er geen risico dat mensen je wachtwoord zouden kunnen lezen. In het ergste geval kunnen ze het getal lezen, maar dat kunnen ze onmogelijk omvormen naar jouw wachtwoord. Dat betekent ook dat op het moment dat je je wachtwoord invoert, de website of applicatie het ingevoerde wachtwoord eerst zal hashen om nadien het bekomen getal te vergelijken met het opgeslagen getal.

Een eenvoudige manier om een tekst te hashen is: de ***letters omzetten naar een getal***, al deze ***getallen met elkaar te vermenigvuldigen*** en tot slot de ***rest te berekenen van de deling van dit product door de maximale hashwaarde***. (Om te vermijden dat de gehashte getallen immens groot kunnen zijn, wordt er steeds een maximale hashwaarde vastgelegd.)

Hier zie je een voorbeeld van hoe je dat kan doen met de eerste vijf letters van het alfabet en een maximale hashwaarde van 100:

A	***B***	***C***	***D***	***E***
2	3	5	7	11

Deze tabel koppelt aan elke letter een getal. Je berekent de hash van de tekst ***ACCE*** door de volgende bewerking uit te voeren:

(2 x 5 x 5 x 11) mod 100
= 550 mod 100
= 50.

In de rechtse tabel zie je de hashwaarde voor een aantal wachtwoorden. Merk op dat meerdere wachtwoorden dezelfde hashwaarde kunnen krijgen. Dit zorgt ervoor dat je nooit met 100 % zekerheid van een hashwaarde terug kan gaan naar het originele wachtwoord.
In de praktijk is de kans op gelijke hashwaarden wel heel klein.

Merk op dat deze werkwijze gebruikmaakt van ***priemgetallen***. Priemgetallen met elkaar vermenigvuldigen is heel eenvoudig voor de computer.
De omgekeerde bewerking, de priemfactoren zoeken van een heel groot getal (in de praktijk groter dan 10^{600}), is heel moeilijk.

Paswoord	***Hash***
DAACD	80
CBDAB	30
DBCEB	65
ACBEA	60
ACCDD	50
EEDBC	5
BCCDC	25
CEBAE	30
BABCA	80
CDECE	75

Uitdaging: Kan jij de hash berekenen van het wachtwoord BBCDAA?

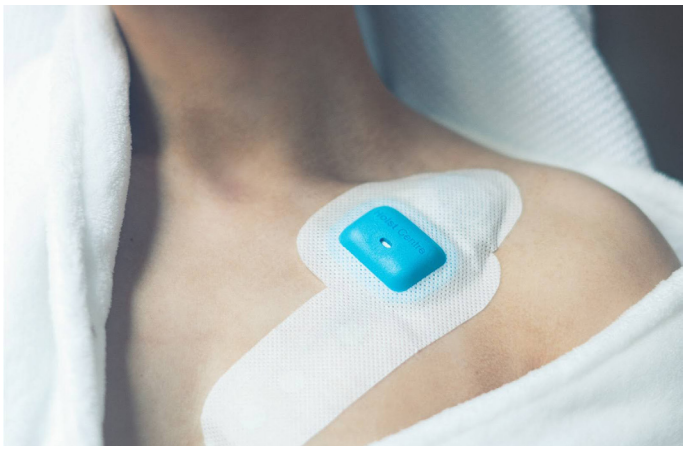
Moderne hash-algoritmes werken volgens een gelijkaardig principe maar zijn veel veiliger en een stuk complexer.
Een van de meestgebruikte hash-algoritmes is het ***Secure Hash Algorithm (SHA256)****. Dit algoritme zet een tekst om naar een binair getal van 256 bits. Er zijn dus $2^{256} \approx 10^{77}$ mogelijke waarden voor onze hash. Merk op dat er ongeveer 10^{80} protonen en neutronen in het waarneembare heelal zijn.*

Internet der dingen

Bijna elk elektrisch apparaat bevat tegenwoordig elektronica. Denk bijvoorbeeld aan een vaatwasmachine, een automatische deur of de thermostaat van je verwarming.
De elektronica in deze apparaten krijgt meer en meer de mogelijkheid om verbinding te maken met het internet. Dit zorgt ervoor dat apparaten zowel met jou als met andere apparaten kunnen communiceren. Zo kan je bijvoorbeeld een melding krijgen op je telefoon wanneer jouw vaatwasmachine klaar is of kan de elektronica ervoor zorgen dat de vaatwasmachine pas start wanneer je zonnepanelen voldoende stroom opwekken. ***Al deze met het internet verbonden apparaten vormen samen het 'internet der dingen' of Internet of Things (IoT).***

Deze elektronica is verantwoordelijk voor de sturing van het apparaat. In een vaatwasmachine zal de elektronica er bijvoorbeeld voor zorgen dat het water opwarmt tot de juiste temperatuur en dat het vaatwastablet op het juiste moment in de machine valt. Bij een automatische deur zal de elektronica interpreteren wat een bewegingssensor meet en op basis daarvan de deur openen.

Ook in de ***medische wereld*** zijn er steeds meer apparaten verbonden met het internet. Zo kan de radioloog een echograaf gebruiken die de medische beelden automatisch doorstuurt naar een databank of krijgt een verpleegkundige een melding wanneer er een probleem is met de gemeten vitale waarden van een patiënt.
Om patiënten vroeger te kunnen ontslaan uit het ziekenhuis worden ze steeds meer opgevolgd via wearables. De gegevens die een wearable verzamelt, moeten bij de dokter terechtkomen.



© imec

Daarbij spelen verschillende concepten een rol, zoals authenticatie, databanken, encryptie, datacommunicatie en sensoren.

Uitdaging: Ga in de dagelijkse omgeving op zoek naar vijf verschillende apparaten die met het internet verbonden zijn. Computers, tablets en smartphones tellen niet mee.

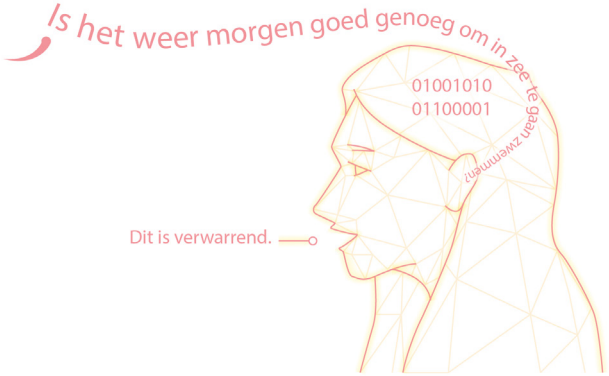
Natuurlijke taalverwerking, grote taalmodellen en chatbots

Je hebt ongetwijfeld al ***taaltechnologie*** gebruikt, bijvoorbeeld om een menukaart automatisch te laten vertalen op reis in het buitenland, om Microsoft Copilot een e-mail te laten opstellen, of om de weg te vinden met je GPS.
Om automatisch een tekst te 'begrijpen' wordt software voor 'natuurlijke taalverwerking' gebruikt. Via kennisgebaseerde systemen of technieken uit machine learning, zoals het trainen van modellen om tekst of geluidsfrequenties te herkennen, kunnen computers op een intelligente manier werken met taal.

Chatbots zijn softwaresystemen die kunnen interageren met mensen via getypte tekstboodschappen. Een chatbot is dus niets anders dan een computer waarmee je kan chatten.

Sommige specialisten laten een chatbot het ***anamnesegesprek*** afnemen. De chatbot vat dat gesprek samen, waarop de dokter de samenvatting voor de consultatie doorneemt. De dokter kan daardoor per patiënt tijd besparen. De chatbot gebruikt ***'natuurlijke taalverwerking' (Natural Language Processing of NLP)*** om de bruikbare informatie uit het gesprek te halen. Op getypte tekst kan bijvoorbeeld ook automatische sentimentanalyse toegepast worden. Een chatbot kan zo merken dat je geïrriteerd raakt als een gesprek stroef verloopt en je dan doorverbinden met een menselijke collega. Ook fysieke robots en spraakassistenten doen dat, zoals je kan lezen op de fiche over spraakherkenning en spraaksynthese.

De meest eenvoudige chatbots, waaronder de eerste chatbots zoals ELIZA, zijn ***kennisgebaseerde systemen***. Bij zulke chatbots zijn verschillende scenario's expliciet geprogrammeerd. Dit leidt automatisch tot beperkingen: als je bijvoorbeeld een vraag aan de chatbot anders formuleert dan geprogrammeerd, dan zal de chatbot de vraag niet herkennen. Zulke chatbots zijn vaak niet populair, maar worden toch nog veel gebruikt.



Moderne chatbots maken gebruik van machine learning, in het bijzonder van ***deep learning***.
Zo zijn ChatGPT en Google Gemini gebaseerd op een ***groot taalmodel (Large Language Model*** of LLM); deze systemen kunnen het volgende woord in een tekst voorspellen op basis van de voorgaande woorden in de tekst, en zorgen ervoor dat de computer steeds beter taal 'begrijpt'.
De ***grote taalmodellen*** maken via ***machine learning***-technieken gebruik van ***word embedding***: de woorden in een tekst worden omgezet naar getallen en daarbij wordt zoveel mogelijk informatie over de woorden opgeslagen via deze getallen, zoals de betekenis van het woord, welke andere woorden er in veel zinnen samen met het woord voorkomen, de plaats van het woord in een zin, en

de context van een zin waarin het woord staat.

Naast chatbots wordt NLP op nog andere manieren toegepast in de sector van de ***gezondheidszorg***. En sinds de komst van de zogenaamde grote taalmodellen lukt dat steeds beter. NLP wordt bijvoorbeeld ingezet om informatie uit een ***elektronisch patiëntendossier*** te halen. Ook ***automatische vertaling*** wordt steeds beter. Gelukkig maar, want in de VS doen spoedgevallendiensten daar vaak een beroep op. Bij ontslag uit spoedgevallendiensten krijgen patiënten soms instructies mee naar huis over welke medicatie ze moeten innemen of wanneer ze op consultatie moeten komen. Omdat niet alle patiënten het Engels voldoende machtig zijn, geven ze deze instructies graag mee in de moedertaal van de patiënt[1].

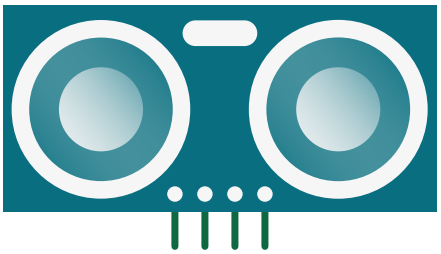
Uitdaging: In de jaren 60 van de vorige eeuw werd de software ELIZA ontworpen op het Massachusetts Institute of Technology (MIT), als een experiment om te onderzoeken of ELIZA kon overtuigen als psychotherapeut.
Chat zelf met ELIZA via dwengo.org/zorg/kaartjes/eliza

De ontwikkelingen in de taaltechnologie leveren nieuwe tools om fake nieuws op te sporen, criminaliteit te bestrijden en de gezondheidszorg efficiënter te maken; ook in de bedrijfswereld zijn er tal van toepassingen.
Je kan meer hierover lezen op de Dwengo-website: over sentimentanalyse, over ChatGPT en co en over grote taalmodellen.

1: Taira, B., Kreger, V., Orue, A., & Diamond, L. (2021). A Pragmatic Assessment of Google Translate for Emergency Department Instructions. Journal of General Internal Medicine, 36(11), 3361–3365.

Sensoren

Sensoren vind je tegenwoordig overal. Ze zijn er dan ook in verschillende soorten en maten. Denk bijvoorbeeld aan een ***bewegingssensor*** die de verlichting controleert, een ***snelheidssensor*** in een flitspaal, of een ***lichtsensor*** in je smartphone die ervoor zorgt dat de helderheid van je scherm automatisch wordt aangepast. Er zijn dus heel wat verschillende soorten sensoren, maar welke fundamentele eigenschap hebben deze sensoren gemeen? ***Elke sensor zet een fysisch fenomeen (bv. temperatuur, licht, bloedsuiker) om in een elektrisch signaal.*** Dit elektrisch signaal kan dan gemeten worden met een computer, die op zijn beurt de waarden kan verwerken, opslaan en analyseren.



Sensoren zijn vaak goedkoop, waardoor ze in heel veel producten ingebouwd worden. Wens je echter een grote nauwkeurigheid of breed bereik (bv. van mg tot enkele kg) dan kan de sensor duur zijn. Moderne ***elektrische wagens***, bijvoorbeeld, bevatten vaak ***meer dan 100 sensoren***; deze sensoren meten eigenschappen zoals de bandenspanning of de temperatuur van de batterij.
Ook in de ***zorgsector*** wordt er gretig gebruikgemaakt van sensoren, bijvoorbeeld om de ***vitale eigenschappen van een patiënt*** op te volgen. Maar het blijft niet bij het registreren van eigenschappen zoals hartslag, bloeddruk en lichaamstemperatuur aan de hand van sensoren, onderzoekers werken ook volop aan zogenaamde biosensoren die de aanwezigheid van bepaalde moleculen kunnen opsporen. Een van de best gekende ***biosensoren*** meet de bloedsuikerspiegel; deze sensor kan patiënten met diabetes ondersteunen bij hun behandeling. Andere soorten biosensoren kunnen dan weer ingezet worden om de aanwezigheid van bepaalde virussen in de lucht op te sporen.

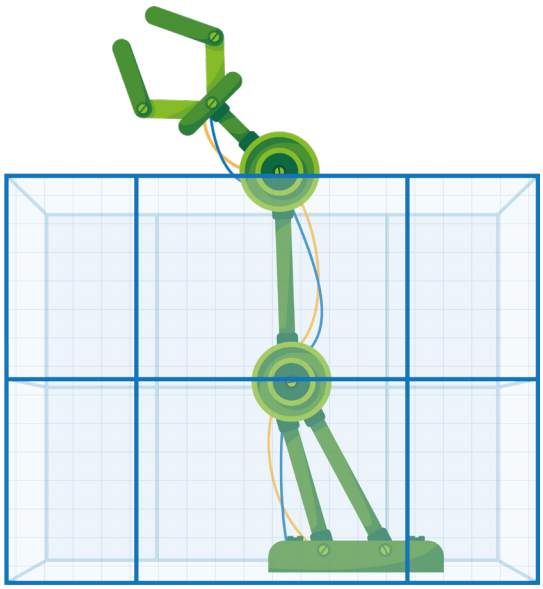
Naast het meten van een fysisch fenomeen zullen veel sensoren deze gemeten waarden ook al deels verwerken. De sensor zal bijvoorbeeld ruis wegfilteren of de gemeten waarde omzetten naar SI-eenheden. Op die manier kan je de waarde van de sensor gemakkelijker interpreteren. De verwerking van de gemeten waarde kan zeer complex zijn. Zo is er bijvoorbeeld de Gentse start-up IntelliProve die een app maakt waarmee je een hartslag kan meten met behulp van de camera van je smartphone. Deze camera bestaat uit miljoenen lichtsensoren die het licht dat op je camera schijnt, registreren. Er zijn drie soorten van deze lichtsensoren, elk gevoelig voor een andere kleur van licht (rood, groen en blauw licht). Je smartphone zal deze gemeten waarden omzetten naar pixels met een RGB-waarde[1]. De app van de Gentse start-up doet dan een analyse van de RGB-waarden van opeenvolgende beelden. Zij zijn erin geslaagd om op die beelden een variatie in huidskleur nauwkeurig genoeg te detecteren zodat ze met de app iemands hartslag kunnen meten door de persoon te filmen.

Uitdaging: Misschien ken je iemand met een smartwatch. Welke sensoren zitten er daarin?

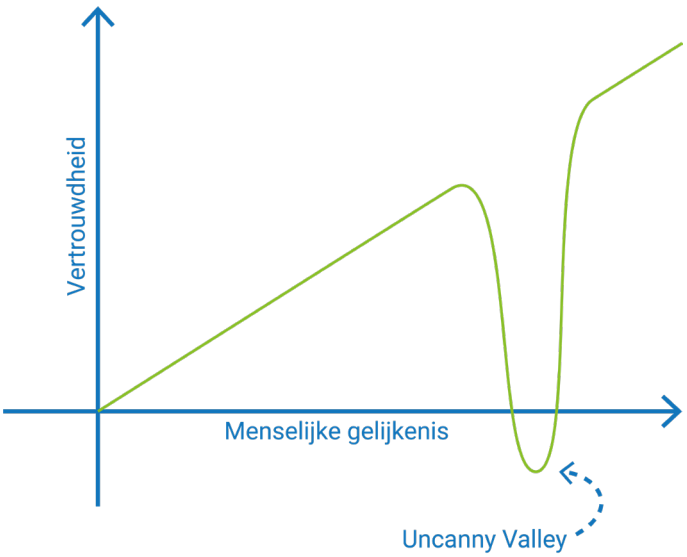
1: Meer info over RGB-waarden kan je vinden in de fiche over digitale beelden.

Sociale robots

Je kent waarschijnlijk het beeld van grote robotarmen die in een fabriek auto's assembleren. Dergelijke ***industriële robots*** kunnen ***één specifieke taak snel en precies uitvoeren***. Ze zijn voorgeprogrammeerd om telkens dezelfde bewegingen uit te voeren en kunnen zich niet aanpassen aan hun omgeving. Om die reden is het heel gevaarlijk om in de buurt van zo'n robot te komen. ***Zo'n robotarm zal niet stoppen als jij op het voorgeprogrammeerde pad komt te staan en kan je daardoor ernstig verwonden***. Dergelijke robots kunnen dus niet gebruikt worden om te interageren met mensen.



Sociale robots zijn specifiek ontworpen om te interageren met mensen. Omdat een dagdagelijkse omgeving veel chaotischer is dan een gecontroleerde industriële productielijn, is het een stuk complexer om deze sociale robots goed te doen werken. Ze hebben bijvoorbeeld heel wat sensoren nodig om te voorkomen dat ze botsen met objecten en personen. Bovendien wordt er van hen verwacht dat ze de mensen rondom hen 'begrijpen', zowel via verbale als non-verbale communicatie, en er op een vriendelijke manier mee omgaan. En ze moeten vooral verschillende taken kunnen uitvoeren (bijvoorbeeld een patiënt in bed leggen of een glas water komen brengen).



Bouwers van sociale robots proberen vaak om die robot zo veel mogelijk op een mens te doen lijken. Dit uiterlijk schept verwachtingen: van een robot met ogen verwacht je dat hij ziet, van een robot met wielen dat hij rijdt, van een androïde robot (een robot die er heel menselijk uitziet) verwacht je ook menselijke handelingen. Wanneer een robot die verwachtingen niet waarmaakt, kan dat teleurstellend zijn en ervaar je de robot mogelijk als iets negatiefs. Het is verwarrend als een robotdier praat of als een robot deels bedekt is met 'huid', maar er ook mechanische onderdelen zichtbaar zijn. Mensen vinden het meestal leuk als een robot er menselijk uitziet, tenzij de robot te veel op een mens lijkt, dan vinden ze dat griezelig. Dit fenomeen heet de ***Uncanny Valley***: hoe meer een robot op een mens lijkt, hoe meer menselijke gedragingen men verwacht en hoe groter de kans dat de robot teleurstelt.

Uitdaging: Ga op zoek naar foto's van robots in de Uncanny Valley.

Spraakherkenning en spraaksynthese

Misschien rijdt er bij jou in de supermarkt ook een robot rond aan wie je kan vragen waar de frisdrank staat. Spraakherkenningstechnologie (spraak naar tekst) én spraaksynthesesoftware (tekst naar spraak) maken het mogelijk om via gesproken taal te communiceren met een fysieke robot of een digitale assistent zoals Siri, Alexa en de voice assistant in de auto.
Spraakherkenningstechnologie zet een geluidsopname om naar een digitaal tekstbestand. Wat jij zegt, wordt zo automatisch omgezet naar geschreven tekst. Software voor 'natuurlijke taalverwerking' zal deze tekst interpreteren en een geschreven antwoord formuleren. Dat antwoord wordt dan met spraaksynthesesoftware omgezet naar geluid om de robot het antwoord te laten uitspreken.

De robot 'begrijpt' dus wat je zegt door de spraakherkenningssoftware in combinatie met 'natuurlijke taalverwerking'. En de spraaksynthesesoftware is er om de robot te laten spreken. Dit is niet eenvoudig. Het systeem moet bijvoorbeeld menselijke spraak kunnen onderscheiden van eventueel achtergrondlawaai. Voor een robot is het ook moeilijk om een tekst te 'begrijpen'. Iedereen drukt zich op zijn eigen manier uit, zelfs in dezelfde taal. Toch slagen grote taalmodellen er soms al in om ironie te herkennen of dialecten van eenzelfde taal van elkaar te onderscheiden. Ook spraaksynthese heeft met uitdagingen te kampen, zoals realistisch stemgeluid: een stem die weinig intonatie vertoont, is niet aangenaam om naar te luisteren.

Dokters gebruiken bijvoorbeeld spraakherkenningssoftware om hun bevindingen bij een onderzoek in een ***elektronisch patiëntendossier*** in te spreken in plaats van te typen.
Spraaksynthese werd ook gebruikt om ***een acteur die door keelkanker zijn stem was verloren terug te laten spreken***. De acteur Val Kilmer werd in 2014 door keelkanker getroffen. Als gevolg van de behandeling is hij moeilijk verstaanbaar en kan hij niet meer communiceren en creatief zijn, zoals hij zou willen. Aan de hand van bestaande geluidsopnames van Kilmers stem bouwde Sonantic een AI-model om de stem van Kilmer zoveel mogelijk te benaderen[1].

Uitdaging: Met NotebookLM van Google kan je een podcast genereren aan de hand van een tekst, bijvoorbeeld het schoolreglement.
Surf naar dwengo.org/zorg/kaartjes/notebooklm en probeer het uit!

1: Flynn, J. (2021). Helping actor Val Kilmer reclaim his voice [Blogpost]. Geraadpleegd op 19 juni 2022 via https://www.sonantic.io/blog/helping-actor-val-kilmer-reclaim-his-voice.

Tracking

Heel wat internetbedrijven zoals Google, YouTube en Facebook halen het grootste deel van hun ***inkomsten uit reclame***. Hun klanten zijn dus niet de gebruikers van hun websites, maar wel de bedrijven die bij hen advertenties plaatsen. ***Aan deze bedrijven verkopen ze een deel van jouw aandacht***; eigenlijk ben jij dus hun product.
Om meer geld te kunnen vragen voor de advertenties moeten ze die op een gerichte manier kunnen inzetten. Een advertentie voor voetbalschoenen heeft immers meer effect op mensen die voetbal spelen dan op mensen die dat niet doen. Om meer te kunnen verdienen willen ze dus ***zoveel mogelijk te weten te komen over jou***. Om die informatie te verzamelen, ***proberen deze bedrijven je op zoveel mogelijk plaatsen te volgen***. Dit heet ***tracking***.

Tracking kan op verschillende manieren. Zo gebruiken websites meestal cookies. Cookies zijn kleine bestanden die kunnen worden opgeslagen in je internetbrowser wanneer je een website bezoekt. ***Cookies zijn vaak nuttig***: zo zorgen ze ervoor dat je niet telkens je gebruikersnaam en wachtwoord moet ingeven wanneer je een website bezoekt. ***Toch is er een specifieke soort van cookies die gebruikt kunnen worden om je te volgen op het internet***. Deze soort cookies zijn de zogenaamde ***third party cookies*** of 'cookies van een derde partij'. Dit zijn cookies die niet door een website zelf worden opgeslagen in je browser, maar bijvoorbeeld door een advertentie op die website. Deze advertentie komt dan van een andere plaats op het internet (bijvoorbeeld van Google). Door dit systeem kan Google te weten komen welke websites jij allemaal bezoekt. Bezoek je dus vaak de website van de lokale voetbalclub, dan is de kans groter dat je reclame voor voetbalschoenen te zien zal krijgen.

Uitdaging: Welke cookies zijn er opgeslagen in jouw internetbrowser?
Ga in de instellingen van je browser op zoek naar de lijst met opgeslagen cookies.
Weet je van al deze websites waarom ze cookies opslaan?

Wist-je-datje: In de meeste browsers kan je instellen dat cookies van derden automatisch geblokkeerd worden. Deze instelling staat echter standaard uit in veel browsers. Je moet die zelf aanzetten indien je deze cookies wil blokkeren.

Er zijn naast cookies nog andere manieren om je te volgen. Zo zullen socialemediaplatformen je gedrag opslaan om te weten wat je interesses zijn. Ook zijn er apps die bijvoorbeeld je locatie kunnen opslaan. Door te achterhalen waar je vaak bent (bv. een specifiek restaurant), komt een bedrijf ook meer over je te weten. Op de Dwengo-website kan je meer lezen over profilering.