Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Bakalářská práce

Systémy umělé inteligence v kamerových systémech

František SCHENK

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

František Schenk

Informatika

Název práce

Systémy umělé inteligence v kamerových systémech

Název anglicky

Artificial Intelligence in Security Camera Systems

Cíle práce

Cílem práce je analyzovat a posoudit účinnost a formy tzv. umělé inteligence v kamerových systémech. Zpracována bude umělá inteligence jak na straně kamer, tak i případně síťových videorekordérů. Oba tyto systémy budou následně porovnány. V závěru práce se autor pokusí zhodnotit možnosti této analýzy a definovat předpoklady pro další vývoj v této oblasti.

Metodika

1) Úvod

2) Cíl práce a metodika

3) Rozbor nástrojů umělé inteligence v kamerových systémech

4) Typické způsoby nasazení a využití

5) Test úspěšnosti vyhodnocení

6) Vyhodnocení testů, finanční analýza

7) Predikce vývoje

8) Závěr

Doporučený rozsah práce

30-40 stran

Klíčová slova

kamerové systémy, umělá inteligence, bezpečnost

Doporučené zdroje informací

FORD, M. – PROKEŠ, J. – VRBA, M. Roboti nastupují : automatizace, umělá inteligence a hrozba budoucnosti bez práce. V Praze: Rybka Publishers, 2017. ISBN 978-80-87950-46-3.

GOSMAN, S. Umělá inteligence a expertní systémy. Praha: Kancelářské stroje, 1990. ISBN 80-7018-004-8.

JANEČKOVÁ, E. – BARTÍK, V. Kamerové systémy v praxi : právní režim z pohledu ochrany osobních údajů a ochrany osobnosti. Praha: Linde, 2011. ISBN 978-80-7201-850-5.

LAŽANSKÝ, J. – MAŘÍK, V. – ŠTĚPÁNKOVÁ, O. Umělá inteligence (2). Praha: Academia, 1997. ISBN 80-200-0504-8.

MAŘÍK, V. – LAŽANSKÝ, J. – ŠTĚPÁNKOVÁ, O. Umělá inteligence. 1. Praha: Academia, 1993. ISBN 80-200-0496-3.

POKORNÝ, M. Umělá inteligence v modelování a řízení. Praha: BEN – technická literatura, 1996. ISBN 80-901984-4-9.

UHLÁŘ, J. – POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY. KATEDRA TECHNICKÝCH PROSTŘEDKŮ BEZPEČNOSTNÍCH SLUŽEB. Technická ochrana objektů. II. díl, Elektrické zabezpečovací systémy II. Praha: Vydavatelství PA ČR, 2005. ISBN 80-7251-189-0.

ZELINKA, I. Umělá inteligence – hrozba nebo naděje?. Praha: BEN – technická literatura, 2003. ISBN 80-7300-068-7.

Předběžný termín obhajoby

2022/23 ZS – PEF

Vedoucí práce

Ing. Ondřej Gojda, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 25. 1. 2023

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 22. 2. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 15. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci ”Systémy umělé inteligence v kamerových systémech” jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2023 _____

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu Ing. Ondřejovi Gojdovi, Ph.D. za vedení práce a cenné rady, Ing. Zdeňkovi Votrubovi, Ph.D. za pomoc s výběrem tématu, a Janě za podporu.

Systémy umělé inteligence v kamerových systémech

Abstrakt

Tato bakalářská práce se věnuje problematice využití umělé inteligence v kamerových systémech. Umělá inteligence se stává stále důležitějším faktorem v oblasti bezpečnosti a ochrany majetku, a to zejména v kombinaci s kamerovými systémy. Tato práce hodnotí možnosti, výhody a omezení nasazení umělé inteligence v kamerových systémech.

Práce se bude nejprve věnovat vysvětlení pojmů a technologií spojených s umělou inteligencí v kamerových systémech. Následně bude provedena analýza existujících řešení a technologií, jako jsou detekce pohybu, rozpoznávání obličejů, identifikace vozidel a sledování objektů v reálném čase, poté problematika kamerového systému v menze ČZU. Nasleduje pokus o předpověď dalšího vývoje umělé inteligence v kamerových systémech. Konec práce se zabývá etickým otázkám spojeným s použitím umělé inteligence v kamerových systémech. Bude zde rozebíráno téma soukromí a ochrany osobních údajů, otázka diskriminace a rizika chybných rozhodnutí, která mohou být způsobena algoritmy umělé inteligence.

Klíčová slova: kamerové systémy, umělá inteligence, bezpečnost

Artificial Intelligence in Security Camera Systems

Abstract

This bachelor's thesis addresses the issue of using artificial intelligence in camera systems. Artificial intelligence is becoming an increasingly important factor in the field of security and property protection, particularly when combined with camera systems. The aim of this thesis is to evaluate the possibilities, advantages, and limitations of deploying artificial intelligence in camera systems.

The thesis will first explain the concepts and technologies associated with artificial intelligence in camera systems. Subsequently, an analysis of existing solutions and technologies, such as motion detection, facial recognition, vehicle identification, and real-time object tracking, will be conducted, followed by the issue of the camera system in CULS canteen. The following part of the thesis will try to forecast development of artificial intelligence in camera systems. The end of the thesis will address ethical issues associated with the use of artificial intelligence in camera systems. This will include topics such as privacy and personal data protection, the question of discrimination, and the risks of incorrect decisions that can be caused by artificial intelligence algorithms.

Keywords: camera systems, artificial intelligence, security

Obsah

1 Úvod

Umělá inteligence se v posledních letech se stala nedílnou součástí našich životů. Tyto sofistikované algoritmy se skrývají téměř ve všech částech moderní technologické infrastruktury. Stejně jako řidič jedoucí po mostě, který se nezajímá o architektonické zpracování mostu a vidí jej pouze jako prostředek k dosažení cíle, uživatelé denně používají umělou inteligenci během svých interakcí s technologiemi, a mohou si dovolit nevnímat komplexní algoritmy na pozadí. a právě tak jako řidič vidí most jako něco zcela běžného, důležitého a přirozeného, uživatelé vidí umělou inteligenci také tak. s umělou inteligencí se setkáváme všude, ať už jde o internetové vyhledavače, sociální sítě, automobily, satelitní navigace, aplikace pro doporučování hudby či kamerové systémy.

Kamerové systémy mají mnoho využití, zejména v oblasti bezpečnosti. Mohou pomoci například předcházet kriminálním aktivitám nebo ochraňovat lidi a nemovitosti. v neposlední řadě umožňují vzdáleně kontrolovat prostory, nahrávat a archivovat záznamy. v kombinaci s umělou inteligencí vznikají nové, silné systémy s možnostmi nad rámec bezpečnosti, které nevyžadují neustálou kontrolu operátorem systému.

2 Cíl práce a metodika

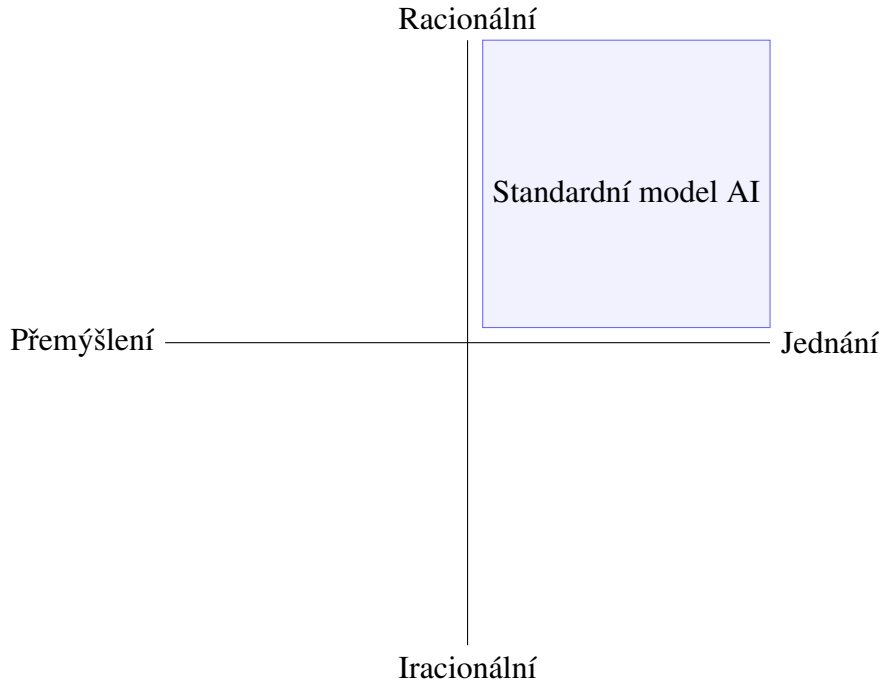
Hlavním cílem práce je posoudit účinnost a formy umělé inteligence v kamerových systémech. v rámci této práce jsou posouzeny dva druhy umělé inteligence (dále AI z anglického výrazu Artificial Intelligence). Jde o AI zabudované do samostatných kamer a AI ve videorekordérech. Oba typy AI jsou analyzovány a srovnány.

Dílčím cílem práce je identifikovat příčiny nesprávného měření počtu lidí kamerovým systémem v menze ČZU. Tohoto cíle bude dosaženo analýzou videozáznamů z již implementovaných kamer.

3 Teoretická část práce

Pro začátek je třeba porozumět tomu, co to vlastně je umělá inteligence (dále AI). Vzhledem k tomu, o jak komplexní téma jde, není stanovená přesná definice AI. Důvodem je to, že vývoj AI má 4 hlavní filozofické směry, které se od sebe výrazně liší. Chceme, aby AI byla inteligentní, co se týče chování, nebo přemýšlení? Vyvíjíme AI, abychom vytvořili model člověka, nebo vyžadujeme optimální výsledky?

To se dá pro lepší pochopení představit jako dvojrozměrný graf, kde na ose X je jednání proti přemýšlení, a na ose Y se nachází lidský (iracionální) a racionální pohled na věc. v každém kvadrantu grafu je jiný pohled na AI, s tím že v praxi nejvyužívanější model jednání se nachází v kvadrantu s racionálním jednáním, jak je zobrazeno na grafu 1.



Graf 1: Směry umělé inteligence

Tento model se zabývá převážně racionálním chováním, z čehož plyne, že nemusí (a pravděpodobně ani nebude) přemýšlet jako člověk, a očekáváme od

něj optimální výsledky. Ideální inteligentní agent tedy vždy v dané situaci volí nejlepší možnou akci (1).

3.1 Rozbor nástrojů umělé inteligence v kamerových systémech

Umělá inteligence poskytuje řadu nástrojů, které v kombinaci s kamerovými systémy nabízí možnost ulehčení a automatizace práce operátorů těchto systémů.

3.1.1 Strojové učení

Za předpokladu, že máme soubor příkladů konceptu, lze definovat učení jako nalezení obecného pravidla, které vysvětluje příklady dané pouze vzorkem omezené velikosti. Tyto příklady jsou obecně označovány jako data. Obtížnost problému strojového učení je podobná problému, kdy se děti učí mluvit ze zvuků, které vydávají dospělí lidé (2 s 131).

Strojové učení ve své podstatě umožňuje programům programovat "samy sebe". Stroj se učí, když po pozorování světa zlepší svoje výsledky. Počítač zanalyzuje data, postaví model na základě těchto dat a použije ho jako hypotézu o světě a jako software, který mu umožní vyřešit daný problém (1 s 667). Za pomoci velkého množství dat a zpětné vazby ze strany uživatelů/vývojářů se software může něco "naučit". Nevýhodou ale je, že vzhledem k tomu, že program programuje sám sebe, jeho logika je pro člověka těžko pochopitelná (3).

Existuje několik druhů strojového učení. Dělí se podle druhu zpětné vazby (1 s 671).

Učení s učitelem (supervised learning) je druh strojového učení, kde agent sleduje páry vstup a výstup a učí se funkci, která mapuje spojení mezi vstupem a výstupem. Například při analýze snímků z kamer mohou být vstupy obrázky a výstupy by byly popisky jako "chodec" nebo "autobus". AI se v tomto případě naučí funkci poznávání objektů na obrázku ulice.

Další formou strojového učení je učení bez učitele (unsupervised learning). V tomto případě se AI učí bez explicitní zpětné vazby. To se využívá hlavně při shlukové analýze, kdy se software snaží detekovat potenciálně užitečné vzory ve velkém množství dat. Například při analýze několika milionů obrázků z internetu může AI sloučit všechny obrázky, na kterých je to, co by člověk označil za kočky.

Třetím druhem strojového učení je zpětnovazební učení (reinforcement learning). V tomto případě se AI učí na základě série zpětných vazeb, které spadají do dvou tříd. Jde o ”odměny” a ”tresty”. v případě, že bychom AI učili hrát hru, AI vyhrála, dostane odměnu - kladnou zpětnou vazbu, a pokud by prohrála, dostane trest - zápornou zpětnou vazbu. Samotný agent má za úkol zjistit, co vedlo k jeho výhře, nebo prohře.

Cílem strojového učení je vznik funkce, která pracuje s velkým množstvím dat v praxi, a ne jen s daty používanými na trénink.

3.1.2 Deep learning

Deep learning, česky ”hluboké učení”, je specifická disciplína strojového učení. Učení může probíhat jak s učitelem, tak i bez učitele.

Hluboké učení má jako vzor chování biologické neuronové sítě. Proto se při deep learningu využívají takzvané umělé neuronové sítě. Neuronové sítě jsou sady výpočetních jednotek, které jsou reprezentované umělými neurony a jsou spojeny velkým množstvím umělých synapsí. Tyto synapse mají určitou váhu, která reprezentuje sílu spojení dvou neuronů (4 s 6).

Název hluboké učení vychází z faktu, že rozhodovací obvody jsou organizovány do velkého množství vrstev, což znamená, že výpočetní cesta rozhodování má spoustu kroků. Hluboké učení je nejrozšířenější technika strojového učení pro účely počítačového vidění, strojového překladu, a nebo například syntézy obrázků (1 s 801).

Hlavní funkce neuronových sítí jsou:

- Schopnost učit se
- Organizace dat
- Adaptovat se ze zkušeností a zpětné vazby
- Schopnosti zobecňování
- Tolerance chyb neboli schopnost systému pracovat i přes výskyt chyby
- Distribuovaná paměť

Každý neuron v neuronové síti se dá reprezentovat jako linárně regresní model složený ze vstupních dat, synaptické váhy, prahové hodnoty a výstupu (5).

3.1.3 Počítačové vidění

Počítačové vidění je základní funkce kamerových systémů vybavených umělou inteligencí. Samostatné počítačové vidění je disciplína, která se zabývá získáváním obrazu, tedy fotografií nebo videa, jeho zpracováním, získáváním dat z obrazu a případně s jeho manipulací (6).

Počítačové vidění se zabývá dvěma jádrovými problémy. Jde o rekonstrukci a poznávání (reconstruction and recognition). Rekonstrukce se zabývá vytvářením modelu ze zachyceného obrazu nebo série obrazů. Ke tvorbě 3D modelů se využívá buď kamerový systém s několika kamerami s různými úhly pohledu na scénu, nebo speciální 3D kamery s několika čočkami. Novinkou je tvorba modelů i z jednoho obrazu (7), ale jde o tak novou technologii, že ještě není široce rozšířena. Opačný proces, tedy tvorba obrazu ze 3D dat, je samozřejmě možná, a ve většině případů i jednodušší.

Poznávání je proces, kdy AI rozpoznává a navzájem od sebe rozlišuje různé objekty zachycené na obraze na základě vizuálních dat. Rozlišování objektů funguje na principu zjednodušování reprezentace důležitých dat a redukce detailů. Toho je dosaženo pomocí následujících 4 technik: detekce hran, analýza textur, optical flow a segmentace (6).

Rozlišování hran je nejjednodušší technika. Hrana vzniká tam, kde existuje velký rozdíl v jasu sousedních pixelů.

Při analýze textur se počítačové vidění zaměřuje na rozdíl od hodnot jasu na vzory na povrchu objektů na scéně. Textura se tedy zaměřuje na kusy obrazu, zatímco rozlišování hran zkoumá přímo pixely. Příkladem strojem rozlišitelné textury mohou být okna budov, stehy na pleteném svetru, leopardí kůže, trávník, štěrk na cestě nebo dav lidí na stadionu.

Optical flow se na rozdíl od výše uvedených technik, které se aplikují na statické obrázky, používá na videu, ať už jde o zpětně puštěný záznam nebo o přímý přenos. Optical flow vzniká tam, kde dochází k pohybu objektů na scéně. Pokud se objekt pohne, změní se jeho poloha na obraze. Optical flow je relativní vzhle-

dem k poloze kamery. Vzdálené objekty budou mít menší optical flow než objekty blíže ke kameře, které se pohnuly o stejnou vzdálenost (**introToVidproc**).

Segmentace je proces, při kterém se obrázek rozdělí na skupiny podobných pixelů. Podstatou této techniky je seskupení částí obrazu, na kterých mají pixely podobné vlastnosti, jako jas, barvu, a které jsou součástí nějaké textury. Tyto vlastnosti se uvnitř objektu nebo v jeho součásti liší relativně minimálně. Oproti detekci hran má segmentace tu výhodu, že dokáže určit jednotný objekt i v případě, že je jeho součástí nějaká hrana. (1).

3.1.4 Videoanalýza

Videoanalýza s využitím umělé inteligence staví na počítačovém vidění. Zaměřuje se na extrakci užitečných dat ze zachyceného videozáznamu. Tyto data mohou být například počet lidí nebo identifikace speciálních objektů a osob (8).

Existují 3 hlavní druhy videoanalýzy:

- Fixní algoritmová analýza
- Videoanalýza s učící se umělou inteligencí
- Systémy pro rozpoznávání obličejů

(9, s 122) První dva výše zmíněné druhy dosahují stejného cíle, a to rozhodování, jestli nedochází k nechtěnému nebo podezřelému pohybu v záběru kamery. v případě, že ano, dostane operátor systému hlášení. Rozdíly jsou v přístupu k řešení problému. Systémy s fixními algoritmy mají zabudované určité funkce, které operátor nakonfiguruje podle svých potřeb. Každá funkce hledá specifické chování. Tyto funkce mohou být například:

- Vstup do zakázaného prostoru
- Chůze špatným směrem po chodbě
- Rozpoznávání poznávacích značek automobilů

a tak dále. Tyto funkce jsou podrobněji rozebrány v kapitole ”Typické způsoby nasazení a využití”.

Videoanalýza s učící se umělou inteligencí funguje úplně jinak. Učící se algoritmus je jako nepopsaný list. Po napojení na kameru systém analyzuje několik týdnů záznam. Až pak může informovat operátora o nevyžádaném nebo podezřelém chování. AI zkoumá záznam, učí se, jak vypadá běžný den, běžná noc, co se děje v pracovních dnech a co se děje o víkendech. Na základě těchto dat může upozornit na chování sledovaných subjektů, které vystupuje z normy, tedy není konzistentní s tím, co je vyhodnoceno jako běžné chování v danou dobu.

Třetím zmíněným druhem videoanalýzy je rozpoznávání obličejů. To se využívá pro řízení přístupů a k identifikaci nepovolaných osob. Typické systémy pro rozpoznávání obličejů srovnávají body na tváři s tvářemi v systémové databázi.

3.2 Typické způsoby nasazení a využití

Tato kapitola se věnuje praktickým příkladům nasazení kamerových systémů s umělou inteligencí.

3.2.1 Detekce obličejů a lidí

Detekce obličejů a lidí je podkategorie spadající do informační bezpečnosti. Ta se stará o zajištění důvěrnosti, integrity a dostupnosti informací ve všech podobách. Existuje velké množství nástrojů a technik pro management bezpečnosti informací. Tradičně se využívají hesla a osobní identifikační čísla PIN (personal identification number). Hesla a piny ale mají tu nevýhodu, že je v horším případě může využít třetí strana pro neautorizovaný přístup k informacím, a v lepším případě je uživatel jednoduše zapomene, čímž ztratí přístup k daným informacím. Novější bezpečnostní systémy proto využívají ověřování na základě biometrických charakteristik jedince. Biometrické ověřovací metody využívají unikátní fyzické nebo biologické charakteristiky každého člověka. Mezi biometrické metody patří čtení otisků prstů, identifikace hlasu, sken oční sítnice nebo rozpoznávání obličejů (10 s 1).

Rozpoznávání obličejů je široce používaná metoda díky tomu, že je spolehlivá, přijatá společností a je aplikovatelná na velké množství lidí najednou. Rozpoznávání obličejů probíhá ve dvou fázích. První fází je detekce obličeje a druhou fází je jeho rozpoznání/identifikace. Kamerové systémy pro rozpoznávání obličejů

nejdříve určují, zda-li se na scéně nachází obličej. Pokud ano, určí jeho polohu na obraze. Poté nastává druhá fáze a tyto obličeje jsou srovnány s autorizovanými obličeji v systémové databázi.

Umělou inteligenci lze vytrénovat k autorizaci obličejů, pokud jsou jí dodány 3 soubory dat - soubor obrázků bez obličejů, soubor autorizovaných obličejů a soubor neznámých obličejů. AI se nejdříve naučí rozpoznávat obličeje od ostatních objektů, a poté identifikaci autorizovaných osob. Nicméně moderní kamerové systémy mají zabudované algoritmy pro identifikaci osob, takže není třeba investovat velké množství času do strojového učení.

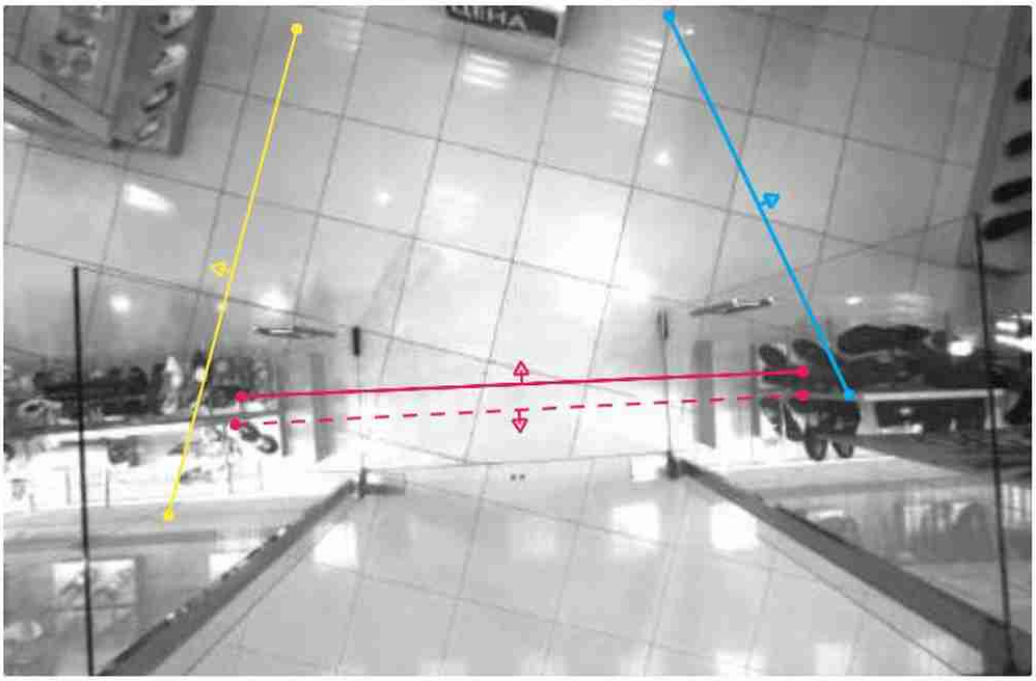
Detekce lidí není omezená jenom na rozpoznávání obličejů. AI je schopné identifikovat i co lidé na scéně dělají. To se dá vyžít například pro sledování "potloukání". Tyto algoritmy hlídají proud lidí. Pokud zjistí, že se člověk nebo skupina lidí zastavili, začne je sledovat. Po uplynutí určité doby informuje operátora o možném podezřelém shromáždění ve sledovaném prostoru. To se využívá například pro prevenci krádeží a tvorby graffiti (11).

3.2.2 Počítání osob a aut

Pro počítání lidí a aut se v kamerových systémech využívá counting line, česky počítací linka. Counting line se nastavuje v konfiguračním softwaru kamer tak, že se "nakreslí" přímka přes scénu. Obrázek 1 zobrazuje záběr kamery se třemi počítacími linkami. Horizontální linka počítá lidi procházející dveřmi, postranní linky počítají kolik lidí šlo doleva a kolik šlo doprava. Pokud člověk v záběru přímku překročí, započítá se. Před spuštěním je třeba určit, který směr překročení přímky kamera počítá.

Kalibrace počítací přímky se provádí v ovládacím softwaru a spočívá v nastavení šířky objektů, které přímku překročí. Pro příklad špatné kalibrace si můžeme představit kameru počítající vozidla na dálnici. Pokud bude šířka objektů kalibrována na dodávkách, užší osobní automobily a motorky se nezapočítají (12).

Aby byly kamery počítající lidi co nejpřesnější, je potřeba je umístit tak, aby mířila jejich čočka kolmo k zemi. Důvodem je to, že rozpoznávání samostatných lidí od skupinek je jednodušší, pokud na ně systém pohlíží přímo shora. Dále je třeba dosáhnout co nejlepších světelných podmínek, přičemž i silné stíny a nebo



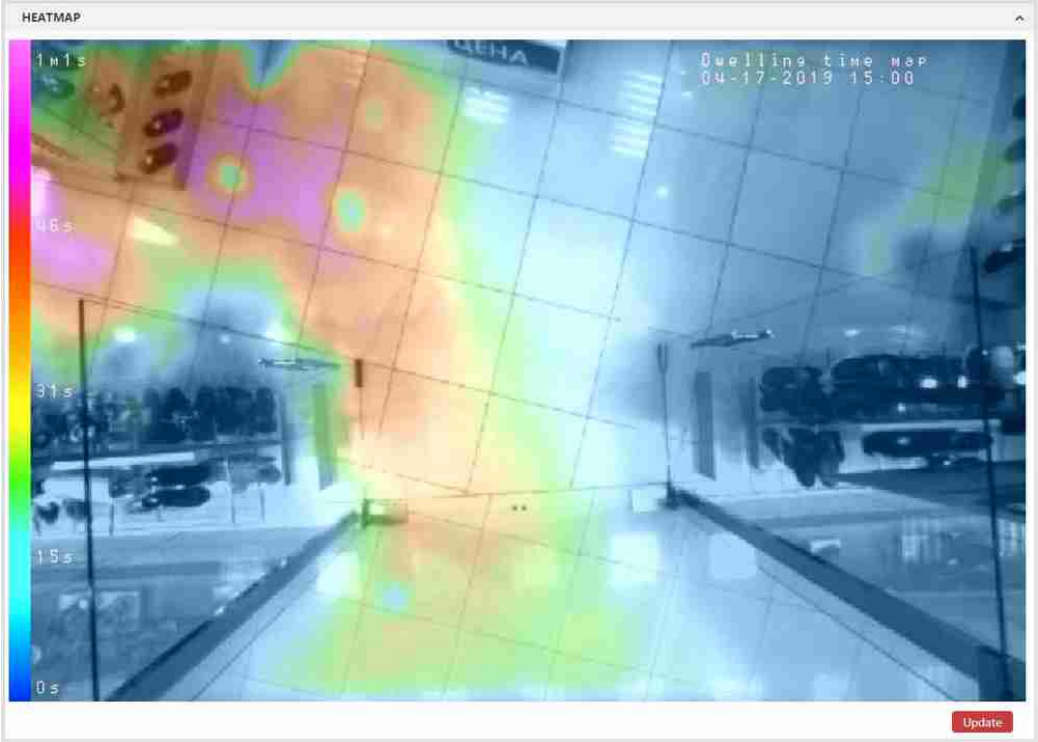
Obrázek 1: Počítací linka (IDTElectronics, 2020)

odlesky mohou způsobovat problémy při počítání.

3.2.3 Tepelné mapy

Data pořízená z detekce lidí a počítání osob se dají využít na tvorbu takzvaných tepelných map, neboli heatmap. Heatmapa je technika vizualizace dat, která ukazuje velikost daného jevu jako barvu na dvourozměrném grafu. Rozdíly v barvě, reprezentované buď odstínem nebo intenzitou, ukazují, jak je jev seskupen v prostoru (13).

V našem případě může být grafem plán místa, na kterém provozujeme kamerový systém. Heatmapa ukáže, kde se lidé nejvíce shlukují nebo kde tráví nejvíce času. Heatmapy se využívají k porozumění chování návštěvníků. Například kamerový systém s funkcí tvorby heatmapy, nainstalovaný v obchodním domě, poskytuje informace o tom, do kterých částí obchodu zákazníci chodí nejčastěji, kam nechodí vůbec, jaké zboží hledají, co upoutá jejich pozornost, a tak dále. Heatmapy na obrázku 2 ukazuje vysokou koncentraci zákazníků v levé horní části



Obrázek 2: Příklad heatmapy (IDTElectronics, 2020)

scény.

Mimo heatmapy fungující na principu počtu lidí se dají tvořit i heatmapy na principu sledování orientace hlavy návštěvníků. To se využívá zejména v obchodech. Tato heatmapa poskytuje přímo informace o tom, jaký obsah přitahoval největší pozornost zákazníků na určitých pozicích (13).

3.2.4 Počítání obsazenosti parkovišť

Obsazenost parkovišť lze počítat třemi způsoby. První funguje i bez kamerového systému, a to na základě počtu zvednutí závor. Zbylé dva postupy využívají kamery.

První možností je nastavení počítací přímky u vjezdu a výjezdu. To se využívá hlavně ve vnitřních parkovištích.

Na vnějších parkovištích bez kamer u vjezdu lze použít identifikaci volných

parkovacích míst. Tyto systémy využívají strojové vidění pro označování volných parkovacích míst a nepotřebují k tomu ani záznam, stačí v pravidelném časovém intervalu pořídit fotku parkoviště. To snižuje náklady na provoz sítě. Identifikace volných parkovacích míst může být přesnější než počítací linka, ale tato technika vyžaduje kameru umístěnou vysoko nad parkovištěm, a v případě, že je parkoviště moc velké na to, aby ho zabrala jedna kamera, vyžaduje soustavu několika kamer, což může být nákladné a ve výsledku nepraktické (14).

3.2.5 Rozpoznávání registračních značek

Rozpoznávání registračních značek (zkratka ANPR z anglického výrazu automatic number-plate recognition) vozidel využívá OCR technologii. OCR je zkratka pro Optical Character Recognition, česky optické rozpoznávání znaků. Jde o software, který je schopný identifikovat znaky na zaznamenaném obraze a převést je na text.

ANPR probíhá následovně. Při příjezdu auta do záběru určí umělá inteligence, ve které části obrazu se nachází poznávací značka. Následně upraví obraz tak, aby došlo k co nejefektivnější aplikaci OCR algoritmů, jak je vidět na obrázku 3.

Obrázek 3: Ukázka úpravy obrázku poznávací značky pro aplikaci OCR (Wikimedia.org, 2006)

Rozpoznávání registračních značek se využívá pro kontrolu platnosti regis-

trace aut, automatické otevírání závor u vjezdů, a nebo pro elektronický výběr mýta.

Problém s ANPR může nastat se zahraničními registračními značkami. Správně konfigurovaný ANPR systém by měl být schopný identifikovat poznávací značky z různých regionů, aby byl efektivní. Je tedy potřeba správně identifikovat rozdíly ve fontu, barvě pozadí a velikostmi znaků a mezer.

3.2.6 Prevence požáru a bezpečnost práce

Umělá inteligence a kamerové systémy jsou dobrý nástroj pro kontrolu bezpečnosti práce, prevenci úrazů a brzkou detekci požárů.

Díky schopnosti AI rozpoznávat objekty na obraze existují systémy schopny kontroly bezpečnosti práce. Tyto systémy mají širokou škálu schopností. Jednou z nich je kontrola nošení osobních ochranných pracovních pomůcek. AI dokáže identifikovat pracovníky, kteří nemají svoje ochranné pomůcky (reflexní vesty, přilby, laboratorní pláště, masky, bezpečnostní brýle apod.) a informují o tom administrátora systému, nebo jiného dozorčího pracovníka. Také jsou současné systémy schopny identifikovat nebezpečné chování zaměstnanců. Jako příklad lze uvést šplhání na stroje, shlukování, vchod do cesty vyhrazené pro stroje a podobně (15).

Další funkcí je prevence nehod. Kamerové systémy můžou kontrolovat věci jako výskyt překážek na cestách strojů, průchodnost chodeb, dodržování zavřených nebo otevřených dveří, detekci rozlití tekutých látek, porušení zákazu vstupu, nebo minimální a maximální počet zaměstnanců v místnosti nebo u stroje. Zvláště detekce shlukování a dodržování bezpečné vzdálenosti bylo často používané v posledních několika letech od začátku pandemie v roce 2020 (16).

V případě porušení těchto pravidel dojde minimálně k upozornění administrátora kamerového systému. Není ale problém integrovat kamerový systém dále a spojit s ním třeba spuštění alarmu, dálkově ovládané dveře a další bezpečnostní a zabezpečovací prvky.

Pokud výše popsaný systém selže a dojde k porušení bezpečnosti práce a k následnému požáru, může být k jeho detekci využit právě systém kamer. v současnosti existuje několik různých druhů senzorů pro detekci požárů. Mezi ně patři in-

fračervené termokamery. Tyto kamery identifikují místa se zvýšenou teplotou v záběru kamery. Termokamery se dají použít venku ve vnitřních prostorech a vidí i ve tmě. Mohou oznámit požár dříve, než ho odhalí lidé. Při vyhodnocení požáru je možné automaticky spustit alarm, hasicí systém, nebo dokonce odstřihnout přívod paliv jako plyn nebo propan.

3.2.7 Detekce vniknutí a virtuální plot

Detekce vniknutí je jedním z hlavních cílů zabezpečovacích systémů. Soustava senzorů hlídá prostředí a informuje operátora v případě, že dojde k nepovolenému vniknutí do zakázaných prostorů. Existují různé druhy zabezpečovacích zařízení, například senzory hlásící přerušení magnetického pole při otevření dveří, dále například infračervené senzory aktivované teplem člověka, nebo právě kamery (9 s 206). Kamerové systémy v zabezpečení se dají využít jako detektory pohybu nebo pro virtuální plot.

Detekce pohybu využívá motion flow techniku pro identifikaci pohybu, který pak hlásí operátorovi systému. Kamery pro detekci pohybu se využívají v případě, nechceme-li jakýkoliv pohyb na scéně.

Virtuální plot se využívá tehdy, kdy vystavění reálného plotu není možné. Například ve vnitřních prostorech. Pokud chce operátor kamerového systému začít využívat virtuální plot, musí v nastavení kamery nebo nahrávacího zařízení určit, jaká část scény má být nepřístupná. v případě, že by nějaký objekt vstoupil do zakázané zóny, dostane operátor oznámení v podobě alarmu na místě nebo formou e-mailu nebo sms zprávy (17). Umělá inteligence v kamerových systémech s funkcí virtuálního plotu navíc dokáže rozeznávat, jaké objekty vstoupily do zakázané oblasti, a na základě toho rozhodnout, jestli spustit alarm nebo ne. Například můžeme sledovat zónu, která je nepřístupná lidem, ale auta chceme nechat projíždět. Systémy s umělou inteligencí jsou schopny rozpoznat lidi například od aut a malých zvířat, a tak informují operátora jen v případě, že do scény vstoupí člověk. Výhodou virtuálního plotu od pouhé detekce pohybu je snížení počtu falešných poplachů. Zatímco algoritmy pro detekci pohybu mohou za pohyb označit i třeba dopadající světlo ze světlometů kolem projíždějícího auta, umělá inteligence virtuálních plotů se zaměřuje na rozpoznávání různých objektů (17).

3.3 Srovnání kamer s vestavěným AI s kamerami s AI v rekordérech

V úvodu této kapitoly je vhodné uvést, co to je rekordér. Rekordéry jsou důležitou součástí kamerového systému. Jde o speciální hardware, ke kterému jsou připojeny všechny kamery v systému. Rekrodér umožňuje administrátorovi spravovat kamerovou síť a poskytuje funkce na zpracování a ukládání videa z kamer.

3.3.1 AI v kamerách

Samotné kamery mají z pravidla méně funkcí než v případě, že jsou napojeny na rekordér. Chytré kamery se dají rozdělit na kamery pro konečné spotřebitele a na kamery určené pro firemní zákazníky.

Kamery pro spotřebitele se vyznačují velkým množstvím funkcí založených na cloudovém zpracování nahraného videa. Tyto kamery bývají napájené z baterie, připojují se do sítě pomocí wi-fi, záznam nahrávají buď na SD kartu nebo do cloudového úložiště výrobce, a poskytují minimální nastavení s omezeným strojovým učením. Obraz se nahrává do cloudu výrobce, který poskytuje další služby jako identifikaci lidí, zvířat a objektů, jako například rozpoznání doručeného balíčku před vstupními dveřmi. Další běžnou funkcí je aktivace na základě detekce pohybu. Kamera může být většinu času neaktivní, a nahrávání se zapne až v případě, že dojde k pohybu na scéně. Mezi přednosti tohoto druhu kamer patří cenová dostupnost a možnost integrace do internetu věcí (internet věcí je síť zařízení, která jsou vybavena elektronikou, softwarem, senzory a síťovou konektivitou, která umožňuje těmto zařízením se propojit a vyměňovat si data). Jsou vhodné pro zabezpečení domácností a menších podniků, ale jejich omezené možnosti a v mnohých případech nutnost pravidelné platby předplatného pro odemčení pokročilých funkcí je nevhodná pro uživatele a instituce s náročnějšími požadavky. 18

Naproti tomu kamery pro firemní zákazníky mají pokročilé funkce, mezi které patří počítání lidí a aut, identifikace obličejů (a nálad), kontrola nošení bezpečnostních pomůcek (brýle, masky, respirátory a podobně), detekce shlukování nebo virtuální plot. Procesy umělé inteligence probíhají v reálném čase přímo na zaznamenaném

obrazu. Tyto kamery mají zpravidla lepší možnosti nastavení a nástroje pro práci se strojovým viděním než kamery pro koncové spotřebitele. (19)

3.3.2 AI v rekordérech

Umělá inteligence v rekordérech poskytuje stejné nástroje, jako pokročilé AI kamery. K rekordérům se dají připojit klasické kamery bez AI. Videoanalýzu pak provádí přímo rekordér, což vede k přidání umělé inteligence do stávajícího kamerového systému.

Mimo dříve zmíněné funkce jsou rekordéry schopny strojového učení s cílem snížení počtu falešných poplachů, které mohou vzejít ze špatné identifikace objektu kamerovým systémem. Dále dokážou některé rekordéry spolupracovat s databázemi, což se dá využít například v kombinaci s rozpoznávání obličejů. v databázi mohou být zapsáni zaměstnanci, a rekordér může identifikovat, kde se daný člověk v databázi nachází (20).

Jednou z hlavních předností využití rekordéru v oblasti umělé inteligence jsou samostatné procesory určené pro umělou inteligenci. Jde o speciální čipy, které jsou navržené pro optimální běh umělé inteligence. To vede k rychlejšímu běhu funkcí využívajících strojové učení, deep learning a další AI aplikace v porovnání s běžnými procesory (21).

Nevýhodou umělé inteligence v rekordérech je zpracovávání komprimovaného přenosu. Kamery komprimují záznamy před odesláním do rekordéru. Tato funkce sice umožňuje nižší objem přenesených dat, ale komprese vede ke vzniku artefaktů v obrazu, což AI může identifikovat jako pohyb. v tom případě dochází k falešnému poplachu (22).

4 Praktická část práce

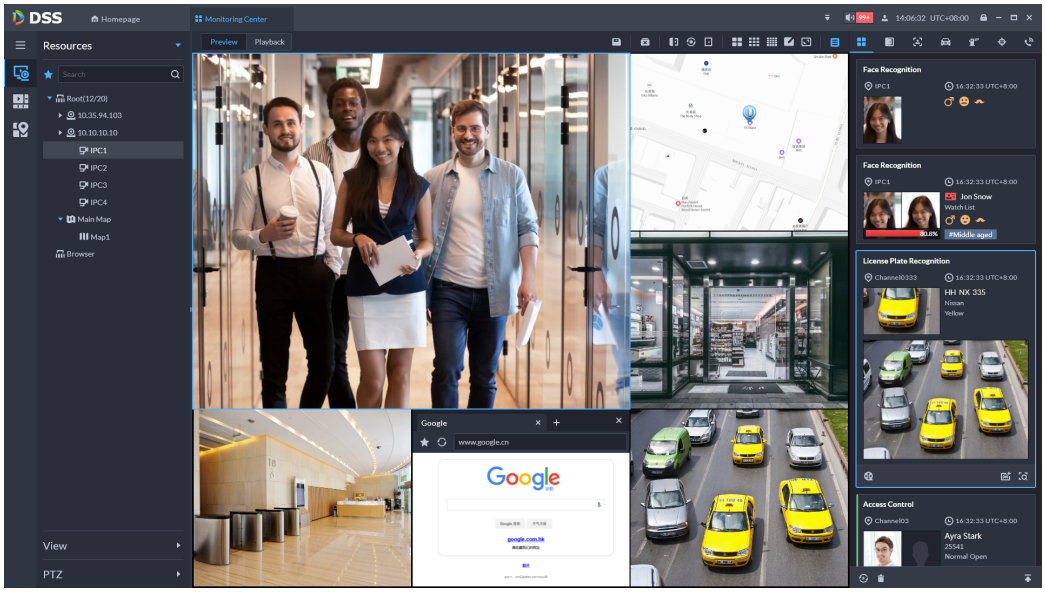
Praktická část práce se zabývá problémem s kamerami v menze ČZU. Nad vchodem a východem jsou umístěny kamery s vestavěnou AI, které mají za úkol počítat osoby v menze. Kamera nad východem je ale problémová a nepočítá správně. Chybovost kamery je mnohem větší než uvádí výrobce jako přípustnou chybu. Statistiky v ovládacím softwaru pak ukazují, že se menza postupně plní a na konci dne se v ní nachází ještě řada lidí. Jednoduchý pohled na prázdnou halu ale určí, že konečné statistiky se liší od skutečnosti.

Úkolem je zanalyzovat záznamy z problémové kamery. Zjistit, jestli mají nezapočítaní lidé nějaký společný znak, a navrhnout nastavení, které by tyto chybu vyřešilo.

Chybná kamera je Dahua IPC-HDW8341X-3D, zobrazena na obrázku 4. Jde o kameru s vestavěnou umělou inteligencí. Kamera má 2 videosenzory s rozlišením 3 megapixely a infračervenou diodu, která zlepšuje obraz ve tmě. Umělá inteligence v kameře je schopna hlubokého učení se zaměřením na rozpoznávání lidí a vozidel. Podle výrobce je kamera schopna rozpoznávání obličejů, počítání lidí, identifikace poznávacích značek, zaznamenávání dopravní statistiky, a tak dále. (19)

Obrázek 4: Kamera Dahua IPC-HDW8341X-3D (Dahua Security, 2021)

Kamery jsou ovládány pomocí softwaru Dahua DSS Pro. Jde o program pro správu kamerových systémů. Tento program spravuje kamery v kampusu ČZU. Detail uživatelského rozhraní programu je na obrázku 5.

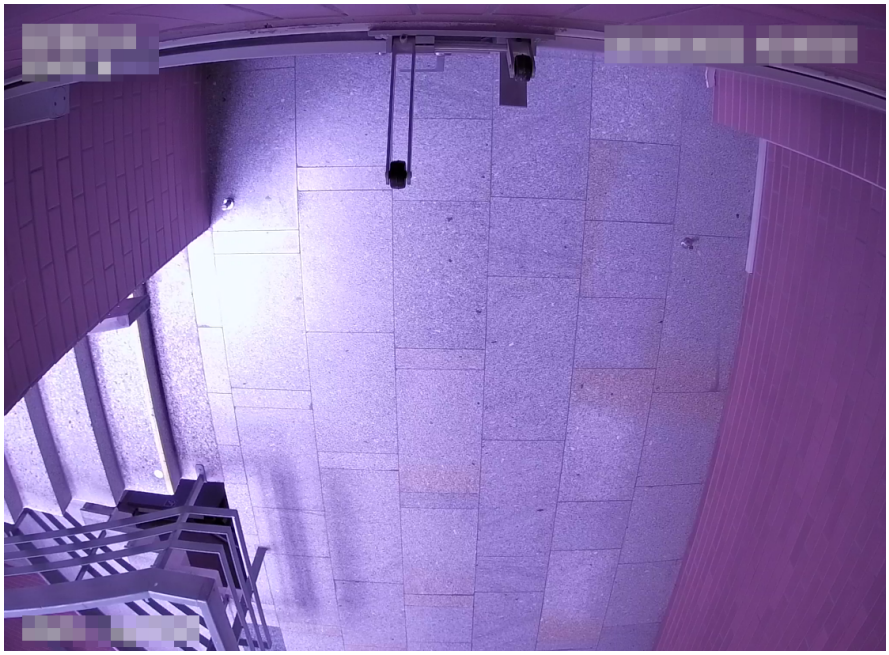


Obrázek 5: Uživatelské rozhraní programu Dahua DSS Pro (Dahua Security, 2021)

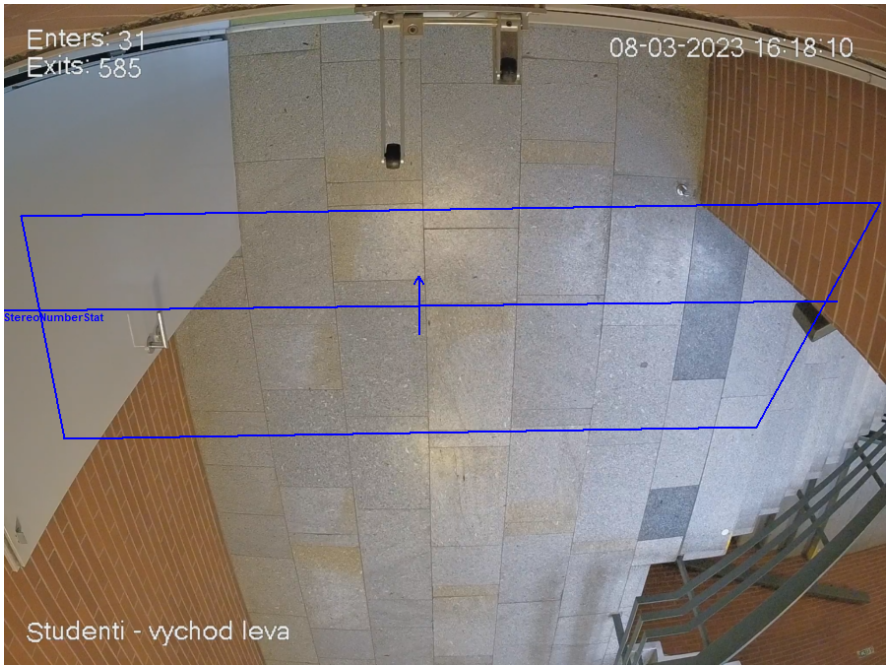
Kamera je umístěna nad východem z menzy ČZU a jejím cílem je počítat osoby cestou z menzy. Na záběru kamery je nastavená počítací linka. Pro potřeby analýzy byly pořízeny záznamy mezi 5. a 9. zářím 2022. Záznamy byly pořizovány od 10:00 do 14:00 hodin. v běžném provozu nejsou záznamy nahrávány, počítání lidí funguje v reálném čase na přímém záběru kamery. Před získáním přístupu k záznamům je potřeba podepsat smlouvu o mlčenlivosti. Záběr kamery je na obrázku 6. Na obrázku 7 je pro porovnání záběr funkční kamery v menze ČZU.

4.1 Test úspěšnosti vyhodnocení

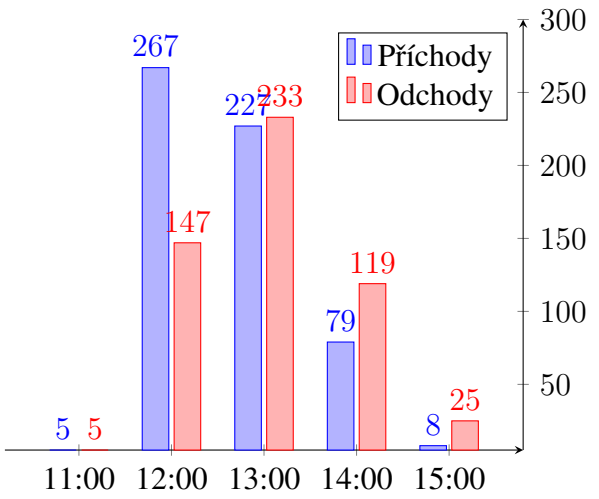
Důkazem, že kamera nepočítá dobře, jsou data, která poskytuje software pro správu kamer. Software zaznamenává počet příchodů a odchodů, a na základě toho udává, kolik lidí se nachází v menze. Data z prvního dne měření zobrazuje graf 2.



Obrázek 6: Záběr chybové kamery nad východem z menzy. (ČZU 2022)

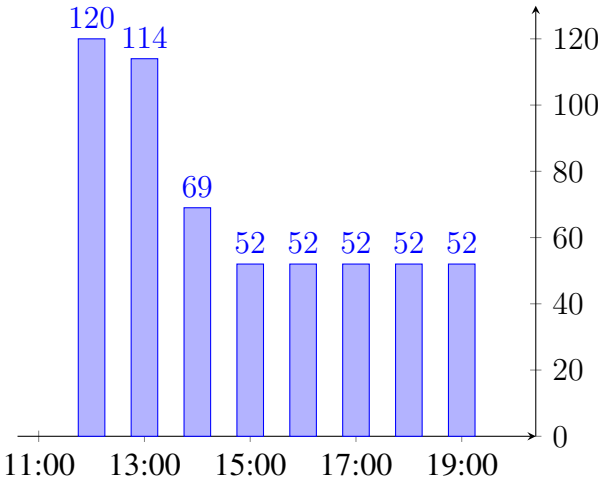


Obrázek 7: Záběr funkční kamery (ČZU 2023)

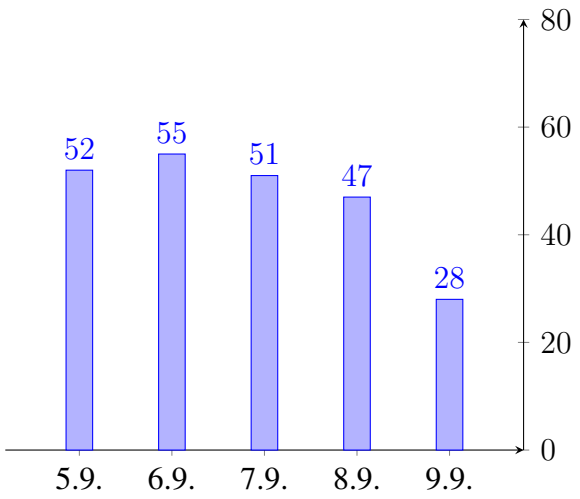


Graf 2: Počet příchodů a odchodů z menzy 5.9.2023

Graf 3 ukazuje počet osob v menze. Zde je vidět probléové chování kamery. Konečný počet lidí v menze by měl být ideálně nulový. Nicméně je nahlášeno 52 osob stále v menze po zavírací době. Tento trend přetrvával po celou dobu měření. Konečné počty osob jsou zobrazeny na grafu 4.



Graf 3: Rozdíl počtu příchodů a odchodů 5.9.2023



Graf 4: Rozdíly příchodů a odchodů během prvního měření

Prvotní hypotéza, proč kamera nefunguje správně, předpokládá, že chybová kamera je plně funkční. To by znamenalo, že všechny osoby, které kamera vynechá, mají něco společného. Například všechny nezapočítaní lidé nosí tmavé oblečení, mají určitou barvu vlasů, jsou moc vysocí na to, aby je kamera započítala, a podobně.

Hypotéza se testovala analýzou nahraných záznamů. Při každém nezapočítaném průchodu byl pořízen snímek obrazovky. Na konci bylo pořízeno téměř 200 snímků.

Pro to, aby kamera počítající lidí byla co nejpřesnější, je třeba, aby byla kamera ve správné výšce a aby byl obraz co nejčitelnější, tedy v záběru by neměly být silné stíny a odlesky. Kamera u východu je umístěna ve výšce doporučené výrobcem (22). Na pořízených snímcích obrazovky se ukázalo, že kamera má tendenci vynechávat lidi v pravé horní části obrazu, těsně kolem dveří. Tam je také nejsilnější kontrast mezi odleskem světla na podlaze a stínem za otevřenými dveřmi. Silný růžový odstín záběru kamery také může omezit schopnost vestavěné AI rozpoznávat objekty. Nicméně hardwarová výbava kamery zahrnuje 2 čočky pro záběr ze dvou perspektiv, a infra červenou diodou pro zlepšení obrazu za nedostatku světla.

4.2 Vyhodnocení testu, finanční analýza

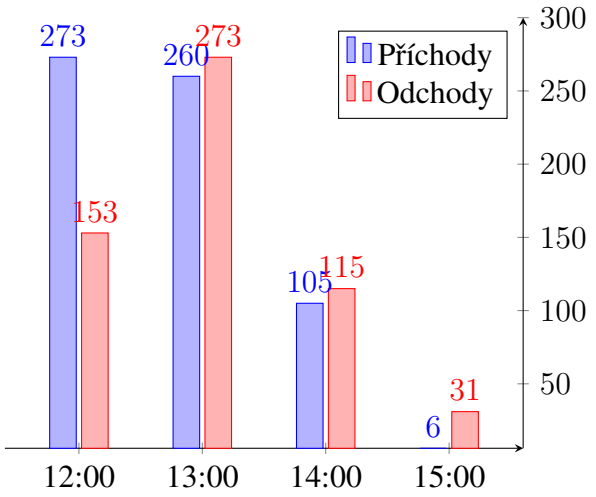
4.2.1 Vyhodnocení testu

Výsledky analýzy záznamu jsou ukázány na tabulce 1. Z analýzy je zřejmé, že kamera propouští značné množství lidí. Podle výrobce by měla mít až 98% přesnost (19), ale kamera v menze má až 8% chybovost.

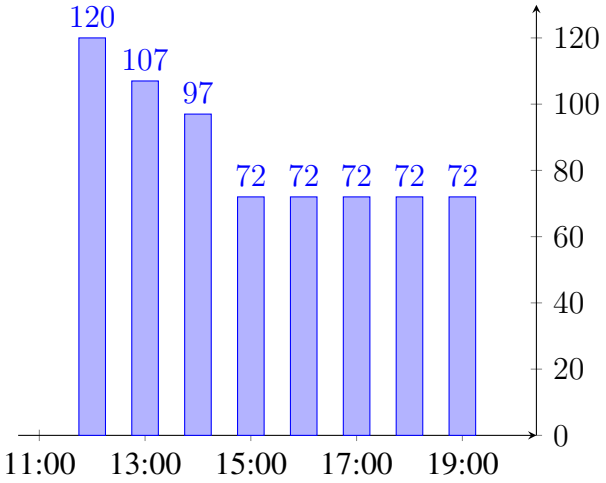
Den	Počet lidí napočítaný kamerou	Počet lidí napočítaný ručně
5.9.22	502	537
6.9.22	547	591
7.9.22	534	566
8.9.22	523	568
9.9.22	429	468

Tabulka 1: Porovnání počtu lidí napočítaných kamerou a ručně

Data z prvního dne měření jsou na grafu 5. Na první pohled vypadá graf v pořádku, ale kamery napočítaly nepřijatelné množství lidí, kteří v menze ”zůstali”, jak je zobrazeno na grafu 6.

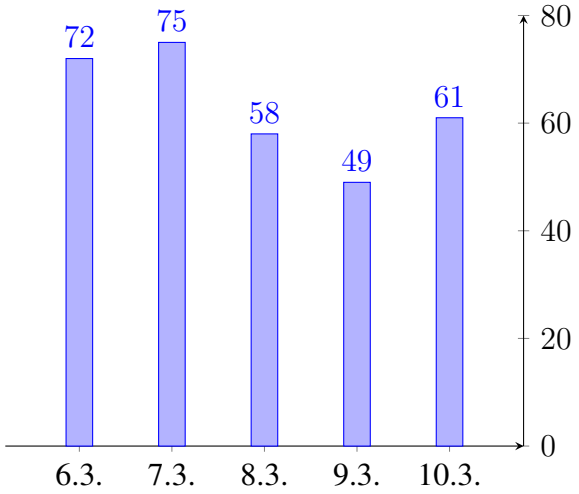


Graf 5: Počet příchodů a odchodů z menzy 6.3.2023



Graf 6: Počet příchodů a odchodů z menzy 6.3.2023

Tento trend pokračoval, stejně jako během prvního měření, po celou dobu měření s novým nastavením. Výsledky druhého měření jsou zobrazeny na grafu 7.



Graf 7: Rozdíly příchodů a odchodů během druhého měření

4.2.2 Finanční analýza

Cena kamery s funkcí počítání osob se pohybuje mezi 27 000 Kč a 32 000 Kč (23), pokud požadujeme podobnou výbavu, jako má stávající kamera. Kamery jsou dvě, jedna kamera se nachází nad vchodem, druhá nad východem. Výbava kamerami tedy může vyjít 52 000 Kč až 64 000 Kč. Obě kamery jsou pravděpodobně

připojené do rekordéru. Rekordéry mají dle výbavy cenové rozpětí od 5 000 Kč do 184 000 Kč (24). Pokud jde pouze o počítání lidí, dá se využít levnější rekordér, nicméně pro odborné použití jsou nejlevnější rekordéry nevhodné. Pro možnost rozšíření kamerové sítě v budoucnu se vyplatí připlatit za rekordér, který má více vstupů kamer a rozšiřitelné úložiště. Pro potřeby této práce se dá usoudit cena rekordéru kolem 55 000 Kč. Počítá se s tím, že software rekordéru je v jeho ceně. Mezisoučet dosahuje až 114 000 Kč pouze za hardware. Dále se musí započítat cena instalace hardware a školení s novým zařízením. Cena instalace závisí na době trvání a marži dodavatele (25). Ceny školení se mohou vyšplhat až k 10 000 Kč za osobu. Tabulka 2 popisuje čtyři možné situace, které se od sebe liší počtem kamer a potřebou vybírat dražší možnosti. Školení v tabulce ukazuje cenu pro jednoho zaměstnance.

Položka	**1 kamera levně**	**1 kamera draze**	**2 kamery levně**	**2 kamery draze**
Kamery	27 000	32 000	52 000	64 000
Rekordér	20 000	55 000	20 000	55 000
Instalace	14 160	23 600	14 160	23 600
Školení	1 500	9 900	1 500	9 900
Celkem	62 660	120 500	87 660	152 500

Tabulka 2: Odhadované ceny kamerového systému v Kč

Cena jednoho turniketu se pohybuje v rozmezí 15 000 Kč a 40 000 Kč (26). Existují i výrazně dražší turnikety v podobě klece s karuselovými dveřmi, ale tato možnost je pro menzu značně nepraktická. Je možné využít pouze 1 turniket, který by fungoval jako počítadlo příchodů i odchodů, ale to by značně omezilo už tak sníženou rychlost proudu lidí. Před turniketem by se tvořily fronty vzhledem k tomu, že záznamy ukázaly, že menzu opouštějí skupinky až 10 lidí najednou. Je tedy potřeba zvýšit počet turniketů u vchodu a umístit alespoň jeden i k východu. Další dva turnikety by pořizovací cenu zdvojnásobily. Instalace se pohybuje kolem 36 000 Kč za jeden turniket (27) a v poslední řadě je potřeba najmout alespoň jednoho zaměstnance, který kontroluje chod a případně řeší problémy. Platy se pohybují v rozmezí 19 000 Kč a 25 000 Kč měsíčně (28). Tabulka 3 zobrazuje 5

možných situací, které se od sebe liší počtem nainstalovaných turniketů a jejich výbavou.

Z výsledků finanční analýzy lze usoudit, že pro menzu je výhodnější kamerový systém. Kamera počítající osoby je rychlejší než turniket, netvoří fronty, a instalace je výrazně levnější. Navíc v případě menzy ČZU ani není potřeba kupovat nový rekordér a školit zaměstnance, protože nová kamera se dá zapojit do již existujícího a fungujícího kamerového systému.

Položka	**1 turniket**	**2 turnikety levně**	**2 turnikety draze**	**4 turnikety levně**	**4 turnikety draze**
Turnikety	15 000	30 000	80 000	60 000	160 000
Instalace	36 000	72 000	72 000	144 000	144 000
Školení	1 500	1 500	9 500	1 500	9 500
Celkem	52 500	103 500	161 500	205 500	313 500
Zaměstnanec	+ 19 000 měsíčně	+ 19 000 měsíčně	+ 25 000 měsíčně	+ 19 000 měsíčně	+ 25 000 měsíčně

Tabulka 3: Odhadované ceny turniketů v Kč

4.3 Zhodnocení výsledků

Pokus o identifikaci společných znaků nezapočítaných osob byl neúspěšný, a proto se nedalo předně odhadnout, proč kamera nepočítá správně. Byly navrženy změny nastavení kamery s cílem omezit efekt odlesků a upravit záznam kamery tak, aby neměl výstup tak výrazně narůžovělou barvu. Bohužel tyto změny neměly vliv na chybovost kamery. Z výsledků pokusu plyne, že kamera nad východem z menzy je chybná. Změna nastavení kamery sice mírně zlepšila kvalitu obrazu, ale počítání osob je stále problémové.

Řešením problému je reklamace kamery nebo nákup nové.

4.4 Predikce vývoje

Kamerové systémy se neustále zlepšují, stejně jako ostatní technologie. Cílem této části práce je pokusit se přiblížit budoucnost bezpečnostních kamerových

systémů.

4.4.1 Možná zlepšení

Trendy posledních několika let jasně ukazují na neustálé zvyšování rozlišení v zařízeních s kamerami. Také se zvyšuje kvalita obrazu, přestože dosahujeme do bodu, ve kterém může mít nezkušený pozorovatel problémy rozeznávat od sebe dvě různě vysoká rozlišení obrazu.

Téměř s jistotou se dá říci, že 5G standard mobilní sítě bude čím dál využívanější, a to i v kamerových systémech. Hlavní výhodou 5G je vysoká přenosová rychlost. To je ideální pro přenos záznamů s vysokým rozlišením. Celou situaci ještě mohou zlepšit nové formáty kódování videa, jako například AV1, který je přímo určený na streamování videa přes internet se zaměřením na kvalitu obrazu a relativně malém objemu přenesených dat.

Zrychlení internetového připojení a snížení objemu přenesených dat umožňuje širší využití cloudových řešení v oblasti bezpečnosti. Objevují se firmy, které se zaměřují na provozování bezpečnostních funkcí v cloudu. Cloudové bezpečnostní služby (anglicky Surveillance as a Service) poskytují dostupné videozáznamy odkudkoliv, různé AI funkce, neustálou podporu, nástroje pro integraci do stávajícího IT prostředí podniku a další funkce. Firmy se rozhodují pro využití těchto služeb na základě nízké vstupní ceny, velkého úložného místa pro záznamy, a dostupnost. Toto řešení má ale i své nevýhody, zejména závislost na internetovém připojení, a nutnost věřit poskytovateli, protože ve své podstatě jde o zasílání citlivých dat na cizí servery. Další nevýhodou je celková rychlost cloudového řešení. v současnosti není cloudové úložiště záznamů vhodné pro firemní zákazníky, kteří vyžadují častý a rychlý přístup k záznamům. Vyhledávání událostí na záznamu se stává nepoužitelným, protože při každém přetočení je potřeba daný kus záznamu stáhnout. Může tak dojít až k několikaminutovému čekání při skoku v záznamu (22). Firmy, které poskytují zabezpečení, jsou navíc lákavým cílem pro hackery, jelikož po získání přístupu k datům takovéto společnosti mohou hackeři získat citlivé informace o firmách a jednotlivcích, kteří využívají tyto služby (29).

Chytré funkce se nebudou omezovat pouze na deep learning, detekci hran a rozpoznávání objektů, ale také bude čím dál běžnější úprava obrazu v reálném

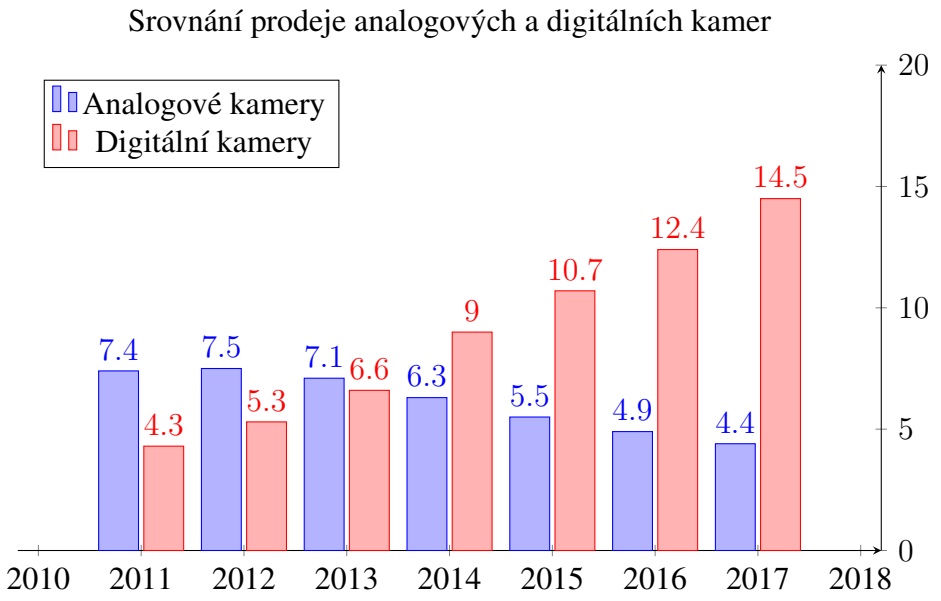
čase. Nvidia uvolnila AI software, který upravuje obraz tak, aby člověk na záznamu vypadal, jako že se dívá přímo do kamery (30). Předpokládané užití je pro video hovory a přímé přenosy, nicméně technologie úpravy záznamu v reálném čase má potenciál dostat se v nějaké podobě i do bezpečnostních kamer.

Další příklad nové technologie s potenciálem pro bezpečnostní kamery byla představena společností Apple v roce 2021. Jejich Center Stage je určena pro video hovory a využívá širokoúhlé kamery. Pokud se člověk na kameře vzdálí od zařízení, Center Stage ho sleduje, neustále zabírá, a upravuje obraz tak, aby ani na kraji nebyl deformovaný.

Obrázek 8: Ukázka opravy deformovaného obrazu pomocí AI (Tech Prolonged, 2019)

Kamerové systémy s podobnou technologií by se mohly zaměřit na důležitou část scény. Například namísto záběru celého obrazu by se kamera mohla sama zaměřit na člověka, který se pohybuje v zakázaném prostoru.

Podle dat z Statista.com klesá prodej analogových kamer ve prospěch digitálních IP bezpečnostních kamer od roku 2012, jak je vidět na grafu 5. Dá se říci, že přestože analogové kamery mají svoje výhody a rozhodně si zaslouží místo na trhu, dlouhodobě budou dále ustupovat digitálním kamerám.



Graf 8: Srovnání prodeje analogových a digitálních kamer, hodnoty v miliardách USD (Statista.com, 2017)

4.4.2 Otázka soukromí a bezpečnosti

Se zdokonalováním kamerových systémů úzce souvisí soukromí a bezpečnost těchto systémů. Tato kapitola se zaměřuje na několik konceptů týkajících se bezpečnosti kamerových systémů.

Existují technologické firmy, jejichž hlavním zdrojem příjmů je prodej dat o uživatelích. Kamerové systémy mají potenciál tento sběr dat rozšířit. Například kamerové systémy s AI v obchodech jsou schopné určit pohlaví, věk a náladu zákazníků, a ukazovat zákazníkům reklamy na základě těchto dat. To vše bez zapojení rozpoznávání obličejů (31).

Rozpoznávání obličejů se používá pro identifikaci osob, například na letištích v některých zemích nebo v totalitních státech pro kontrolu občanů (32). v některých případech se tato technologie využívá k identifikaci občanů na protestech a účastníků nepokojů (33). Velké databáze obličejů mají vlády a provozovatelé internetových služeb jako Meta (Facebook) a nebo Alphabet (Google). v případě úniku dat dojde k nepovolenému přístupu k informacím až milionů lidí.

Dalším důležitým faktorem v oblasti bezpečnosti kamerových systémů je je-

jich správná konfigurace. Na internetu existují veřejně přístupné databáze špatně zabezpečených IP kamer. Případný útočník má možnost sledovat internetové kamery a využívat vyhledávače obličejů pro identifikaci lidí na záznamu (32).

Identifikace pomocí softwarového rozpoznávání obličejů není a pravděpodobně v dohledné době nebude 100% přesná. Několik systémů pro identifikaci obličejů je zaujatých, a kvůli trénovacím datům lépe identifikují bílé muže než ženy, a s lidmi ostatních etnických příslušností mohou dosahovat až 35% chybovosti (34).

Biometrické přihlašování také není bez chyby. Na rozdíl od hesel, kdy by měli uživatelé využívat jedinečná hesla pro každou využívanou službu, biometrické přihlašování je jako používání stejného hesla ke všemu. Navíc, v případě prolomení hesla uživatel jednoduše změní heslo, ale v případě padělání otisku prstu nebo obelstění rozpoznávání obličeje možnost změny identifikačního tokenu neexistuje. Slabé systémy na identifikaci obličeje lze obelstít pouhou fotkou autorizované osoby. I silnější zabezpečení, jako například Windows Hello, lze obejít fotkou, ačkoliv musí být upravena tak, aby jí bez problému nasnímala infračervená kamera, která je součástí identifikačního systému(35).

Existuje několik způsobů, jak oklamat kamery určené pro rozpoznávání obličejů. Mezi ně patří

- oblečení se speciálními vzory
- infračervené diody
- speciální make-up s geometrickými vzory

Kamerové systémy a umělá inteligence má vysoký potenciál užití, zvláště, pokud se obě technologie spojí. Z důvodu možného zneužití je ale třeba přistupovat k těmto technologiím s opatrností.

5 Závěr

Umělá inteligence je nezbytnou součástí moderních kamerových systémů. Díky sofistikovaným algoritmům a rozsáhlým datasetům jsou tyto systémy schopny rozpoznávat a klasifikovat objekty a chování s vysokou přesností a efektivitou. Tento vývoj přináší nejen bezpečnostní výhody, ale také nové možnosti pro sledování a analýzu chování zákazníků a návštěvníků prostorů, což může být pro podnikání velmi užitečné.

Nicméně, jak bylo v této práci popsáno, existují také některé výzvy, které s sebou používání umělé inteligence v kamerových systémech přináší. Patří sem například ochrana soukromí a bezpečnost dat, správné trénování algoritmů a minimalizace falešných poplachů. Tyto výzvy musí být řešeny a řízeny s odpovídajícími protokoly a standardy.

V závěru lze tedy konstatovat, že umělá inteligence je v kamerových systémech nezbytnou součástí, která přináší řadu výhod a nových možností. Je však důležité zajistit, aby byla používána v souladu s etickými zásadami a standardy, a aby byla využívána pro zlepšení života lidí a podnikání jako celek.

6 Seznam použitých zdrojů

1. Russel S a Norvig P. Artificial Intelligence: A Modern Approach (Fourth edition). 978-1-292-40113-3. Pearson, 2022.
2. Camstra F a Vinciarelli A. Machine Learning for Audio, Image and Video Analysis: Theory and Applications (Second Edtion). 978-1-4471-6735-8. Springer, 2015.
3. Fry H. Hello World: Jak zůstat člověkem ve světe algoritmů. Ed. Outrata F. 978-80-7601-246-2. Vyšehrad, 2018.
4. Silva INd. Artificial Neural Networks: A Practical Course. 978-3-319-43162-8. Springer, 2017.
5. IBM: What are neural networks? Dostupné z `www.ibm.com/topics/neural-networks`. [Cit. 4.10.2022]. 2021.
6. Jeremy C. Think Autonomous: Introduction to video processing. Online, dostupné z `https://www.thinkautonomous.ai/blog/computer-vision-from-image-to-video-analysis/`. [Cit. 20.10.2022]. 2020.
7. Bastian M. Nvidia's latest open-source AI generates 3D models from a single 2D image. Mixed-news 2022. Online, dostupné z `mixed-news.com/en/nvidias-latest-open-source-ai-generates-3d-models-from-a-single-2d-image/`. [Cit. 11.11.2022].
8. Klingler N. Video Analytics in Practical AI Applications. viso.ai 2022. Online, dostupné z `viso.ai/computer-vision/video-analytics-ultimate-overview/`. [Cit. 28.10.2022].
9. Fennelly LJ. Effective Physical Security. 9780128044629. Effective Physical Security, 2017.
10. Datta AK, Datta M a Banerjee PK. Face Detection and Recognition: Theory and Practice. 978-1482226546. Chapman a Hall/CRC, 2015.

11. Kuba P. FAQ Zone - What is loitering detection? Anglecam.com 2022. Online, dostupné z https://help.angelcam.com/en/articles/6796438-what-is-loitering-detection. [Cit 4.11.2022].

12. Clearview Communications: People counting technology. Online, dostupné z clearview-communications.com/people-counting-technology-cctv-cameras-video-demonstration/. [Cit. 26.11.2022]. 2020.

13. Nsoft Vision: Understand visitors with heat maps. Online, dostupné z www.nsoft.vision/use-cases/understand-visitors-with-heat-maps. [Cit. 9.11.2022].

14. Smartiple: Poznáváme obsazenost parkovišť. Online, dostupné z smartiple.com/#parkinto. [Cit. 29.10.2023]. 2020.

15. Intenseye: CoreAI Behavioral safety. Online, dostupné z www.intenseye.com/products/core-ai/behavioral-safety. [Cit. 11.11.2022].

16. Intenseye: CoreAI Housekeeping. Online, dostupné z www.intenseye.com/products/core-ai/housekeeping. [Cit. 11.11.2022].

17. Gazzola R. Virtual Fences Using Video Analytics Help Businesses to Protect an Area. Surveillancesecure.com 2021. Online, dostzpné z urveillancesecure.com/virtual-fences-using-video-analytics-help-businesses-to-protect-an-area-from-intrusion/. [Cit. 28.10.2022].

18. Ring security cameras. Online, dostupné z https://eu.ring.com/pages/security-cameras. [Cit 14.1.2023].

19. Dahua DH-IPC-HDW8341X-3D datasheet. Online, dostupné z https://www.dahuasecurity.com/asset/upload/uploads/soft/20190225/DH-IPC-HDW8341X-3D_Datasheet_201902251.pdf. [Cit. 28.2.2023]. 2019.

20. DahuaWiki: Create face database. Online, dostupné z https://dahuawiki.com/images/cache/6/60/AI/Instructions/Create_Face_Database.html. [Cit 14.1.2023].

21. Hikvision: Network Video Recorders. Online, dostupné z https://www.hikvision.com/en/products/IP-Products/Network-Video-Recorders/. [Cit 14.1.2023].

22. Gojda O. Řízený rozhovor. 2023.

23. Discomp: Speciální IP Kamery. Onlie, dostupné z www.discomp.cz/kamery-a-zabezpeceni-ip-kamery-specialni_c15904722.html. [Cit. 4.3.2023].

24. Discomp: IP NVR - záznam. Online, dostupné z www.discomp.cz/kamery-a-zabezpeceni-ip-nvr-zaznam_c7068037.html. [Cit. 4.3.2023].

25. Satom: Ceník instalací. Online, dostupné z www.satom.cz/cenik. [Cit. 4.3.2023].

26. AZ Pohony: Turnikety jako sofistikovaná kontrola vstupů. Online, dostupné z www.azpohony.cz/turnikety/c1218. [Cit. 4.3.2023].

27. Cominfo Security, konzultace s obchodním oddělením. e-mail. 2023.

28. Indeed.cz: Kolik si vydělá pracovník na pozici ostrahy? Online, dostupné z cz.indeed.com/career/pracovnk-ostrahy/salaries. [Cit. 4.3.2023].

29. Thrope J. The rise of Video Surveillance as a Service. International Security Journal 2022. Online, dostupné z internationalsecurityjournal.com/video-surveillance-as-a-service/. [Cit. 29.12.2022].

30. Delgado G. NVIDIA Broadcast 1.4 Adds Eye Contact and Vignette Effects With Virtual Background Enhancements. Nvidia.com 2023. Online, dosupné z www.nvidia.com/en-us/geforce/news/jan-2023-nvidia-broadcast-update/. [Cit. 28.2.2023].

31. Getalfi. Facial Recognition Advertising: The Future is Here. Getalfi 2021. Online, dostupné z www.getalfi.com/advertising/facial-recognition-advertising-future-is-here/. [Cit. 14.1.2023].

32. Fong J. What Facial Recognition Steals From Us. Vox.com 2019. Online, dostupné z www.vox.com/recode/2019/12/10/21003466/facial-recognition-anonymity-explained-video. [Cit. 29.12.2022].

33. Vincent J. FBI Used Factial Recognition to identify a Capitol rioter from his girlfirend's Instagram posts. The Verge 2021. Online, dostupné z www.theverge.com/2021/4/21/22395323/fbi-facial-recognition-us-capital-riots-tracked-down-suspect. [Cit. 29.12.2022].

34. Goode L. Facial recognition software is biased towards white men, researcher finds. The Verge 2018. Online, dostupné z www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error. [Cit. 29.12.2022].

35. Deeg M a Philipp B. Biometricks: Bypassing an Enterprise-Grade Biometric Face Authentication System. online, dostupné z www.syss.de/pentest-blog/2017/syss-2017-027-biometricks-bypassing-an-enterprise-grade-biometric-face-authentication-system/. [Cit 9.12.2022]. 2017.

7 Seznam obrázků, tabulek a grafů

Seznam obrázků

Seznam tabulek

Seznam grafů