



GEZICHTSHERKENNING IN TOEGANGSCONTROLE.

EEN **WHITEPAPER** MOGELIJK GEMAAKT DOOR BOON EDAM


BOON EDAM
YOUR **ENTRY** EXPERTS.



INLEIDING.

In deze whitepaper wordt beschreven hoe toegangscontrole door middel van gezichtsherkenning werkt. Ook gaat het in op de aspecten waar u rekening mee moet houden bij het selecteren van een toegangscontrolesysteem gebaseerd op gezichtsherkenning. Aangezien het gebruik van gezichtsherkenning een nieuwe technologie op de markt is, bent u wellicht benieuwd welke aspecten er een rol spelen wanneer u een gezichtsherkenningssysteem wil toepassen. Na het lezen van deze whitepaper zult u een beter inzicht hebben in wat gezichtsherkenning in toegangscontrole precies inhoudt en waar u rekening mee dient te houden bij het aanschaffen van een dergelijk systeem.

SOORTEN BIOMETRIE

Biometrische kenmerken zijn alle meetbare eigenschappen van de mens. Biometrie wordt steeds meer toegepast in toegangscontrole. De vier meest gebruikte vormen zijn:

IRISSCAN

Elke menselijke iris heeft unieke eigenschappen. Tijdens een irisscan worden putjes, strepen en gleuven in de iris herkend en omgezet in een iriscode. Deze code kan dan vergeleken worden met een database om toegang te verlenen.

HANDPALMADERS

Door middel van infrarood licht wordt het unieke ader -en haarvatenstelsel in de hand gemeten. Ook meten sommige handpalmlezers bijvoorbeeld lijnen en verdikkingen in de hand. Deze informatie vormt een uniek profiel dat gekoppeld kan worden aan een geautoriseerd persoon.

VINGERAFDRUK

Er bestaan verschillende soorten vingerafdrukscanners. Al deze scanners meten het unieke lijnenpatroon dat zich in de huid bevindt. De gemeten data kan gebruikt worden om te bepalen of toegang verleend wordt.

GEZICHTSHERKENNING

De laatste vorm van biometrie in toegangscontrole is gezichtsherkenning. Hierbij filtert een algoritme het menselijk gezicht uit een foto of videobeeld. In enkele milliseconden worden de unieke punten in het gezicht van de mens vastgelegd en omgezet naar een unieke code.

De gezichtsherkenningsssoftware vergelijkt vervolgens deze code met een database. Wanneer een overeenkomst gevonden is, kan bepaald worden wie er op het beeld staat en of er wel of niet toegang verleend moet worden.





GEZICHTSHERKENNING

Gezichtsherkenning kan op verschillende manieren worden toegepast. Deze whitepaper spitst zich toe op de toegangscontrole. Hieronder worden kort de verschillen uiteengezet:

MASSASURVEILLANCE

Bij massasurveillance wordt gezichtsherkenning gebruikt om individuen te herkennen in een mensenmassa. Om dit te verwezenlijken is specialistische hardware en zware software vereist.

PERSOONLIJK

Deze vorm van gezichtsherkenning, veelal toegepast op mobiele apparaten zoals smartphones, maakt gebruik van relatief simpele software en hardware. Het doel hierbij is om een gezicht te gebruiken als alternatief voor een pincode.

FORENSISCH OPSPOREN

Gezichtsherkenning kan ook gebruikt worden om de route van een persoon te reconstrueren op basis van opgenomen videobeeld. Met behulp van deze data kan bijvoorbeeld achterhaald worden waar een gezocht persoon geweest is in de afgelopen 24 uur.

TOEGANGSCONTROLE

Tot slot kan gezichtsherkenning toegepast worden binnen toegangscontrole. Belangrijk hierbij is om de software real-time te laten werken, waarbij er informatie van camera's op verschillende locaties vergeleken wordt met een database. Afhankelijk van de grootte van deze database wordt er gekozen voor een server die snel genoeg kan berekenen of iemand geautoriseerd is, waarna de toegangspoort geopend kan worden.

IN DEZE WHITEPAPER:



VOORDELEN
GEZICHTSHERKENNING



COMPONENTEN
GEZICHTSHERKENNING



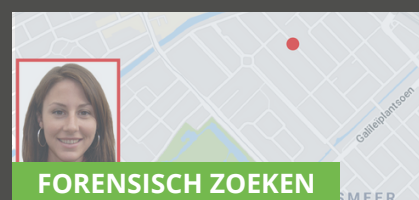
TECHNISCHE
ASPECTEN



IN DE PRAKTIJK



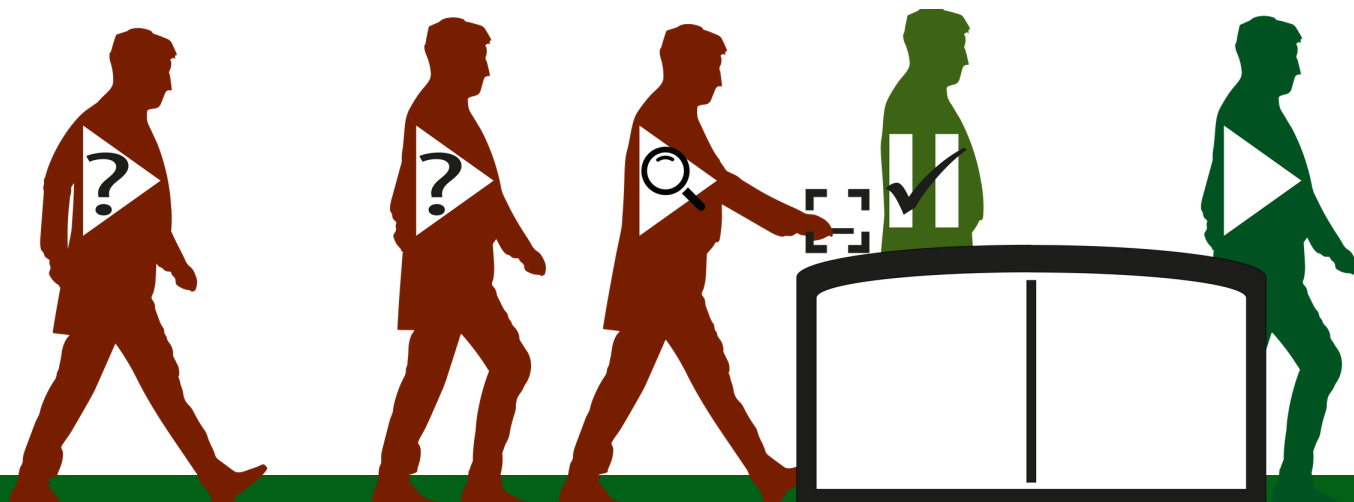
DIGITALE
VEILIGHEID



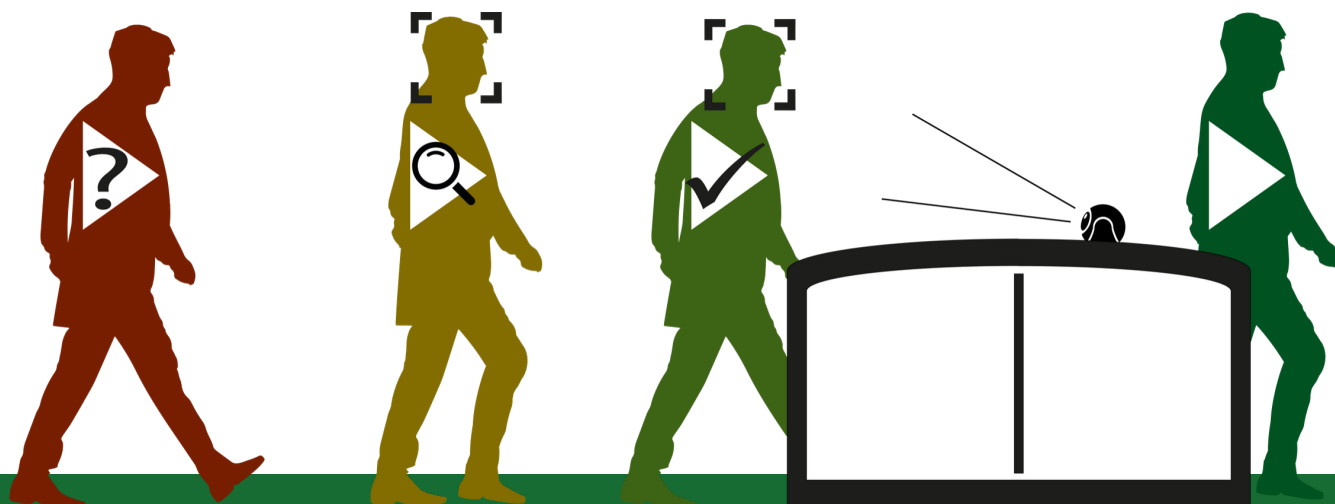


VOORDELEN GEZICHTSHERKENNING.

'KLASSIEKE' KAARTLEZER



GEZICHTSHERKENNING



VERBETERDE DOORSTROMING

Eén van de grootste voordelen van gezichtsherkenning in toegangscontrole is dat de persoon die toegang wil krijgen geen wachttijd heeft bij de toegang. Doordat de software het gezicht van een naderend persoon registreert voordat hij bij de toegangspoort is, kan in de tijd dat deze persoon de toegangscontrole benadert bepalen of deze persoon toegang mag hebben tot het pand. Wanneer de geautoriseerde persoon zich vlak voor of in de poort bevindt zal het systeem deze openen. Zo wordt voorkomen dat een ander persoon door de geopende poort kan lopen. Als resultaat kan de persoon op een vloeiende manier door de toegangscontrole lopen.



ALTIJD SNELLE TOEGANG

Doordat biometrische gezichtsherkenning gebaseerd is op iets dat je als persoon altijd bij je hebt, zal het nooit voorkomen dat je voor een dichte deur staat. Het feit dat alle gezichten uniek zijn, maakt het mogelijk om de eigenschappen van het gelaat te gebruiken om mensen van elkaar te onderscheiden en te identificeren.

Als bijkomend voordeel hoeft je als gebruiker bijna niet meer actief mee te werken als je bij een toegangscontrolepunt aankomt. Zodra je gezicht in de focus van de camera valt, kan de software kijken of je geautoriseerd bent. Toegangspassen worden dus overbodig en kunnen dus ook niet meer vergeten worden. Daarnaast hoeft je ook niet meer te wachten tot je collega zijn pas tussen zijn spullen heeft gezocht en heb je je handen vrij om je jas en tas mee naar binnen te nemen.

GEEN DOORGEGEVEN PAS

Een van de dingen die regelmatig voorkomt in de toegangscontrole is het doorgeven van de persoonlijke toegangspas aan een collega. Dit oneigenlijke gebruik zorgt ervoor dat onbevoegde personen een pand kunnen betreden. Door gebruik te maken van gezichtsherkenning kan een onbekend individu niet zomaar door de toegangscontrole lopen.

Daarnaast maakt het toepassen van gezichtsherkenning in toepassingscontrole het dus onmogelijk om een toegangspas te stelen of te kopiëren. Het resultaat is een verbetering van het algehele veiligheidsniveau.



BIOMETRIE IS CONTACTLOOS

Veel mensen aarzelen even voordat ze hun iris of vinger laten scannen. Deze (onbewuste) aarzeling wordt veroorzaakt doordat ze het systeem niet kennen of doordat ze het niet prettig vinden om actief een lichaamsdeel aan de scanner aan te bieden. Naast dat dit de snelheid van de doorgang belemmert, zorgt dit er ook nog eens voor dat de toegangscontrole als minder gebruiksvriendelijk wordt ervaren.

Een groot voordeel van gezichtsherkenning is dat een camera de gebruiker op afstand registreert. Hierdoor hoeft de gebruiker dus geen ongemakkelijke houding aan te nemen of fysiek contact te hebben met de toegangspoort. Zodra de persoon binnen het ingestelde bereik van de camera komt, zal deze de persoon verifiëren en, zonder dat deze hoeft te vertragen, toegang kunnen verlenen.



COMPONENTEN GEZICHTSHERKENNING.

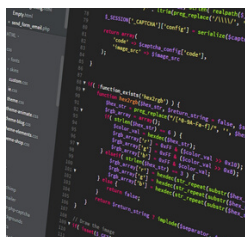
Bij het kiezen voor gezichtsherkenning in toegangscontrole moet men rekening houden dat het systeem uit verschillende componenten bestaat. Deze componenten zijn vaak afkomstig van verschillende partijen en moeten met elkaar verbonden worden. Hierdoor is het belangrijk om goed te inventariseren welke leveranciers met elkaar een soepel werkend systeem kunnen bouwen. In het algemeen zullen de volgende componenten met elkaar samen werken:



CAMERA & ANDERE SENSOREN

De camera is een belangrijke schakel in de betrouwbare toepassing van gezichtsherkenningsoftware. Er zijn diverse camera's beschikbaar met een hoge kwaliteit. Uit ervaring blijkt dat zorgvuldige selectie op technisch maar ook op esthetisch gebied van toegevoegde waarde is op het gebruik en acceptatie.

Het selectieproces gaat verder dan alleen megapixels: ook lichtgevoeligheid, type lens en rekenkracht van de chip zijn belangrijke elementen. Ook kan er gekozen worden om extra sensoren te nemen die een echt gezicht van bijvoorbeeld een gezicht op een foto kunnen onderscheiden.



GEZICHTSHERKENNINGSSOFTWARE

Ook wel het hart van het systeem. De gezichtsherkenningsssoftware zet gezichten om in een code, welke hij vervolgens vergelijkt met een vooropgezette database. Deze herkenning gebeurt door een serie algoritmes. De gezichtsherkenningsssoftware is vaak onafhankelijk van andere toegangscontrolesoftware. Hierdoor is mogelijk om een stand-alone systeem te creëren, waarbij de software op een externe processor gedraaid wordt.

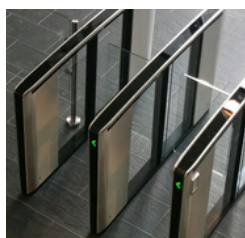
Belangrijk is dat dat de software en het systeem voldoen aan de Algemene Verordening Gegevensbescherming (AVG) en voorzien zijn van de juiste encryptiestandaarden.



TOEGANGSCONTROLESYSTEEM

Vaak bestaat een toegangscontrolesysteem uit meerdere softwareoplossingen. Deze oplossingen zijn veelal een integraal onderdeel van een Security Management of Building Management System. Het is dus mogelijk dat de gezichtsherkenningsssoftware geïntegreerd moet worden in een dergelijk systeem.

In de praktijk betekent dit dat verschillende modules aan elkaar worden gelinkt, die vervolgens vanuit één centraal programma te beheren zijn. De module 'gezichtsherkenningsssoftware' zal in dat geval geïntegreerd worden middels een API.



FYSIEKE TOEGANG

Wanneer gezichtsherkenning toegepast wordt bij toegangscontrole is dit altijd in combinatie met een fysiek toegangsproduct. Zonder deze barrière is het immers niet mogelijk om onbevoegde personen te weren. Voor de barrière bestaan verschillende opties die elke een ander niveau van beveiliging met zich meebrengen.

De componenten zijn op verschillende manieren te configureren. Zo is het mogelijk om één fysiek product te leveren waarin gezichtsherkenning volledig geïntegreerd heeft, maar ook om de componenten los van elkaar toe te passen.



TECHNISCHE ASPECTEN.



LICHTOMSTANDIGHEDEN

Een van de belangrijkste aspecten voor de juiste implementatie van gezichtsherkenning is de hoeveelheid licht in de ruimte waar de camera geplaatst wordt. In het geval van toegangscontrole vindt de gezichtsherkenning vaak binnen plaats en is het mogelijk om de lichtomstandigheden te beïnvloeden.

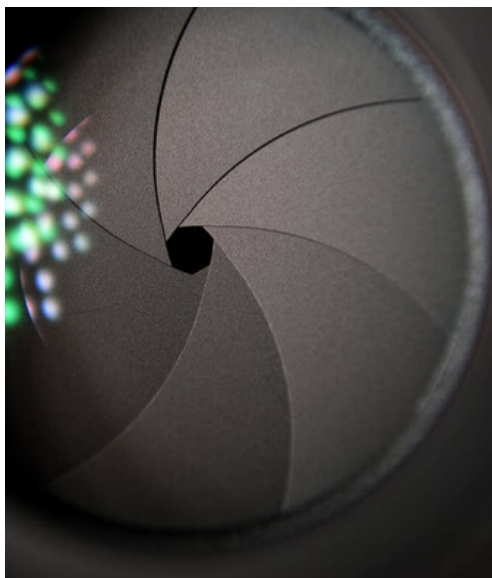
Overbelichting is hierbij een grote uitdaging. Denk aan felle zon, glasreflecties of ruimtes met een hoog atrium. Door de schommelingen in de hoeveelheid licht wordt er veel van de camera en gezichtsherkenningsoftware gevergd. Onderbelichting daarentegen is makkelijker te corrigeren. Vaak is een aanpassing in de camera instellingen al genoeg om gezichten goed te kunnen herkennen. Het is verstandig om een expert in te schakelen voor de juiste instellingen.

CAMERAPOSITIE

Bij het plaatsen van de camera dient goed nagedacht te worden over het beeld dat de camera op zal nemen. Hoe dichters de camera zich bij de persoon bevindt die toegang wenst te krijgen, hoe beter de kwaliteit van het beeld zal zijn.

Ook de positie van de camera ten opzichte van de gebruiker is belangrijk. Het is beter de camera te plaatsen op een plek waar de gebruiker naartoe kijkt wanneer hij door de toegangscontrole wil lopen. De gebruiker hoeft dan geen extra handelingen te verrichten om te kunnen worden herkend.

Tot slot kan er vanuit esthetisch oogpunt gekozen worden om de camera in het toegangsproduct te verwerken, of om hem op een externe plek te bevestigen.



CAMERAFOCUS

Bij de installatie van de camera is het van groot belang om na te denken over de focus van de camera. Deze dient te liggen op de plek waar het gezicht gescand wordt. Het focuspunt moet niet te ver van de toegangscontrole liggen (om voorschieten te voorkomen), maar ook niet te dichtbij (waardoor de gebruiker moet wachten op toegang).

De camerafocus is ook bepalend voor het spectrum waarbinnen een gezicht herkend kan worden. Dit is af te stellen door binnen de software een deel van het beeld te selecteren waarbinnen de gezichtsherkenning plaats vindt.



IN DE PRAKTIJK.

GEBRUIKERSFLOW

In de praktijk blijkt dat het gebruiken van beveiligde doorloopsluizen zorgt voor een natuurlijke voorwaartse positie van de gebruiker. Zij zullen zich in één lijn met het gezicht voorwaarts gericht door het product bewegen. Op deze manier wordt een relatief kleine zone gecreëerd waarbinnen alle gezichten van de gebruikers voorbij zullen komen.

Een belangrijk voordeel van gezichtsherkenning in een toegangscontroleproduct is dat het de flow van gebruikers verbetert. Dit wordt gerealiseerd doordat de gebruikers zich allemaal in dezelfde richting begeven en als continue stroom door de sluis bewegen. De gezichtsherkenning zorgt ervoor dat de authenticatiesnelheid hoog genoeg is om de snelheid van deze stroom mensen te waarborgen.



AANBIEDEN VAN HET GEZICHT

Eerder in deze whitepaper staat dat de gebruiker geen extra handelingen hoeft te verrichten wanneer gebruik gemaakt wordt van gezichtsherkenning in de toegangscontrole. Een voorwaarde hiervoor is dat de gebruiker zich bewust is dat de gezichtsherkenningssoftware in staat moet kunnen zijn om het gezicht te scannen.

In de praktijk betekent dit dat de gebruiker zijn of haar gezicht grotendeels onbedekt moet blootstellen aan de camera. Het betreden van de toegang met bijvoorbeeld een mondkapje of terwijl de gebruiker achter zich kijkt is dan ook niet mogelijk. Medewerking vanuit de gebruiker is dus vereist om het systeem te laten werken.

INTERACTIE MET GEBRUIKER

Bij het gebruik van gezichtsherkenning, en bij toegangscontrole in het algemeen, is het belangrijk dat er goede terugkoppeling is naar de gebruiker. Wanneer meerdere personen kort achter elkaar van een toegang gebruik maken, kunnen optische en akoestische signalen aan de gebruiker verduidelijken welke beslissing de software maakt.

Gezichtsherkenning leent zich om gebruikt te worden in een situatie waar er veel repeterende gebruikers voorkomen. Eén keer aanmelden volstaat om de gebruiker zo lang als gewenst toegang te geven. Ook zullen repeterende gebruikers gewend raken met de interactie met het toegangscontroleproduct.





DIGITALE VEILIGHEID.



ENCRYPTIE

Om te zorgen dat gegevens en beelden die via een netwerk verstuurd worden niet zo maar gehackt kunnen worden, maakt gezichtsherkenningssoftware gebruik van encryptie. Encryptie betekent dat digitale (beeld)informatie wordt versleutelt of gecodeerd. Zonder kennis over hoe deze versleuteling tot stand komt is het voor een buitenstaander onmogelijk om de informatie uit te kunnen lezen.

Er bestaan verschillende methodes om data te encrypten. Afhankelijk van de bestaande infrastructuur en het (bestaande) videomanagementssoftwareplatform kiest men een passende oplossing. Hierbij kijkt men bijvoorbeeld of de data via een open of gesloten netwerk verzonden wordt.

FRAUDEDETECTIE

Op het gebied van fraudedetectie ontwikkelt de gezichtsherkenningstechnologie zich snel. Hierbij wordt er gezocht naar manieren om te voorkomen dat het systeem 'voor de gek' gehouden wordt door bijvoorbeeld een foto aan de camera te tonen. Er zijn op dit moment twee methodes om fraude te detecteren en preventie toe te passen:

1. **Hardwarematige detectie** door middel van 3D-sensoren die de structuur van het gezicht scannen. Een variant hierop is een sensor die de reflectie uitleest van een patroon gekleurde lichtstralen dat op het gezicht wordt geschoten.
2. **Softwarematige detectie** waarbij minimale verschillen in het videobeeld gedetecteerd worden. Hiervoor is veel (video)rekenkracht nodig, waardoor men gebruik moet maken van grotere en krachtigere servers.



GDPR/AVG

Zoals eerder in deze whitepaper te lezen is, 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 om te weten dat biometrische gegevens gerekend worden tot een bijzondere categorie persoonsgegevens. Deze bijzondere categorie persoonsgegevens mag, onder voorwaarden, gebruikt worden om personen te identificeren. De data dient dan alléén gebruikt wordt voor authenticatie of beveiligingsdoeleinden. Daarnaast moet de beheerder van het systeem aan kunnen tonen dat de verwerking van de gegevens voldoet aan deze regelgeving. Het is dus wettelijk toegestaan om gezichtsherkenning toe te passen in toegangscontrole.



CONCLUSIE.

Het doel van deze whitepaper is om u een eerste inzicht te geven wat gezichtsherkenning in toegangscontrole precies inhoudt en waar u rekening mee moet houden bij het selecteren van het juiste gezichtsherkenningssysteem voor uw bedrijf. Hierbij is het onderscheid tussen verschillende soorten biometrie en verschillende soorten gezichtsherkenning uiteen gezet. Daarbij kunt u lezen wat de voordelen zijn van gezichtsherkenning ten opzichte van een klassiek toegangscontrolesysteem.

Vervolgens hebben we u zowel kennis laten maken met de verschillende componenten van een gezichtsherkenningssysteem in de toegangscontrole als met de belangrijkste technische en praktische aspecten die van invloed zijn op een gezichtsherkenningssysteem. Tot slot vertelt deze whitepaper kort hoe gezichtsherkenning toegepast kan worden met betrekking tot digitale veiligheid en de huidige regelgeving over AVG/GDPR.

AANBEVELINGEN

Boon Edam heeft met deze whitepaper geprobeerd u meer inzicht te geven in de randvoorwaarden en vereisten van gezichtsherkenning. Wij zijn ervan overtuigd dat de technologie gezichtsherkenning zich de afgelopen jaren bewezen heeft en dat deze in de toekomst steeds meer gebruikt zal worden. Daarbij onderstrepen wij dat de gezichtsherkenning toegepast kan worden in bijna alle beveiligingsniveaus van toegangscontrole. Aan de hand van uw wensen betreffende het inzetten van gezichtsherkenning en de situatie waarin deze ingezet moet worden (denk hierbij aan het aantal mensen dat het systeem moet herkennen, de locatie(s) waar deze gebruikt wordt, etc.) helpen wij u graag met het selecteren en implementeren van het juiste systeem.

Voor meer informatie over gezichtsherkenning in toegangscontrole kunt u contact met Boon Edam opnemen. Onze Entry Experts komen graag bij u langs voor een vrijblijvend adviesgesprek.

FAQ.

Als ik als gebruiker door een toegangspoort met gezichtscontrole wil lopen, zal deze punten van mijn gezicht omzetten in een code en vergelijken met een database. Betekent dit dat er een foto van mij wordt opgeslagen?

Bij het creëren van de database is het niet nodig om de gezichten van gebruikers op te slaan, een lijst met alle hash-codes is hiervoor voldoende. Ook bij het gebruik van een toegangsproduct zal er geen foto opgeslagen hoeven te worden om mee te kunnen vergelijken. In de realiteit kan het zo zijn dat gezichtsherkenningsinstallaties foto's (tijdelijk) opslaan om zo de software te kunnen optimaliseren. Deze staan dan op een stand-alone server en kunnen niet met derden worden gedeeld.

Wordt er naast deze hash-code nog andere data opgeslagen?

Bij traditionele toegangscontrolesystemen wordt in principe het moment geregistreerd waarop een bevoegd persoon het gebouw betreedt, dit geldt in principe dus ook voor gezichtsherkenningsinstallaties. Het is mogelijk om deze instelling aan te passen waardoor deze data niet wordt opgeslagen.

Is het mogelijk om deze vorm van gezichtsherkenning toe te passen op andere entreeoplossingen dan toegangspoortjes?

Het is mogelijk om gezichtsherkenningsoftware toe te passen op verschillende andere entreeoplossingen. Als u hierin geïnteresseerd bent, gaan wij graag met u in gesprek over de mogelijkheden.

WERELDWIJD AANWEZIG.

Wij zijn al meer dan 140 jaar actief in de productie van premium esthetische en beveiligde toegangsooplossingen 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.com/contact



OVER DE AUTEUR

Jonas Oijevaar is Business Accelerator bij Boon Edam. Hij houdt zich bezig met het integreren van nieuwe technologieën in bestaande toegangscontroleproducten. Daarbij adviseert en begeleidt hij klanten die geïnteresseerd zijn in het testen en toepassen van de nieuwste high-tech oplossingen. Bent u geïnteresseerd in gezichtsherkenning en wilt u meer weten? Of heeft u vragen over hoe u het beste gezichtsherkenning kan toepassen bij uw entree? Neem dan gerust contact op: Jonas.oijevaar@boonedam.com
+31 (0)6 20 74 09 60



Boon Edam Nederland B.V.

T +31 (0) 299 38 08 08

E info@boonedam.nl

I www.boonedam.nl


BOON EDAM
YOUR ENTRY EXPERTS.