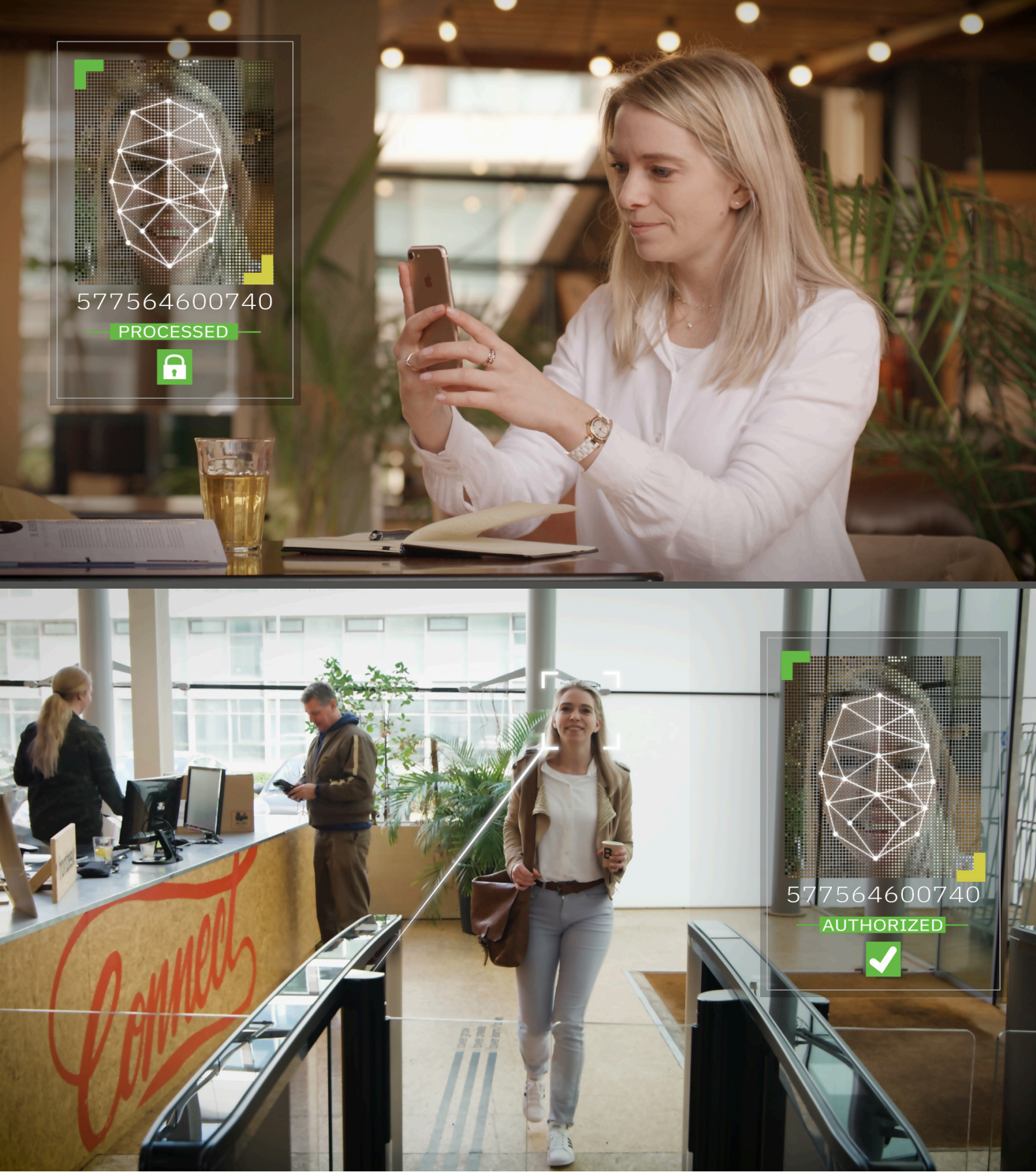


GEZICHTSHERKENNING IN **TOEGANGSCONTROLE.**

EEN **WHITEPAPER** MOGELIJK GEMAAKT DOOR BOON EDAM

BOON EDAM
YOUR **ENTRY** EXPERTS.

INLEIDING.

In deze whitepaper wordt toegelicht hoe toegangscontrole op basis van gezichtsherkenning werkt. Daarnaast gaan we in op de aandachtspunten waarmee u rekening moet houden bij het selecteren van een toegangscontrolesysteem dat gebruikmaakt van gezichtsherkenning. Aangezien gezichtsherkenning een relatief nieuwe technologie is op de markt, bent u wellicht benieuwd welke aspecten een rol spelen wanneer u overweegt zo'n systeem toe te passen. Na het lezen van deze whitepaper zult u een duidelijker inzicht hebben in wat gezichtsherkenning binnen toegangscontrole precies inhoudt en waar u op moet letten bij de aanschaf van een dergelijk systeem.

SOORTEN **BIOMETRIE**

Biometrische kenmerken zijn alle meetbare eigenschappen van het menselijk lichaam. Biometrie wordt steeds vaker ingezet binnen toegangscontrole. De vier meest gebruikte vormen zijn:

IRISSCAN

Elke menselijke iris heeft unieke kenmerken. Tijdens een irisscan worden putjes, lijntjes en groeven in de iris herkend en omgezet in een iriscode. Deze code wordt vervolgens vergeleken met een databank om toegang te verlenen.

HANDPALMADERS

Met behulp van infraroodlicht wordt het unieke netwerk van aders en haarvaten in de hand gemeten. Sommige handpalmlezers registreren daarnaast ook lijnen en verdikkingen in de hand. Deze gegevens vormen een uniek profiel dat gekoppeld kan worden aan een geautoriseerde persoon.

VINGERAFDRUK

Er bestaan verschillende types vingerafdrukscanners. Al deze scanners meten het unieke lijnenpatroon in de huid. De geregistreerde gegevens kunnen vervolgens gebruikt worden om te bepalen of toegang verleend wordt.

GEZICHTSHERKENNING

De laatste vorm van biometrie binnen toegangscontrole is gezichtsherkenning. Hierbij filtert een algoritme het menselijke gezicht uit een foto of videobeeld. Binnen enkele milliseconden worden de unieke kenmerken van het gezicht vastgelegd en omgezet in een unieke code.

De gezichtsherkenningssoftware vergelijkt deze code vervolgens met een databank. Wanneer er een overeenkomst wordt gevonden, kan worden bepaald wie er op het beeld staat en of toegang al dan niet verleend moet worden.









GEZICHTSHERKENNING

Gezichtsherkenning kan op verschillende manieren worden toegepast. Deze whitepaper focust op het gebruik binnen toegangscontrole. Hieronder lichten we kort de verschillende toepassingen toe:

MASSAMONITORING

Bij massasurveillance wordt gezichtsherkenning ingezet om individuen te herkennen in een mensenmassa. Om dit mogelijk te maken, is gespecialiseerde hardware en krachtige software nodig.

PERSOONLIJK

Deze vorm van gezichtsherkenning, vaak toegepast op mobiele toestellen zoals smartphones, maakt gebruik van relatief eenvoudige software en hardware. Het doel is om het gezicht te gebruiken als alternatief voor een pincode.

FORENSISCHE OPSPORING

Gezichtsherkenning kan ook worden ingezet om de route van een persoon te reconstrueren op basis van opgenomen videobeelden. Met deze gegevens kan bijvoorbeeld achterhaald worden waar een gezochte persoon zich de voorbije 24 uur heeft bevonden.

TOEGANGSCONTROLE

Tot slot kan gezichtsherkenning worden toegepast binnen toegangscontrole. Het is daarbij belangrijk dat de software in real-time werkt, waarbij camerabeelden van verschillende locaties vergeleken worden met een databank. Afhankelijk van de grootte van deze databank wordt gekozen voor een server die snel genoeg kan bepalen of iemand geautoriseerd is, waarna de toegangspoort geopend kan worden.

IN DEZE **WHITEPAPER:**

VOORDELEN VAN GEZICHTSHERKENNING
COMPONENTEN VAN GEZICHTSHERKENNING
TECHNISCHE ASPECTEN
IN DE PRAKTIJK
DIGITALE VEILIGHEID



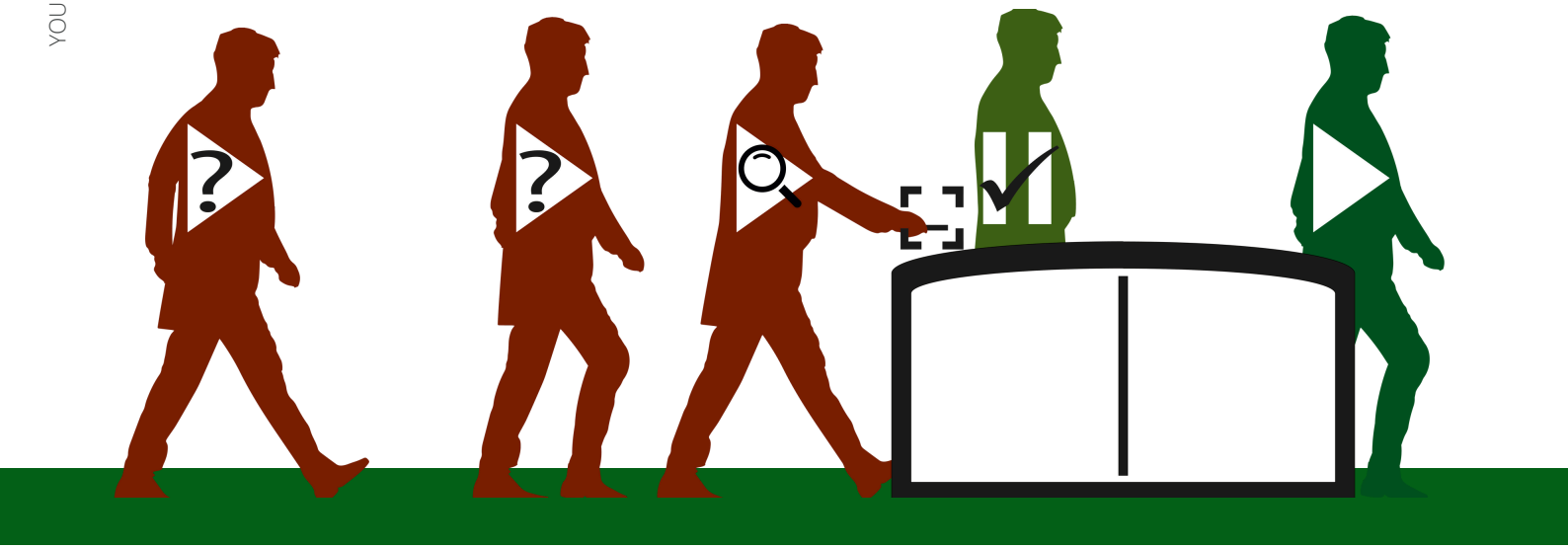




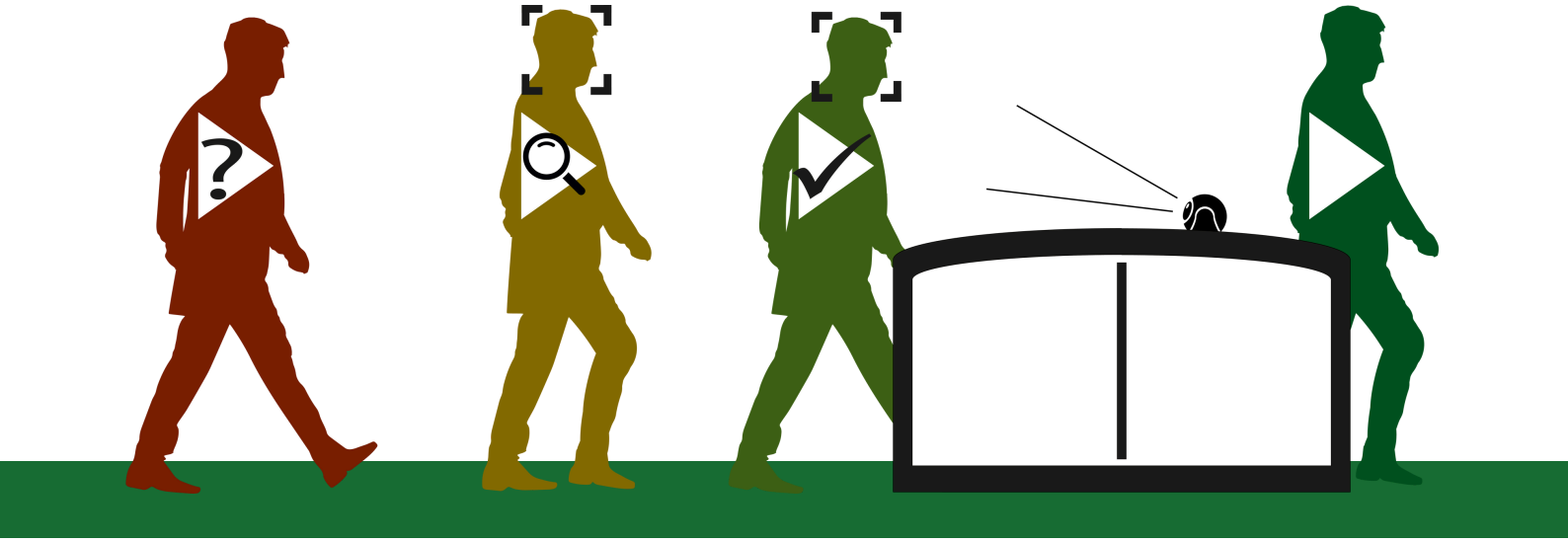


VOORDELEN VAN GEZICHTSHERKENNING.

‘KLASSIEKE’ **KAARTLEZER**



GEZICHTSHERKENNING



VERBETERDE **DOORSTROMING**

Een van de grootste voordelen van gezichtsherkenning binnen toegangscontrole is dat de persoon die toegang wenst geen wachttijd ervaart aan de toegang. De software registreert het gezicht van een naderende persoon nog vóór die de toegangspoort bereikt. Tijdens het benaderen kan zo worden bepaald of de persoon geautoriseerd is om het gebouw te betreden. Bevindt de geautoriseerde persoon zich vlak voor of in de poort, dan opent het systeem automatisch. Zo wordt voorkomen dat een andere persoon ongewenst mee naar binnen wandelt. Het resultaat is een vlotte, veilige en contactloze doorgang door de toegangscontrole.



ALTIJD SNELLE TOEGANG

Omdat biometrische gezichtsherkenning gebaseerd is op iets wat u altijd bij zich draagt - uw gezicht - zult u nooit voor een gesloten deur staan. Het feit dat elk gezicht uniek is, maakt het mogelijk om de eigenschappen van het gelaat te gebruiken om personen van elkaar te onderscheiden en correct te identificeren.

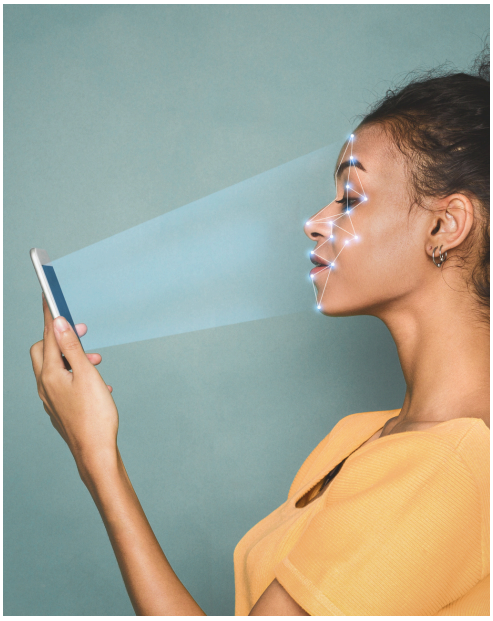
Een bijkomend voordeel is dat u als gebruiker nauwelijks nog actief hoeft mee te werken wanneer u een toegangscontrolepunt nadert. Zodra uw gezicht in het gezichtsveld van de camera komt, controleert de software automatisch of u geautoriseerd bent. Toegangspassen worden daarmee overbodig en kunnen dus ook niet meer vergeten worden. Bovendien hoeft u niet te wachten tot een collega zijn badge tussen zijn spullen heeft gezocht, en hebt u uw handen vrij om bijvoorbeeld uw jas en tas mee naar binnen te nemen.

GEEN DOORGEGEVEN BADGE

Een vaak voorkomend probleem binnen toegangscontrole is het doorgeven van een persoonlijke toegangsbadge aan een collega. Dit oneigenlijk gebruik maakt het mogelijk dat onbevoegde personen een gebouw betreden. Door gebruik te maken van gezichtsherkenning kan een onbekend individu niet zomaar door de toegangscontrole geraken.

Bovendien maakt gezichtsherkenning het onmogelijk om een toegangsbadge te stelen of te kopiëren. Het resultaat is een duidelijke versterking van het algemene veiligheidsniveau.





BIOMETRIE IS CONTACTLOOS

Veel mensen aarzelen wanneer hen gevraagd wordt om hun iris of vinger te laten scannen. Die (onbewuste) aarzeling ontstaat vaak omdat ze het systeem niet kennen of het onaangenaam vinden om actief een lichaamsdeel tegen een scanner te houden. Dit belemmert niet alleen de vlotte doorgang, maar zorgt er ook voor dat de toegangscontrole als minder gebruiksvriendelijk wordt ervaren.

Een groot voordeel van gezichtsherkenning is dat een camera de gebruiker vanop afstand registreert. Daardoor hoeft de gebruiker geen ongemakkelijke houding aan te nemen of fysiek contact te maken met de toegangspoort. Zodra de persoon zich binnen het ingestelde bereik van de camera bevindt, wordt hij of zij automatisch geverifieerd en kan toegang verleend worden, zonder dat vertraging optreedt.

COMPONENTEN VAN GEZICHTSHERKENNING.

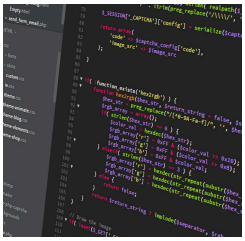
Bij de keuze voor gezichtsherkenning binnen toegangscontrole moet er rekening mee gehouden worden dat het systeem uit verschillende componenten bestaat. Deze componenten zijn vaak afkomstig van verschillende leveranciers en moeten correct op elkaar worden afgestemd. Daarom is het belangrijk om goed in kaart te brengen welke partijen samen een vlot en betrouwbaar werkend systeem kunnen realiseren. In het algemeen werken de volgende componenten met elkaar samen:



CAMERA EN ANDERE SENSOREN

De camera is een cruciale schakel in de betrouwbare werking van gezichtsherkenningssoftware. Er zijn diverse camera's beschikbaar van hoge kwaliteit. Uit ervaring blijkt dat een doordachte selectie, zowel op technisch als esthetisch vlak, bijdraagt aan het gebruiksgemak en de acceptatie door de gebruikers.

Het selectieproces gaat verder dan enkel het aantal megapixels: ook lichtgevoeligheid, het type lens en de rekenkracht van de chip zijn belangrijke factoren. Daarnaast kan er gekozen worden voor extra sensoren die in staat zijn een echt gezicht te onderscheiden van bijvoorbeeld een afbeelding op een foto.



GEZICHTSHERKENNINGSSOFTWARE

Ook wel het kloppend hart van het systeem. De gezichtsherkenningssoftware zet gezichten om in een code, die vervolgens wordt vergeleken met een vooraf ingestelde databank. Deze herkenning gebeurt via een reeks algoritmes. De gezichtsherkenningssoftware werkt vaak onafhankelijk van andere toegangscontrolesoftware. Daardoor is het mogelijk om een stand-alone systeem op te zetten waarbij de software draait op een externe processor.

Het is essentieel dat zowel de software als het systeem voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en gebruikmaken van de juiste encryptiestandaarden.



TOEGANGSCONTROLESYSTEEM

Een toegangscontrolesysteem bestaat vaak uit meerdere softwareoplossingen. Deze maken meestal deel uit van een geïntegreerd Security Management- of Building Managementsysteem. Het is dus mogelijk dat de gezichtsherkenningssoftware moet worden geïntegreerd in een dergelijk platform.

In de praktijk betekent dit dat verschillende modules met elkaar verbonden worden en vervolgens centraal beheerd kunnen worden via één programma. De module 'gezichtsherkenningssoftware' wordt in dat geval geïntegreerd via een API.



FYSIEKE TOEGANG

Wanneer gezichtsherkenning wordt toegepast binnen toegangscontrole, gebeurt dit altijd in combinatie met een fysiek toegangsproduct. Zonder zo'n barrière is het namelijk niet mogelijk om onbevoegde personen effectief te weren. Er bestaan verschillende types barrières, elk met hun eigen niveau van beveiliging.

De componenten kunnen op uiteenlopende manieren geconfigureerd worden. Zo is het mogelijk om één fysiek product te voorzien waarin gezichtsherkenning volledig geïntegreerd is, maar ook om de componenten afzonderlijk van elkaar toe te passen.

TECHNISCHE ASPECTEN.



LICHTOMSTANDIGHEDEN

Een van de belangrijkste aspecten voor een correcte implementatie van gezichtsherkenning is de hoeveelheid licht in de ruimte waarin de camera wordt geplaatst. Bij toegangscontrole gebeurt gezichtsherkenning vaak binnen, waardoor de lichtomstandigheden in zekere mate beïnvloedbaar zijn.

Overbelichting vormt daarbij een grote uitdaging. Denk aan felle zon, glasreflecties of ruimtes met een hoog atrium. Door de wisselende lichtinval wordt zowel van de camera als van de gezichtsherkenningssoftware veel gevraagd. Onderbelichting is daarentegen eenvoudiger te corrigeren. Vaak volstaat een aanpassing in de camerainstellingen om gezichten correct te kunnen herkennen. Het is aangeraden om hiervoor een expert in te schakelen die de juiste afstellingen kan voorzien.

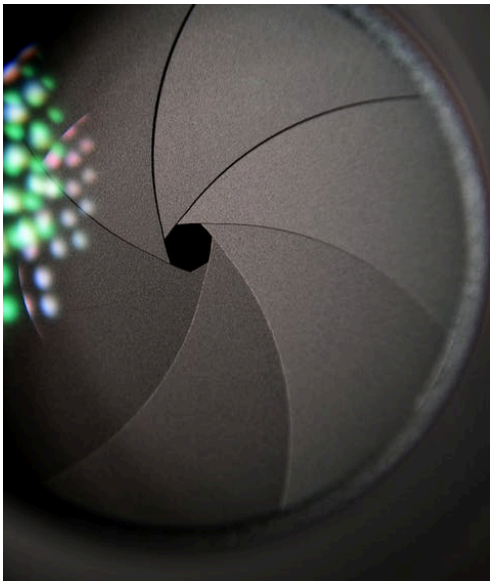
CAMERAPOSITIE

Bij het plaatsen van de camera is het belangrijk goed na te denken over het beeld dat deze zal registreren. Hoe dichter de camera zich bij de persoon bevindt die toegang wenst, hoe beter de beeldkwaliteit doorgaans zal zijn.

Ook de positie van de camera ten opzichte van de gebruiker speelt een cruciale rol. Idealiter wordt de camera geplaatst op een plek waar de gebruiker automatisch naartoe kijkt wanneer hij of zij de toegangscontrole nadert. Zo zijn er geen extra handelingen nodig om herkend te worden.

Tot slot kan er om esthetische redenen gekozen worden om de camera te integreren in het toegangsproduct of om deze extern te bevestigen.





CAMERAFOCUS

Bij de installatie van de camera is het cruciaal om goed na te denken over de focus. Die moet gericht zijn op de zone waar het gezicht gescand wordt. Het focuspunt mag niet te ver van de toegangscontrole liggen (om te voorkomen dat personen te vroeg worden herkend), maar ook niet te dichtbij (zodat gebruikers niet hoeven te wachten op toegang).

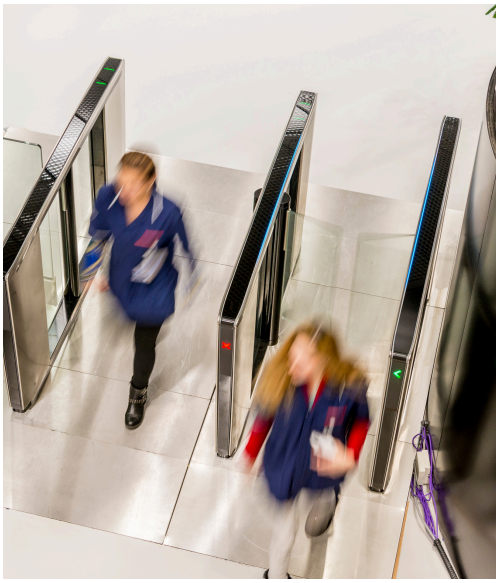
De camerafocus bepaalt ook het herkenningsgebied waarbinnen een gezicht succesvol kan worden gedetecteerd. Dit kan in de software ingesteld worden door een specifiek deel van het camerabeeld te selecteren waarin de gezichtsherkenning actief is.

IN DE PRAKTIJK.

GEBRUIKERSFLOW

In de praktijk blijkt dat het gebruik van beveiligde doorloopsluizen zorgt voor een natuurlijke, voorwaartse houding van de gebruiker. Mensen bewegen zich in één lijn, met het gezicht naar voren gericht, door het toegangsproduct. Zo ontstaat een relatief compacte zone waarbinnen alle gezichten goed zichtbaar zijn voor herkenning.

Een belangrijk voordeel van gezichtsherkenning in een toegangscontroleoplossing is dat het de doorstroom van gebruikers optimaliseert. Doordat iedereen zich in dezelfde richting beweegt en de sluis als een continue stroom passeert, blijft de flow behouden. De gezichtsherkenning zorgt ervoor dat de authenticatiesnelheid voldoende hoog ligt om deze stroom moeiteloos te ondersteunen.





AANBIEDEN VAN HET GEZICHT

Eerder in deze whitepaper werd aangegeven dat de gebruiker geen extra handelingen hoeft te verrichten wanneer gezichtsherkenning wordt toegepast binnen toegangscontrole. Een belangrijke voorwaarde hiervoor is dat de gebruiker zich ervan bewust is dat de gezichtsherkenningssoftware het gezicht correct moet kunnen scannen.

In de praktijk betekent dit dat het gezicht grotendeels onbedekt en duidelijk zichtbaar moet zijn voor de camera. Toegang verkrijgen met bijvoorbeeld een mondmasker of terwijl men achterom kijkt, is dan ook niet mogelijk. Een minimale vorm van medewerking van de gebruiker is dus vereist om het systeem correct te laten functioneren.

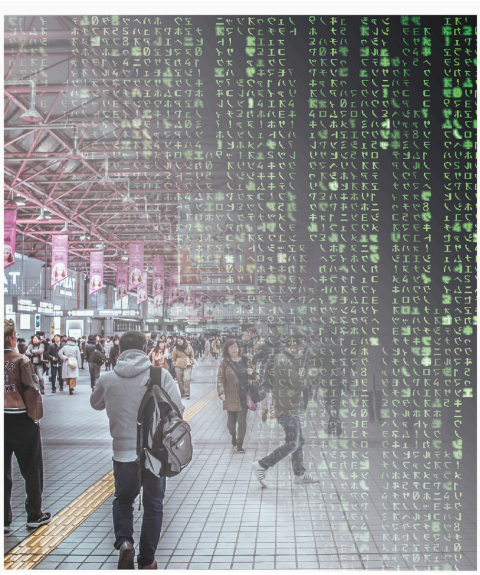
INTERACTIE MET DE GEBRUIKER

Bij het gebruik van gezichtsherkenning en bij toegangscontrole in het algemeen is het belangrijk dat er duidelijke terugkoppeling is naar de gebruiker. Wanneer meerdere personen kort na elkaar gebruikmaken van een toegang, kunnen optische en akoestische signalen verduidelijken welke beslissing de software neemt.

Gezichtsherkenning is bijzonder geschikt voor omgevingen met veel terugkerende gebruikers. Eénmalige registratie volstaat om een gebruiker voor langere tijd toegang te verlenen. Bovendien raken frequente gebruikers snel vertrouwd met de interactie met het toegangscontrolesysteem.



DIGITALE VEILIGHEID.



ENCRYPTIE

Om te voorkomen dat gegevens en beelden die via een netwerk worden verstuurd eenvoudig gehackt kunnen worden, maakt gezichtsherkenningssoftware gebruik van encryptie. Encryptie houdt in dat digitale (beeld)informatie wordt versleuteld of gecodeerd. Zonder inzicht in de wijze waarop deze versleuteling is opgebouwd, is het voor onbevoegden onmogelijk om de informatie te lezen.

Er bestaan verschillende methoden om data te versleutelen. Afhankelijk van de bestaande infrastructuur en het videomanagementsoftwareplatform wordt een gepaste oplossing gekozen. Daarbij wordt onder meer gekeken of de data via een open of gesloten netwerk wordt verstuurd.

FRAUDEDETECTIE

De technologie rond gezichtsherkenning maakt snelle vooruitgang op het vlak van fraudedetectie. Er wordt voortdurend gezocht naar manieren om te voorkomen dat het systeem misleid wordt, bijvoorbeeld door een foto voor de camera te houden. Momenteel bestaan er twee methoden om fraude op te sporen en preventieve maatregelen te treffen:

- **Hardwarematige detectie:** via 3D-sensoren die de structuur van het gezicht scannen. Een alternatieve methode maakt gebruik van sensoren die de reflectie analyseren van een patroon van gekleurde lichtstralen dat op het gezicht wordt geprojecteerd.
- **Softwarematige detectie:** door het identificeren van minimale verschillen in videobeelden. Deze aanpak vereist aanzienlijke (video)rekenkracht, waardoor gebruikgemaakt moet worden van zwaardere en krachtigere servers.





GDPR/AVG

Zoals eerder in deze whitepaper vermeld, maakt gezichtsherkenning gebruik van biometrische gegevens. In het kader van de Uitvoeringswet Algemene Verordening Gegevensbescherming (AVG) en de General Data Protection Regulation (GDPR) is het belangrijk te weten dat biometrische gegevens onder de bijzondere categorie persoonsgegevens vallen. Deze mogen, onder strikte voorwaarden, worden gebruikt voor identificatiedoeleinden.

De gegevens mogen uitsluitend worden verwerkt voor authenticatie- of beveiligingsdoeleinden. Daarnaast moet de beheerder van het systeem kunnen aantonen dat de verwerking van deze gegevens volledig in overeenstemming is met de geldende regelgeving.

Het gebruik van gezichtsherkenning binnen toegangscontrole is dus wettelijk toegestaan, mits aan alle voorwaarden wordt voldaan.

CONCLUSIE.

Het doel van deze whitepaper is om u een eerste helder inzicht te bieden in wat gezichtsherkenning binnen toegangscontrole precies inhoudt en met welke aandachtspunten u rekening moet houden bij de selectie van het juiste systeem voor uw organisatie. We hebben het onderscheid toegelicht tussen verschillende vormen van biometrie en toepassingen van gezichtsherkenning. Daarnaast kreeg u een overzicht van de belangrijkste voordelen ten opzichte van klassieke toegangscontrolesystemen.

Verder maakten we u vertrouwd met de diverse componenten van een gezichtsherkenningssysteem en de technische en praktische factoren die van invloed zijn op een correcte werking. Tot slot werd kort ingegaan op digitale veiligheid en de toepasselijke regelgeving rond AVG/GDPR.

AANBEVELINGEN

Met deze whitepaper wil Boon Edam u helder inzicht geven in de voorwaarden en aandachtspunten bij het gebruik van gezichtsherkenning binnen toegangscontrole. Wij zijn ervan overtuigd dat gezichtsherkenning zich de afgelopen jaren ruimschoots heeft bewezen en dat deze technologie in de toekomst steeds vaker toegepast zal worden. Ze is geschikt voor vrijwel elk beveiligingsniveau. Afhankelijk van uw wensen en de situatie waarin gezichtsherkenning wordt ingezet, zoals het aantal te herkennen personen, de locaties van toepassing en het gewenste veiligheidsniveau, ondersteunen wij u graag bij het kiezen en implementeren van een passende oplossing.

Wenst u meer informatie over gezichtsherkenning in toegangscontrole? Neem dan gerust contact op met Boon Edam. Onze Entry Experts komen met plezier bij u langs voor een vrijblijvend adviesgesprek.

VEELGESTELDE VRAGEN.

Als ik als gebruiker door een toegangspoort met gezichtsherkenning wil lopen, zal het systeem punten van mijn gezicht omzetten in een code en deze vergelijken met een database. Betekent dit dat er een foto van mij wordt opgeslagen?
Bij het opstellen van de database is het niet nodig om de gezichten van gebruikers op te slaan. Een lijst met hash-codes volstaat. Ook tijdens het gebruik van een toegangsoplossing hoeft er geen foto opgeslagen te worden om een vergelijking te kunnen maken. In de praktijk kan het voorkomen dat gezichtsherkenningssystemen tijdelijk foto's opslaan om de softwareprestaties te optimaliseren. Deze beelden worden dan lokaal bewaard op een stand-alone server en zijn niet toegankelijk voor derden.

Wordt er, naast deze hash-code, nog andere data opgeslagen?
Bij traditionele toegangscontrolesystemen wordt in principe geregistreerd op welk moment een bevoegde persoon het gebouw betreedt. Dit geldt in grote lijnen ook voor gezichtsherkenningssystemen. Het is echter mogelijk om deze instellingen aan te passen, zodat dergelijke gegevens niet worden opgeslagen.

Is het mogelijk om deze vorm van gezichtsherkenning toe te passen op andere toegangsoplossingen dan toegangspoortjes?
Het is mogelijk om gezichtsherkenningssoftware toe te passen op verschillende andere toegangsoplossingen. Bent u hierin geïnteresseerd? Dan gaan wij graag met u in gesprek over de mogelijkheden.

WERELDWIJD AANWEZIG.

Wij zijn al 150 jaar actief in de productie van premium esthetische en beveiligde toegangsoplossingen in Nederland, de Verenigde Staten en China. Wij kunnen vol vertrouwen zeggen dat onze vestigingen wereldwijd te vinden zijn. In landen zonder eigen Boon Edam-vestiging werkt onze Global Export-divisie samen met exclusieve distributeurs of biedt ze directe verkoop en services. Door onze wereldwijde aanwezigheid hebben wij uitgebreide kennis van lokale markten en hun unieke toegangseisen.

Bezoek onze website om een Boon Edam-expert in uw regio te vinden: **www.boonedam.be/contact**

Boon Edam Belux BV
T +32 (0) 14 21 67 17
E be.info@boonedam.com
I www.boonedam.com

BOON EDAM
YOUR **ENTRY** EXPERTS.