

Teemu Liimatta

**Huijareiden havaitseminen moninpelivideopeleissä tekoälyn
avulla.**

Tietotekniikan kandidaatintutkielma

16. toukokuuta 2023

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Teemu Liimatta

Yhteystiedot: ,tnliimvy@jyu.fi

Ohjaaja: Timo Tiihonen

Työn nimi: Huijareiden havaitseminen moninpelivideopeleissä tekoälyn avulla.

Title in English: Using AI in multiplayer video games to detect cheaters.

Työ: Kandidaatintutkielma

Opintosuunta: Kaikki opintosuunnat

Sivumäärä: 22+0

Tiivistelmä: Videopelihuijaaminen on yleinen ongelma, joka vaikuttaa ennen kaikkea pelaajien ja peliteollisuuden intresseihin. Huijaaminen voi ilmetä monin tavoin ja aiheuttaa pelien epätasapainoa, turhautumista, peliyhteisöjen hajoamista ja taloudellisia tappioita. Kirjallisuuskatsauksen tarkoituksena on tutkia, miten tekoälyä voidaan hyödyntää videopelihuijaamisen havaitsemisessa ja torjumisessa. Tekoälyllä on monia sovelluksia pelialalla, ja se voi analysoida suuria määriä pelidataa, tunnistaa huijaamisen merkkejä ja malleja, reagoida huijaamiseen reaaliaikaisesti ja oppia uusista huijausmuodoista. Kirjallisuuskatsauksessa tarkastellaan erilaisia tekoälymenetelmiä ja -tekniikoita, joita on käytetty tai ehdotettu videopelihuijaamisen havaitsemiseen ja torjumiseen. Lisäksi käsitellään tekoälyyn liittyviä haasteita ja mahdollisuuksia videopelihuijaamisen yhteydessä sekä esitetään avoimia tutkimuskysymyksiä ja -aukkoja aiheesta.

Avainsanat: AI,Cheating, FPS,

Abstract: Video game cheating is a common problem that affects the interests of the gaming industry and players. Cheating can manifest in many ways and can cause game imbalance, player frustration, community breakdown, and loss of revenue for game developers. The purpose of the literature review is to examine how artificial intelligence can be used to detect and prevent video game cheating. AI has many applications in the gaming industry, and it can analyze large amounts of game data, identify cheating signs and patterns, react to cheating

in real-time, and learn about new forms of cheating. The aim of the literature review is to map out what types of AI methods and techniques have been used or proposed to detect and prevent video game cheating, what challenges and opportunities are associated with AI in the context of video game cheating, and what research gaps and questions exist on the topic.

Keywords: AI,Cheating, FPS,

Sisällys

1	JOHDANTO	1
2	VIDEOPELIHUIJAAMINEN JA SEN HAVAITSEMINEN	2
2.1	Videopelihuijaaminen	2
2.1.1	Videopelihuijaamisen määritelmä ja luokittelu.....	2
2.1.2	Huijaaminen taloudellisten etujen saavuttamiseksi	3
2.1.3	Huijaaminen itseilmaisuuksiin tai identiteetin luomiseksi.....	3
2.1.4	Huijaamisen seuraukset peliyhteisölle	4
2.1.5	Huijaaminen yksinpeleissä	4
2.2	Videopelihuijaamisen torjumisen keinoja, jotka eivät hyödynnä tekoälyä	5
2.3	Tekoäly.....	6
3	AINEISTO JA MENETELMÄT	7
4	TULOKSET JA ANALYYSI AI:N KÄYTTÖSTÄ HUIJAAMISEN ESTOSSA	8
4.1	Tekoälymenetelmät ja -tekniikat videopelihuijaamisen havaitsemisessa ja torjumisessa.....	8
4.2	Tekoälyn haasteet ja mahdollisuudet videopelihuijaamisen yhteydessä	9
5	TUTKIMUKSEN TÄRKEIMMÄT HAVAINNOT JA JOHTOPÄÄTÖKSET	11
5.1	Havainto 1: AI:n väärinkäyttö huijaamisessa	11
5.2	Havainto 2: Kehittyneet huijausmenetelmät	11
5.3	Havainto 3: AI:n potentiaali huijaustorjunnassa	11
5.4	Johtopäätökset	12
5.5	Tutkimusaukot ja -kysymykset aiheesta.....	12
5.6	Tutkimuksen merkitys, rajoitukset	13
	LÄHTEET	15

1 Johdanto

Videopelit ovat suosittu ja monipuolinen viihdemuoto, joka tarjoaa pelaajille erilaisia elämyksiä ja haasteita. Videopelaaminen voi olla myös sosiaalista toimintaa, jossa pelaajat kilpailevat tai tekevät yhteistyötä muiden pelaajien kanssa verkossa. Valitettavasti videopelaamiseen liittyy myös ongelmia, joista yksi on huijaaminen. Huijaaminen tarkoittaa sitä, että pelaaja käyttää epäreiluja keinoja saadakseen etua pelissä. Huijaaminen voi pilata pelikokemuksen rehellisiltä pelaajilta ja aiheuttaa taloudellisia menetyksiä pelinkehittäjille (Blackburn ym. 2014).

Huijaamisen havaitseminen ja torjuminen on vaikea tehtävä, sillä huijarit kehittävät jatkuvasti uusia menetelmiä kiertääkseen pelien suojausmekanismeja. Tämän vuoksi tarvitaan uusia ratkaisustrategioita huijaamisen vastaiseen taisteluun. Tämän tutkielman tarkoituksena on tutkia tekoälyn käyttömahdollisuuksia videopelihuijausten havaitsemisessa ja torjumisessa.

Tekoäly on tieteenala, joka pyrkii luomaan älykkään käyttäytymisen omaavia tietokoneohjelmia tai -laitteita. Tekoäly voi hyödyntää esimerkiksi koneoppimista, neuroverkkoja tai syväoppimista oppiakseen pelidatasta ja tunnistamaan poikkeavia tai epänormaaleja tapahtumia (Yannakakis ja Togelius 2018). Tekoälyn avulla voidaan mahdollisesti parantaa huijaustentorjunnan tehokkuutta, nopeutta ja luotettavuutta (Santos-Neto ym. 2020).

Tutkimuksen tavoitteena on selvittää, miten tekoäly voi auttaa tunnistamaan ja rajoittamaan videopelihuijauksen haittoja. Tutkielman rakenne on seuraava: Luvussa 2 esitellään videopelihuijausten tyyppisiä ja motiiveja sekä niiden vaikutuksia pelialaan ja pelaajiin. Luvussa 2 myös kuvataan tekoälyn peruskonsepteja ja sovellusalueita sekä sen potentiaalia huijaustentorjunnassa. Luvussa 3 käydään läpi tutkimuksen tekomenetelmät. Luvussa 4 arvioidaan erilaisia tekoälymenetelmiä huijaustentunnistuksessa ja -estossa sekä niiden hyötyjä ja haasteita. Luvussa 5 pohditaan tutkielman tuloksia ja johtopäätöksiä sekä ehdotetaan jatkotutkimuksen aiheita.

2 Videopelihuijaaminen ja sen havaitseminen

Tässä luvussa esitellään tutkielman teoreettinen viitekehys, joka sisältää tarvittavan taustatiedon videopelihuijauksista ja niiden tunnistamisesta poikkeamien avulla. Tämän tutkielman teoreettinen viitekehys koostuu kahdesta osasta, jotka käsittelevät videopelihuijausten ja tekoälyn välisiä suhteita. Alaluvussa 2.1 esitellään erilaisia videopelihuijauksia, niiden tyyppisiä ja motiiveja, sekä määritellään videopelihuijaaminen konseptina. Alaluvussa 2.2 käsitellään tapoja, miten huijaamista pyritään estämään. Alaluvussa 2.3 käsitellään tekoälyn peruskonsepteja ja sovellusalueita videopelimaailmassa, ja sitä, miten sitä voidaan hyödyntää huijauksen estossa. Näiden alalukujen avulla pyritään antamaan lukijalle tarvittava taustatieto videopelihuijauksista ja tekoälystä, jotta hän voi ymmärtää paremmin näiden kahden aihealueen välisiä suhteita.

2.1 Videopelihuijaaminen

Videopelihuijaaminen on ilmiö, jossa pelaaja tai pelaajaryhmä pyrkii saavuttamaan epäreilun edun tai aiheuttamaan haittaa muille pelaajille videopelissä rikkomalla pelin sääntöjä tai hyväksikäyttämällä pelin virheitä (Blackburn ym. 2014). Videopelihuijaus voi olla teknistä tai sosiaalista, eli se voi perustua peliohjelmiston manipulointiin tai muiden pelaajien harhaanjohtamiseen (Carter, Gibbs ja Arnold 2012). Videopelihuijaus voi tapahtua sekä yksinpeliä moninpelimuodoissa ja se voi olla joko tahallista tai tahatonta (Yee ym. 2007).

2.1.1 Videopelihuijaamisen määritelmä ja luokittelu

Videopelihuijaaminen on ilmiö, joka haastaa pelien suunnittelijoiden ja pelaajien välisen sopimuksen pelin säännöistä ja tavoitteista (Blackburn ym. 2014). Huijaaminen voi olla yksilön tai ryhmän toimintaa, joka pyrkii saamaan epäreilua etua tai haittaamaan muita pelaajia (Yan ym. 2005). Huijaaminen voidaan jakaa kahteen päätyyppiin: tekniseen ja sosiaaliseen (Carter, Wadley ja Gibbs 2012). Tekninen huijaaminen perustuu peliohjelmiston muokkaamiseen tai hyväksikäyttämiseen esimerkiksi huijausohjelmien tai -laitteiden avulla. Sosiaalinen huijaaminen perustuu muiden pelaajien manipulointiin tai pettämiseen esimerkiksi valehtele-

malla, kiristämällä tai varastamalla (Lewis ja Wardrip-Fruin 2010). Huijaamisen motiivit ja seuraukset vaihtelevat sen mukaan, millaisessa peliympäristössä se tapahtuu. Yksi mahdollinen tapa erottaa erilaiset peliympäristöt on seuraava (Kowert ym. 2015):

- Yksinpelit: Pelejä, joita pelataan yksin ilman muita ihmispelaajia. Tällöin huijaaminen voi olla tapa muuttaa pelin vaikeustasoa tai lisätä sen hauskuutta. Huijaamisella ei ole vaikutusta muiden pelaajien kokemukseen.
- Moninpelit: Pelejä, joita pelataan verkossa muiden ihmispelaajien kanssa. Tällöin huijaaminen voi olla tapa saada kilpailuetua tai häiritä muita pelaajia. Huijaamisella voi olla vaikutusta muiden pelaajien kokemukseen ja peliyhteisön dynamiikkaan.
- E-urheilu: Kilpailullista videopelaamista, jossa pelaajat osallistuvat turnauksiin tai liigoihin. Tällöin huijaaminen voi olla tapa voittaa palkintoja tai mainetta. Huijaamisella voi olla vaikutusta e-urheilun rehellisyyteen ja uskottavuuteen.

2.1.2 Huijaaminen taloudellisten etujen saavuttamiseksi

Yksi mahdollinen motiivi huijaamiselle moninpeleissä on reaaliarahan ansaitseminen. Joissakin peleissä pelaajat voivat kehittää pelihahmonsa tasoja ja hankkia tavaroita, joilla on arvoa pelin sisällä tai sen ulkopuolella. Huijaamalla pelaajat voivat saada näitä resursseja nopeammin ja helpommin kuin rehellisesti pelaamalla. Sitten he voivat myydä niitä muille pelaajille tai kolmansille osapuolille oikeaa rahaa vastaan (Heeks 2008). Tämä voi aiheuttaa epätasapainoa pelin taloudessa ja vaikuttaa muiden pelaajien kokemukseen (Lehdonvirta ja Ernkvist 2011). Huijaaminen reaaliarahan ansaitsemiseksi voi kuitenkin olla riskialtista sekä huijareille että ostajille.

2.1.3 Huijaaminen itseilmaisuuksiin tai identiteetin luomiseksi

Toinen mahdollinen motiivi huijaamiselle moninpeleissä on itseilmaisuus tai identiteetin luominen. Huijarit voivat nauttia siitä, että he ovat erilaisia kuin muut pelaajat tai että he voivat rikkoa pelin sääntöjä ja normeja (Consalvo 2007). Huijaaminen voi myös olla osa sosiaalista vuorovaikutusta, jossa huijarit jakavat huijausmenetelmiään tai haastavat muita pelaajia (Huhh 2008). Itseilmaisuun tai identiteettiin liittyvä huijaaminen voi kuitenkin aiheuttaa

myös negatiivisia seurauksia huijareiden itsensä kannalta.

2.1.4 Huijaamisen seuraukset peliyhteisölle

Huijaaminen voi vähentää pelin haastavuutta ja mielenkiintoisuutta, mikä voi johtaa kyllästymiseen ja lopettamiseen (Yee 2006). Huijaaminen voi myös heikentää huijareiden itsetuntoa ja pelitaitoja, jos he eivät pysty saavuttamaan haluamiaan tuloksia ilman huijausta (Lee ym. 2012). Lisäksi huijaaminen voi aiheuttaa sosiaalista eristämistä tai konflikteja muiden pelaajien kanssa, jotka eivät hyväksy huijaamista (Ruckenstein 1991).

Vaikka huijaaminen voi olla houkuttelevaa joillekin pelaajille, on tärkeää ymmärtää sen haitalliset vaikutukset peliyhteisölle ja pelin tekijöille. Huijaaminen voi johtaa epätasapainoon pelissä ja heikentää muiden pelaajien kokemusta. Se voi myös aiheuttaa taloudellisia menetyksiä pelin tekijöille, jos huijaukset liittyvät reaaliarahan ansaitsemiseen. Siksi pelinvalvojat pyrkivät yleensä estämään huijaamista ja rankaisemaan huijareita.

2.1.5 Huijaaminen yksinpeleissä

Huijaaminen ei ole vain moninpelien ilmiö, vaan sitä voi esiintyä myös yksinpelissä (Passmore ym. 2020). Yksinpelissä huijaaminen tarkoittaa sitä, että pelaaja käyttää pelissä epäreiluja tai sääntöjen vastaisia keinoja saadakseen etua itselleen. Huijaaminen voi olla esimerkiksi pelin vaikeustason muuttamista, tallennustiedostojen muokkaamista tai koodien käyttöä (Passmore ym. 2020).

Yksi mahdollinen motiivi huijaamiselle yksinpelissä on hauskanpito. Pelaaja voi haluta kokeilla erilaisia tapoja pelata tai nähdä mitä pelissä tapahtuu, kun hän käyttää huijauksia. Huijaukset voivat tarjota pelaajalle uusia kokemuksia tai haasteita pelissä (Consalvo 2007). Huijaukset voivat myös auttaa pelaajaa selviytymään vaikeista kohdista tai pääsemään eteenpäin juonessa (King ym. 2011).

Hauskanpitoon liittyvä huijaaminen yksinpelissä ei välttämättä aiheuta negatiivisia seurauksia pelaajalle tai muille osapuolille. Pelaaja voi pitää huijauksia osana omaa pelikokemustaan eikä häiritse muita pelaajia sillä tavalla kuin moninpeleissä (Consalvo 2007). Pelaaja voi

myös valita milloin ja miten paljon hän käyttää huijauksia omien mieltymystensä mukaan.

Toinen mahdollinen motiivi huijaamiselle yksinpelissä on kilpailullisuus. Pelaaja voi haluta saavuttaa parempia tuloksia tai suorituksia kuin muut pelaajat tai kuin itsensä aiemmin. Huijaukset voivat antaa pelaajalle etua esimerkiksi ajan, pisteiden tai tason suhteen (King ym. 2011). Huijaukset voivat myös auttaa pelaajaa saamaan lisää arvostusta tai tunnustusta muilta pelaajilta esimerkiksi sosiaalisessa mediassa tai verkkoyhteisöissä (Passmore ym. 2020).

Kilpailullisuuteen liittyvä huijaaminen yksinpelissä voi kuitenkin aiheuttaa myös negatiivisia seurauksia pelaajalle tai muille osapuolille. Pelaaja voi menettää pelin haasteen tai nautinnon, jos hän käyttää huijauksia liikaa tai väärin (King ym. 2011). Pelaaja voi myös joutua epärehellisyys- tai vilpin syytteeseen, jos hän väittää saavuttaneensa tuloksensa ilman huijauksia (Passmore ym. 2020). Lisäksi pelaaja voi rikkoa pelin tekijöiden oikeuksia tai ehtoja, jos hän käyttää huijauksia, jotka vaikuttavat pelin toimintaan tai sisältöön (Consalvo 2007).

Videopelihuijaaminen on monimutkainen ja monitahoinen ilmiö, jolla on erilaisia syitä ja seurauksia. Huijaaminen voi olla hauskaa, hyödyllistä tai haastavaa pelaajalle, mutta se voi myös olla epäreilua, vahingollista tai laitonta muille osapuolille. Huijaamisen eettisyys ja hyväksyttävyyys riippuu useista tekijöistä, kuten pelityypistä, peliympäristöstä ja pelikulttuurista.

2.2 Videopelihuijaamisen torjumisen keinoja, jotka eivät hyödynnä tekoälyä

Videopelihuijaamisen torjuntaan on kehitetty monia erilaisia keinoja, jotka sisältävät sekä teknisiä estoja että sanktioita kiinni jääneille.

Anti-cheat-ohjelmat ovat ohjelmia, jotka tunnistavat ja estävät huijausohjelmien käytön pelissä. Esimerkiksi Easy™ Anti-Cheat on alan johtava anti-huijauspalvelu, joka torjuu hakereita ja huijareita moninpelitietokonepeleissä käyttämällä hybridianti-huijausmekanismeja ("Easy Anti-Cheat", n.d.).

Pelin sisäiset rangaistukset ovat keinoja rajoittaa huijaajien toimintaa tai estää heidän pe-

laamisensa kokonaan. Esimerkiksi CS:GO käyttää pelikieltoja Overwatch-järjestelmässään (“Steam Support”, n.d.).

Laitteistotason estot estävät huijaajia luomasta uusia tilejä samalla laitteella. Esimerkiksi Valorant jakaa laitteistobanneja; jos sinut havaitaan huijarina, koko laitteistosi bannataan ja kaikki tulevat tilisi PC:ltäsi merkitään (Das 2021).

2.3 Tekoäly

Tekoälyllä tarkoitetaan tietokonejärjestelmiä, jotka pystyvät suorittamaan tehtäviä, jotka vaativat älykkyyttä ihmisiltä (Russell 2010). Tällaiset järjestelmät kykenevät oppimaan, sopeutumaan ja parantamaan suorituskyykyään kokemuksen kautta. Tekoäly voi perustua erilaisiin menetelmiin ja algoritmeihin, kuten koneoppimiseen, syväoppimiseen, neuroverkkoihin ja evoluutioalgoritmeihin (Poole, Goebel ja Mackworth 1998).

Tekoälyn sovelluskohteita ovat esimerkiksi kuvantunnistus, luonnollisen kielen käsittely, ääntunnistus ja päätöksenteon tuki (Yannakakis ja Togelius 2018). Tekoäly on myös yhä enemmän läsnä erilaisissa peleissä ja pelisovelluksissa, joissa se voi toimia esimerkiksi tekoälyvastustajina tai huijausten havaitsemisessa ja torjunnassa (Santos-Neto ym. 2020).

Tekoälyn kehitys on ollut nopeaa viime vuosina, ja sen avulla on saavutettu merkittäviä edistysaskeleita monilla eri aloilla (Scharre 2018). Tulevaisuudessa tekoälyn odotetaan yleistyvän entisestään ja muuttavan monia perinteisiä toimintatapoja sekä tuovan mukanaan uusia mahdollisuuksia ja haasteita.

3 Aineisto ja menetelmät

Tässä luvussa esitellään tutkimuksen käyttämä aineisto ja menetelmät, jotka on valittu tutkimuskysymysten ja tavoitteiden pohjalta.

Menetelmät perustuvat kirjallisuuskatsaukseen, jossa valittu aineisto analysoitiin ja jäseneltiin tutkimuskysymysten ja tavoitteiden mukaisesti. Aineiston analyysissä käytettiin muun muassa sisällönanalyysiä ja teemoittelu.

Tutkimuksen tavoitteena oli koota yhteen tutkimustuloksia ja -menetelmiä tekoälyn käytöstä huijareiden havaitsemiseksi moninpelivideopeleissä sekä arvioida tekoälyn mahdollisuuksia ja haasteita tässä yhteydessä.

Aineisto koostuu alan tieteellisistä artikkeleista ja julkaisuista ja peliyrityksiltä saaduista tiedoista.

Peliryhtyksiltä saatava tieto on toinen tärkeä aineistolähde tässä tutkimuksessa. Pelirytykset ovat niitä toimijoita, jotka kehittävät ja tarjoavat videopelipalveluita pelaajille. Pelirytykset ovat myös niitä toimijoita, jotka kohtaavat videopelihuijausta omassa liiketoiminnassaan. Peliryhtyksiltä saatava tieto voi sisältää esimerkiksi pelien teknisiä ominaisuuksia, huijaustapauksien tilastoja tai huijaustorjuntatoimenpiteitä. Peliryhtyksiltä saatavan tiedon etuna on se, että se tarjoaa konkreettista ja ajankohtaista tietoa videopelihuijauksen nykytilasta ja haasteista.

Aineiston valinnassa käytettiin hakusanoja kuten "multiplayer games", "cheating detection" ja "artificial intelligence" tietokannoissa kuten ACM Digital Library, IEEE Xplore ja Google Scholar. Aineistona käytettiin tutkimusartikkeleita, jotka käsittelevät tekoälyn käyttöä moninpelivideopeleissä huijareiden havaitsemiseksi. Artikkelit kattavat erilaisia pelejä ja huijaustyyppisiä sekä erilaisia tekoälymenetelmiä, jotka on kehitetty huijausten havaitsemiseksi.

4 Tulokset ja analyysi AI:n käytöstä huijaamisen estossa

AI voi auttaa estämään huijaamista videopelien yhteydessä monin tavoin. Yksi tapa on käyttää koneoppimista pelaajien käyttäytymisen analysointiin ja epätyypillisten toimintojen havaitsemiseen, jotka voivat viitata huijaamiseen (Alkhalifa 2016). Esimerkiksi, jos pelaaja suorittaa jatkuvasti tehtäviä, jotka ovat lähes mahdottomia ihmisen suorittaa, se voi olla merkki jonkinlaisesta huijauksesta.

Toinen tapa, jolla AI voi auttaa huijaamisen estämisessä, on analysoida pelidataa, joka lähetetään keskusspalvelimelle. Tämän datan analysoinnin avulla AI-järjestelmä voi havaita kaavoja, jotka voivat viitata huijaamiseen, ja ryhtyä asianmukaisiin toimenpiteisiin, kuten varoittaa pelaajia tai poistaa heidät pelistä, jos he jatkavat huijaamista (Islam ym. 2022).

AI voi myös auttaa pelikehittäjiä parantamaan huijaamisen estäviä toimenpiteitä tarjoamalla näkemyksiä siitä, miten huijaukset toimivat ja miten niitä voidaan havaita. Tämä voi auttaa kehittäjiä luomaan tehokkaampia huijaamisen estojärjestelmiä, jotka pystyvät paremmin havaitsemaan ja estämään huijaamista (modl.ai 2022; published 2021).

4.1 Tekoälymenetelmät ja -tekniikat videopelihuijaamisen havaitsemisessa ja torjumisessa

Videopelien huijaaminen on merkittävä ongelma, joka vaikuttaa peliyhteisöjen kokemukseen ja pelinkehittäjien tuloihin. Tekoälyn (AI) soveltaminen huijaamisen havaitsemiseen ja torjumiseen on noussut esille lupaavana ratkaisuna tähän ongelmaan. Tässä osiossa tarkastellaan erilaisia tekoälymenetelmiä ja -tekniikoita, joita voidaan käyttää videopelihuijausten havaitsemiseen ja estämiseen.

Yksi AI:n sovellus huijaamisen torjunnassa on koneoppiminen (ML). ML-menetelmät, kuten päätöspuut, tukivektorikoneet (SVM) ja naiivit Bayes-luokitellut, ovat osoittautuneet tehokkaiksi huijaavien pelaajien käyttäytymisen tunnistamisessa (Spijkerman ja Marie Ehlers 2021). Esimerkiksi Spijkerman et al. (Spijkerman ja Marie Ehlers 2021) tutkivat hiiren dynamiikan käyttöä pelaajakäyttäytymisen mittaamisessa ja totesivat päätöspuiden olevan tarkin

menetelmä rehellisten pelaajien käyttäytymisen havaitsemiseen.

Toinen tekoälytekniikka, joka on saanut huomiota huijaamisen havaitsemisessa, on syväoppiminen (Zhang 2021). Zhang ehdotti online-pelien huijaustenestojärjestelmän parantamista syväoppimisen avulla. Tämä menetelmä hyödyntää kuvantunnistusta ja ennustavia algoritmeja tunnistaakseen huijaukseen viittaavia malleja pelin aikana.

Koneoppimisen lisäksi tekoälyn selitettävyyys (XAI) on noussut esiin tärkeänä tekijänä huijaamisen havaitsemisessa ja torjumisessa (Tao ym. 2020). XAI-menetelmät, kuten visualisointi ja analyysi, voivat auttaa pelaajia ja pelinkehittäjiä ymmärtämään paremmin AI:n tekemiä päätöksiä huijaamisen havaitsemiseksi ja estämiseksi.

Yhteenvedona voidaan todeta, että tekoälyllä on merkittävä rooli videopelihuijausten havaitsemisessa ja torjumisessa. Koneoppimismenetelmät, kuten päätöspuut ja syväoppiminen, sekä selitettävän tekoälyn sovellukset ovat osoittautuneet tehokkaiksi lähestymistavoiksi tämän ongelman ratkaisemiseksi.

4.2 Tekoälyn haasteet ja mahdollisuudet videopelihuijaamisen yhteydessä

Vaikka tekoäly (AI) tarjoaa lupaavia ratkaisuja videopelihuijausten havaitsemiseen ja torjumiseen, se ei ole täysin ongelmatonta. Tässä osiossa käsitellään AI:n haasteita ja mahdollisuuksia, kun sitä sovelletaan videopelihuijausten torjuntaan.

Yksi haaste AI:n käytössä huijaamisen havaitsemisessa on sen kyky pysyä ajan tasalla huijausohjelmien jatkuvasti kehittyessä. Huijarit kehittävät jatkuvasti uusia menetelmiä ja työkaluja, jotka voivat kiertää olemassa olevat suojausjärjestelmät (Das 2021). Esimerkiksi äskettäin kehitetty huijaustyökalu hyödyntää koneoppimista ja tietokoneen näkökykyä tarjotakseen automaattista tähtäämistä, joka on lähes mahdotonta havaita (published 2021). Tämänkaltaiset edistyneet huijausmenetelmät vaativat vastaavasti kehittyneempiä AI-ratkaisuja niiden havaitsemiseksi ja estämiseksi.

Toinen haaste liittyy AI:n väärinkäyttöön itse huijaamisessa. On raportoitu, että huijarit ovat käyttäneet AI:ta kehittääkseen omia huijausohjelmiaan (“AIs Are Getting Better At Playing

Video Games...By Cheating” 2018). Tämä tarkoittaa, että AI voi toimia sekä hyökkäävänä että puolustavana osapuolena pelihuijausten kontekstissa. Pelinkehittäjien on oltava tietoisia tästä kaksoisroolista ja pyrittävä kehittämään tehokkaita vastatoimenpiteitä estääkseen AI:n väärinkäytön.

Huolimatta näistä haasteista, AI tarjoaa myös merkittäviä mahdollisuuksia videopelihuijausten torjunnassa. Esimerkiksi koneoppimisen ja syväoppimisen soveltaminen huijaamisen havaitsemiseen voi parantaa nykyisten suojausjärjestelmien tehokkuutta ja reagointikykyä (Spijkerman ja Marie Ehlers 2021; Zhang 2021). Lisäksi selitettävän tekoälyn (XAI) käyttö voi auttaa pelaajia ja pelinkehittäjiä ymmärtämään paremmin AI:n tekemiä päätöksiä ja siten kehittämään entistä tehokkaampia huijaustentorjuntaratkaisuja (Tao ym. 2020).

Tekoäly voi olla tehokas havaitsemaan huijaamista videopelissä analysoimalla reaaliaikaisia tietoja ja havaitsemalla odottamattomia muutoksia tai poikkeavuuksia (Marks, n.d.). Esimerkiksi Featurespacen kehittämä koneoppimisjärjestelmä voi tehdä koulutetun arvauksen poikkeavuuden todennäköisestä syystä (Marks, n.d.).

MMO-peleissä, joissa tiedot ovat salattuja, tekoäly voi analysoida salattua liikennettä palvelimen ja käyttäjän välillä reaaliajassa huijausten havaitsemiseksi (“AI is driving the next generation of video game cheats and exploits”, n.d.). Modl.ai:ssa he keskittyivät koneoppimiseen ja käyttäytymisperusteiseen havaitsemiseen seuraamalla ihmispelaajien käyttäytymistä ja käyttämällä tätä tietoa poikkeavan käyttäytymisen havaitsemiseen (modl.ai 2022).

Kaiken kaikkiaan tekoäly voi olla tehokas havaitsemaan huijaamista videopelissä tarjoamalla lisää työkaluja ja oivalluksia pelikehittäjille ja operaattoreille. On kuitenkin tärkeää huomata, että mikään järjestelmä ei ole täydellinen ja saattaa silti esiintyä tilanteita, joissa huijaaminen jää huomaamatta.

Tekoälyllä on potentiaalia ratkaista monia videopelihuijaukseen liittyviä haasteita, kuten automatisoida huijausten havaitsemisprosessia ja tarjota reaaliaikaista huijausten torjuntaa. Kuitenkin tekoälyn käyttöön liittyy myös eettisiä haasteita, kuten yksityisyyden suoja ja oikeudenmukaisuus huijausten syyllisyyden arvioinnissa. lisäksi tekoälymenetelmät ovat alttiita uusille huijaustekniikoille, mikä vaatii jatkuvaa kehittämistä ja päivitystä (“AIs Are Getting Better At Playing Video Games...By Cheating” 2018).

5 Tutkimuksen tärkeimmät havainnot ja johtopäätökset

Tässä tutkimuksessa tarkasteltiin tekoälyn (AI) soveltamista videopelihuijausten havaitsemiseen ja torjumiseen. Analysoimalla erilaisia lähteitä saatiin selville, että AI tarjoaa sekä haasteita että mahdollisuuksia huijaustentorjunnassa. Tärkeimmät havainnot ja johtopäätökset esitellään seuraavassa.

5.1 Havainto 1: AI:n väärinkäyttö huijaamisessa

Yksi keskeinen havainto on, että AI:ta voidaan käyttää paitsi huijausten havaitsemiseen myös itse huijaamisen apuvälineenä (“AIs Are Getting Better At Playing Video Games...By Cheating” 2018). Tämän vuoksi pelinkehittäjien on oltava tietoisia AI:n kaksoisroolista ja kehitettävä vastatoimenpiteitä estääkseen sen väärinkäytön.

5.2 Havainto 2: Kehittyneet huijausmenetelmät

Toinen merkittävä havainto on, että huijarit kehittävät jatkuvasti uusia menetelmiä ja työkaluja, jotka voivat kiertää olemassa olevat suojausjärjestelmät (Das 2021). Esimerkiksi koneoppimista ja tietokoneen näkökykyä hyödyntävät huijaustyökalut ovat lähes mahdottomia havaita (published 2021). Tämän vuoksi AI-ratkaisujen on pysyttävä ajan tasalla ja kehittyvä jatkuvasti vastatakseen näihin haasteisiin.

5.3 Havainto 3: AI:n potentiaali huijaustentorjunnassa

Huolimatta haasteista, AI tarjoaa merkittäviä mahdollisuuksia videopelihuijausten torjunnassa. Koneoppimisen ja syväoppimisen soveltaminen huijaamisen havaitsemiseen voi parantaa nykyisten suojausjärjestelmien tehokkuutta ja reagointikykyä (Spijkerman ja Marie Ehlers 2021; Zhang 2021). Lisäksi selitettävän tekoälyn (XAI) käyttö voi auttaa pelaajia ja pelinkehittäjiä ymmärtämään paremmin AI:n tekemiä päätöksiä ja siten kehittämään entistä tehokkaampia huijaustentorjuntaratkaisuja (Tao ym. 2020).

5.4 Johtopäätökset

Tutkimuksen perusteella voidaan todeta, että tekoälyllä on sekä haasteita että mahdollisuuksia videopelihuijausten havaitsemisessa ja torjumisessa. Vaikka AI:n väärinkäyttö ja jatkuvasti kehittyvät huijausmenetelmät muodostavat haasteita, AI:n soveltaminen huijaustentorjuntaan tarjoaa myös merkittäviä mahdollisuuksia parantaa peliyhteisöjen kokemusta ja vähentää huijaamisen vaikutuksia pelinkehittäjien tuloihin.

5.5 Tutkimusaukot ja -kysymykset aiheesta

Vaikka tämän tutkimuksen tulokset osoittavat, että tekoälyllä on potentiaalia huijausten havaitsemisessa ja torjumisessa, on vielä useita tutkimusaukkoja ja kysymyksiä, jotka vaativat lisää huomiota. Näitä ovat esimerkiksi:

- Miten AI:n väärinkäyttö huijaamisessa voidaan estää?
 - Koska AI:ta voidaan käyttää myös itse huijaamisen apuvälineenä (“AIs Are Getting Better At Playing Video Games...By Cheating” 2018), on tärkeää ymmärtää, miten pelinkehittäjät voivat estää AI:n väärinkäytön. Tähän liittyviä kysymyksiä ovat esimerkiksi se, miten tunnistaa AI-pohjaiset huijaustyökalut ja miten kehittää tehokkaita vastatoimenpiteitä niiden torjumiseksi.
- Miten AI-pohjaiset huijaustentorjuntaratkaisut voivat pysyä ajan tasalla kehittyvien huijausmenetelmien kanssa?
 - Jatkuvasti kehittyvät huijausmenetelmät, kuten koneoppimista ja tietokoneen näkökykyä hyödyntävät työkalut (published 2021), asettavat haasteita AI-pohjaisten huijaustentorjuntaratkaisujen kehittämiseksi. Tämän vuoksi on tärkeää tutkia, miten AI-ratkaisut voivat pysyä ajan tasalla ja kehittyä jatkuvasti vastatakseen näihin haasteisiin.
- Miten selitettävän tekoälyn (XAI) soveltaminen voi parantaa huijaustentorjuntaa?
 - Selitettävän tekoälyn (XAI) käyttö voi auttaa pelaajia ja pelinkehittäjiä ymmärtämään paremmin AI:n tekemiä päätöksiä (Tao ym. 2020). On kuitenkin tarpeen tutkia, miten XAI voidaan integroida tehokkaasti huijaustentorjuntaratkaisuihin

ja millaisia vaikutuksia sillä on huijaamisen havaitsemiseen ja torjumiseen.

- Miten AI-pohjaiset ratkaisut vaikuttavat pelaajien kokemuksiin ja peliyhteisöihin?
 - Vaikka AI:n soveltaminen huijaustorjuntaan voi parantaa peliyhteisöjen kokemusta ja vähentää huijaamisen vaikutuksia pelinkehittäjien tuloihin, on tärkeää tutkia myös, miten nämä ratkaisut vaikuttavat pelaajien kokemuksiin ja peliyhteisöjen dynamiikkaan. Esimerkiksi, miten AI-pohjaiset huijaustorjuntaratkaisut vaikuttavat pelaajien luottamukseen pelin reiluuteen ja miten ne voivat parantaa tai heikentää sosiaalisia vuorovaikutuksia peliyhteisöissä.
- Miten AI-pohjaiset ratkaisut vaikuttavat pelaajien kokemuksiin ja peliyhteisöihin?
 - Vaikka AI:n soveltaminen huijaustorjuntaan voi parantaa peliyhteisöjen kokemusta ja vähentää huijaamisen vaikutuksia pelinkehittäjien tuloihin, on tärkeää tutkia myös, miten nämä ratkaisut vaikuttavat pelaajien kokemuksiin ja peliyhteisöjen dynamiikkaan. Esimerkiksi, miten AI-pohjaiset huijaustorjuntaratkaisut vaikuttavat pelaajien luottamukseen pelin reiluuteen ja miten ne voivat parantaa tai heikentää sosiaalisia vuorovaikutuksia peliyhteisöissä.

5.6 Tutkimuksen merkitys, rajoitukset

Tämän tutkimuksen merkitys on monitahoinen. Ensinnäkin se auttaa ymmärtämään tekoälyn potentiaalia huijausten havaitsemisessa ja torjumisessa videopeleissä. Tämä on tärkeää, koska huijaaminen heikentää pelaajien kokemusta ja voi aiheuttaa taloudellisia menetyksiä pelinkehittäjille (Consalvo 2007). Lisäksi AI-pohjaiset ratkaisut voivat auttaa parantamaan peliyhteisöjen laatua ja vähentämään huijaamisen vaikutuksia niiden dynamiikkaan (Chen, Duh ja Phang 2009).

Vaikka tämän tutkimuksen tulokset ovat lupaavia, on olemassa useita rajoituksia. Ensinnäkin AI-pohjaisten huijaustorjuntaratkaisujen kehittäminen edellyttää suurta määrää dataa pelaajien käyttäytymisestä, mikä voi olla haasteellista kerätä ja käsitellä (Lewis ja Wardrip-Fruin 2010). Toiseksi AI-ratkaisujen tehokkuus riippuu niiden kyvystä pysyä ajan tasalla kehittyvien huijausmenetelmien kanssa, mikä voi vaatia jatkuvaa päivitystä ja kehittämistä (published 2021). Kolmanneksi AI-pohjaisten ratkaisujen käyttöön liittyy myös eettisiä ky-

symyksiä, kuten pelaajien yksityisyyden suojaaminen ja AI:n väärinkäytön estäminen huijauksen apuvälineenä (“AIs Are Getting Better At Playing Video Games...By Cheating” 2018).

Lähteet

“AI is driving the next generation of video game cheats and exploits”. AI Business. n.d. Viitattu 16. toukokuuta 2023. <https://aibusiness.com/computer-vision/ai-is-driving-the-next-generation-of-video-game-cheats-and-exploits>.

“AIs Are Getting Better At Playing Video Games...By Cheating”. Kotaku. 2018, 13. marraskuuta 2018. Viitattu 16. toukokuuta 2023. <https://kotaku.com/earlier-this-year-researchers-trying-to-teach-an-ai-to-1830416980>.

Alkhalifa, Salman. 2016. “Machine Learning and Anti-Cheating in FPS Games”. Tohtorinväitöskirja, syyskuu. <https://doi.org/10.13140/RG.2.2.21957.86242>.

Blackburn, Jeremy, Nicolas Kourtellis, John Skvoretz, Matei Ripeanu ja Adriana Iamnitchi. 2014. “Cheating in Online Games: A Social Network Perspective”. *ACM Trans. Internet Technol.* (New York, NY, USA) 13, numero 3 (toukokuu). ISSN: 1533-5399. <https://doi.org/10.1145/2602570>.

Carter, Marcus, Martin Gibbs ja Michael Arnold. 2012. “The Demarcation Problem in Multiplayer Games: Boundary-Work in EVE Online’s eSport”. *Game Studies*, <https://gamestudies.org/1501/articles/carter>.

Carter, Marcus, Greg Wadley ja Martin Gibbs. 2012. ““Friendly, Don’t Shoot!”: How Communication Design Can Enable Novel Social Interactions”. Teoksessa *Proceedings of the 24th Australian Computer-Human Interaction Conference*, 72–75. OzCHI ’12. Melbourne, Australia: Association for Computing Machinery. ISBN: 9781450314381. <https://doi.org/10.1145/2414536.2414548>.

Chen, Vivian Hsueh-Hua, Henry Been-Lirn Duh ja Ng Cheng Kiang Phang. 2009. “Understanding Social Interaction in World of Warcraft”. *Proceedings of International Conference on Advances in Computer Entertainment Technology*, 21–24. <https://dl.acm.org/doi/10.1145/1690388.1690393>.

Consalvo, Mia. 2007. *Cheating: Gaining Advantage in Videogames*. The MIT Press, toukokuu. ISBN: 9780262270748. <https://doi.org/10.7551/mitpress/1802.001.0001>.

- Das, Abhimannu. 2021. "Why Is Cheating Almost Impossible to Stop in Video Games?" AFK Gaming, 1. helmikuuta 2021. Viitattu 16. toukokuuta 2023. <https://afkgaming.com/esports/news/6521-why-is-cheating-almost-impossible-to-stop-in-video-games>.
- "Easy Anti-Cheat". n.d. Viitattu 16. toukokuuta 2023. <https://www.easy.ac/en-us/>.
- Heeks, Richard. 2008. "Current Analysis and Future Research Agenda on "Gold Farming": Real-World Production in Developing Countries for the Virtual Economies of Online Games". *Development Informatics Working Paper Series*, <https://dx.doi.org/10.2139/ssrn.3477387>.
- Huhh, Jun-Sok. 2008. "Culture and business of PC bangs in Korea". *Games and Culture* 3 (1): 26–37.
- Islam, Md Shihabul, Bo Dong, Swarup Chandra, Latifur Khan ja Bhavani Thuraisingham. 2022. "GCI: A GPU-Based Transfer Learning Approach for Detecting Cheats of Computer Game". *IEEE Transactions on Dependable and Secure Computing*, <https://doi.org/10.1109/TDSC.2020.3013817>.
- King, Daniel L, Paul H Delfabbro, Mark D Griffiths ja Michael Gradisar. 2011. "Assessing clinical trials of Internet addiction treatment: A systematic review and CONSORT evaluation". *Clinical psychology review* 31 (7): 1110–1116.
- Kowert, Rachel, Jens Vogelgesang, Ruth Festl ja Thorsten Quandt. 2015. "Psychosocial causes and consequences of online video game play". *Computers in Human Behavior* 45:51–58.
- Lee, Yu-Hao, Carrie Heeter, Brian Magerko ja Ben Medler. 2012. "Gaming mindsets: Implicit theories in serious game learning". *Cyberpsychology, behavior, and social networking* 15 (4): 190–194.
- Lehdonvirta, Vili, ja Mirko Ernkvist. 2011. "Knowledge Map of the Virtual Economy: Converting the Virtual Economy into Development Potential", <https://openknowledge.worldbank.org/bitstream/handle/10986/2249/646650WP0Know100Box0361527B0PUBLIC0.pdf?sequence=1&isAllowed=y>.

Lewis, Aaron, ja Noah Wardrip-Fruin. 2010. "Mining Game Statistics from Web Services: A World of Warcraft Armory Case Study". *Proceedings of the Fifth International Conference on the Foundations of Digital Games (FDG)*, <https://dl.acm.org/doi/10.1145/1822348.1822366>.

Marks, Paul. n.d. "The AI that learns our habits and knows when people cheat". Viitattu 16. toukokuuta 2023. <https://www.bbc.com/future/article/20170126-the-ai-that-knows-when-you-cheat-by-learning-your-habits>.

modl.ai, Team. 2022. "How to Detect Cheaters in Video Games Using Machine Learning". Modl.ai | AI Engine for game development, 21. helmikuuta 2022. Viitattu 16. toukokuuta 2023. <https://modl.ai/detect-cheaters-using-ml/>.

Passmore, Cale J, Mathew K Miller, Jun Liu, Cody J Phillips ja Regan L Mandryk. 2020. "A Cheating Mood: The Emotional and Psychological Benefits of Cheating in Single-Player Games". *Proceedings of the Annual Symposium on Computer-Human Interaction in Play*, 58–70.

Poole, David I, Randy G Goebel ja Alan K Mackworth. 1998. *Computational intelligence*. Nide 1. Oxford University Press New York.

published, Aaron Klotz. 2021. "New FPS Cheating Tool Uses Machine Learning, Is Impossible to Detect". Tom's Hardware, 12. heinäkuuta 2021. Viitattu 16. toukokuuta 2023. <https://www.tomshardware.com/news/impossible-to-detect-cheating-tool>.

Ruckenstein, Michael. 1991. "Homo ludens: a study of the play element in culture". *Leisure and Ethics* 237.

Russell, Stuart J. 2010. *Artificial intelligence a modern approach*. Pearson Education, Inc.

Santos-Neto, Elizeu, Marjory Da Costa-Abreu, Claudio Sergio de Souza Baptista, Rodrigo de Oliveira Albuquerque Robalinho, Abel Guilhermino de Andrade Lira Neto, Carlos Eduardo Maciel Costa Pinto Junior ja Fernando Buarque de França Benevides Barbosa Filho. 2020. "Machine learning for cheat detection in gaming: A systematic literature review". *Expert Systems with Applications*.

- Scharre, Paul. 2018. *Army of none: Autonomous weapons and the future of war*. WW Norton & Company.
- Spijkerman, Ruan, ja Elizabeth Marie Ehlers. 2021. "Cheat Detection in a Multiplayer First-Person Shooter Using Artificial Intelligence Tools". Teoksessa *2020 The 3rd International Conference on Computational Intelligence and Intelligent Systems*, 87–92. CIIS 2020. New York, NY, USA: Association for Computing Machinery, helmikuu. ISBN: 978-1-4503-8808-5, viitattu 25. tammikuuta 2023. <https://doi.org/10.1145/3440840.3440857>.
- "Steam Support :: Banned by Game Developer (Game Ban)". n.d. Viitattu 16. toukokuuta 2023. <https://help.steampowered.com/en/faqs/view/46DB-4CEC-F7E9-49E5>.
- Tao, Jianrong, Yu Xiong, Shiwei Zhao, Yuhong Xu, Jianshi Lin, Runze Wu ja Changjie Fan. 2020. "XAI-Driven Explainable Multi-view Game Cheating Detection". Teoksessa *2020 IEEE Conference on Games (CoG)*, 144–151. ISSN: 2325-4289. Elokuu. <https://doi.org/10.1109/CoG47356.2020.9231843>.
- Yan, Jeff, Hyun Jin Choi, Tae Wan Kim ja Jin Ho Park. 2005. "A survey of cheating in online games". Teoksessa *Proceedings of the Fourth Annual Workshop on Network and Systems Support for Games (NetGames'05)*.
- Yannakakis, Georgios N, ja Julian Togelius. 2018. "Artificial intelligence for games: A survey". *IEEE Transactions on Games*.
- Yee, Nick. 2006. "Motivations for play in online games". *CyberPsychology & behavior* 9 (6): 772–775.
- Yee, Nick, Jeremy N. Bailenson, Nicolas Ducheneaut, Mateusz Urbanek, Asa Chang ja Dan Merget. 2007. "The Unbearable Likeness of Being Digital: The Persistence of Nonverbal Social Norms in Online Virtual Environments". *CyberPsychology Behavior*.
- Zhang, Qinghao. 2021. "Improvement of Online Game Anti-Cheat System based on Deep Learning". Teoksessa *2021 2nd International Conference on Information Science and Education (ICISE-IE)*, 652–655. Marraskuu. <https://doi.org/10.1109/ICISE-IE53922.2021.00153>.