ARTIKEL LOSS PREVENTION & SECURITY | EDITION 2.0 | APRIL 2013

Ganzen als logistiek beveiliger

Hanteren van aloude principes

Breda,	19 april 2013
Onze ref.:	9024D267/MLo/it v2.0
Titel:	Ganzen als logistiek beveiliger
Auteur:	Michael Lokerse Consultant Facilities

Groenewout
Nijverheidssingel 313
Postbus 3290
4800 DG BREDA
T: +31 (0) 76 - 5330440
F: +31 (0)76 - 5310191
E: mail@groenewout.com
I: www.groenewout.com

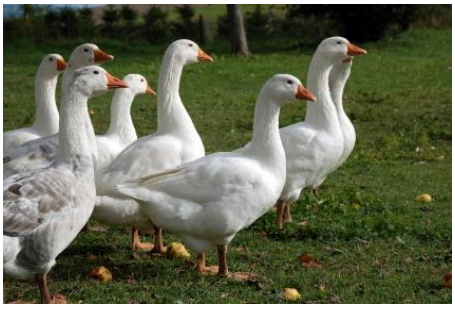
GROENEWOUT

1 HANTEREN VAN ALOUDE PRINCIPES

In het jaar 390 veroverden de Galliërs de stad Rome. De bewoners van de stad hadden zich teruggetrokken naar het Capitool, de burcht van Rome. Met als doel om ook de laatste vesting in de stad te overmeesteren beklommen de Galliërs midden in de nacht de Capitolijnse rotsen, zo stilletjes, dat zelfs de waakhonden hen niet hoorden; de ganzen echter begonnen onrustig te gakken en redden daardoor het hart van de stad. De Galliërs werden teruggedreven naar het noorden en later door Caesar geheel onderworpen.

In dit voorbeeld van beveiligen uit de Romeinse tijd waren de Capitolijnse rotsen de fysieke maatregelen. Deze zorgden voor vertraging van de aanval, de ganzen op hun beurt alarmeerden de bewoners van de stad waardoor zij in de gelegenheid gesteld werden om maatregelen te nemen tegen de Galliërs.

Het toen gehanteerde security concept van een eerste barrière, vroegtijdige detectie en signalering, vertraging en adequate opvolging is nu nog steeds een basisprincipe voor buitenbeveiliging.



Figuur 1: Ganzen onderdeel van de omtrekbeveiliging bij een politiebureau in Brazilië.

Het inzetten van ganzen voor de beveiliging van logistieke centra zou ook nu nog mogelijkheden bieden.

Helaas loopt dit vanzelfsprekend al snel tegen veel praktische bezwaren aan. Door technologische ontwikkelingen kan de waakzaamheid van de ganzen vervangen worden door processorkracht, videoresolutie en software.

1.1 Omtrekbeveiliging

Om met behulp van omtrekbeveiliging vroegtijdig een inbraak te kunnen detecteren zijn er een aantal technieken die al enkele decennia worden toegepast, bijvoorbeeld actief infrarood-, radar-, grond- en hekwerkdetectie. Naast deze mogelijkheden is buitendetectie met behulp van camera's en specifieke software weer in opkomst.

Bij de introductie van buitendetectie met behulp van camera's aan het begin van deze eeuw werden de beloftes vaak niet waar gemaakt. Het aantal loze meldingen was te hoog of de detectiezekerheid onvoldoende. Naast de technische beperkingen lagen de kosten vaak ook hoger dan bij de al beproefde systemen. Door technologische en bedrijfsmatige trends is het nu beschikbare beveiligingsconcept aanzienlijk verbeterd. Steeds meer processorkracht, videoresolutie en bandbreedte zorgen er samen voor dat er meer resources zijn voor zogenaamde videocontentanalyse.

1.2 Videocontentanalyse

Het automatisch interpreteren van videosignalen om zo gebeurtenissen te kunnen signaleren wordt videocontentanalyse genoemd. Dit kan gezien worden als de geautomatiseerde variant van de biologische visuele cortex[1].

Door deze vergelijking te maken is video content analyse ook te omschrijven als een vorm van kunstmatige intelligentie die het mogelijk maakt camerabeelden voor meer dan alleen observatie of registratie te gebruiken.

Bij videocontentanalyse voor buiten-beveiliging is het mogelijk om personen automatisch te detecteren en kan een meldkamer direct het betreffende videobeeld gepresteerd krijgen. Ook kan een systeem een duidelijk onderscheid maken tussen personen en bijvoorbeeld een konijn dat in het beeldvlak van de camera loopt. In onderstaande afbeelding ziet u een kader dat door videocontentanalyse automatisch om een persoon wordt heen gelegd en doorgestuurd kan worden naar de centralist van een meldkamer.

Figuur 2: Detectie met behulp van videocontentanalyse.

Een groot voordeel videocontentanalyse is dat ook in bepaalde situaties observatie of voorbereiding voor een inbraak of overval opgemerkt kan worden. Door de kunstmatige intelligentie zijn systemen in staat om bijvoorbeeld een buurtbewoner die zijn hond langs het hek uitlaat te onderscheiden van een persoon die bij het hek stilstaat.

Een praktijkvoorbeeld is de gewelddadige overval medio maart 2013 bij een depot van geldtransportbedrijf Brink's in Best. Uit de media komt het beeld naar voren dat de overvallers, voordat zij met springstof een buitendeur opende, het hekwerk geforceerd hebben[2]. Mogelijk had videocontentanalyse de dreiging eerder kunnen opmerken. Hierdoor was er voor de opvolging meer tijd beschikbaar om op deze dreiging te anticiperen.

Het voorbeeld illustreert de mogelijkheid om een dreiging eerder te signaleren, zoals ook in de Romeinse tijd waar de ganzen tijdig de Romeinen waarschuwden. In het voorbeeld van Brink's is door de overvallers excessief geweld gebruikt. Het spreekt voor zich dat alleen eerdere signalering in zo'n situatie niet voldoende is. Om een dergelijke dreiging af te kunnen slaan moet voldoende vertraging opgebouwd kunnen worden en een opvolging die hiervoor voldoende is geoutilleerd.

Logistieke centra

Voor omtrekbeveiliging met behulp van videocontentanalyse lenen logistieke centra zich uitstekend. In veel situaties zijn er al camera's aanwezig. Verder zijn er vaak relatief grote open ruimtes met veel verharding en kan door de lange zichtlijnen het bereik van de camera's over het algemeen maximaal benut worden.

1.3 Werking videocontentanalyse

Voor automatische beeldinterpretatie zijn er een aantal mogelijkheden. De meest eenvoudige analyse is gebaseerd op het detecteren van veranderingen in beeldpixels. Bij omtrekbeveiliging zou deze analyse echter tot veel loze alarmmeldingen leiden. Voor deze toepassing is dan ook een meer uitgebreide analyse nodig. Bij een voor omtrekbeveiliging geschikte analysetechniek worden camerabeelden gesplitst in een statische achtergrond en een aantal bewegende objecten.

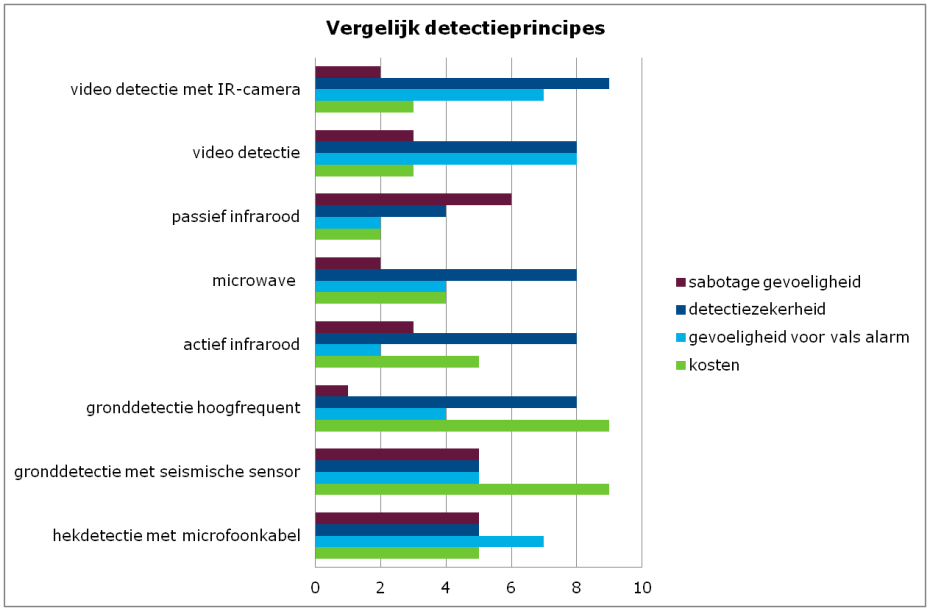
Uit de bewegende objecten wordt daarna met behulp van sofware de positie, grootte, bewegingsrichting, tijdstip etc. gedestilleerd en vergeleken met de opgegeven alarmcondities. De exacte werking, de kwaliteit van de signalering en

extra functies zoals het parallel laten lopen van verschillende algoritmes is leveranciers- afhankelijk. Verder is er ook variatie te vinden waar de analyse als zodanig plaatsvindt.

Bij gebruik van videocontentanalyse voor omtrekbeveiliging wordt door de aanwezigheid van storende factoren, zoals wisselende weersomstandigheden, variatie in lichtniveaus, plasvorming, strooilicht van langs rijdende auto's e.d. veel processorkracht gevraagd om voldoende detectiezekerheid te kunnen geven bij een acceptabel niveau van loze meldingen. Grofweg zijn er drie systemen om de videobeelden te analyseren. Wij zien dat voor omtrekbeveiliging oplossingen op basis van server- of distributed architecture het beste presteren. In de bijlage vind u een vergelijking van de drie oplossingen wanneer ingezet voor omtrekbeveiliging.

1.4 Vergelijk detectietechnieken

Om inzicht te geven in de prestaties van buitendetectie zijn in onderstaand overzicht de meest gangbare technieken met elkaar vergelijken. Dit op basis van kosten, gevoeligheid voor vals alarm, detectiezekerheid en sabotagegevoeligheid. Vanzelfsprekend zijn de waardes een indicatie en sterk afhankelijk van de specifieke omstandigheden. Door de bredere inzetbaarheid van het camerasysteem zijn bij videodetectie alleen de kosten meegenomen die betrekking hebben op uitbreiding van het systeem met videocontentanalyse.



Tabel 1: Prestaties meest gangbare detectie technieken

Uit de grafiek valt op te maken dat videodetectie goed presteert op het gebied van kosten, detectiezekerheid en sabotage gevoeligheid maar relatief slecht presteert wanneer gekeken wordt naar de gevoeligheid voor valse alarmen. Deze negatieve systeemeigenschap is goed te ondervangen doordat videodetectie het mogelijk maakt beveiligingsmaatregelen procesmatig te benaderen.

1.5 Ketensamenwerking

Door de videobeelden, al dan niet op basis van infraroodtechniek of thermische camera's, automatisch te analyseren wordt een indringer vroegtijdig gedetecteerd. Door het grote verschil in buitencondities, stoorinvloeden en de (on)mogelijkheden van algoritmes geeft videocontentanalyse zoals aangegeven meer meldingen dan met de traditionele elektronische maatregelen. Groot voordeel van videocontentanalyse is dat er van het alarm altijd direct videobeelden beschikbaar zijn. De meldkamer is hierdoor in de gelegenheid om het betreffende videobeeld te verifiëren en alleen bij een incident de opvolging te alarmeren.

Voor een optimale werking van videocontentanalyse is ketensamenwerking tussen systeemintegrator en de meldkamer noodzakelijk. Bij veel loze meldingen wordt de centralist van de meldkamer onnodig belast en kan er een situatie ontstaan waarbij mogelijk te snel een melding wordt afgedaan als loos. Ook worden er mogelijk kosten gemaakt die voorkomen hadden kunnen worden. Het is daarom noodzakelijk om zowel met de systemintegrator als de meldkamer gezamenlijk afspraken te maken over de prestaties van het gehele systeem.

Naast de gebruikelijke prestatieafspraken zoals responsetijd, time-to-fix, first time right is het bij videocontentanalyse wenselijk om heldere afspraken te maken over de verificatie van de videobeelden. Een mogelijkheid is om met de betrokken partijen een vaste jaarlijkse fee overeen te komen waarin de verificatie van alle videobeelden is opgenomen. Het is dan in het gezamenlijk belang van zowel de systemintegrator als de meldkamer om het aantal meldingen te beperken en zo wordt de opdrachtgever van het beveiligingsysteem niet met onverwachte kosten geconfronteerd.

1.6 Breder toepasbaar binnen de logistiek

Door de mogelijkheden die videocontentanalyse biedt kan deze techniek breder ingezet worden dan alleen voor beveiligingsdoeleinden. Een voorbeeld is het tellen van het aantal bezoekers of het detecteren van spookrijders op snelwegen. Voor toepassing binnen de logistiek is videocontentanalyse ook geschikt voor:

- Signaleren status van de docks
- Signaleren achterlaten en weghalen van goederen
- Detectie geparkeerde voertuigen
- Signaleren van zonebetreding
- Signaleren van obstructies in gangen en verkeerswegen
- Optimaliseren inzet persoonsbeveiliging voor multi-site oplossingen

Naast deze bestaande mogelijkheden lopen er ook onderzoeksprojecten om oplossingen te ontwikkelen welke informatie uit videoanalyse linken aan informatie uit warehouse management systemen. Een voorbeeld hiervan is het door de Belgische overheid gesubsidieerde SecureWMS-project.

1.7 Conclusie

Door videocontentanalyse toe te passen kan een nieuw of in sommige gevallen bestaand cameraysteem breder ingezet worden. Daarnaast biedt videocontent-analyse de mogelijkheid om omtrekbeveiliging naar een hoger plan te brengen. Wij merken dat er binnen de markt toch enige koudwatervrees is voor het toepassen van videocontentanalyse voor omtrekbeveiliging.

GROENEWOUT

Deze vrees was begin deze eeuw zeker terecht, maar het afgelopen decennium is deze techniek ook binnen de gebouwbeveiliging volwassen geworden.

Er zijn inmiddels in Nederland een aantal logistieke centra waar videocontentanalyse succesvol is ingezet. Ook door verzekeraars wordt deze techniek, wanneer passend binnen in een maatwerkplan, voor hoog risico objecten erkend. Wij verwachten dan ook dat door de specifieke kenmerken van logistieke centra, zoals het risicoprofiel en de aanwezigheid van relatief grote open ruimtes, deze techniek veel mogelijkheden biedt en over een aantal jaren breed toegepast zal zijn.

En tenslotte, maar daarom niet minder belangrijk: het beveiligen van logistieke centra vraagt om een brede benadering, kennis van het bedrijfsproces en het risicoprofiel. Het zwaartepunt ligt in veel situaties bij de medewerkers, gevolgd door het wegnemen van gelegenheid en passende procedures. Het implementeren van techniek zoals videocontentanalyse is net als alle andere technische maatregelen de laatste schakel. In praktijk zien wij dat vaak deze laatste stap is overbelicht, terwijl voor de opdrachtgever juist deze maatregelen de hoogste kosten met zich meebrengen. Een valkuil is om bij het analyseren van de risico's al snel voor een technische oplossing te kiezen, maar verstandiger is om de probleemstelling open en zonder commerciële belangen te benaderen om zo kokervisie te voorkomen.

2 OVER DE SCHRIJVER

Voor vragen over dit artikel, kunt u contact opnemen met Michael Lokerse, lokerse@groenewout.com of telefoonnummer +31 (0)76 533 04 40 / +31 (0)6 50 20 15 71. Voor meer informatie over Groenewout verwijzen wij u graag naar onze website www.groenewout.com.

Michael Lokerse is Consultant Facilities bij adviesbureau Groenewout. Michael heeft een Bachelor Degree in Elektrotechniek, Werktuigkunde en Bedrijfskunde en meer dan 15 jaar ervaring met het ontwerpen, realiseren en beheren van gebouwgeboden installaties.

Voor Groenewout was Michael werkzaam als adviseur safety en security bij de Politie Rotterdam-Rijnmond. Vanaf 2009 in de functie van projectmanager gebouwinstallaties. Expertise: safety en security, project management en integraal ontwerpen.

Bronvermelding

1 - TNO Defensie en veiligheid notitie Terminologie en Taxonomie van videocontentanalyse d.d. 12 juli 2010

2 – OmroepBrabant artikel d.d. 22 maart 2013: Beveiliging van filiaal Brink's in Best onvoldoende

Bijlage: vergelijkingsmatrix architectuur videocontentanalyse

BIJLAGE - Vergelijkingsmatrix architectuur videocontentanalyse

Systeem architectuur	**Edge based architecture**	**Server based architecture**	**Distributed architecture**
Locatie video content analyse	Beeldanalyse in of nabij camera's.	Beeldanalyse op centrale server.	Beeldanalyse verdeeld over camera en centrale server.
Detectieprestaties	-	-/+	++
	Het beeldmateriaal uit de camera is nog niet gecomprimeerd en is daardoor ideaal voor beeldanalyse. Echter vergt dit per camera geavanceerde reken- kracht. Bij de meeste gangbare systemen is deze bij de camera beperkt waardoor de detectieprestaties laag zijn.	Het beeldmateriaal wat naar de centrale server verstuurd wordt is gecomprimeerd om zo de benodigde bandbreedte te beperken. Bij het comprimeren is er beeldinformatie verloren gegaan wat een nadelige invloed heeft op de detectieprestaties.	In de camera wordt een eerste beeldanalyse gemaakt. De gegevens uit deze analyse wordt vervolgens naar de centrale server gestuurd en door de server verder geanalyseerd.
Mogelijkheden	-	++	++
	Over het algemeen slechts een aantal analyse mogelijkheden.	Uitgebreide analyse mogelijkheden.	Uitgebreide analyse mogelijkheden.
Schaalbaarheid	++	-	++
	De server is over het algemeen alleen nodig voor het instellen en beheer en is geschikt voor een groot aantal camera's	De server capaciteit is geschikt voor het aansluiten van een beperkt aantal camera's (bijvoorbeeld 4, 16 of 32)	Een server kan een groot aantal camera's verwerken.
Benodigde bandbreedte	++	-	++
	Voor de werking van beeldanalyse is er slechts een beperkte datastroom per camera.	Al het beeldmateriaal wordt op de server verwerkt waardoor een aanzienlijke datastroom richting de server nodig is.	Data wordt alleen verstuurd wanneer een gebeurtenis is gedetecteerd.
Upgrade mogelijkheden	-	-/+	-/+
	Nieuwe software versies vragen om een firmware update op iedere camera. Dit kan bij grotere systemen tegen praktische bezwaren aanlopen. Bij introductie van nieuwe algoritme kan vervangen van de hardware noodzakelijk zijn.	Een nieuwe software versie kan eenvoudig op de centrale server geïnstalleerd worden. Wanneer de nieuwe algoritmes meer proces-sorcapaciteit vragen kan er tegen systeembeperkingen aangelopen worden.	Een nieuwe software versie kan eenvoudig op de centrale server geïnstalleerd worden. Wanneer de nieuwe algoritmes meer processorcapaciteit vragen kan tegen systeem-beperkingen aangelopen worden.
Initiële kosten	Laag	Middel-Hoog	Middel-Hoog
	Door de eenvoudigere systeemopzet zijn de kosten van een deze oplossing over het algemeen lager.	Indicatief kengetal totale systeem inclusief observatie: € 25,- per m^2 beveiligde buitenzone (DC 10.000 m^2, € 100.000)	Indicatief kengetal totale systeem inclusief observatie: € 25,- per m^2 beveiligde buitenzone (DC 10.000 m^2, € 100.000)
Exploitatie kosten	Hoog	Middel-Laag	Middel-Laag
	Door de beperkte intelligentie zal een systeem jaarlijks veel loze meldingen genereren, wat leidt tot een onnodige zware belasting van de meldkamer en eventueel de alarmopvolging.	Kosten sterk afhankelijk van aantal camera's en type overeenkomst met system integrator en meldkamer.	Kosten sterk afhankelijk van aantal camera's en type overeenkomst met system integrator en meldkamer.