Tampereen yliopisto

Ella Rinnemaa

TURVALLISUUSUHAT HAHMONTUNNISTUSTA HYÖDYNTÄVÄSSÄ RIKOSTEKNISESSÄ VIDEOANALYYSISSÄ

Kandidaatintutkielma
Informaatioteknologian ja viestinnän tiedekunta
Joulukuu 2022

TIIVISTELMÄ

Ella Rinnemaa: Turvallisuusuhat hahmontunnistusta hyödyntävässä rikosteknisessä videoanalyysissä
Kandidaatintyö
Tampereen yliopisto
Tieto- ja sähkötekniikan kandidaattiohjelma, tietotekniikka
Joulukuu 2022

Tämän työn tavoite on selvittää, millaisia turvallisuusuhkia hahmontunnistusta hyödyntävä rikostekninen videoanalyysi sisältää ja millä keinoilla näitä uhkia pyritään lieventämään.

Laaja videovalvonnan hyödyntäminen on johtanut alati kasvavaan tiedon määrään. Tämän myötä keskiöön on noussut videokuvan rikosteknisen analysoinnin automatisaatio, joka usein toteutetaan hyödyntämällä konenäön hahmontunnistusta. Rikostutkinnassa virheellisillä havainnoilla on vakavia seurauksia, joten uusien menetelmien käyttöönottoa on erityisen tärkeä tarkastella kriittisesti. Tällaisessa tarkastelussa painoarvo on uhkien kartoittamisella. Uhkien tunnistaminen on ehto sille, että järjestelmien toiminnasta voidaan tehdä turvallista.

Työssä aihetta lähestytään tutustumalla ensin älykkääseen videoanalyysiin, joka koostuu aineiston keräämisestä kameralaitteella ja sen erittelystä kohteentunnistusalgoritmien avulla. Turvallisuusuhkien löytämisessä on ollut avainasemassa tämän teknologisen toteutuksen tarkastelu ja arviointi. Kysymykset siitä, miten aineistoa kerätään, kuinka kohteentunnistusalgoritmeja koulutetaan ja millä tavalla algoritmit käsittelevät tietoa, olivat hyödyllisiä uhkien selvittämisessä. Lisäksi lähteet, kuten Shancang Lin ja muiden kirjoittama artikkeli *Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation* (2019) sekä Youngkyun Chan ja muiden konferenssiartikkeli *A Study on the Security Threats and Privacy Policy of Intelligent Video Surveillance System Considering 5G Network Architecture* (2020), täydensivät havaintoja kuvaamalla yksityiskohtaisemmin tiettyjen toiminnan vaiheiden sisältämiä uhkia. Vastaavasti kun uhkia oltiin eritelty tarpeeksi, alettiin esittämään kysymyksiä siitä, kuinka uhkia voidaan ehkäistä tai korjata. Erilaisia ratkaisuehdotuksia valittiin tarkasteltavaksi sen mukaan, onko ehdotus konkreettinen ja kuinka suurta näkyvyyttä se on saavuttanut. Euroopan unionin laatima *Artificial Intelligence Act* (2021) oli antoisa niin uhkien kuin ratkaisuehdotusten kartoittamisessa.

Työssä havaitaan, että keskeisiä teknologisia haasteita ovat neuroverkkojen koulutuksessa käytettävien datajoukkojen rajallisuus, videoiden väärentäminen ja yleinen järjestelmien välisten suojausten vaarantuminen, videokuvan ja -käsittelyn laadulliset puutteet sekä ihmistutkijoiden rajallinen teknologinen osaaminen. Eettisiä haasteita ovat puolestaan henkilötietojen käsittelyn ja säilömisen aiheuttama yksityisyydensuojan vaarantuminen sekä henkilöstön liiallinen luotto teknologisiin ratkaisuihin. Toisaalta lähestymistapoja ongelmiin havaitaan myös useita. Huomattavaa onkin, että esimerkiksi väärennettyjen videoiden paljastaminen on itsessään mittava tutkimusala. Myös lainsäädäntöä on kehitetty vastaamaan erityisesti yksityisyydensuojaa koskeviin huolenaiheisiin. Uhkia ja ratkaisuehdotuksia pohdittaessa havaitaan myös, että merkittävä tekijä turvallisuusuhkien pienentämisessä on haasteiden ja niitä lieventävien tekijöiden huomioon ottaminen ehkäisevästi jo teknologian suunnitteluvaiheessa. Tutkielman tulokset siis osoittavat, että uhkia on runsaasti, ja toisaalta myös sen, että uhkia vastaamaan on jo kehitetty parannusehdotuksia. Tulokset viittaavat myös siihen, että uhkien konkretisoitumisen välttäminen vaatii niiden huomioimisen järjestelmän koko elinkaaren ajan.

Avainsanat: konenäkö, hahmontunnistus, rikostekninen videoanalyysi, rikostekniikka, videovalvonta, turvallisuusuhka

SISÄLLYSLUETTELO

1. JOHDANTO

Poliisityössä hyödynnetään yhä laajemmin digitaalista todistusaineistoa, ja kysyntä teknologisille sovelluksille on kasvanut. Rikosteknistä kuva-analyysia käytetään rikostutkinnassa esimerkiksi todistajanlausunnon todentamiseen, käsiteltävän tapauksen tapahtumakulun selvittämiseen, todistusaineiston keräämiseen tai joissain tapauksissa jopa epäillyn tunnistamiseen (Li et al., 2019). Sittemmin kuva-analyysin rinnalle on noussut videoanalyysi, kun erilaisia videokamerasovelluksia, kuten CCTV-välineistöä (engl. closed-circuit television) ja poliisien haalarikameroita, on otettu käyttöön (Farrington & Welsh, 2009). Staattinen videointi ja sen analysointi ihmisen toimesta ovat kuitenkin ominaisuuksiltaan rajallisia, joten viime aikoina konenäön ja sen moninaisten ominaisuuksien, kuten hahmontunnistuksen, hyödyntäminen on yleistynyt (Seldev & Shana, 2019). Tarkoituksena on tehostaa videomateriaalin analysointia automatisoimalla sen sisällön todentaminen. Samaan aikaan kun kysyntä valvonnan tehostamiselle kasvaa, järjestelmien sisältämät haasteet ja niiden muodostamat uhat ovat jääneet vähemmälle huomiolle (Farid & Thakkar, 2021). Erityisesti rikosteknisessä viitekehyksessä virheellisillä havainnoilla on tunnistetusti vakavia seurauksia. Puutteellinen turvallisuusuhkien kartoittaminen johtaa epäluotettaviin järjestelmiin, mikä puolestaan johtaa siihen, ettei rikosteknistä videoanalyysia tai rikostutkintaa ylipäätään voida suorittaa asianmukaisesti. Kritiikitön uuden teknologian käyttöönotto voi johtaa tilanteeseen, jossa saatuja havaintoja ei osata selittää, mutta niille annetaan ylin päätäntävalta.

Tämän tutkielman tavoitteena on selvittää, millaisia turvallisuusuhkia konenäön hahmontunnistusominaisuutta hyödyntävään rikostekniseen videoanalyysiin liittyy. Lisäksi tutkitaan mahdollisia parannusehdotuksia, joilla lieventää uhkia. Tutkielman löydökset perustuvat tutkimusartikkeleihin, jotka käsittelevät hahmontunnistusta rikosteknisessä viitekehyksessä sekä hahmontunnistuksen hyödyntämisessä havaittuja ongelmia kuin myös niiden ratkaisuehdotuksia.

Työssä havaitaan, että keskeisiä teknologisia haasteita ovat neuroverkkojen koulutuksessa käytettävien datajoukkojen rajallisuus, videoiden väärentäminen ja yleinen järjestelmien välisten suojausten vaarantuminen, videokuvan ja -käsittelyn laadulliset puutteet

sekä ihmistutkijoiden rajallinen teknologinen osaaminen. Eettisiä haasteita ovat puolestaan henkilötietojen käsittelyn ja säilömisen aiheuttama yksityisyydensuojan vaarantuminen sekä henkilöstön liiallinen luotto teknologisiin ratkaisuihin. Toisaalta lähestymistapoja ongelmiin havaitaan myös useita. Huomattavaa onkin, että esimerkiksi väärennettyjen videoiden paljastaminen on itsessään mittava tutkimusala. Myös lainsäädäntöä on kehitetty vastaamaan erityisesti yksityisyydensuojaa koskeviin huolenaiheisiin. Työssä havaitaan, että tämänhetkinen teknologisten ratkaisuehdotusten lähestymistapa on ristiriidassa kehitteillä olevien lakisääteisten vaatimusten kanssa. Uhkia ja ratkaisuehdotuksia pohdittaessa havaitaan myös, että merkittävä tekijä turvallisuusuhkien pienentämisessä on haasteiden ja niitä lieventävien tekijöiden huomioon ottaminen ehkäisevästi jo teknologian suunnitteluvaiheessa. Tutkielman tulokset osoittavat, että uhkia on runsaasti, ja toisaalta myös sen, että uhkia vastaamaan on jo kehitetty parannusehdotuksia. Tulokset viittaavat myös siihen, että uhkien konkretisoitumisen välttäminen vaatii niiden huomioimisen järjestelmän koko elinkaaren ajan.

Tutkielman toisessa luvussa määritellään rikostekninen videoanalyysi ja eritellään siihen sisältyvät vaiheet. Luvussa kolme käsitellään konenäköä ja syvennytään hahmontunnistuksen teknologiseen kuvaukseen. Neljännessä luvussa esitellään havaitut turvallisuusuhat. Luvussa käsitellään uhkia sekä teknologisesta että eettisestä näkökulmasta. Luvussa viisi esitetään ehdotettuja parannuksia ja nykyisiä kehityssuuntia. Luvussa kuusi käsitellään tutkimuksen tuloksia ja arvioidaan tavoitteiden täyttymistä. Luku seitsemän on tutkielman yhteenveto ja siinä kuvataan tutkielma pääpiirteittäin.

2. RIKOSTEKNINEN VIDEOANALYYSI

Visuaalisella multimedialaitteistolla kuvattu kuvien sarja muodostaa liikkuvan kuvan eli videon. Video koostuu siis kuvista tai tarkemmin ottaen kuvaruuduista. Kuvankäsittely on kuvasta tai videon kuvaruudusta saadun syötteen käsittelemistä, ja sen tuloste voi liittyä kuvan ominaisuuksiin tai sen parametreihin. Tässä tutkielmassa kuvankäsittelyn sovellusalueena ovat videon kuvaruudut. Videoanalytiikassa analysoidaan useita kuvaruutuja ja niiden välisiä suhteita (Li et al., 2019).

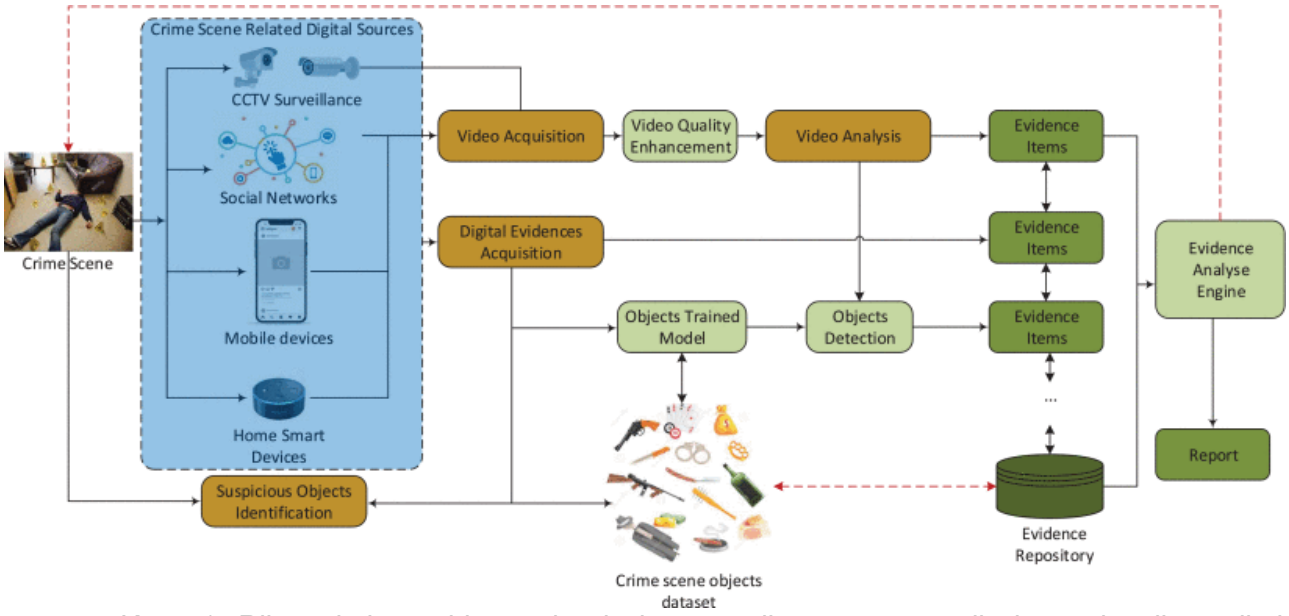
Rikosteknisen videoanalyysin pääasiallisena tarkoituksena on havaita ja todentaa todistusaineistona käytettävää materiaalia, kuten epäilyttäviä esineitä. Videoanalyysissa hyödynnetään rikospaikalta kuvattua videota. Videon lähteenä voi olla esimerkiksi valvontakamera, sosiaalinen media, matkapuhelin tai kodin älylaite (Li et al., 2019).

Videoanalyysi saa alkunsa videon hankkimisesta, joka tapahtuu edellä mainitun välineistön kautta. Saatua syötettä voidaan pyrkiä parantelemaan niin, että sen analysointi on mahdollisimman vaivatonta. Tämä tarkoittaa muun muassa videon kuvan laadun asianmukaista parantamista. Perinteinen analyysi suoritetaan ihmisen toimesta niin, että tutkija erittelee olemassa olevien tietojen ja oman kyvykkyytensä perusteella videosta tutkinnan kannalta olennaisia esineitä tai henkilöitä (Li et al., 2019). Tämä voi käytännössä olla sitä, että tutkija havaitsee kuvaruudussa aseen. Hahmontunnistusta hyödyntävässä analyysissa kohteentunnistusalgoritmi käsittelee materiaalin. Algoritmi on koulutettu tunnistamaan epäilyttäviä kohteita ja sen toiminta perustuu *syväoppiviin neuroverkkoihin* (engl. deep-learning neural networks) (Li et al., 2019). Seuraavassa luvussa syvennytään kohteentunnistusalgoritmien toimintaan.

Analyysin jälkeen havaitut kohteet joko nimetään todistusaineistoksi tai hylätään tutkinnan kannalta tarpeettomina. Sitten todistusaineet analysoidaan ja raportoidaan eteenpäin.

Alla olevassa kuvassa on prosessia havainnollistava kaavio. Edellä kuvailtu prosessi on kuvassa ylimmäisenä ja etenee vasemmalta oikeaan alanurkkaan. Prosessi alkaa rikospaikalta, josta on hankittu videokuvaa. Videon kuvan laatua parannetaan, jonka jälkeen

se analysoidaan joko automaattisesti hahmontunnistuksen avulla tai manuaalisesti ihmisen toimesta. Lopulta mahdollinen todistusaineisto eritellään ja analysoidaan, minkä jälkeen ne kirjataan tukinnan raporttiin.



Kuva 1. Rikosteknisen videoanalyysin kuvaus alkaen vasemmalla kuvatulta rikospaikalta ja edeten *Video Acquisition* -laatikosta nuolten osoittamalla tavalla (Li et al., 2019).

Kuten kuvasta voidaan huomata myös laite, jolla syötevideo on kuvattu, voidaan määritellä todistuasaineistoksi.

Rikostekninen videoanalyysi on toissijainen keino kerätä ja tunnistaa todistusaineistoa. Ensisijaisesti epäilyttävät esineet ja muut tutkinnan kannalta olennaiset asiat pyritään tunnistamaan heti rikospaikalla eikä myöhemmin kamerakuvasta.

3. HAHMONTUNNISTUS RIKOSTEKNISESSÄ VIDEOANALYYSISSÄ

Konenäkö on yksi tekoälyn tutkimusalueista. Konenäkö koostuu metodeista, joilla analysoidaan, havaitaan ja yhdistetään kuvia (Thangharaj & Vaishali, 2022). Hahmontunnistus on eräs tällainen metodi, ja sitä käytetään nimensä mukaisesti kuvien tai kuvaruutujen sisällön tunnistamiseen. Rikosteknisessä viitekehyksessä hahmontunnistusta käytetään pääasiallisesti tunnistamaan uhkaa indikoivat esineet, kuten aseet ja hylätyt matkatavarat. Hahmontunnistusta voidaan käyttää myös rikoksesta epäillyn kasvojen tunnistamiseen. Esineiden ja kasvojen lisäksi konenäöllä voidaan tunnistaa uhkaavaa käytöstä, mutta se perustuu osittain eri mekanismeihin kuin pelkkä kohteentunnistus (Nash & O'Shea, 2015). Hahmontunnistusta hyödyntävässä videoanalyysissä kohteiden havaitseminen, tunnistaminen ja tarpeen mukaan myös jäljittäminen on automatisoitu. Hahmontunnistusta hyödynnetään nykyään rikollisen toiminnan ehkäisyssä, selvittämisessä ja jopa reaaliaikaisessa tunnistamisessa (Cha et al., 2020).

Hahmontunnistus koostuu *kuvan luokittelusta* (engl. image classification) ja *kohteen paikannuksesta* (engl. object localization). Kuvan luokittelu tarkoittaa sitä, että syötekuvasta tunnistetaan, mitä se esittää ja sisältää. Kohteen paikannus on puolestaan sitä, että tunnistetaan, missä luokan määrittävä kohde kuvassa sijaitsee (Świeżewski, 2020). Hahmontunnistus toteutetaan *kohteentunnistusalgoritmeilla* (engl. object detection algorithm).

3.1 Konvoluutioneuroverkot

Kohteentunnistusalgoritmit hyödyntävät neuroverkkoja. Neuroverkoilla viitataan laskennallisiin malleihin, jotka perustuvat yhdistyvään laskentaan ja koostuvat toisiinsa kytketyistä solmuista eli neuroneista. Perusajatus on se, että neuroverkko oppii esimerkkien avulla tunnistamaan muuttujien väliset riippuvuussuhteet. Useat hahmontunnistusalgoritmit hyödyntävät konvoluutioneuroverkkoja, jotka eroavat perinteisistä neuroverkoista siten, että ne soveltuvat arkkitehtuuriltaan erityisesti kuvien käsittelyyn (Choo & Jarrett, 2021).

Konvoluutioneuroverkot koostuvat konvoluutiokerroksista, jotka voidaan mieltää ikään kuin suodattimien sarjaksi. Hahmontunnistuksen yhteydessä suodattimet erittelevät kuvasta olennaisia piirteitä, kuten reunoja, pystyviivoja, vaakaviivoja, kaarteita ja muita, sekä luovat niiden perusteella *piirrekartan* (engl. feature map). Yksi suodatin koostuu *kerneliksi* (engl. kernel) kutsutusta matriisista ja se liitetään kuvaan konvoluutio-operaatiolla. Konvoluutio-operaatio on eräänlainen matriisien kertolasku, jossa syötekuvasta eritelty pikselimatriisi kerrotaan kernelillä. Tulo on tuloskuva, jonka sisällöstä sitten poimitaan edellä mainittuja piirteitä. Kerneli käy läpi syötekuvaa *harppauksin* (engl. stride) eli se käsittelee tietyn määrän pikseleitä kerrallaan (Nash & O'Shea, 2015). Konvoluutiokerrosten pinoaminen mahdollistaa sen, että ylemmät eli syötekuvaa lähimmät kerrokset erittelevät yksinkertaisia kuvan piirteitä, kuten viivoja, ja syvemmät kerrokset havaitsevat monimutkaisempia piirteitä, kuten muotoja ja hahmoja.

Kun kerrokset ovat muodostaneet piirrekartat, suoritetaan niiden *alinäytteistys* (engl. pooling), mikä käytännössä tuottaa tiivistelmiä syötteenä olleista piirrekartoista ja täten vähentää parametreja, joita syväneuroverkon tulee oppia. Alinäytteistys myös vähentää verkon laskennallisten operaatioiden määrää ja sitä voidaan käyttää tilaamaan lisää konvoluutiokerroksia. Konvoluutiokerrosten ja alinäytteistyksen avulla luodaan syöte, jonka perusteella syväneuroverkko tekee lopullisen ennusteen kuvan sisältämistä hahmoista. Syväneuroverkko on datajoukkojen avulla koulutettu tunnistamaan tiettyjä luokkia. Hahmontunnistuksessa hyödynnetään useimmiten *ohjattua oppimista* (engl. supervised learning), mikä tarkoittaa sitä että neuroverkko on koulutettu tunnistamaan kohteita ohjatusti niin, että sille on kerrottu oikea lopputulos. Verkolle on esimerkiksi opetusdatana syötetty kuva porkkanasta ja merkitty, että tulosteessa tulisi olla havaittu porkkana. Näin verkko on oppinut tuottamaan samankaltaisesta datasta ennusteen.

3.2 Kohteentunnistusalgoritmit

Eräs laajasti hyödynnetyistä kohteentunnistusalgoritmeista on YOLO. On epäselvää, käytetäänkö YOLOa vielä rikosteknisessä viitekehyksessä, mutta monissa tutkimuksissa sitä käsitellään juuri tällä sovellusalueella (Choensawat et al., 2018; Li et al., 2019; Sun et al., 2022). Mikäli käytännön rikosteknisiä sovelluksia ei vielä ole, on kuitenkin erittäin todennäköistä, että tulevaisuudessa tätä algoritmia hyödynnetään laajasti videovalvonnassa (Choo & Jarrett, 2021). On siis perusteltua käsitellä sitä tässä viitekehyksessä.

YOLOn yleisen suosion syynä on korkea suorituskyky, joka mahdollistaa muun muassa sen, että algoritmi kykenee käsittelemään videokuvaa reaaliaikaisesti. YOLOn ensimmäinen sukupolvi julkaistiin vuonna 2015 ja siitä on sittemmin julkaistu useita iteratiivisesti paranneltuja versioita. Algoritmin nimi on lyhenne sanoista You Only Look Once eli suomeksi “katsot vain kerran”. YOLO hyödyntää hahmontunnistuksessa DarkNet-53-konvoluutioneuroverkkoa, joka koostuu 53:sta konvoluutiokerroksesta. DarkNet-53 sisältää monia *hyppyjä* (engl. skip connection), jotka ovat olennainen osa YOLOn toiminnallisuutta muun muassa mahdollistaen sen pienen prosessointiajan. On havaittu, että syvemmät konvoluutiokerrokset eivät kykene oppimaan yksinkertaisia funktioita, joita aiemmat kerrokset puolestaan käsittelevät tehokkaasti. Hypyt ehkäisevät tämän ongelman siten, että yhden konvoluutiokerroksen tuottama tulos säilötään ja jätetään huomiotta välittömästi sitä seuraavan kerroksen laskuissa. Hypätyissä kerroksissa laskenta suoritetaan muuten normaalisti ja lopulta tulos summataan sen operaation tulokseen, joka aiheutti hypyn.

Kohteentunnistusalgoritmit perustuvat joko luokitteluun tai regressioon. Luokittelussa hyödynnetään dataa, joka on jaettu ryhmiin. Kohteentunnistusalgoritmeissa tämä useimmiten toteutetaan niin, että kuva jaetaan alueisiin, joista sitten konvoluutiokerrosten avulla luokitellaan sisältö. Regressioon perustuva algoritmi puolestaan käsittelee jatkuvaa dataa ja luo ennusteen uudelle arvolle. Ennuste luodaan syötearvojen lisäksi opetusdatan pohjalta. Regressioon perustuva kohteentunnistusalgoritmi ei siis ennalta rajaa kuvaa alueisiin, vaan toteuttaa rajauksen ja ennustuksen kertaluontoisella neuroverkon ajolla. YOLO on regressioon perustuva algoritmi (Divvala et al., 2016).

YOLO tekee kohteiden rajauksen suorakulmion muotoisilla *laatikoilla* (engl. bounding boxes). Laatikko koostuu keskipisteestä, leveydestä, korkeudesta ja cis -arvosta (alempana yhtälössä c), joka vastaa kohteen luokkaa eli esimerkiksi autoa, laukkua tai muuta vastaavaa. Lisäksi on p_c -arvo, joka on todennäköisyys siitä, että rajattu alue sisältää jonkin kohteen (Świeżewski, 2020). Yhden rajaavan laatikon lauseke on siis

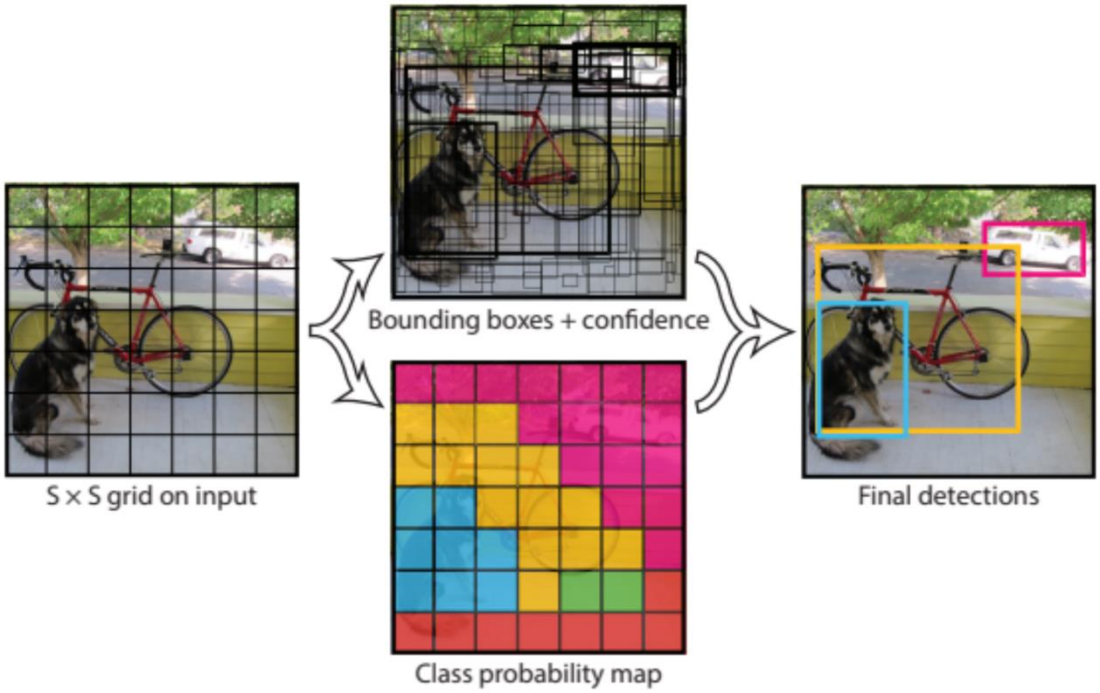
$$y = (p_c, b_x, b_y, b_h, b_w, c), \tag{1}$$

missä piste (b_x, b_y) on keskipiste, vakio b_h korkeus ja b_w leveys.

YOLO jakaa kuvan soluihin, minkä se toteuttaa tyypillisesti 19x19-solukolla. YOLO kykenee käsittelemään minkä kokoisia kuvia tahansa, kunhan ne voidaan muuttaa

608x608 -kokoon. Koko, johon kuva tulisi muuttaa, vaihtelee eri YOLOn versioissa, ja esimerkiksi viidennessä ja seitsemännessä versiossa koko on 640x604. Koko on merkityksellinen siksi, että DarkNet-53 tekee piirrekarttoja käyttäen kernelin harppauksia, joiden koko on 8, 16 tai 32. Luvun 608 ja luvun 32 osamäärä on 19, minkä vuoksi tämä on tyypillinen solukon koko. Yksittäinen solu luo viisi rajaavaa laatikkoa, koska mahdollisia kohteita voi olla enemmän kuin yksi. Suurin osa soluista ja laatikoista eivät kuitenkaan sisällä mitään kohteita, minkä vuoksi p_c -arvo on hyödyllinen. Sen arvon perusteella poistetaan laatikot, jotka epätodennäköisimmin sisältävät kohteen, sekä laatikot, joilla on suurin jaettu pinta-ala. Päällekkäisten laatikoiden poistamista kutsutaan englanniksi *non-max suppression* -prosessiksi (Świeżewski, 2020). Algoritmin tuloste on laatikolla rajattu kohde, jonka kehyksessä lukee arvio sen luokasta. Myöhemmissä versioissa myös luokan todennäköisyys on arvioitu. Tämä tarkoittaa sitä, että laatikon kehyksessä lukee luokan lisäksi desimaaliluku siitä, kuinka todennäköisesti laatikko sisältää kyseisen kohteen.

Alla olevassa kuvassa on yksinkertaisesti havainnollistettu ensimmäisen version YOLO-algoritmin toimintaa. Vasemmalla sijaitsevasta syötekuvasta luodaan ensin ruudukko, jonka solut sitten luovat laatikoita ja vaativat arvion sille todennäköisyydelle, että onko kuvassa jokin kohde tai tarkemmin mikä kohde kuvassa on. Lopulta kun päällekkäiset laatikot on poistettu ja jäljelle ovat jääneet laatikot, joissa kunkin havaitun kohteen luokan todennäköisyys on suurin, tulostetaan varsinaiset havainnot.



Kuva 2. YOLOv1 -algoritmin kohteentunnistusprosessi (Świeżewski, 2020).

4. TURVALLISUUSUHAT

Turvallisuusuhkien tarkastelu on tässä luvussa jaettu teknisten haasteiden ja eettisten uhkien kuvailuun. Tekniseksi uhaksi määritellään tässä työssä sellaiset asiat, joiden myötä teknologian tuottamien tulosten luotettavuus voidaan kyseenalaistaa tai jotka vaikeuttavat teknologian käyttöä. Eettisiä uhkia kuvaillan aihealueen rajaamisen puitteissa suppeasti. Niissä keskitytään tarkastelemaan asioita, jotka voivat aiheuttaa kansalaisille haittaa.

4.1 Tekniset haasteet

Hahmontunnistusta hyödyntävässä videoanalyysissä käsiteltävä data on kerätty pääasiassa valvontakameroista. Data ei siis välttämättä täytä niitä laadullisia vaatimuksia, joita tarvitaan tehokkaan ja juridisesti pätevän videoanalyysin laatimiseen. Heikkolaatuisesta videokuvasta on haasteellista, ellei mahdotonta, automaattisesti tunnistaa yksityiskohtia, vaikka kuvaruudun mittakaavaa muutettaisiin (Abdul et al., 2021). Mittakaavan muutos, erityisesti kuvan suurennus, yleensä johtaa kuvan sumentumiseen, pikselöitymiseen tai muutoin tekee siitä epätarkemman. Lisäksi on havaittu, että mahdollisuudet parantaa kuvan tarkkuutta sen oton jälkeen ovat varsin rajalliset (Li et al., 2019). Kuvan laadun parantamista käsitellään tarkemmin luvun viisi ensimmäisessä alaluvussa.

Videon laatuun vaikuttaa olennaisesti kuvauspaikan valotus, joka rikospaikoilla harvoin on hyvä. Useasti kuvauspaikka on hämärä tai pimeä, vaikka kameroiden sijoittamisella ja asentamisella pyritään saavuttamaan paras mahdollinen valotus. Lisäksi ali- tai ylivalottuneita kuvaruutuja pitää manuaalisesti säätää, jotta videokuvaa voidaan käsitellä kokonaisuutena (Gadekallu et al., 2021). Videon laadun heikkenemiseen vaikuttaa myös tiedostokoon pienentäminen. Valvontajärjestelmät usein pakkaavat videotiedostot tiiviisti, jotta muistin käyttö on mahdollisimman tehokasta. Tämä voi johtaa vaikeasti palautettavaan tietokatoon, kuten juuri videon laadun heikkenemiseen (Li et al., 2019).

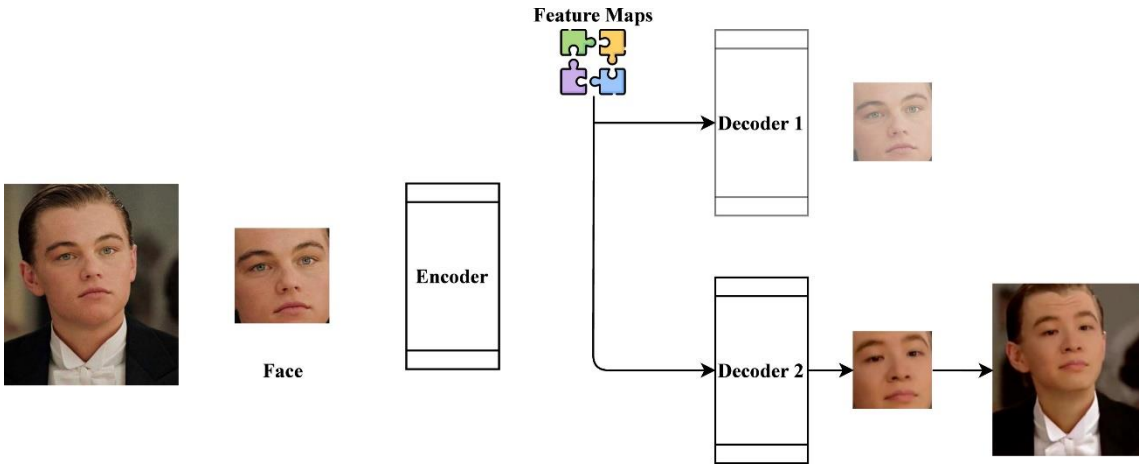
Hahmontunnistuksen soveltamisessa erityisen haasteen aiheuttaa ihmistutkijoiden rajallinen ymmärrys syväoppimisen toiminnasta. Alan asiantuntijatkaan eivät vielä osaa täysin selittää, miten hahmontunnistusalgoritmien hyödyntämien konvoluutioneuroverkkojen oppiminen tapahtuu tai miten syväneuroverkko tuottaa varsinaisen ennusteen. Tämä johtaa siihen, että verkon arkkitehtuurin muuttaminen muodostuu mahdottomaksi, koska

olennaisten parametrien vaikutusta prosessiin ei tunneta (Gadekallu et al., 2021). Algoritmeja on siis vaikea optimoida eikä esimerkiksi ihanteellista konvoluutiokerrosten määrää voida arvioida. Lisäksi nopeasta kehityksestään huolimatta tehokkaimmissakin kohteentunnistusalgoritmeissa on puutteita. YOLO-algoritmi ei esimerkiksi kykene erittelemään kahta erittäin lähellä toisiaan olevaa hahmoa ja se usein epäonnistuu havaitsemaan kooltaan pieniä hahmoja.

Syväoppimista hyödyntävissä järjestelmissä neuroverkkojen koulutukseen käytettävien datajoukkojen rajallisuus muodostuu ongelmaksi. Vaikka useita datajoukkoja kyetään yhdistelemään kuvaruutujen kokonaisuudeksi, yleisesti saatavilla olevat datajoukot ovat rikosteknisessä viitekehyksessä kooltaan jopa pieniä ja usein eroavat luokille annetuilta määritelmiltään. Tämä johtaa ristiriitaisuuksiin kohteentunnistuksessa. (Gadekallu et al., 2021)

Teknologinen kehitys saavuttaa rikosteknisen tutkimuksen samanaikaisesti kuin rikolliset. Tämä tarkoittaa sitä, että sama teknologia, joka mahdollistaa tehokkaamman rikostutkimuksen, mahdollistaa myös tehokkaamman rikollisuuden. Eräs enenevissä määrin haasteeksi muodostuva ilmiö on videoiden väärentäminen, johon voidaan käyttää esimerkiksi deep fake -tekniikkaa. Deep fake -video näyttää samalta kuin alkuperäinen video, mutta jokin olennainen ominaisuus on väärennetty (Gadekallu et al., 2021). Deep fake -tekniikkaa käytetään lähinnä kasvojen ja äänen väärentämiseen. Tekniikka perustuu koneoppimisen menetelmiin, joissa hyödynnetään *autoenkoodaajia* (engl. autoencoder) ja *generatiivisia kilpailevia verkostoja* (engl. generative adversarial network**)** eli GANeja. Yksinkertaisesti ilmaistuna deep fake muodostuu, kun autoenkoodaaja tuottaa alkuperäisestä syötekoodista piirrekarttoja, jotka sitten syötetään GANillle. Kuten konvoluutioneuroverkkojen tapauksessa, piirrekartta sisältää kuvaruudusta eriteltyjä piirteitä eli esimerkiksi viivoja ja muotoja. GANin tehtävä on varmistaa, että neuroverkko ei pysty tunnistamaan eroa alkuperäisen ja väärennöksen välillä. GAN koostuu kahdesta neuroverkosta, joista toinen on *generaattori* (engl. generator) ja toinen on *diskriminaattori* (engl. discriminator). Verkot kilpailutetaan niin, että generaattori tuottaa piirrekartoista väärennöksiä, joita diskriminaattori pyrkii havaitsemaan. Kilpailun myötä generaattori kykenee tuottamaan yhä tarkempia väärennöksiä, minkä myötä diskriminaattori ei lopulta tunnista eroa alkuperäisen ja väärennetyn piirrekartan välillä (Alkan & KoÇak, 2022). Alla olevassa kuvassa havainnollistetaan, miten deep fake luodaan. Alkuperäinen syötäkuva

rajataan niin, että autoenkoodaaja kykenee tuottamaan kuvassa näkyvistä kasvoista piirrekarttoja (kuvassa ”feature maps”). Kuvassa Decoder 1 ja Decoder 2 edustavat GANin neuroverkkoja. Decoder 1 on tässä havainnollistuksessa diskrimaattori, joka vertaa väärennöksiä alkuperäiseen piirrekarttaan ja Decoder 2 on generaattori, joka tuottaa väärennöksiä.



Kuva 3. Havainnollistus, siitä miten deepfake -video luodaan (Gadekallu et al., 2021)

Deepfake -videot ovat yksi oire suuremmasta ongelmasta, joka on salauksien heikkeneminen. Merkittävä osa salauksia purkavista ohjelmistoista on vapaasti kenen tahansa saatavilla, mikä kasvattaa rikollisen toiminnan mahdollisuuksia (Gadekallu et al., 2021). Haasteena on erityisesti hyökkäykset, jotka kohdistuvat yhteyden muodostamiseen videolaitteen ja verkossa toimivan pilvipalvelun välillä (Cha et al., 2020). Turvallinen yhteys on ehto sille, että välitetty data on luotettavaa ja siten käyttökelpoista rikosteknisessä viitekehyksessä.

4.2 Eettiset uhat

Rikostekninen hahmontunnistusta hyödyntävä videoanalyysi on tehokkuudestaan huolimatta yhä riippuvainen ihmistutkijan pätevyydestä. Tämä johtuu siitä, että hyödynnettävät teknologiat ovat valtaosin yhä kehittyviä eivätkä siten aina tuota tarkkoja, kokonaisuuden huomioon ottavia tai ylipäätään täysin luotettavia tuloksia (Choo & Jarrett, 2021).

On tarpeellista, että hahmontunnistusta hyödyntävässä rikostutkinnassa tutkijat ovat teknologiaan perehdytettyjä ja että heillä on taidot sekä analysoida että ymmärtää teknologian tuottamia tuloksia. Todellinen uhka muodostuu, kun ihmistutkijoiden roolia vähätellään tai kokonaan sivuutetaan siinä uskossa, että hyödynnettävät teknologiset sovellukset tuottavat objektiivisesti tosia tuloksia.

Huomionarvoista on, että teknologinen kehitys itsessään on myös haaste konenäköä hyödyntävälle videoanalyysille. Käsiteltävän tiedon suuri määrä ja videokuvan jakautuneet lähteet ovat vaikeita hallita yhdenvertaisesti. Lisäksi alati kehittyvä teknologia vaatii, että rikostekniset menetelmät ja riippuvuuksia sisältävät järjestelmät kehittyvät samalla nopeudella.

Valvotun yksilön yksityisyydensuojaan liittyvät huolet ovat myös lisääntyneet. Keskeinen kysymys on se, kuinka hyvin älykkäät valvontalaitteet noudattavat Euroopan unionin tietoturvaa koskevaa lainsäädäntöä, erityisesti Euroopan unionin (EU) General Data Protection Regulation -asetusta eli GDPR:ia. GDPR takaa EU:n kansalaisille tietoturvaan liittyviä oikeuksia, jotka suurimmaksi osaksi koskevat henkilötietojen käsittelyä. Tällaisia oikeuksia ovat muun muassa henkilötietojen pseudonymisointi (engl. pseudonymisation) ja salaus (engl. encryption) sekä se, että tiedonkäsittelyssä toteutetaan suojatusti (Ashghar et al., 2019). Ongelmallista on se, että vaikka GDPR:ssa määritellään näitä erinäisiä vaatimuksia, niiden toimeenpanoon ei neuvota, vaan se jää toteuttajan eli usein palveluntarjoajan vastuulle (Ashghar et al., 2019).

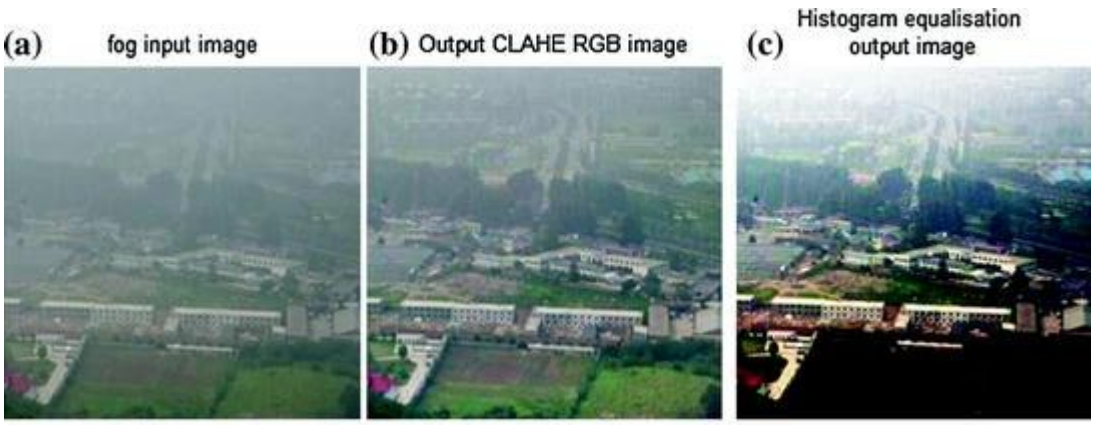
5. TURVALLISUUSUHKIEN LIEVENTÄMINEN

Älykkäisiin valvontalaitteisiin liittyviä teknologisia turvallisuusuhkia pyritään pienentämään kehittämällä ja parantamalla olemassa olevia ratkaisuja. Eettisten haasteiden hallinnassa luotetaan pääasiassa lainsäädännön kehitykseen. Tässä luvussa tarkastellaan joitakin uhkien lieventämisen kehityssuuntia ja parannusehdotuksia, jotka tällä hetkellä ovat keskustelun ytimessä.

5.1 Kuvan laadun parantaminen

Kuten edellisessä luvussa havaittiin, videokuvan huono laatu on keskeinen haaste rikosteknisessä videoanalyysissä. Kuvan laatua on mahdollista jälkikäteen parantaa erilaisilla menetelmillä. Yksi yleisesti hyödynnetyistä kuvan laatua parantavista algoritmeista on CLAHE eli englanniksi ”contrast-limited adaptive histogram equalization”. CLAHE:sta povataan ratkaisua myös rikosteknisen videoanalyysin kuvan laadun ongelmaan. (Li et al., 2019)

Kuvan histogrammi kertoo kuvan yleisen valotusarvon eli sen, kuinka valon määrä jakautuu yksittäisille pikseleille. CLAHE pohjautuu histogrammin täsmäämiseen. Perinteisessä histogrammitasauksessa valotusarvo tasataan kuvan pikseleiden suhteen niin, että kuvan yleinen kontrasti paranee (Marimuthu, 2022). CLAHE jakaa syötekuvan pieniin alueisiin, joita kutsutaan *laatoiksi* (engl. tiles). Jokaiselle laatalle luodaan yksittäinen histogrammin tasaus, mutta viereisten laattojen kontrastia pyritään rajoittamaan niin, että muodostuva kohina on mahdollisimman vähäistä. CLAHEn on havaittu tuottavan edeltäjiään tarkempia tuloksia ja sen vahvuus on erityisesti kohinan vähäisyys (Garg et al., 2018). Alla olevassa kuvassa on vertailtu kuvan laatua parantavia menetelmiä. Vertailusta voidaan huomata että ainakin silmämääräisesti CLAHE (b-kuva) tuottaa tarkemman tulostekuvan kuin pelkkä histogrammitasaus (c-kuva).



Kuva 4. CLAHE-algoritmin (b) ja histogrammitasauksen (c) tulostekuvat verrattuna alkuperäiseen kuvaan (a). (Agalya et al., 2016)

Vaikka CLAHE mielletään soveltuvaksi videovalvontaan, mahdollisuudet sen hyödyntämiseen automatisoidussa videoanalyysissä ovat rajalliset. CLAHE-algoritmia voidaan hyödyntää hahmontunnistuksessa niin, että kohteentunnistusalgoritmin syöteaineiston laatua on ensin kohennettu CLAHEn avulla (Li et al., 2019). Reaaliaikaiseen hahmontunnistukseen se ei kuitenkaan vielä vaikuta soveltuvan. On myös epäselvää, voidaanko kuvan laadun parantamisen ja hahmontunnistuksen menetelmät jotenkin integroida toisiinsa.

5.2 Väärennettyjen videoiden havaitseminen

Väärennettyjen videoiden havaitsemiseen on kehitetty lukuisia metodeja, jotka valtaosin perustuvat syväoppiviin algoritmeihin ja joiden mekanismin ytimessä on poikkeavuuksien havaitseminen.

Artikkelissaan *Deep Learning for Object-Based Forgery in Advanced Video* (2017) Bo Guan ja muut kuvailevat konvoluutioneuroverkkoja hyödyntävää väärennösten havaitsemismenetelmää. Menetelmän tarkoitus on havaita videolla esiintyviin *hahmoihin kohdistuvia väärennöksiä* (engl. object forgery), joita ovat tyypillisesti hahmon kopioiminen ja sen sijainnin muuttaminen tai hahmon poistaminen videosta. Menetelmä koostuu videon kuvaruutujen esikäsittelystä sekä neuroverkon kouluttamisesta. Videon esikäsittelyssä lasketaan erotus peräkkäisten kuvaruutujen harmaaväriskaalojen välillä ja luodaan erotuksen pohjalta kuva. Tämä kuva jaetaan sitten pienempiin *kuvajoukkoihin* (engl. image patch). Neuroverkon kouluttamisessa hyödynnetään *asymmetrista datan täydentämistä*

(engl. asymmetric data augmentation), mikä tarkoittaa sitä, että aineistoon lisätään väärennettyjä kuvaruutuja. Positiiviset havainnot eli väärennetyksi luokitellut kuvajoukot koostuvat sekä väärennetyistä että koskemattomista kuvaruuduista. Negatiiviset havainnot koostuvat vain koskemattomista kuvaruuduista. Väärennetystä materiaalista luodaan huomattavasti enemmän kuvajoukkoja, jotta väärennettyjen ja koskemattomien kuvaruutujen eroavaisuuksista tehtäisiin mahdollisimman täsmälliset havainnot. Ajatuksena on, että neuroverkko oppii datan täydennyksen avulla tunnistamaan, kuinka suuri peräkkäisten kuvaruutujen harmaaväriskaalojen erotus on väärennetyissä kuvajoukoissa. Ennen kuin data syötetään konvoluutioneuroverkkoon, sitä käsitellään muun muassa niin, että laskenta yksinkertaistuu ja että väärennetyn datan tunnusmerkit vahvistuvat. Guan ja muut havaitsivat tutkimuksissaan, että menetelmä on tehokkaampi kuin perinteiset tekniikat, jotka eivät perustu neuroverkkojen syväoppimiseen.

Myös deep fake -videoväärennösten havaitsemiseen on useita tekniikoita. Artikkelissaan *Exposing Deep Fakes Using Inconsistent Head Poses* (2019) Yuezun Li ja muut esittelevät metodin, jossa väärennösten aiheuttamat epäyhdenmukaisuudet havaitaan kasvojen asentojen 3D-mallinusta hyödyntäen. Yksinkertaistettuna kyseessä on laskemallinen malli, joka vertailee kasvojen koordinaattien yhdenmukaisuutta kameran kulman koordinaatteihin. Tutkimuksessa hyödynnetään tietoa siitä, että väärennöksissä keskelle kasvoja piirretyt koordinaatit eivät vastaa kasvojen reunoille piirrettyjen koordinaattien asentoa.

5.3 Lainsäädäntö

Kuten aiemmin todettiin, eettisten uhkien ehkäisyssä lainsäädännön mielletään olevan avainasemassa. Euroopan unionin vuonna 2018 toimeenpanema General Data Protection Regulation -asetus (GDPR) on saavuttanut merkittävän aseman erityisesti yksityisyydensuojan tukena. Sittemmin on kuitenkin havaittu, ettei GDPR ole täysin riittävä säätelemään esimerkiksi tekoälyä hyödyntäviä järjestelmiä. Euroopan unioni onkin julkaissut tekoälysovelluksia koskevan lakiehdotuksen Artificial Intelligence Act (AI Act).

AI Act -asetuksen tarkoitus on GDPR:n tavoin asettaa vähintään Euroopan unionin laajuinen lakisääteinen standardi tekoälyä hyödyntäville järjestelmille. Lain laatiminen on vielä kesken eikä se siis toistaiseksi ole lainvoimainen. AI Act:ssa tekoälyjärjestelmät jaotellaan kolmeen eri riskikategoriaan. Älykkäät videovalvontalaitteet ovat määritelty korkean riskin sovelluksiksi. Asetuksessa määritellään useita vaatimuksia, joita tulee

noudattaa korkean riskin sovelluksien kehittämisessä ja käytössä. (Buttinger et al. 2022) Keskeisiä vaatimuksia ovat:

- *Riskienhallinta* (engl. risk management system): riskien havaitseminen, tunnistaminen ja käsittely läpi järjestelmän elinkaaren.
- *Datan hallinta ja valvonta* (engl. data & data governance): tekoälymallien kouluttamisessa, arvioinnissa ja testauksessa käytettävän datan hallinnointi ja valvonta.
- *Teknologian dokumentointi* (engl. technical documentation): kokonaisvaltainen ja ajan tasalla oleva dokumentaatio käytettävästä teknologiasta.
- *Käytön taltiointi* (engl. record keeping): vähimmäisvaatimuksia noudattava kirjanpito teknologian käytöstä.
- *Läpinäkyvyys ja käyttäjien tiedottaminen* (engl. transparency and provision of information to users): järjestelmän toiminta on läpinäkyvää ja käyttäjät ovat tietoisia muun muassa palveluntarjoajasta ja järjestelmän käyttökohteesta.
- *Valvonta ihmisen toimesta* (engl. human oversight): ihmisen ja koneen välinen vuorovaikutus, jossa ihminen toimii järjestelmän valvojana.
- *Täsmällisyys, kestävyys ja kyberturvallisuus* (engl. accuracy, robustness and cybersecurity): järjestelmän virheettömyys ja kyky suojautua tahallisilta hyökkäyksiltä.

AI Act:n toimeenpanon povataan tekevän tekoälysovelluksista turvallisempia erityisesti aloilla, joilla automatisoinnin seuraukset voivat olla vakavia, kuten lääketieteessä ja rikostutkinnassa (Buttinger et al., 2022). Huomattavaa on, että asetuksessa on vaatimuksia, jotka liittyvät järjestelmän rakenteeseen, tarkemmin siihen mitä järjestelmä pitää sisältää. Tällaisia vaatimuksia ovat yllä luetelluista ainakin riskienhallinta, datan hallinta ja valvonta sekä vaatimukset koskien järjestelmän täsmällisyyttä, kestävyyttä ja kyberturvallisuutta. Vaikka suurimmassa osassa järjestelmistä on jo varmasti olemassa jonkinlainen virheidenhallintajärjestelmä, asettaa vaatimukset uudenlaisen paineen sille, että nämä riskit otetaan huomioon jo järjestelmän suunnitteluvaiheessa. GDPR:n ja tulevaisuudessa myös AI Act:n vaatimusten kanssa linjassa olevilla suunnitteluratkaisulla lienee merkittävä rooli yksityisyyteen ja muihin eettisiin aiheisiin liittyvien riskien ehkäisemisessä (Ashghar et al., 2019).

6. KESKUSTELU

Hahmontunnistuksen hyödyntäminen rikosteknisessä videoanalyysissä tarjoaa kilpailukykyisen vaihtoehdon manuaaliselle todistusaineiston haravoimiselle. Yhä tarkemmat kohteentunnistusalgoritmit kykenevät tunnistamaan ja paikantamaan rikostutkinnan kannalta olennaisia kohteita ihmissilmää tehokkaammin. Siinä missä analyysin automatisointi tuottaa uusia ja parempia ratkaisuja, sisältää se myös odottamattomia haasteita. Tutkimuksessa esille nousseita haasteita ovat muun muassa videoiden väärentäminen, videokuvan heikkolaatuisuus, neuroverkkojen koulutuksessa käytettävien datajoukkojen rajallisuus sekä ihmistutkijoiden rajallinen ymmärrys käytettävästä teknologiasta. Lisäksi havaittiin eettisiä uhkia, kuten yksityisyydensuojan vaarantuminen sekä kritiikitön suhtautuminen automatisointiin. Hahmontunnistuksen avulla saavutettujen havaintojen luotettavuus kärsii, kun haasteita ei oteta huomioon tai riskinhallinta on puutteellista. Joihinkin haasteisiin, kuten videoiden väärentämiseen, ennalta vaikuttaminen voi olla vaikeaa, mutta rikosteknisessä viitekehyksessä täysin välttämätöntä. Toisaalta esimerkiksi videokuvan laadun parantaminen ja rikostutkijoiden teknologisen ymmärtämisen lisääminen vaikuttavat lähtökohtaisesti helposti lähestyttäviltä haasteilta, mutta vaativat huomattavasti resursseja.

Tutkimuksessa käytetyistä artikkeleista ilmeni kattavasti haasteita, mutta yhtenäistä näkemystä siitä, miten niitä tulisi käsitellä, ei löytynyt. Erityisesti eettisten uhkien kannalta pohdinta vaikuttaa olevan runsasta, mutta käytännön ratkaisut vähissä. Näiden uhkien suhteen luotetaan paljon lainsäädännön kehitykseen, mutta se on varsin hidasta. On haastavaa luoda yhdenmukaisia säädöksiä alati uusia kehityssuuntia ottavalle ja nopeasti kehittyvälle teknologialle. Suurin osa ratkaisuehdotuksista keskittyy ilmenevien ongelmien korjaamiseen jälkikäsittelyssä ongelmien ehkäisyn sijaan. Vastapainona tälle lähestymistavalle EU:n AI Act:ssa vaaditaan riskien ennaltaehkäisyä läpi järjestelmän koko elinkaaren. Mielenkiintoista on, missä määrin uhkia kyetään ehkäisemään hahmontunnistusta hyödyntävässä videoanalyysissä. Riskien ennaltaehkäisyn suhteen ainakin hahmontunnistuksen reaaliaikainen hyödyntäminen vaikuttaisi olevan mahdotonta, sillä videokuvan oikeellisuudesta ei välttämättä voida samanaikaisesti varmistua. Sen sijaan esikäsitelty materiaali, jonka kuvan laatua on parannettu ja jonka oikeellisuus on varmistettu, voidaan syöttää kohteentunnistusalgoritmille. Tämä kuitenkin johtaa kysymykseen siitä, onko tällainen usean prosessin sarja lopulta tehokkaampaa kuin perinteinen, ihmi-

sen suorittama videoanalyysi. Peräti uusi tutkimushaaste lieneekin siinä, miten turvallisuusuhat kyetään huomioimaan jo älykkäiden valvontajärjestelmien suunnitteluvaiheessa.

Tutkimusmenetelmä oli pääosin asianmukainen, vaikka toisinaan artikkeleiden saatavuus muodostui ongelmaksi. Useat aihetta käsittelevät tutkimusartikkelit olivat maksullisia, joten hyödynnettäviä lähteitä tuli rajata. Osassa lähteenä käytetyissä artikkeleissa on päätelmiä, jotka perustuvat näihin maksullisiin artikkeleihin, eikä niiden todenmukaisuudesta täten voi täysin vakuuttua. Tutkimuksessa käytetyistä artikkeleista harvoin kävi ilmi, hyödynnetäänkö käsiteltäviä teknologioita ja menetelmiä rikostutkinnassa vai onko niiden käyttöönotto vasta suunnitteilla. Tähän lienee vaikuttavan se, että käyttäjä on poliisi eli valtiollinen elin ja täten tieto on jossain määrin salaista.

7. YHTEENVETO

Rikosteknistä videoanalyysiä pyritään tehostamaan konenäön hahmontunnistusominaisuuden avulla. Rikosteknisessä videoanalyysissä valvontakameran videokuvasta havaitaan ja todennetaan todistusaineistona käytettävää materiaalia, kuten epäilyttäviä esineitä. Videoanalyysin automatisoinnilla tarkoitetaan sitä, että ihmisen sijasta hahmontunnistusmekanismi suorittaa kohteiden tunnistamisen (Li et al., 2019). Hahmontunnistuksessa hyödynnetään kohteentunnistusalgoritmeja, jotka käyttävät konvoluutioneuroverkkoja ja luovat syötekuvasta ruudukon, jonka solut erittelevät, määrittelevät ja lopulta luokittelevat siinä esiintyvät hahmot. (Świeżewski, 2020)

Älykäs videoanalyysi sisältää useita haasteita. Teknologisia haasteita ovat muun muassa videoiden väärentäminen, videokuvan heikkolaatuisuus, neuroverkkojen koulutuksessa käytettävien datajoukkojen rajallisuus sekä ihmistutkijoiden rajallinen ymmärrys käytettävästä teknologiasta. Videoiden väärentämisen havaitsemiseen on kehitetty useita menetelmiä, jotka pääasiassa pohjautuvat syväoppivien neuroverkkojen hyödyntämiseen ja joiden keskiössä on alkuperäisen ja väärennetyn materiaalin välisten poikkeavuuksien havaitseminen. Videokuvan heikkoa laatua pyritään puolestaan parantamaan asianmukaisella valotuksella, kameran asennoilla ja jälkikäsittelyssä kuvan laatua parantavilla laskennallisilla menetelmillä. Datajoukkojen kasvattamista ja ihmistutkijoiden teknologisen osaamisen lisäämistä pyritään saavuttamaan ainakin lainsäädännön, kuten Euroopan unionin Artificial Intelligence Act -lakialoitteen (AI Act), esittämien vaatimusten avulla. Eettisiä huolenaiheita, kuten yksityisyydensuojan vaarantumista ja kritiikitöntä teknologian käyttöönottoa, pyritään niitäkin lieventämään lainsäädäntöön vedoten.

Sekä uhkia että niiden parannusehdotuksia tutkitaan suhteellisen aktiivisesti, mutta yhtenäistä linjaa on vaikea saavuttaa. Keskeiseksi lähestymistavaksi muodostuu uhkien huomioon ottaminen jo videoanalyysin automatisoinnin suunnitteluvaiheessa. Riskien ennaltaehkäisyä painotetaankin EU:n AI Act -lakialoitteessa. Tällä hetkellä kuitenkin suurin osa varsinkin teknologisista ratkaisuehdotuksista perustuu ilmenevien ongelmien korjaamiseen niiden ehkäisyn sijaan.

LÄHTEET

Agalya P., Gopalakrishna M., Hanumantharaju M., (2016). ”A Detailed Review of Color Image Contrast Enhancement Techniques for Real Time Applications”. Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing, 435, 487-497. https://link.springer.com/chapter/10.1007/978-81-322-2757-1_48

Alkan M. & KoÇak A., (2022). "Deepfake Generation, Detection and Datasets: a Rapid-review". 2022 15th International Conference on Information Security and Cryptography (ISCTURKEY), 86-91. https://ieeexplore.ieee.org/document/9931802

Asghar M., Fleury M., Herbst M., Lee B., Kanwal N., Qiao Y., (2019). "Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective". IEEE Access, 7, 111709-111726. https://ieeexplore.ieee.org/document/8793058

Buttinger C., Kaltenbrunner L., Kieseberg P., Temper M., Tjoa S., (2022). "Security considerations for the procurement and acquisition of Artificial Intelligence (AI) systems," 2022 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 1-7, https://ieeexplore.ieee.org/document/9882675

Cha Y., Kim H., Kim T., Kim P., (2020). "A Study on the Security Threats and Privacy Policy of Intelligent Video Surveillance System Considering 5G Network Architecture". 2020 International Conference on Electronics, Information, and Communication (ICEIC), 1-4. https://ieeexplore.ieee.org/document/9051302

Choensawat W., Santad T., Silapasupphakornwong P., Sookhanaphibarn K., (2018). "Application of YOLO Deep Learning Model for Real Time Abandoned Baggage Detection". 2018 IEEE 7th Global Conference on Consumer Electronics (GCCE), 157-158. https://ieeexplore.ieee.org/document/8574819

Choo K. & Jarrett A., (2021). “The impact of automation and artificial intelligence on digital forensics”. WIREs Forensic Science, 3(6), 1-17. https://doi.org/10.1002/wfs2.1418

Divvala S., Farhadi A., Girschick R., Redmon J., (2016). “You Only Look Once: Unified, Real-Time Object Detection”. Cornell University arXiv, 1-10. https://doi.org/10.48550/arXiv.1506.02640

Farid H. & Thakkar N., (2021). "On the Feasibility of 3D Model-Based Forensic Height and Weight Estimation". IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 953-961. https://ieeexplore.ieee.org/document/9522965

Farrington D. & Welsh B., (2009). “Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis”. Justice Quarterly, 26(4), 716-745. https://www.tandfonline.com/doi/full/10.1080/07418820802506206

Gadekallu T., Jalil Z., Javed A., Piran M., Suh D., Zehra W., (2021). ”A comprehensive survey on digital video forensics: Taxonomy, challenges, and future directions”. Engineering Applications of Artificial Intelligence, 106, 1-14. https://www.sciencedirect.com/science/article/pii/S0952197621003043

Garg D., Garg N., Kumar M., (2018). “Underwater image enhancement using blending of CLAHE and percentile methodologies”. Multimedia Tools and Applications, 77(20), 26545-26561. http://link.springer.com/10.1007/s11042-018-5878-8

Guan B., Shi Y., Weng S., Yao Y., (2018). “Deep Learning for Detection of Object-Based Forgery in Advanced Video”. Symmetry, 10(1), 1-10. https://doi.org/10.3390/sym10010003

Li S., Xiao J., Xu Q., (2019). “Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation”. IEEE access 7, 55432–55442. https://ieeexplore.ieee.org/document/8700194/

Li Y., Lyu S., Yang X., (2019). "Exposing Deep Fakes Using Inconsistent Head Poses". 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 8261-8265. https://ieeexplore.ieee.org/abstract/document/8683164

Marimuthu P., (2022). ”Image Contrast Enhancement Using CLAHE”. Internet-artikkeli, Julkaistu 17.08.2022. Luettu 12.12.2022. https://www.analyticsvidhya.com/blog/2022/08/image-contrast-enhancement-using-clahe/

Seldev C. & Shana L., (2019). "Video Surveillance using Deep Learning - A Review". 2019 International Conference on Recent Advances in Energy-efficient Computing and Communication (ICRAECC),1-5. https://ieeexplore.ieee.org/document/8995084

Świeżewski J., (2020). “YOLO Algorithm and YOLO Object Detection”. Internet-artikkeli. Julkaistu 22.5.2020. Luettu 20.11.2022. https://appsilon.com/object-detection-yolo-algorithm/

Thangaraj D. & Vaishali B., (2022). "Innovative Facial Expression Identification for Criminal Identification using Unsupervised Machine Learning and Compare the Accuracy with CNN Classifiers". International Conference on Business Analytics for Technology and Security (ICBATS), 1-4. https://ieeexplore.ieee.org/abstract/document/9759043

Nash R. & O’Shea K., (2015). “An Introduction to Convolutional Neural Networks”. Cornell University arXiv, 1-10. http://arxiv.org/abs/1511.08458

Sun S., Wang, C., Wang Y., Zhang H. Zhang Y., Zhou, Y, (2022). “Automatic detection of indoor occupancy based on improved YOLOv5 model”. Springer, Neural Computing and Applications,1-25. https://doi.org/10.1007/s00521-022-07730-3