

Identifikace osob pomocí kamerového systému

Adam Kubeš

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Adam Kubeš
Osobní číslo: A22226
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Prezenční
Téma práce: Identifikace osob pomocí kamerového systému
Téma práce anglicky: Identification of Individuals Using a Camera System

Zásady pro vypracování

1. Vypracujte literární rešerši zaměřenou na kamerové systémy.
2. Seznamte se s legislativou pro provoz kamerových systémů.
3. Proveďte analýzu trhu zaměřenou na identifikaci osob prostřednictvím kamer.
4. Seznamte se s volně dostupným softwarem pro identifikaci osob.
5. Proveďte identifikaci osob pomocí kamery za různých provozních podmínek a vyhodnoťte spolehlivost systému.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. JANEČKOVÁ, Eva a BARTÍK, Václav. *Kamerové systémy v praxi : právní režim z pohledu ochrany osobních údajů a ochrany osobnosti*. Praha: Linde Praha, 2011. ISBN 9788072018505.
2. DATTA, Asit Kumar; DATTA, Madhura a BANERJEE, Pradipta. *Face detection and recognition : Theory and Practice*. London, New York: CRC Press, 2016. ISBN 9781482226546.
3. KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. Praha: Cricetus, 2006. ISBN 80-902938-2-4.
4. LOVEČEK, Tomáš a NAGY, Peter. *Bezpečnostné systémy: kamerové bezpečnostné systémy*. Žilina: žilinská univerzita, 2008. ISBN 978-80-8070-893-1.
5. LUDĚK, Lukáš. *Bezpečnostní technologie, systémy a management*. II. Zlín: VeRBuM, 2011. ISBN 978-80-87500-19-4.
6. LIBICH, Jan. *Víme, proč máte na fotkách ošklivý šum. Jak pracuje snímací čip v digitálu*. Online. Technet.idnes.cz. 2007. Dostupné z: https://www.idnes.cz/technet/audio-foto-video/vime-proc-mate-na-fotkach-osklivy-sum-jak-pracuje-snimaci-cip-v-digitalu.A070625_094646_tec_foto_jlb. [cit. 2024-10-22].

Vedoucí bakalářské práce: **prof. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **11. prosince 2024**

Termín odevzdání bakalářské práce: **2. června 2025**



doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 11. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....

podpis autora

ABSTRAKT

Bakalářská práce se zaměřuje na identifikaci osob prostřednictvím kamerového systému a jejich následné využití. V práci jsou popsány druhy kamerových systémů a následné zpracování obrazu z kamerových systémů. Pro identifikaci osob je využíván systém Axxon. V praktické části je testována spolehlivost systému při vstupu osob do budovy.

Klíčová slova: Kamerové systémy, Legislativa, Identifikace osob, Software pro rozpoznání obličejů

ABSTRACT

The bachelor's thesis focuses on the identification of persons through a camera system and their subsequent use. The thesis describes the types of camera systems and subsequent image processing from camera systems. The Axxon system is used to identify people. In the practical part, the reliability of the system is tested when people enter the building.

Keywords: Camera systems, Legislation, Identification of persons, Facial detection and recognition software

Na tomto místě bych rád poděkoval mému vedoucímu práce prof. Mgr. Milanu Adámkovi, Ph.D. za vedení mé bakalářské práce a odborné rady při tvorbě práce. Dále bych chtěl poděkovat své bývalé střední škole za možnost realizovat praktickou část na jejich pozemku a použít s jejich souhlasem testovací subjekty ze stejné školy.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 KAMEROVÉ SYSTÉMY.....	13
1.1 ANALOGOVÉ KAMEROVÉ SYSTÉMY	14
1.2 IP KAMEROVÉ SYSTÉMY	15
1.3 HLAVNÍ KOMPONENTY KAMERY	16
1.3.1 Objektiv.....	16
1.3.2 Ohnisková vzdálenost	17
1.3.3 Světelnost	17
1.3.4 Clona	18
1.3.5 Hloubka ostrosti	19
1.3.6 Fotocitlivé prvky	20
1.3.7 CCD senzor	20
1.3.8 CMOS senzor	21
1.3.9 DPS senzory	22
1.4 PŘENOSOVÉ MÉDIUM.....	23
1.5 METALICKÉ PŘENOSOVÉ CESTY.....	23
1.5.1 Koaxiální kabel	24
1.5.2 Kroucená dvojlinka	24
1.5.3 Optické vlákno	26
1.6 ZÁZNAMOVÉ ZAŘÍZENÍ.....	27
1.7 DVR	28
1.8 DVR NA BÁZI PC	28
1.9 NVR	29
1.10 PARAMETRY VIDEOREKORDÉRŮ	30
2 TYPY KAMER.....	31
3 LEGISLATIVA A NORMY.....	33
3.1 KAMEROVÉ SYSTÉMY Z HLEDISKA ZPRACOVÁNÍ OSOBNÍCH ÚDAJŮ	34
3.2 KAMERY SE ZÁZNAMEM VE ŠKOLSTVÍ.....	35
3.2.1 Shrnutí	36
3.3 NORMY	38
4 ZPRACOVÁNÍ OBRAZU	41
4.1 DATABÁZE OSOB	44
5 ROZPOZNÁNÍ OBLIČEJE OSOB.....	45
5.1 NÍZKOÚROVŇOVÁ ANALÝZA	47
5.1.1 Hrany.....	47
5.1.2 Analýza úrovní šedi.....	48

5.1.3	Analýza založená na pohybu	49
5.2	AKTIVNÍ TVAROVÝ MODEL	49
5.2.1	Analýza příznaků	50
5.2.2	Statistické přístupy	52
5.3	METODY ROZPOZNÁVÁNÍ OBLIČEJE	52
5.3.1	Metoda založená na geometrických příznacích	52
5.3.2	Rozpoznávání obličeje na základě podprostorů	53
5.3.3	Rozpoznávání obličeje založené na neuronových sítích	53
5.3.4	Metoda založená na korelaci	54
5.3.5	Přístup pomocí podpůrných vektorových strojů (SVM)	55
5.4	TECHNIKY REKONSTRUKCE OBLIČEJE	55
5.4.1	Třidimenzionální rozpoznávání obličeje	56
5.4.2	Extrakce příznaků	57
5.4.3	Globální extrakce příznaků	58
5.4.4	Třidimenzionální morfovateľný model	58
II	PRAKTICKÁ ČÁST	60
6	SOFTWARE PRO IDENTIFIKACI OSOB	61
6.1	VYBRANÉ SOFTWARE	62
7	DETEKCE OSOB POMOCÍ VYBRANÉHO SOFTWARE	65
7.1	AXXONONE SOFTWARE	65
7.2	POUŽÍVANÉ PRVKY	66
7.3	PROCES NASTAVENÍ A NÁSLEDNÉ DETEKCE	69
7.4	PROVEDENÍ DETEKCE A NÁSLEDNÉ VYHODNOCENÍ	75
7.5	SHRNUTÍ VÝSLEDKŮ	80
	ZÁVĚR	82
	SEZNAM POUŽITÉ LITERATURY	83
	SEZNAM OBRÁZKŮ	87
	SEZNAM TABULEK	89
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	90

ÚVOD

V posledních letech se výrazně zvyšuje poptávka po bezpečnostních systémech, které by zajistily ochranu osob a majetku v různých typech objektů, jako jsou veřejné budovy, školy, komerční prostory či instituce státní správy. Jedním z nejefektivnějších způsobů zvýšení bezpečnosti jsou kamerové systémy, které díky moderním technologiím umožňují nejen sledování prostoru, ale i identifikaci jednotlivých osob. Význam těchto systémů roste v kontextu rostoucích bezpečnostních rizik, kdy je důležité nejen zaznamenat pohyb osob, ale také správně identifikovat konkrétní jedince.

Identifikace osob pomocí kamerových systémů je komplexní proces zahrnující kombinaci hardwaru a softwaru, které spolupracují na zachycení, přenosu a zpracování obrazu. Mezi nejvyužívanější technologie v této oblasti patří rozpoznávání obličeje, které je schopno na základě biometrických údajů určit totožnost osoby. Tento způsob identifikace má své specifické požadavky na kvalitu obrazu, světelné podmínky a konfiguraci kamerového systému.

Moje bakalářská práce se zabývá problematikou identifikace osob prostřednictvím kamerových systémů s využitím softwaru Axxon. V teoretické části je provedena analýza různých typů kamerových systémů, jejich základních komponent, funkcionalit a legislativního rámce, který upravuje použití těchto technologií. Praktická část se zaměřuje na testování systému Axxon při vstupu osob do budovy s cílem ověřit jeho spolehlivost a přesnost v reálných podmínkách. Dále je analyzována účinnost detekce při různých světelných podmínkách a v prostředí s vyšší koncentrací osob.

Cílem této práce je vyhodnotit efektivitu použití kamerového systému Axxon při identifikaci osob. Výsledky mohou přispět k lepšímu porozumění problematice identifikace pomocí kamerových systémů a nabídnout konkrétní doporučení pro praxi.

I TEORETICKÁ ČÁST

1 KAMEROVÉ SYSTÉMY

VSS tedy česky Dohledový videosystém byl dřív známý jako CCTV (v překladu uzavřený televizní okruh). Jedná se o systém kamerového sledování, který přenáší obraz na omezený počet monitorů nebo záznamových zařízení. Jejich přenos tedy není veřejný, nelze k nim přistupovat vzdáleně. Používaným kamerám v tomto systému se říká průmyslová kamera nebo také průmyslová televize. [1]

Základní rozdělení kamer:

Analogové

Digitální (IP)

Hybridní

Funkce kamerových systémů je založena na kombinaci hardwaru a softwaru, které umožňují zaznamenávat, přenášet a ukládat obrazový materiál.

Základní prvky kamerového systému obsahují:

Kamery

Napájení

Přenosové medium

Záznamové zařízení

Zobrazovací zařízení [1]

Kamery byly definovány výše a následně budou více rozebrány. Napájení lze řešit dvěma způsoby. První z nich je pomocí **technologie PoE**, to znamená, že pomocí ethernetového kabelu lze bezpečně přenášet data i napájení. Standardně je dosah napájení do 100 m. Druhý je napájení ze zdroje **AC/DC** o napětí v rozsahu 12 V až 48 V. Přenosová média slouží pro přenos dat z kamer do záznamového nebo monitorovacího zařízení. Výběr vhodného vodiče záleží na požadavcích systému. Existují možnosti buď drátového, nebo bezdrátového řešení. [1]

Základní dělení na:

Metalické vedení

Optické vedení

Radiové vedení

Základní charakteristiky přenosových médií podle toho, co nás při výběru vhodného média zajímá.

Jsou to:

Odolnost vůči EMI

Útlum

Šířka přenosového pásma

Přenosová rychlost

Přenosová kapacita

Přenosový výkon [1]

Záznamové zařízení slouží k ukládání zachycených dat z připojených kamer. Máme na výběr z **DVR, NVR**. [1]

Pro zobrazení záznamu slouží zobrazovací zařízení. Mezi ně se řadí televize, monitory, telefony a třeba plátna. [1]

1.1 Analogové kamerové systémy

Analogové kamerové systémy fungují na základě drátového přenosového média a obvykle poskytují nižší kvalitu obrazu než digitální kamery. Nejčastěji se pro přenos využívá koaxiální kabel zakončený BNC konektorem. Vzdálenost, na kterou lze signál přenášet, je obvykle omezena na přibližně 100 metrů. [1][2]

AHD (Analog High Definition) kamerový systém nahrazuje tradiční analogový přenos obrazu a umožňuje přenos ve vysokém rozlišení prostřednictvím koaxiálního kabelu. AHD technologie umožňuje přenos dat na vzdálenost až 500 metrů. Pro záznam se používají rekordéry s kompresní technologií H.264. Technologie AHD byla představena v roce 2015. Nabízí lepší rozlišení, které je srovnatelné s IP kamerami, avšak je cenově výhodnější a umožňuje instalaci na stávající kabeláž po analogových kamerách. [2][3]

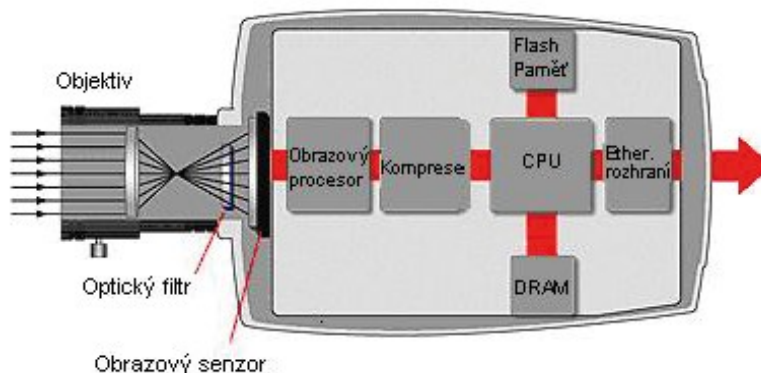


Obrázek 1 Analogová kamera

(zdroj:[4])

1.2 IP kamerové systémy

IP kamerové systémy jsou moderní a flexibilní řešení pro monitorování objektů. Na rozdíl od analogových kamerových systémů používají IP kamerové systémy síťové připojení k přenosu dat přes síťové kabely Ethernet nebo bezdrátově přes Wi-Fi. Mají také vysokou kvalitu obrazu jako analogové kamerové systémy. Vzhledem k připojení na internet lze přistupovat k datům z IP kamerového systému vzdáleně prostřednictvím aplikací nebo webového rozhraní. Jsou dražší než analogové kamerové systémy. [2][5]



Obrázek 2 IP kamera - schéma

(zdroj:[6])

To, co lidské oko vnímá jako obraz, je pro obrazový čip kamery interpretováno jako světlo různých vlnových délek. CCD nebo CMOS čip přeměňuje tento světelný signál na elektrický náboj. Výstup z čipu je analogový signál u CCD nebo digitální signál u CMOS. Před dopadem na čip světlo prochází objektivem, kde dochází k vykreslení scény. MFT (kreslicí funkce) popisují zkreslení obrazu v závislosti na clonových číslech a ohniskových

vzdálenostech objektivu. Mezi objektivem a světlocitlivým čipem je optický filtr, který zajišťuje průchod požadovaných vlnových délek světla, které jsou pro IP kameru potřebné. Po zpracování světelného signálu vzniká digitální signál, který je následně odeslán do obrazového procesoru. Tento procesor se zaměřuje na zpracování signálu v digitální formě, přičemž při úpravách je využíváno lidské vnímání. Díky kompresi je signál zredukován, což slouží k snížení nároků na šířku pásma při přenosu nebo na kapacitu úložišť pro digitální data. Dále přecházíme k specifickým komponentám pro IP kamery, mezi které patří CPU, DRAM a Flash paměť. CPU spolu s operační a Flash pamětí zajišťují komunikaci s okolními zařízeními, přičemž CPU také řídí různé operace v kameře, jako je ovládání a nastavení funkcí. Po zpracování je signál přes Ethernetové rozhraní odeslán do dalších zařízení. [2][7]



Obrázek 3 IP kamera

(zdroj:[8])

1.3 Hlavní komponenty kamery

Hlavními součástmi analogových kamerových systémů jsou objektiv a fotocitlivý senzor. U IP kamer se k těmto komponentám přidává také elektronika. Objektiv, spolu s ovládáním zoomu a clony, tvoří úvodní část kamery, která má za úkol zachytit obraz sledované scény. Za objektivem se nachází fotocitlivý senzor, který obraz převádí do elektrického signálu, což umožňuje jeho digitální zpracování. V IP kamerových systémech probíhá digitalizace dat prostřednictvím mikroprocesoru a elektronických součástek. Tato zařízení zároveň komprimují data, která jsou následně ukládána na úložiště, přenášena do záznamových zařízení nebo zobrazovacích systémů. [1] [9]

1.3.1 Objektiv

Objektiv je tvořen několika čočkami a dalšími prvky uspořádanými podél optické osy. Během ostření nebo zoomování se jednotlivé části pohybují tak, aby vytvořily požadovaný

obraz. Jeho hlavní funkcí je promítnout zmenšený obraz sledované scény na povrch fotocitlivého snímače kamery. Mezi zásadní vlastnosti objektivu patří ohnisková vzdálenost, světelnost, clona a hloubka ostroty. [1][2][9]

1.3.2 Ohnisková vzdálenost

Ohnisková vzdálenost, často označovaná jako focus, je definována jako vzdálenost od optického středu objektivu k rovině snímáče, kde se ostře zobrazují objekty ve velmi vzdálených (nekonečných) polohách. Tato vzdálenost ovlivňuje šířku a úhel záběru – obecně platí, že kratší ohnisková vzdálenost poskytuje širší úhel záběru. Pozorovací úhly snímané scény se určují na základě kombinace délky ohniskové vzdálenosti a typu použitého snímáče. [1][2]

U některých objektivů lze ohniskovou vzdálenost plynule měnit pomocí transfokátoru. Podle možnosti úpravy ohniskové vzdálenosti se objektivy rozdělují do tří kategorií. Objektivy s pevnou ohniskovou vzdáleností mají tuto hodnotu nastavenou výrobcem a není možné ji měnit. Objektivy s proměnnou ohniskovou vzdáleností umožňují manuální nastavení otáčením části objektivu. Třetí kategorií jsou objektivy s elektronickým ovládáním změny ohniska, kde se nastavení provádí prostřednictvím motoru. [1][2][10]



Obrázek 4 Ohnisková vzdálenost u objektivu

(zdroj:[11])

1.3.3 Světelnost

Světelnost objektivu vyjadřuje jeho maximální schopnost propouštět světlo. Platí, že čím nižší je hodnota světelnosti (označovaná clonovým číslem F), tím více světla objektiv

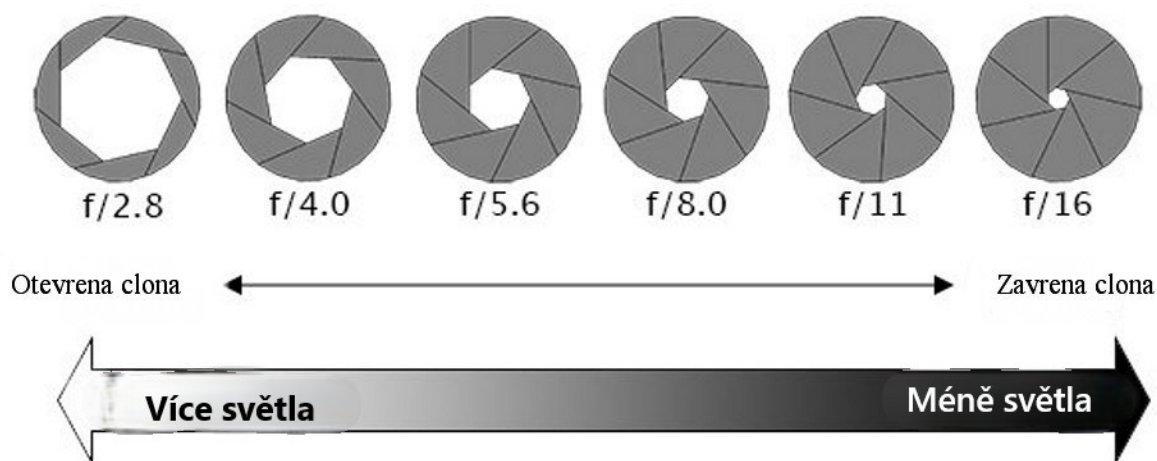
dokáže zachytit. Nejmenší clonové číslo F udává maximální světelnost objektivu a je obvykle uvedeno v technické dokumentaci. Vyšší světelnost (nižší hodnota F) umožňuje zkrátit dobu expozice, což snižuje riziko rozmazání snímku při fotografování pohybujících se objektů nebo za slabého osvětlení. [2]

1.3.4 Clona

Clona slouží k regulaci množství světla procházejícího objektivem a dopadajícího na fotocitlivý snímač. Tento mechanický prvek je tvořen kovovými lamelami, které vytvářejí nastavitelný otvor pro průchod světla. Velikost clony přímo ovlivňuje rozlišovací schopnost objektivu, tedy jeho schopnost vykreslit detaily snímané scény. Zavíráním clony se zpočátku zlepšuje kvalita obrazu, avšak při příliš malém otevření dochází k jejímu zhoršení.

Clonové číslo (f) představuje poměr ohniskové vzdálenosti k průměru otvoru clony. Nižší clonové číslo znamená menší světelné ztráty a vyšší kvalitu objektivu. Hodnoty clonového čísla odpovídají geometrické řadě: 1; 1,4; 2; 2,8; 4; 5,6; 8; 11; 16; 22; 32.

Podle způsobu ovládání se clony dělí na tři typy. Objektivy s pevnou clonou mají hodnotu clony pevně nastavenou výrobcem. U objektivů s manuálním ovládáním může uživatel clonu nastavovat podle svých potřeb. Třetí variantou jsou objektivy s automatickým ovládáním clony, kde je její nastavení řízeno elektronikou a servomechanismem. [1][2][10]



Obrázek 5 Clona objektivu

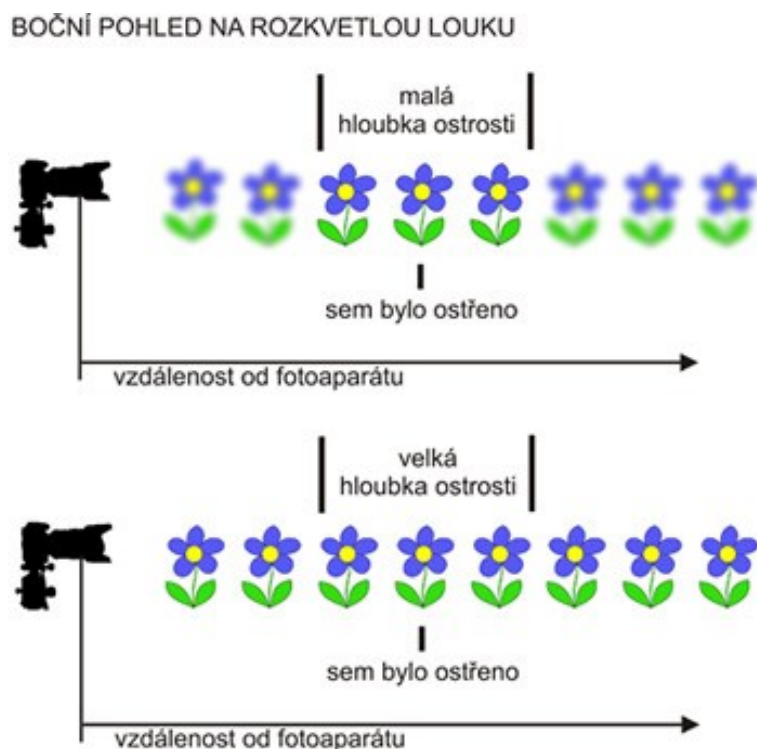
(zdroj:[12])

1.3.5 Hloubka ostrosti

Hloubka ostrosti (DOF) označuje oblast před a za zaostřeným bodem, ve které jsou objekty zobrazeny jako ostré, přestože dochází k určité ztrátě detailů. Tento rozsah je subjektivní, protože mezi ostrým a neostrým zobrazením neexistuje přesná hranice. Hloubka ostrosti je výrazně ovlivněna hodnotou clony – vyšší clonové číslo zvětšuje hloubku ostrosti, zatímco nižší clonové číslo ji zmenšuje.

Mezi faktory, které ovlivňují hloubku ostrosti, patří:

- **Clona objektivu:** užší clona (vyšší clonové číslo) zvyšuje hloubku ostrosti
- **Vzdálenost fotografovaného objektu:** čím větší je vzdálenost, tím větší je hloubka ostrosti
- **Ohnisková vzdálenost:** delší ohnisková vzdálenost zmenšuje hloubku ostrosti
- **Velikost optického snímáče:** větší snímáče mají menší hloubku ostrosti při stejném nastavení než menší snímáče [2]



Obrázek 6 Hloubka ostrosti – příklad

(zdroj:[13])

1.3.6 Fotocitlivé prvky

Fotocitlivé prvky tvoří základ optických a zobrazovacích zařízení, protože reagují na dopadající světlo a přeměňují jeho energii na elektrický signál. Světlo procházející objektivem kamery se pomocí systému čoček soustředí na snímací čip. Na tomto čipu fotocitlivé prvky převádějí světlo na elektrický proud, který je následně zpracován elektronikou kamery na analogový nebo digitální obraz. Ten lze dále upravovat nebo přenášet.

V praxi existuje několik typů fotocitlivých prvků, přičemž mezi nejčastěji používané patří CCD senzory, Super CCD senzory, CMOS senzory a DPS senzory. Každý typ se liší svými konstrukčními principy, výrobními technologiemi a vlastnostmi, což zásadně ovlivňuje technické parametry a možnosti výsledných kamer.

1.3.7 CCD senzor

Objektiv promítá zmenšený obraz sledované scény na plochu snímacího prvku CCD. Tento prvek je tvořen světlocitlivými buňkami, které díky fotoelektrickému jevu přeměňují dopadající světelné záření na elektrický signál. Struktura CCD snímáče je tvořena množstvím snímacích buněk (pixelů) uspořádaných do pravidelné mřížky, přičemž CCD je polovodičová součástka. [9]

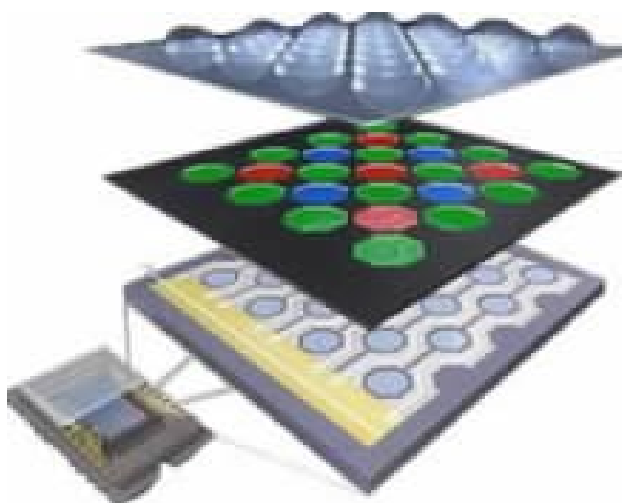
Světlo ve formě fotonů dopadá na křemíkovou destičku, kde se ukládá jako elektrický náboj v potenciálových jámách. Tyto jámy umožňují volný pohyb uvolněných elektronů, čímž dochází k akumulaci náboje. Každá potenciálová jáma odpovídá jednomu pixelu CCD senzoru. Množství zachyceného náboje je ovlivněno intenzitou dopadajícího světla a délkou expozice čipu světlu. [9]

V CCD snímáči se náboj z jednotlivých buněk postupně posouvá směrem k okraji snímáče, kde jej posuvný registr přenáší do zesilovače a následně do A/D převodníku. Informace o barvě se získává pomocí barevných RGB filtrů umístěných před jednotlivými snímacími buňkami. Tyto filtry umožňují zachycení barevné informace potřebné pro výsledný obraz. [1][2][9][10]

Super CCD je typ CCD technologie, která vychází z poznatku, že lidské oko citlivěji vnímá vertikální a horizontální linie než diagonální. Proto je u Super CCD senzorů struktura oproti tradičnímu řešení posunutá o 45°. Světlocitlivé buňky mají tvar osmiúhelníku místo klasického čtverce. Tento tvar zajišťuje efektivní pokrytí plochy a zjednodušuje interpolaci

pixelů. Díky této inovaci je senzor citlivější, má širší dynamický rozsah a rychlejší načítání dat, což umožňuje pořizování snímků při rychlosti až 30 snímků za sekundu ve vysokém rozlišení. Senzory samy o sobě neodlišují barvy světla, pouze registrují jeho intenzitu, nikoliv vlnovou délku, která by určovala barvu. Při tvorbě barevného obrazu se vychází z principu aditivního míchání základních barev RGB, inspirovaného fyziologickým vnímáním barev lidským okem. [1][2][9][10]

Pomocí CCD senzorů lze zaznamenat barevný obraz dvěma způsoby. Prvním je použití tří samostatných CCD snímačů, přičemž každý snímač je vybaven barevným filtrem pro jednu ze základních barev RGB. Druhým způsobem je umístění barevných filtrů na jednotlivé buňky jednoho CCD snímače v šachovnicovém vzoru. V současnosti se pro barevné filtry využívají dvě komplementární trojice barev, a to RGB (červená, zelená, modrá) a CMY (azurová, purpurová, žlutá). [1][2][9][10]



Obrázek 7 Super CCD

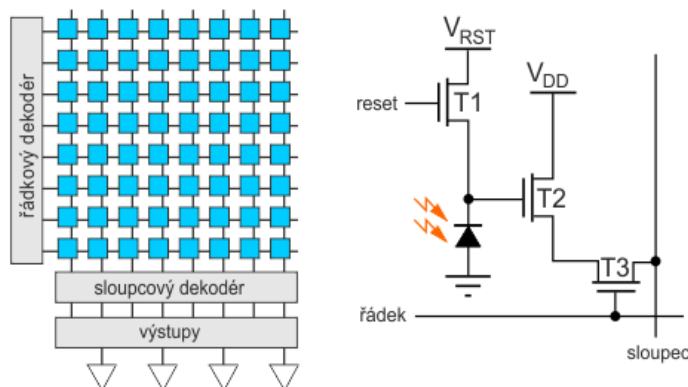
(zdroj:[14])

1.3.8 CMOS senzor

CMOS senzor je tvořen pravidelně uspořádanými snímacími buňkami, které jsou citlivé na dopadající světlo. Technologie výroby CMOS senzorů je složitější než u CCD senzorů, ale výrobně levnější, protože se využívá stejný výrobní proces jako u běžných integrovaných obvodů. CMOS snímač umožňuje vyšší hustotu prvků na čipu. Obvody pro zpracování obrazu, včetně A/D převodníku a zesilovače, jsou integrovány přímo v CMOS čipu. Každá buňka obsahuje vlastní elektronické obvody pro digitalizaci obrazu, což znamená, že digitalizace probíhá u každé buňky zvlášť. Tento způsob konstrukce zkracuje dobu čtení

obrazu z čipu a snižuje spotřebu energie. CMOS senzor poskytuje již zpracovaný digitální signál, což zjednodušuje konstrukci kamery. [1][2][9][10]

Princip fungování CMOS snímače lze přiblížit na základě aktivního třítranzistorového zapojení. Proces vyčítání pixelů probíhá postupně, pixel po pixelu, za pomoci řádkového a sloupcového dekodéru. Obraz zachycený senzorem je postupně načítán a následně zpracováván v příslušných obvodech, přičemž zpracování probíhá na frekvencích od jednotek až stovek megahertzů, což odpovídá času na pixel v řádu mikrosekund až nanosekund. Každý pixel je tvořen několika tranzistory a fotodiodou, která mění světelný signál na elektrický. Dopadající světlo generuje na fotodiodě náboj, který lze změřit a určit intenzitu osvětlení daného pixelu. Dále následuje tranzistor T2, jehož úkolem je zesílit signál z diody. Tranzistor T3 slouží k identifikaci konkrétního pixelu. Pokud je aktivní řádkový signál, lze detekovat proud na sloupcovém výběru a vyčíst informaci o jednom pixelu. Před zachycením další fotografie je nutné všechny pixely vrátit do výchozího stavu, což znamená vynulování signálu na diodách. Tento reset provádí tranzistor T1. [1][2][9][10]



Obrázek 8 Princip CMOS snímače

(zdroj:[15])

1.3.9 DPS senzory

DPS je revoluční technologie, která poskytuje jeden z nejkvalitnějších obrazů mezi současnými technologiemi. Vylepšené snímání a následná digitalizace zobrazených bodů zajišťují dokonalou reprodukci barev při vyšším dynamickém rozsahu. Tento zvýšený dynamický rozsah zlepšuje kvalitu obrazu u scén s extrémně světlými nebo tmavými oblastmi. Tato vlastnost je zvláště výhodná pro bezpečnostní kamerové systémy, které musí snímat špatně osvětlená místa. Technologie využívá multisnímání (Multi-Sample technology) ke zvýšení množství informací, což vede k vyšší kvalitě obrazu. Každý bod je

nezávisle snímán několikrát pro jeden snímek, aniž by došlo k jakékoli ztrátě informací. Systém obrazu určí optimální čas pro snímání a uloží informaci o snímaném bodě ještě před jeho saturací. [2]

1.4 Přenosové médium

V aplikacích monitorování objektů, kde je často velká vzdálenost mezi kamerou a zařízením pro zpracování videosignálu s monitorem, je potřeba efektivně přenášet videosignál. K dispozici jsou různé možnosti přenosu, včetně metalických okruhů, které jsou běžně používány. V některých speciálních případech je možné využít také bezdrátový přenos videosignálu nebo přenos po optických vláknech, což umožňuje pokrytí větších vzdáleností s vysokou kvalitou signálu.

Rozhodnutí pro každý druh přenosu závisí na těchto aspektech:

- počtu kamer
- vzdálenosti jednotlivých komponentů videosystému
- ekonomickém porovnání náročnosti jednotlivých variant
- druhu a vlivu prostředí, v němž je videosystém nasazován [1]

1.5 Metalické přenosové cesty

Přenosové médium využívající metalické vodiče lze zjednodušeně považovat za homogenní vedení, kde jsou elektrické parametry rovnoměrně rozloženy, což znamená, že ve všech bodech vedení mají stejné elektrické vlastnosti. Mezi primární parametry tohoto vedení patří odpor, indukčnost, kapacita a vodivost, které závisí na frekvenci přenášeného signálu, použitém materiálu a konstrukci vedení. Tyto veličiny se obvykle vyjadřují na 1 km vedení. Sekundární parametry homogenního vedení zahrnují měrnou vlnovou míru přenosu, jejíž reálná část, nazývaná "měrný vlnový útlum", vyjadřuje, jak moc se zmenší výkon signálu při jeho průchodu kabelem jednotkové délky, a měří se v dB/m. Imaginární část měrné vlnové míry přenosu se nazývá měrný fázový posuv a udává se v jednotkách rad/km. Tento posuv vyjadřuje zpoždění fáze šířící se vlny na jednotku délky vedení a jeho hodnota závisí na typu a specifických parametrech vedení. [1]

1.5.1 Koaxiální kabel

Tento typ pasivního asymetrického přenosového média se skládá ze dvou vodičů, přičemž jeden je označován jako středový vodič a druhý tvoří izolační vrstvu kolem prvního vodiče. Celý kabel je následně obalen plastem z vnější strany. Vnitřní vodič je obvykle vyroben z mědi, může být i postříbřený a může být buď plný, nebo splétaný. Průměr tohoto vodiče je klíčovým faktorem, který ovlivňuje útlum. Prostor kolem vnitřního vodiče je vyplněn dielektrikem, které je často tvořeno upraveným polyethylenem nebo teflonem. Foliové stínění, které není součástí všech typů koaxiálních kabelů, je umístěno kolem dielektrika a bývá pod vodivým opletením, které tvoří vnější vodič. Toto stínění je tvořeno splétaným měděným vodičem a jeho hlavním úkolem je chránit středový vodič před vnějším elektromagnetickým polem, přičemž může také sloužit jako zemnění pro vnitřní vodič. [1]

U koaxiálního kabelu dochází k přenosu signálu ve formě rozdílu napětí mezi středním vodičem a stíněním, přičemž stínění je připojeno k zemi (kostře zařízení) a má nulovou hodnotu napětí. Tento typ kabelu umožňuje přenos stejnosměrného proudu, filtraci nízkofrekvenčních signálů, ale jeho nejčastější funkcí je přenos elektromagnetického vlnění o vysoké frekvenci. Velkou výhodou koaxiálního kabelu je jeho vysoká elektromagnetická kompatibilita (EMS) a velmi nízká elektromagnetická interference (EMI). Tento kabel je jednoduše použitelný k přenosu nejen hlasu, ale i videa. [1]



Obrázek 9 Koaxiální kabel

(zdroj:[16])

1.5.2 Kroucená dvojlinka

Tento druh metalického vedení je tvořen párem, resp. několika páry vodičů, které jsou po celé své délce pravidelným způsobem zkrouceny a následně jsou pravidelně obtočeny i

jednotlivé páry v daném vedení. Nutnost zkroucení vodičů je důležitá, protože souběžné vodiče se chovají jako anténa, čímž by docházelo k vyzařování elektromagnetického vlnění v okolí vedení, a právě zkroucením je tento efekt výrazně snížen. Obtočením vodičů v páru jsou minimalizovány přeslechy, tzv. EMI a ztráty způsobené kapacitním odporem. Je nutné dodržet pravidelné a dimenzované kroucení vodičů, a to nejběžněji 1x každých 7,5 až 10 cm. Vodiče jsou obvykle vyrobeny z mědi, mohou být plné nebo splétané a počet párů je různý (2, 4, 6, 8, 25, 50, 100), pro síťové aplikace jsou použity 2 páry (Ethernet 10 Mb/s a 100 Mb/s) nebo 4 páry (Ethernet 1 Gb/s a 10 Gb/s), dielektrikum obalující vodiče je nejčastěji polyetylen. Kroucená dvojlinka se používá při tzv. symetrickém vedení signálu, což znamená, že jsou si oba vodiče rovnocenné a signál je vyjádřen rozdílem potenciálů obou vodičů. Každý pár vodičů má fóliové stínění a taktéž splétané nebo fóliové stínění se nachází kolem všech párů. Vnější plášť je z PVC. [1]

Základní kategorizace kroucené dvojlinky se provádí podle způsobu stínění, přičemž rozlišujeme tři základní typy:

Nestíněné (UTP)

Stíněné (ScTP/FTP)

UTP – nestíněný kabel z nestíněných kroucených párů

ScTP/FTP – kroucená dvojlinka se stínící fólií po povrchu kabelu, jedinou pro všechny páry dohromady

STP – oplétaný a fólií stíněný kabel s fóliovými stíněními jednotlivých kroucených párů [1]

Výhoda kroucené dvojlinky je zejména snadné napojení jednotlivých zařízení, nízká cena a v případě kabelu S/FTP jeho velmi dobrá EMS a nízké EMI. Nevýhodou kroucené dvojlinky je v případě již zmiňovaného S/FTP kabelu její tloušťka, a z toho důvodu se s ním obtížně pracuje. UTP má horší EMS než koaxiální kabel a současně UTP signály nemohou být bez regenerace přenášeny na větší vzdálenost. [1]

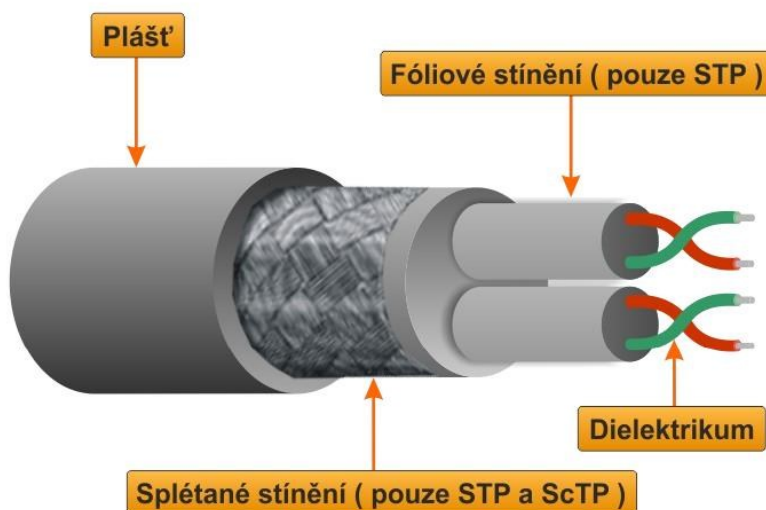
Klasifikace kabelů Twisted Pair, ze které jsem vybral ty vhodné k využití pro kamerové systémy:

Kategorie 5: Pracuje v šířce pásma do 100 MHz. Rozvody pro počítačové sítě s přenosovou rychlostí 100 Mbit/s, resp. 1 Gbit/s v případě využití všech 8 vláken. V současné době nahrazena kategorií 5E.

Kategorie 5E: Pracuje rovněž v šířce pásma do 100 MHz, avšak vyžaduje nové způsoby měření parametrů a v některých parametrech je přísnější. Cílem je provozovat 1 Gbit/s.

Kategorie 6: Pracuje s šířkou pásma 250 MHz. Využívá se pro ultrarychlé páteřní aplikace v oblasti lokálních sítí. V současné době nejpopulárnější kabeláž pro nově budované rozvody.

Kategorie 6A: Pracuje s šířkou pásma 500 MHz. Používá se pro zvláště rychlé páteřní aplikace v oblasti lokálních sítí. Využívá se pro 10 Gbit/s. [1]



Obrázek 10 Kroucená dvojlinka

(zdroj:[17])

1.5.3 Optické vlákno

Přenos pomocí optických vláken umožňuje sdílení informací s menšími ztrátami na delší vzdálenosti a při vyšších přenosových rychlostech dat než jiné formy komunikace, a to rychlostí až 16 Tb/s/100 km. Přenos informace je v tomto případě zprostředkován světelným paprskem, tedy prostřednictvím kvant záření – fotonů. Z toho důvodu jsou optická vlákna zcela imunní vůči EMI působení sousedících elektrických záření. Použití optických kabelů zaručuje úplnou odolnost přenášeného signálu vůči zkreslení způsobenému atmosférickými podmínkami. Kvalitu signálu také neovlivňuje vzdálenost. [1]

Samotné optické vedení je tvořeno pomocí souboru optických vláken seskupených do optického kabelu, kterým lze přenášet světelný signál až do vzdálenosti 100 km bez

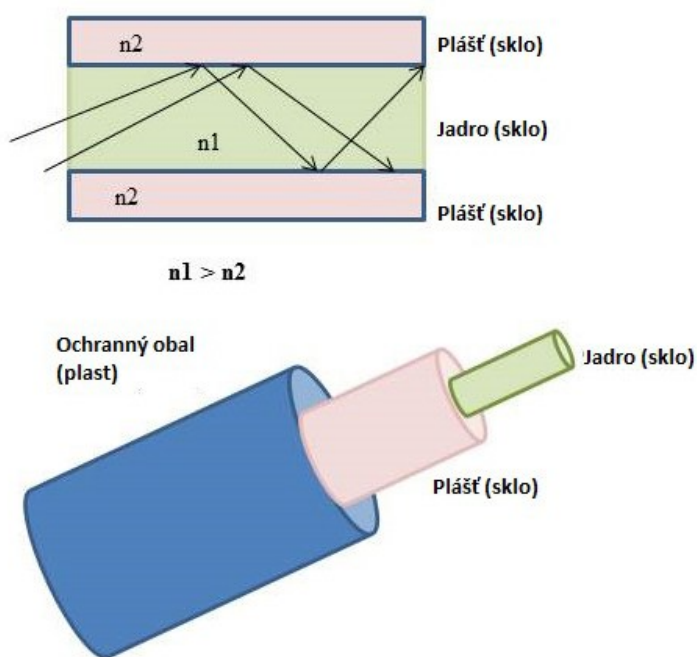
potřebného zesílení signálu na přenosové trase díky malému útlumu signálu na vláknech. Data lze přenášet vysokou rychlostí, až 100 Gb/s na jedné vlnové délce. [1]

Rozlišujeme dva typy:

Jednovlákno (SMF) – delší vzdálenosti, malé ztráty

Mnohavlákno (MMF) – kratší vzdálenosti do 0,5 km

Obecně lze říci, že ve srovnání s metalickými vodiči vykazují optická vlákna kromě již zmíněných vlastností (minimální útlum signálu, velký dosah, velká šířka přenosového pásma, vysoké rychlosti přenosu, nízká hmotnost, vysoká ohebnost) také odolnost vůči přeslechům a vyzařování, jsou chemicky odolné, teplotně stabilní a jsou relativně bezpečné vůči odposlechu. Nevýhody optických vláken jsou komplikovanější spojování jednotlivých vláken, omezenost v ohybu, zvyšování křehkosti v nižších teplotách. [1]



Obrázek 11 Optické vlákno

(zdroj:[18])

1.6 Záznamové zařízení

Zařízení pro ukládání dat slouží k ukládání zachyceného obrazu z připojených kamer pro další použití nebo jen k archivaci dat. V dnešní době existuje mnoho různých druhů záznamových zařízení dle komunikačního signálu, jednotlivé typy jsou popsány dále. [1]

1.7 DVR

DVR neboli videorekordér slouží k záznamu, přehrávání a ukládání signálu z připojených kamer. Obrazový záznam se dále ukládá na pevný disk nebo jiné interní nebo externí záznamové zařízení. Před vytvořením záznamu videorekordér transformuje analogový signál na digitální, probíhá komprimace dat a pak probíhá záznam a přenos videosignálu. Kvalita a cena záznamového zařízení záleží na kvalitě komprese obrazového signálu. [1]

Velmi důležitou vlastností je samotná kompatibilita kamer s videorekordérem, kamery musí mít stejný standard jako videorekordér, např. ONVIF, PSIA atd. Jedním z nejrozšířenějších standardů je již dříve zmíněný ONVIF, který obsahuje ovladače pro kompatibilitu mezi různými zařízeními jako IP kamery, videorekordéry a ostatní zařízení pro ovládání. [1]

Důležitými parametry DVR jsou délka záznamu, datový tok, zálohování napájení, zálohování dat, export dat nebo integrace s ostatními systémy. [1]



Obrázek 12 Ukázka DVR

(zdroj:[19])

1.8 DVR na bázi PC

K záznamu videosignálu lze použít i běžný osobní počítač, který musí obsahovat sběrnici, k níž lze připojit kamery. V případě síťových kamer je nutný síťový konektor RJ-45 a v případě analogových kamer je zapotřebí speciální PCI kartu se vstupy a obvody pro digitalizaci analogového videa se záznamem na pevný disk počítače. Takové systémy

většinou běží na operačním systému Windows a kvalita kamerového systému záleží na vhodném softwaru nainstalovaném v PC pro jeho správu. Speciální software provádí všechny základní funkce jako vyhledávání, přehrávání, logování událostí, šifrování záznamu. K základní instalaci lze jednoduše přidávat rozšiřující moduly jako například inteligentní video analýzy, rozpoznávání dopravních značek, počítání osob, rozpoznání obličeje, rozpoznávání směru pohybu, detekce zanechaného předmětu atd. [1]

1.9 NVR

Síťový videorekordér pracuje jako normální síťový disk, který zpracovává, uchovává a umožňuje přehrávání dat z kamer ve formě záznamu. Některé modely disponují i dodatečnými inteligentními funkcemi. Některé modely využívají inteligentní funkce kamer, což například znamená decentralizovaný výpočetní výkon, kdy se data zpracovávají přímo na jednotlivých kamerách a videorekordér pouze udává pokyny a ukládá záznam.

Každý síťový videorekordér musí obsahovat konektor, pomocí kterého je zařízení připojeno do sítě. Nejčastěji se používá metalické vedení, konkrétně konektor RJ-45. Časté provedení videorekordéru obsahuje hned několik nezávislých konektorů RJ-45, většinou jejich počet je druhou mocninou: 4, 8, 16, 32 nebo 64. Výhodou vícekanálových zařízení je přenosová kapacita a také možnost interního napájení připojených kamer. Tento způsob se nazývá PoE, kdy je polovina vodičů vyhrazena pro napájení ke kameře. [1]



Obrázek 13 Ukázka NVR

(zdroj:[20])

1.10 Parametry videorekordérů

Kompresa videa – udává, který kodek je použitý pro kompresi videa, z čehož vychází i kompresní poměr. Mezi nejzákladnější patří kodeky H.265 / H.264+ / H.264 / MJPEG.

Počet spravovaných kamer – maximální počet připojitelných kamer k danému videorekordéru. Klasicky se jako hranice počtu kamer udávají mocniny dvou: jako 8, 16 nebo 32 kamer.

Rozlišení kamer – maximální rozlišení kamer, které lze zpracovat pomocí daného videorekordéru. Udává se v megapixelech, např. 8.0 Mpix (4K).

Rozlišení na monitor – maximální rozlišení, který daný videorekordér dokáže zobrazit na zobrazovacím monitoru. Typicky se jedná o hodnoty 3840x2160 px, 1920x1080 px, 1280x1024 px, 1280x720 px, 1024x768 px.

Počet RJ-45 portů – udává celkový počet RJ-45 portů, které lze na daném zařízení využít.

Seznam podporovaných protokolů – výpis protokolů, prostřednictvím kterých dokáže systém externě komunikovat: HTTP, TCP/IP, IPv4, IPv6, DHCP, DNS, ONVIF T/S/G, FTP.

Vnitřní úložiště – udává počet volných slotů pro umístění interních disků různých formátů. Společně s počtem je taky uváděna maximální velikost diskového pole. Typicky se udává: 2x SATA HDD, maximální kapacita 10 TB na jeden HDD.

Video nahrávání – udává všechny velikosti videosignálu, které dokáže zařízení zpracovat. Typicky se jedná o hodnoty: 8.0 Mpix, 6.0 Mpix, 5.0 Mpix, 4.0 Mpix, 3.0 Mpix, 1080p, 1.3 Mpix, 720p.

Vstupy a výstupy – počet vstupů a výstupů, které se nacházejí na zadní straně videorekordéru. Např. video výstup 1x HDMI, 1x VGA, počet USB portů.

Ostatní funkce – funkce systému, které jsou defaultně k dispozici. Např. nahrávání, detekce pohybu, zakrytí kamery, odpojení sítě, ztráta videa, chyba HDD. [1]

2 TYPY KAMER

Existuje hodně druhů kamer a není důležité, jestli jsou to analogové nebo IP. Jsou i různá provedení, ve kterých se kamery vyrábějí a lze je použít dle daných možností naší instalace.

Pro analogové kamery jsou nejčastěji využívány typy Bullet a Turret. Analogové kamerové systémy jsou postupně nahrazovány IP kamerovými systémy. Hlavní faktory jsou lepší kvalita obrazu, flexibilita, pokročilé funkce a snadnější instalace.

IP kamery nabízejí alternativu k analogovým kamerám a jsou častěji instalovány. Existují i různé úpravy, které slouží k detekci obličeje nebo SPZ, ale ty sem nezahrnuji. Ve své práci k detekci obličeje použiji software.

Nabízejí větší konstrukční provedení:

1. **Box** – nejstarší provedení, vnější i vnitřní použití, nutnost krytu pro venkovní použití
2. **Dome** – polokulovitý tvar, krytí IP 67, venkovní i vnitřní, možný vznik problémů způsobených vnějšími klimatickými vlivy → nižší viditelnost kamery kvůli odrazu světla ve dne a v nočních hodinách přísvitem
3. **Bullet** – venkovní použití, IR přísvit, krytí IP 67, pevná nebo nastavitelná clona, instalace na vnější stěny nebo stropy budov
4. **Turret** – kompromis mezi Bullet a Dome, vnější i vnitřní využití
5. **Cube** – vnitřní využití, WiFi rozhraní, SD paměť slot
6. **Panoramatické** – díky více obrazovým snímačům lze pozorovat 360° pohled v jednom streamu, možnost integrované PTZ, vnitřní i vnější využití
7. **PTZ** – Pan Tilt Zoom, pohyb objektivu v jednotlivých osách, venkovní i vnitřní prostory [1]



Obrázek 14 Ukázka kamer: vlevo kamera Box, vpravo kamera Dome

(zdroj:[21][22])



Obrázek 15 Ukázka kamer: vlevo Bullet kamera, vpravo Turret kamera

(zdroj:[23][24])



Obrázek 16 Ukázka kamer: vlevo Cube kamera, vpravo panoramatická kamera

(zdroj:[25][26])



Obrázek 17 Ukázka kamery: PTZ kamera

(zdroj:[27])

3 LEGISLATIVA A NORMY

V současné době se stalo obvyklým instalovat kamerové systémy na všech možných místech, většinou jako prostředek k zajištění bezpečnosti osob a ochrany majetku. [28]

Z namátkové analýzy hlavních aplikací vyplývá, že kamerové sledování může sloužit řadě různých účelů, které lze seskupit do několika hlavních kategorií:

- 1) ochrana jednotlivců,
- 2) ochrana majetku,
- 3) veřejný zájem,
- 4) odhalování, prevence a stíhání trestné činnosti,
- 5) získávání důkazů,
- 6) jiné legitimní zájmy. [28]

Při pořizování VSS představuje systém skládající se z kamerového vybavení, úložiště a doplňujících zařízení pro účely přenosu obrazu a vzdálenému ovládání. Při provozování VSS systému, dříve CCTV systému, je nutné respektovat ochranu osobních údajů v souladu s platnou legislativou. Tato problematika byla v ČR v letech 2000 až 2019 upravena zákonem č.101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů. Zákon č.101/2000 Sb. vycházel ze zaručeného práva Listinou základních práv a svobod na ochranu občana před zasahováním do jeho soukromí neoprávněným shromažďováním, zveřejňováním, popř. jiným zneužíváním osobních údajů. Dle § 2 zákona č.101.2000 Sb. byl zřízen Úřad pro ochranu osobních údajů se sídlem v Praze (ÚOOÚ), jehož hlavním úkolem bylo provádět činnost dozorového orgánu pro oblast ochrany osobních údajů. [28]

Pro provoz kamerových systémů vydal ÚOOÚ Stanovisko č. 1/2006, které vymezovalo povinnost práva provozovatele kamerových systémů. Stanovisko ÚOOÚ jednoznačně umožňovalo vyvodit tyto závěry:

1. Za zpracování osobních údajů bylo provozování kamerového systému považováno v případě, byl-li:
 - kromě sledování kamerovým systémem prováděn i záznam pořizovaných záběrů
 - uchovávaná informace v záznamovém zařízení pořizována za účelem jednoznačné identifikace fyzické osoby v souvislosti s určitým jednáním

2. Osobní údaje (obrazové, zvukové) byly uchovány v záznamovém zařízení za předpokladu, že šlo na jejich základě identifikovat (přímo/nepřímo) konkrétní fyzickou osobu.
3. Použití kamerového systému bylo možné i bez souhlasu subjektu údajů (zaznamenané fyzické osoby) dle § 5 odst. 2 písm. e) zákona o ochraně osobních údajů. [28]

Výklad zákona č.101/2000 Sb. a stanovisek vydaných ÚOOÚ bylo možné v rámci problematiky VSS se záznamem shrnout do následujících **povinností správce**:

1. **Provést registraci u ÚOOÚ dle zákona o ochraně osobních údajů.**
 2. **Informovat subjekty o účelu a rozsahu sledování a o způsobu zpracování záznamu.**
 3. **Uchovávat pořízené záznamy jen po dobu nezbytně nutnou.**
 4. **Zabezpečit kamerový systém, vyvarovat se nadměrnému zásahu do soukromí.**
- [28]

Dne 25.5.2018 vešlo v platnost Obecné nařízení o ochraně osobních údajů (GDPR – General Data Protection Regulation). Toto nařízení zásadně změnilo pohled na ochranu osobních údajů. Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů byl v 24.4 2019 zrušen a nahrazen Zákonem č 110/2019 Sb. Zákon o zpracování osobních údajů. V souladu s aktuálně platnou legislativou není třeba dohledový videosystém registrovat u ÚOOÚ. Provozovatel dohledového videosystému má povinnost vést záznamy o činnostech zpracování. Tato povinnost ovšem není úplně nová, záznamy fakticky nahrazují dosavadní registrační formuláře, na rozdíl od dosavadní registrace však tyto záznamy již správce pouze uchovává a nezasílá je již Úřadu pro ochranu osobních údajů. [28]

3.1 Kamerové systémy z hlediska zpracování osobních údajů

Jen málokdo si plně uvědomuje, že pokud je kamerový systém vybaven zařízením pro záznam, tedy kamerovým systémem se záznamem, jedná se o zpracování osobních údajů, což s sebou přináší určité právní důsledky. Provozování takového systému je považováno za zpracování osobních údajů, pokud vedle samotného sledování kamerami dochází i k pořizování záznamů, nebo jsou v záznamovém zařízení uchovávány informace, které mohou sloužit k identifikaci fyzických osob v souvislosti s jejich jednáním. Jinými slovy, jde o technický systém, který automaticky pořizuje a uchovává zvukové, obrazové nebo jiné

záznamy z monitorovaných oblastí, a to buď formou pasivního sledování, pořizování cílených záběrů (například sledování pohybu), nebo reportážního natáčení. [28]

Samotné kamerové sledování fyzických osob bez záznamu není považováno za zpracování osobních údajů podle Zákona o ochraně osobních údajů (ZOOÚ), protože takové systémy nesplňují podmínky pro zpracování osobních údajů, jak je uvedeno v § 4 písm. e) ZOOÚ. To, že se na ně tento zákon nevztahuje, však neznamená, že je možné instalovat kamerové systémy bez jakýchkoli omezení. Je třeba dodržovat zejména ustanovení Občanského zákoníku (OZ), který reguluje ochranu osobnosti. Podle § 12 OZ smí být podobizny, obrazové snímky a obrazové či zvukové záznamy týkající se fyzické osoby nebo jejich projevů osobní povahy pořízeny nebo použity pouze se souhlasem dané osoby. [28]

I při použití kamerového systému se záznamem se nemusí vždy jednat o zpracování osobních údajů. Podle § 4 písm. a) Zákona o ochraně osobních údajů (ZOOÚ) je osobním údajem jakákoliv informace, která se týká určeného nebo určitelného subjektu údajů. Údaje uložené v záznamovém zařízení, ať už obrazové nebo zvukové, jsou osobními údaji pouze tehdy, pokud na základě těchto záznamů lze přímo či nepřímo identifikovat konkrétní fyzickou osobu. Fyzická osoba je považována za identifikovatelnou, pokud jsou na snímku viditelné její charakteristické rozpoznávací znaky, a pokud je možné tyto znaky propojit s dalšími dostupnými informacemi pro úplnou identifikaci osoby. Osobní údaj tedy tvoří souhrn těch identifikátorů, které umožňují spojit danou osobu s konkrétním jednáním zachyceným na snímku. [28]

3.2 Kamery se záznamem ve školství

Kamery nás sledují na každém kroku – na ulicích, v bankách a v posledních letech i ve školách. Kamery na chodbách, ve třídách nebo šatnách se staly běžnou součástí českých škol. Rodiče si však často neuvědomují, že kamerové systémy mohou zasahovat do soukromí jejich dětí a že mohou porušovat jejich práva. Školám naopak hrozí vysoké pokuty za zneužívání kamerových systémů, které mohou dosahovat milionových částek. [28]

Mezi nejčastěji uváděné důvody pro instalaci kamerových systémů se záznamem ve školách patří zajištění bezpečnosti žáků, ochrana majetku školy a žáků před poškozováním a krádežemi, prevence vandalismu, zabránění vniknutí cizích osob do budovy školy a omezení šikany. [28]

Z těchto důvodů bývají kamery nejčastěji umístovány u vstupních dveří do budovy školy, ve vestibulech školy, u vstupů a výstupů do a ze šaten, na školním hřišti (pro monitoring fasády školy), na parkovištích a vstupních branách přístupových komunikací, u vchodu do školní jídelny, na chodbách školy a u vchodu do tělocvičny. [28]

Na některých místech ve školách jsou kamery nastaveny tak, že záznamy pořizují pouze mimo dobu vyučování, na jiných místech je záznam pořízen nepřetržitě. Školy obvykle uvádějí, že kamery nejsou určeny ke sledování zaměstnanců a studentů, ale slouží především k odrazení zlodějů, kteří by se mohli pokusit vstoupit do budovy školy. Záznamy bývají uchovávány obvykle po dobu 24 hodin až 3 dnů, přičemž během prázdnin a víkendů je předpokládaná doba uchovávání delší. [28]

3.2.1 Shrnutí

Jádrem sporu o oprávněnost a legitimnost instalování kamerových systémů je, stejně jako v dalších oblastech, rozpor mezi právem subjektu údajů – v tomto případě žáků, studentů, pedagogů a případných třetích osob – a právem správce osobních údajů chránit svůj majetek. Klíčovou otázkou je, jaká míra soukromí náleží dítěti, a to nejen v souvislosti s ochrannými opatřeními, ale také s respektem k jeho právu na soukromí a osobní integritu. [28]

Jako lidská bytost má dítě právo na soukromí. Článek 16 Úmluvy OSN o právech dítěte stanoví, že žádné dítě nesmí být vystaveno svévolnému zasahování do jeho soukromého života, rodiny, domova nebo korespondence, ani nezákonným útokům na jeho čest a pověst. Toto právo je nezbytné respektovat nejen ze strany jednotlivců, ale i právních zástupců dítěte, kteří mají povinnost chránit a podporovat tento základní princip soukromí. [28]

Instalací kamerového systému se záznamem skutečně dochází ke zpracování osobních údajů, neboť v relativně uzavřeném prostředí, jako je například budova školy, se pravidelně pohybuje určitý okruh osob. V takovém prostředí je nepochybné, že kamery shromažďují informace o konkrétních fyzických osobách, což splňuje definici osobního údaje podle § 4 písm. a) ZOOÚ (Zákon o ochraně osobních údajů). Takové zpracování musí být prováděno v souladu s právními předpisy o ochraně osobních údajů, včetně informování osob o zpracování a zajištění jejich práv na ochranu soukromí. [28]

Při instalaci kamerového systému jako prostředku k zajištění ochrany osob a majetku (a tedy i prostředku zpracování osobních údajů) je nezbytné přistupovat odlišně k jednotlivým monitorovaným prostorům či objektům. To zahrnuje i zohlednění různých

denních režimů v těchto prostorách. Například v některých oblastech školy může být monitorování nezbytné pouze během určité části dne, zatímco v jiných oblastech je nutné zajistit kontinuální dohled. Je důležité, aby instalace kamer odpovídala specifickým potřebám ochrany a zároveň minimalizovala zásah do soukromí osob, které se v daných prostorách nacházejí, v souladu s právními předpisy a zásadami ochrany osobních údajů. [28]

Je nezbytné rozlišovat, zda monitorování kamerovým systémem probíhá pouze v době, kdy se v daném prostoru nemají vyskytovat žádné osoby (např. po vyučování, po pracovní době, o víkendech nebo během prázdnin), nebo zda má být systém v provozu nepřetržitě, tedy i v době, kdy se v budově běžně vyskytují osoby, které plní své úkoly a povinnosti. [28]

Pokud je kamerový systém v provozu pouze v době, kdy se v prostoru nenacházejí osoby, může to mít nižší dopad na ochranu soukromí jednotlivců. Na druhé straně, pokud je systém v provozu nepřetržitě, tedy i během doby, kdy se ve škole nebo jiném objektu pohybují studenti, zaměstnanci a další osoby, je nutné zajistit, aby toto monitorování bylo prováděno v souladu s právními předpisy a zásadami ochrany osobních údajů. To znamená informování osob o přítomnosti kamer, omezení rozsahu monitorování na nezbytně nutné oblasti a respektování práv na soukromí těch, kteří jsou sledováni. [28]

Úřad ve svém stanovisku zdůrazňuje, že studenti, kteří dosáhli věku 15 let, jsou již dostatečně vyspělé osoby, schopné posoudit, zda chtějí, aby jejich osobní údaje byly zpracovávány prostřednictvím kamerového systému ve škole, v níž tráví většinu svého dne. Vzhledem k tomu, že studenti v tomto věku dosahují určité rozumové a volní vyspělosti, by měl správce osobních údajů, tedy škola, získat souhlas přímo od samotných studentů, a nikoliv od jejich zákonných zástupců. [28]

Tento přístup odráží princip autonomie a schopnosti studentů rozhodovat o zpracování jejich osobních údajů, přičemž souhlas by měl být informovaný a svobodný. Při tomto procesu by mělo být zajištěno, že studenti budou plně informováni o účelu monitorování, rozsahu záznamů a dalších podmínkách zpracování jejich osobních údajů. Tímto způsobem by byla respektována jejich práva na ochranu soukromí v souladu s právními předpisy, jako je GDPR. [28]

Je třeba rovněž zohlednit ustanovení § 316 odst. 2 ZP. Je důležité zdůraznit, že není rozhodující, že škola zamýšlí zpracovávat osobní údaje za účelem, který je odlišný od cíleného zpracování údajů svých zaměstnanců, či jejich podrobení otevřenému sledování.

Při provozování kamerového systému by totiž došlo k faktickému sledování zaměstnanců na pracovišti. [28]

Monitorování žáků školy není omezeno stejnými pravidly jako u zaměstnanců, přesto je třeba pečlivě zvážit riziko nepřiměřeného zásahu do práv žáků, zejména s ohledem na účel zpracování osobních údajů, kterým je ochrana majetku a prevence krádeží a vandalismu. [28]

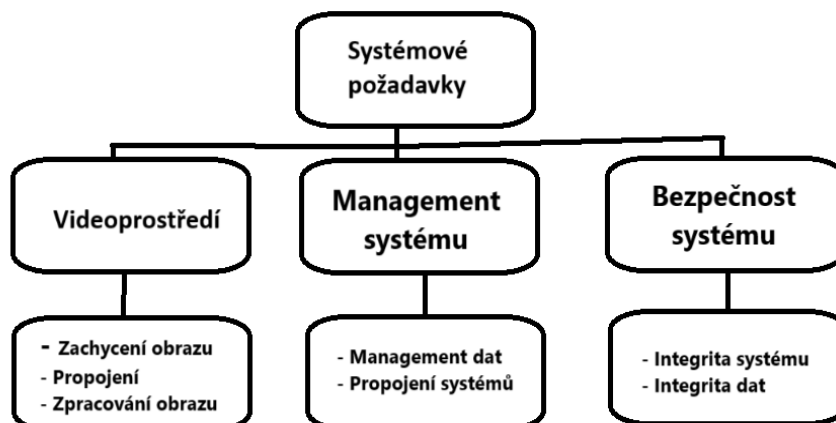
Doba uchování záznamů by měla být v rámci běžného provozu systému omezena na několik dní, přičemž je třeba vzít v úvahu možné odchylky v případě záznamů pořízených během prázdnin. Optimální lhůta by byla maximálně 3 dny, což by umožnilo odhalit nežádoucí chování v přiměřeném čase, vzhledem k běžně deklarovanému preventivnímu účelu a s ohledem na víkendy. [28]

Při zpracování osobních údajů na základě výjimky uvedené v § 5 odst. 2 písm. e) ZOOÚ není vždy nutné splnit informační povinnost v plném rozsahu před zahájením zpracování. V takových případech je správce podle § 11 odst. 5 ZOOÚ povinen informovat subjekt údajů o zpracování osobních údajů bez zbytečného odkladu. [28]

3.3 Normy

Každá věc, kterou chceme instalovat tak podléhá normám. Normy jsou evropské anebo české. Provozovatel se musí normami řídit, jinak může být sankcionován. Pro kamerové systémy je to norma ČSN EN 62676. Jsou zde i její podmnožiny: ČSN EN 62676-1-1, ČSN EN 62676-1-2, ČSN EN 62676-2-1 Video přenosové protokoly - Obecné požadavky ČSN EN 62676-2-2 Video přenosové protokoly - Implementace vzájemné spolupráce IP systémů založených na využití HTTP a REST, ČSN EN 62676-3 Analogové a digitální video rozhraní ČSN EN 62676-4 Pokyny pro aplikace. [9]

První část normy se věnuje systémovým požadavkům na provoz VSS. Zde se definují jednotlivé prvky kamerového systému.



Obrázek 18 Funkční bloky VSS

(upraveno z:[9])

Řeší se v ní také rozdělení prostředí podle okolních fyzikálních vlivů působících na VSS. Nejdůležitější je teplota, vlhkost a technické specifikace budovy. Rozlišujeme zde 4 třídy viz Tabulka 1. [9]

Tabulka 1 Třídy prostředí

Třída	Název prostředí	Teploty [°C]	Příklady
1	Vnitřní	+ 5 až + 40	Obytné místnosti, obchodní objekty
2	Vnitřní všeobecné	- 10 až + 40	Nestálá teplota, chodby, haly, schodiště
3	Venkovní chráněné	- 25 až + 50	Vně budovy, komponenty nejsou plně vystaveny enviromentálním vlivům, přístřešky, terasy
4	Venkovní všeobecné	- 25 až + 60	Vně budovy, komponenty plně vystaveny enviromentálním vlivům prostředí

(upraveno z:[9])

Patří sem také klasifikace stupně zabezpečení u VSS. Tedy rozdělení podle bezpečnostních požadavků v jednotlivých stupních zabezpečení:

- stupeň 1 (nízké riziko) – VSS určený nad situacemi s nízkými riziky. VSS nemá žádnou ochranu proti narušení.

- stupeň 2 (nízké až střední riziko) – VSS určený pro monitorování situací s nízkým až středním rizikem. VSS má nízkou úroveň ochrany proti narušení.
- stupeň 3 (střední až vysoké) – VSS určený pro monitorování situací se středním až vysokým rizikem. VSS má vysokou úroveň ochrany proti narušení.
- stupeň 4 (vysoká rizika) – VSS určený pro monitorování situací s vysokým rizikem. VSS má velmi vysokou úroveň ochrany proti narušení. [9]

ČSN EN 62676-1-2 se věnuje systémovým nastavením pro videopřenos. Jsou zde uvedeny Obecné provozní požadavky, IP přenosové protokoly a Požadavky pro video streamování. [9]

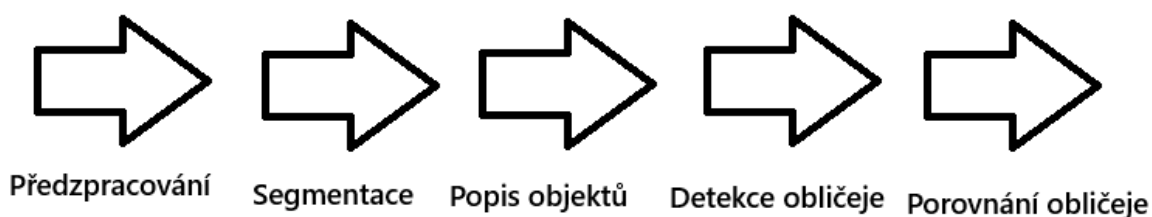
4 ZPRACOVÁNÍ OBRAZU

Zpracování obrazu je klíčovou součástí moderních kamerových systémů, které se využívají v široké škále aplikací, jako je fotografie, dohledové systémy. Tento proces zahrnuje několik fází – od získávání obrazu až po jeho vylepšení, analýzu a rozpoznávání objektů.

Obrázek zobrazuje diagram znázorňující proces rozpoznávání obličeje. Proces je rozdělen do pěti fází:

1. **Předzpracování** – první fáze, která zahrnuje úpravy obrazu, například odstranění šumu, změnu kontrastu nebo normalizaci osvětlení.
2. **Segmentace** – rozdělení obrazu na jednotlivé oblasti s cílem identifikovat relevantní části obrazu, například lidskou tvář.
3. **Popis objektů** – extrakce klíčových vlastností a rysů z obrazu, které pomáhají v dalším rozpoznávání.
4. **Detekce obličeje** – identifikace oblasti obrazu, kde se nachází obličej.
5. **Porovnání obličeje** – srovnání detekovaného obličeje s databází za účelem identifikace nebo ověření identity osoby.

Celý proces se zaměřuje na automatické rozpoznávání obličejů, které se využívá například v biometrických systémech, bezpečnostních aplikacích nebo při odemykání zařízení.



Obrázek 19 Rozpoznání obličeje

(upraveno z: [29])

1. Předzpracování

Tato fáze slouží k úpravě vstupního obrazu tak, aby byl vhodný pro další analýzu. Hlavním cílem je odstranit rušivé prvky a zvýraznit klíčové vlastnosti. Mezi nejdůležitější kroky patří:

- **Úprava kontrastu a jasu** – normalizace světelných podmínek, aby rozdíly mezi různými snímky nebyly příliš výrazné.
- **Odstranění šumu** – použití filtrů (například Gaussovského filtru) k odstranění šumu způsobeného špatnou kvalitou snímku.
- **Změna velikosti obrazu** – převzorkování snímku na standardizovanou velikost, což usnadňuje další zpracování.
- **Převod na stupně šedi** – pokud je snímek barevný, často se převádí na černobílý obraz, což snižuje množství dat a zjednodušuje výpočetní proces.
- **Histogramová ekvalizace** – zlepšení kontrastu obrazu pro lepší detekci rysů obličeje. [29]

2. Segmentace (zelená šipka)

Segmentace slouží k oddělení relevantních částí obrazu od pozadí a dalších nepodstatných prvků. V tomto kroku dochází k:

- **Detekci hran** – ke zvýraznění obrysů objektů.
- **Práhování** – rozdělení obrazu na oblasti podle intenzity pixelů, což pomáhá odlišit různé objekty.
- **Rozdělení obrazu na oblasti** – algoritmy jako Watershed nebo GrowCut se používají k oddělení částí obrazu, které mohou odpovídat lidské tváři.

Cílem segmentace je určit, které části obrazu by mohly obsahovat obličej nebo jeho části (například oči, nos, ústa).[29]

3. Popis objektů

V této části zpracování dochází k rozdělení nalezených obrazů do jednotlivých tříd. Objekty je možné rozdělit do čtyř základních tříd.

Podle:

1. **barvy** – barva je základní vlastností každého objektu a je její výhodou, že není závislá na pozici umístění v obraze. Případné posunutí nebo změna úhlu pozorovatele objektu nejsou problematické pro určení, o jakou barvu se jedná. V obraze objektu můžeme rozeznat, zda je některá barva dominantní nebo určit rozvržení barev.
2. **umístění** – k určení polohy objektů v obraze se používá několik definic. Mezi základní patří určení polohy objektů jedním bodem nebo nalezení maximální a minimální polohy v horizontálním a vertikálním směru.
3. **velikosti** – velikost objektů je možné určovat pomocí počtu pixelů, které ohraničují příslušný objekt. Pro složitější a přesnější výpočty velikosti objektů se používá metoda rotace konvexního mnohoúhelníku.
4. **tvaru** – popsání tvaru objektů patří k nejtěžšímu úkolu. Velký problém pro rozpoznávání objektů v obraze podle tvaru je orientace a s tím spojený úhel, pod kterým je předmět pozorován. Pro určení tvaru objektů v obraze se používají různé šablony. Tvar objektů je možné popsat pomocí hraničních bodů. [30]

4. Detekce obličeje

V této fázi se rozhoduje, zda daná část obrazu skutečně obsahuje obličej. Používají se různé metody:

- **Klasické metody detekce obličejů:**
 - Metody založené na vzorech
 - Aktivní tvarové modely a aktivní modely vzhledu – používají se k rozpoznání specifických rysů obličeje.
- **Moderní metody založené na hlubokém učení:**
 - CNN – například modely jako MTCNN

- OpenCV DNN modul – knihovna OpenCV umožňuje detekci obličejů pomocí hlubokého učení.

5. Porovnání obličeje

Posledním krokem je samotná identifikace nebo ověření identity. V této fázi dochází k porovnání detekovaného obličeje s databází známých obličejů:

- **Identifikace (Identification)** – systém se snaží určit, komu obličej patří. Používají se metody jako:
 - K-nearest neighbors
 - Podpora vektorových strojů (SVM)
 - Umělé neuronové sítě (ANN)
 - Deep learning modely jako FaceNet nebo DeepFace

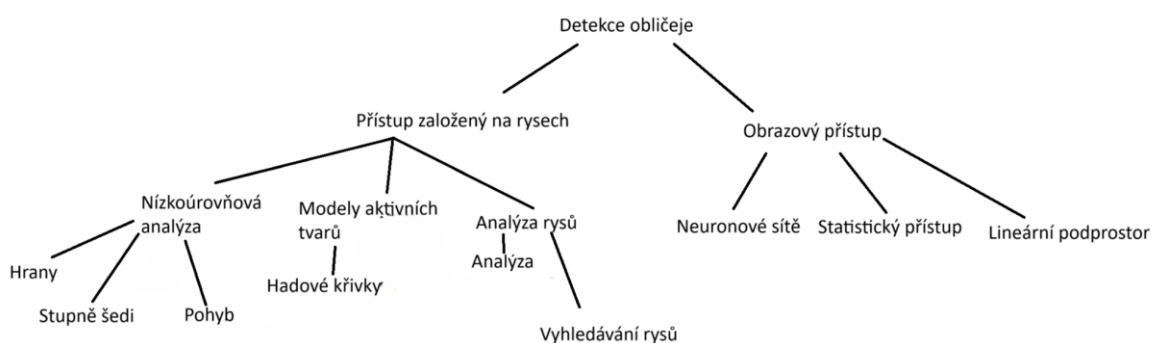
4.1 Databáze osob

Pro samostatné vyhledávání je nutné mít k dispozici databázi osob, ve které se budou osoby vyhledávat.

- Metoda one-to-one (1:1) – ověření skutečnosti, že osoba na aktuálním snímku je na snímku starém několik dnů, týdnů, měsíců nebo let, př. Pasová kontrola
- Metoda one-to-many (1:M) – jde o porovnání snímku jedné osoby s databází určitého počtu lidí, př. Vstup do místnosti
- Metoda many-to-many (M:M) – jde o případ porovnání více osob s databází osob, př. vstupy na stadion, zakázaný vstup má více lidí nasnímaných tedy i více lidí v databázi

5 ROZPOZNÁNÍ OBLIČEJE OSOB

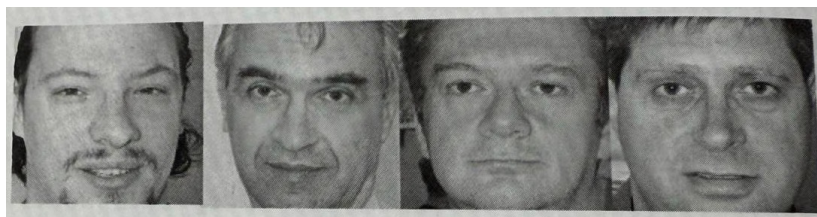
Detekce obličeje je nezbytným prvním krokem v systémech rozpoznávání obličeje s cílem lokalizovat a extrahovat oblast obličeje z pozadí. Lidská tvář je dynamický objekt a má určitou míru variability ve svém vzhledu. Díky tomu je detekce obličeje obtížným problémem, zejména pokud je integrována se systémem počítačového vidění. Byla navržena široká škála technik, od jednoduchých algoritmů založených na hranách až po složené vysokoúrovňové přístupy využívající pokročilé metody rozpoznávání vzorů. [31]



Obrázek 20 Přístupy k technikám detekce obličeje

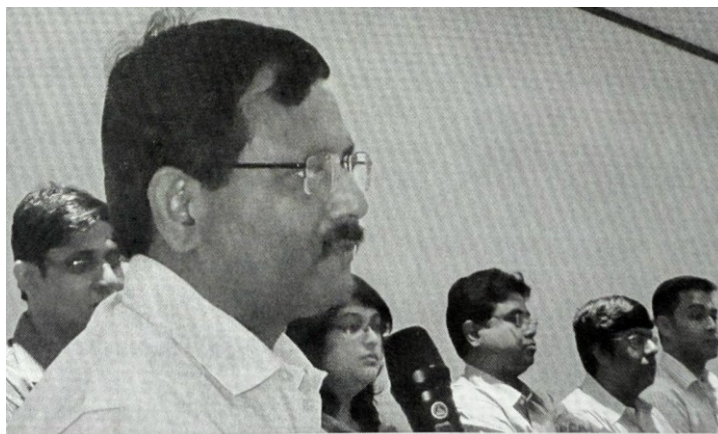
(upraveno z: [30])

Mnoho současných technik rozpoznávání obličejů předpokládá dostupnost čelních obličejů podobných velikostí. Tento předpoklad nemusí platit kvůli různé povaze vzhledu obličeje a podmínkám prostředí. Obrázek 21 ukazuje některé typické testovací snímky používané pro detekci obličeje. V realistických aplikačních scénářích, jako je příklad na obrázku 22, se může tvář vyskytovat na složitém pozadí a v mnoha různých pozicích. Systémy detekce a rozpoznávání, které jsou založeny na obrázcích obličeje, jako na obrázku, pravděpodobně provedou falešnou detekci a rozpoznání, protože některé oblasti pozadí mohou být mylně považovány za obličej. Aby se problém napravil, je zapotřebí vizuální front-end procesor, který lokalizuje a extrahuje oblast obličeje z pozadí. [31]



Obrázek 21 Typické obrázky pro klasifikaci obličejů

(zdroj:[30])



Obrázek 22 Detekční problém

(zdroj:[30])

Při daném libovolném snímku je cílem procesu detekce obličeje určit, zda na snímku není nějaký obličej, a pokud je přítomen, vrátit umístění snímku a rozsah každého obličeje. Výzvy spojené s procesem detekce obličeje lze připsat následujícím faktorům:

- **Zakrytí** – plochy mohou být částečně zakryty jiným objektem. Na snímku se skupinou lidí mohou některé tváře částečně zakrývat jiné tváře.
- **Výraz obličeje** – vzhled obličeje je přímo ovlivněn výrazem obličeje člověka.
- **Póza** – obrázky obličeje se liší v závislosti na relativní pozici obličeje fotoaparátu, jako je čelní namíření, 45°, profil, vzhůru nohama atd.
- **Osvětlení** – při vytváření obrazu obličeje ovlivňují vzhled obličeje také faktory, jako je stav blesku a vlastnosti fotoaparátu. [31]

Bylo navrženo mnoho metod, jak nejprve detekovat rysy obličeje a poté odvodit přítomnost obličeje. Běžně se extrahují rysy obličeje, jako je obočí, oči, nos, ústa a vlasová linie. Na základě extrahovaných prvků byl vytvořen statistický model, který popisuje jejich vztahy a ověřuje existenci obličeje. Jedním z problémů těchto algoritmů založených na vlastnostech je to, že vlastnosti obrazu mohou být vážně poškozeny v důsledku osvětlení, šumu a okluze. [31]

5.1 Nízkoúrovňová analýza

5.1.1 Hrany

Reprezentace hran pro extrakci příznaků byla použita již v raných pracích týkajících se detekce obličejů. Tato detekce byla založena na analýze perokreseb obličejů z fotografií a jejím cílem bylo lokalizovat obličejové rysy. Metoda byla později modifikována navržením hierarchického rámce pro sledování obrysů lidské hlavy. Práce zahrnuje algoritmus sledující linie, implementovaný s omezením zakřivení, které zabraňuje jeho rozptylování šumovými hranami. Detekované rysy uvnitř obrysu hlavy jsou následně podrobeny analýze tvarů a polohy obličeje. [31]

Více současných příkladů technik založených na hranách lze nalézt pro extrakci rysů obličeje a pro detekci obličejů. Při přístupu založeném na hranách k detekci obličejů je nutné označit hrany a přiřadit je k modelu obličeje, aby byla ověřena správnost detekce. Někdy se toho dosahuje označením hran jako levá strana, vlasová linie nebo pravá strana obličeje při čelním pohledu a následným srovnáním těchto hran s modelem obličeje pomocí zlatého řezu pro ideální obličej. Kromě toho byly techniky založené na hranách také aplikovány na detekci brýlí v obličejových obrazech. Bylo použito mnoho různých typů operátorů hran. Mezi operátory používané jako detektory hran patří Sobelův operátor a Marr-Hildrethův operátor. Řiditelné filtrování se skládá ze tří po sobě jdoucích kroků detekce hran, které zahrnují detekci hran, určení orientace filtru jakýchkoli detekovaných hran a postupné sledování sousedních hran pomocí informací o orientaci. Algoritmus umožnil přesnou extrakci několika klíčových bodů oka. [31]

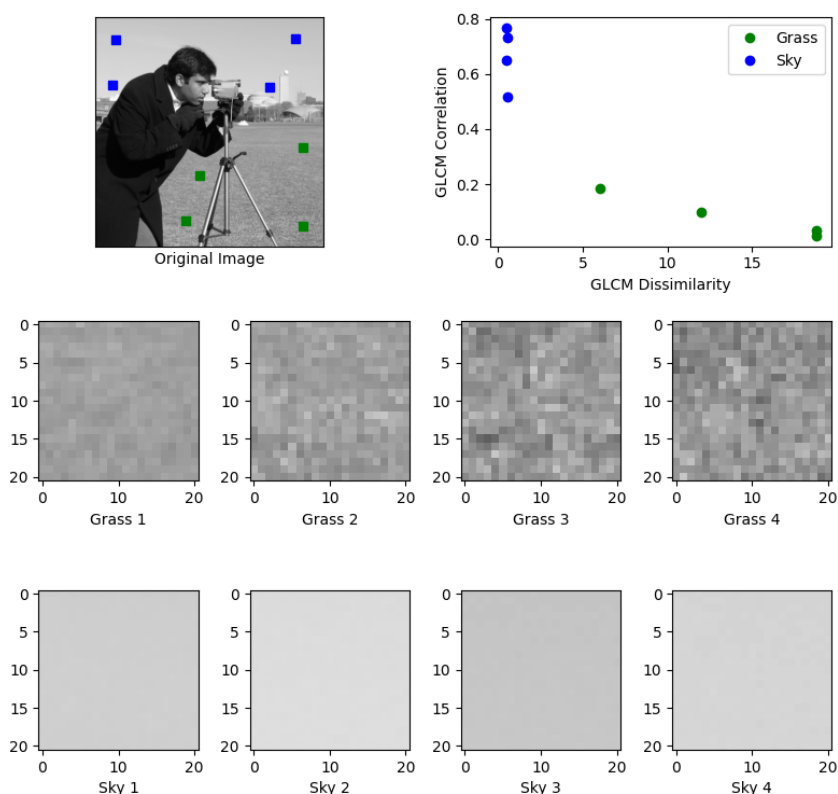


Obrázek 23 Detekce hran

(zdroj:[32])

5.1.2 Analýza úrovní šedi

Kromě detailů hran lze jako příznaky využít i informace o odstínech šedi uvnitř obličeje. Obličejové rysy, jako jsou obočí, zorničky a rty, bývají obecně tmavší než okolní oblasti obličeje. Tato vlastnost je využívána k rozlišení různých částí obličeje. Několik nedávných algoritmů pro extrakci příznaků vyhledává lokální minima šedé úrovně uvnitř segmentovaných oblastí obličeje. V těchto algoritmech jsou vstupní obrazy nejprve vylepšeny kontrastním roztažením a morfologickými operacemi v úrovních šedi, aby se zlepšila kvalita tmavých oblastí a tím se usnadnila detekce. Extrakce tmavých oblastí je dosahována prahováním s nízkou úrovní šedi. Některé algoritmy využívají šablony vážené lidským okem k určení možných poloh párů očí. Lokální maxima, která jsou definována jasným pixelem obklopeným osmi tmavými sousedy, se používají k indikaci světlých oblastí obličeje, jako jsou špičky nosu. Body detekce jsou pak zarovnány s šablonami příznaků pro korelaci měření. [31]



Obrázek 24 Úroveň šedi

(zdroj:[33])

5.1.3 Analýza založená na pohybu

Informace o pohybu jsou pohodlným prostředkem pro lokalizaci pohybujícího se obličeje, když je k dispozici video. Jednoduchým způsobem, jak dosáhnout segmentace pohybu, je analýza rozdílů mezi snímky. Tento přístup, ačkoliv jednoduchý, je schopen efektivně rozeznat pohybující se popředí bez ohledu na obsah pozadí. Pohybující se siluety, které zahrnují obličej a části těla, jsou extrahovány prahováním akumulovaných rozdílů mezi snímky. Existence páru očí je předpokládána měřením horizontálních a vertikálních posunů mezi dvěma sousedními kandidátními oblastmi získanými z rozdílů snímků. [31]

Dalším způsobem měření vizuálního pohybu je odhad pohybujících se obrysů obličeje. Ve srovnání s rozdílem snímků jsou výsledky generované z pohybujících se obrysů obvykle spolehlivější, zejména pokud je pohyb nevýrazný. Na rozdíl od výše popsaných metod, které identifikují pohybující se hrany a oblasti, tyto metody spoléhají na přesný odhad pohybu pomocí rychlostí jasu, tzv. optického toku. Vzhledem k tomu, že odhad je založen na pohybech na krátké vzdálenosti, je velmi citlivý na jemný pohyb. [31]

5.2 Aktivní tvarový model

Na rozdíl od modelů obličeje popsaných v předchozích částech aktivní tvarové modely zobrazují skutečný fyzický, a tedy vyšší úroveň vzhledu obličejových rysů. Jakmile se model dostane do blízkosti určitého rysu, interaguje s lokálními obrazovými prvky (hrany, jas) a postupně se přizpůsobuje tvaru daného rysu. Obecně existují dva typy aktivních tvarových modelů v současné extrakci obličejových rysů. [31]

První typ využívá obecný aktivní obrys (tzv. „hady“). Aby se vzaly v úvahu apriorní znalosti obličejových rysů a pro lepší výkon „hadů“ se zavádějí deformovatelné šablony. Nový obecný flexibilní model, nazvaný „chytrý had“, je také zaváděn pro efektivní interpretaci lidského obličeje. Model je založen na sadě označených bodů, které mohou měnit svou polohu podle trénovací procedury, aby se přizpůsobily určitému tvaru. [31]

Aktivní kontury (hadi) se běžně používají k nalezení obrysu hlavy. Had je nejprve inicializován v blízkosti okraje hlavy, kde se zachytí na blízké hrany, a následně přizpůsobuje tvar hlavy. Typický přirozený vývoj hada spočívá v tom, že se smršťuje nebo roztahuje, a tímto způsobem se kontury přizpůsobují skutečnému obrysu, a nakonec se ustálí ve stabilní poloze. Dvě hlavní úvahy při implementaci hada jsou výběr vhodných energetických členů a technika minimalizace energie. Elastická energie se běžně používá

jako vnitřní energie — je úměrná vzdálenosti mezi centrálními body na hadovi a tím dává hadovi elasticko-pásovou charakteristiku, která ho nutí se smršťovat nebo roztahovat. Vnější energetický člen závisí na typu obrazových prvků. Vedle gradientních informací přitahuje had k oblasti obličeje. Minimalizace energie může být dosažena optimalizačními technikami, jako je nejstrmější sestup. [31]

Ačkoliv jsou hadi obecně schopní lokalizovat obrysy rysů, jejich použití stále naráží na dva problémy. Část kontury se často zachytí na falešné obrazové rysy. Dále hadi nejsou efektivní při extrakci nekonvexních rysů kvůli své tendenci dosáhnout minimálního zakřivení. Tyto problémy jsou řešeny zavedením parametrizovaného modelu hada pro extrakci obrysu hlavy a obličeje. Tento parametrizovaný model směřuje kontury k cílovému tvaru a tím umožňuje rozlišovat falešné rysy a vyhnout se jejich zachycení. Jakmile kontury dosáhnou rovnováhy, model je odstraněn a kontury jsou ponechány, aby se chovaly samostatně jako pár běžných hadů, což vede k finální extrakci obrysu. [31]

Použití modelů hadů pro lokalizaci hranice obličejových rysů není jednoduchý úkol, protože lokální důkazy okrajů obličeje jsou obtížně uspořadatelné do smysluplného celku pomocí obecných kontur. Nízký kontrast v okolí některých těchto rysů rovněž ztěžuje problematicky proces detekce hran. Pojem "hadi" se používá i při zapojení globální informace, například z očí, aby se zvýšila spolehlivost procesu extrakce. [31]

5.2.1 Analýza příznaků

Příznaky generované z analýzy nízké úrovně bývají často nejednoznačné. Například při lokalizaci obličejových oblastí pomocí modelu barvy pokožky mohou být detekovány i pozadí nebo objekty podobné barvy. Toto je případ mapování typu mnoho-na-jedno, které lze vyřešit analýzou příznaků vyšší úrovně. Tato analýza využívá znalosti geometrie obličeje pro charakterizaci a následné ověření různých příznaků z jejich nejednoznačných stavů. Existují dva přístupy v aplikaci geometrie obličeje. První přístup zahrnuje sekvenční vyhledávání strategií založených na relativní poloze jednotlivých obličejových rysů. Druhý přístup seskupuje příznaky jako flexibilní konstelace pomocí různých modelů obličeje. [31]

Techniky vyhledávání příznaků začínají určením výrazných obličejových rysů. Méně výrazné rysy se pak odvozují pomocí antropometrických měření geometrie obličeje. Například malá oblast na větší ploše v hlavě a ramenním scénáři naznačuje přítomnost hlavy, a dvojice tmavých oblastí v obličeji zvyšuje jistotu o existenci obličeje. Dvojice očí je nejčastěji používaným referenčním rysem díky svému typickému uspořádání vedle sebe.

Mezi další rysy patří hlavní osa obličeje, obrys (horní část hlavy) a tělo (pod hlavou), které se rovněž používají. [31]

Algoritmus pro extrakci obličejových rysů začíná hypotézou o vrcholu hlavy a poté algoritmus prohledávání skenuje směrem dolů s cílem najít rovinu očí, která se vyznačuje náhlým zvýšením hustoty hran, měřené poměrem černé a bílé podél horizontálních rovin. Vzdálenost mezi horní částí a rovinou očí je poté použita jako referenční délka. Pomocí této referenční délky je inicializována flexibilní šablona obličeje pokrývající rysy, jako jsou oči a ústa, na vstupním obraze. Tato flexibilní šablona je následně přizpůsobena konečné poloze rysů pomocí nákladové funkce založené na hranách. Systém pro detekci obličeje a jeho rysů, založený na antropometrických principech, zahrnuje také využití míry podobnosti. V tomto systému jsou možné polohy očí stanoveny v binarizovaných předzpracovaných obrazech. Poté algoritmus pokračuje vyhledáváním nosu, úst a obočí. Každý obličejový rys má přiřazenu hodnotící funkci, která slouží k určení nejpravděpodobnějšího kandidáta na daný rys, přičemž váhy jsou určeny podle jejich vizuální důležitosti a ručně nastavených koeficientů. [31]



Obrázek 25 Analýza příznaků

(zdroj:[34])

5.2.2 Statistické přístupy

Na základě práce s detekcí obličeje pomocí maximální pravděpodobnosti je navržen statistický přístup, kde se používá Kullbackova relativní informace (Kullbackova divergence). Trénovací procedura vede k vytvoření sady tabulek s poměry pravděpodobnosti. Aby se dále zlepšil výkon a snížily výpočetní nároky, dvojice pixelů, které přispívají špatně k celkové divergenci, jsou z těchto tabulek odstraněny a v systému detekce obličeje se nepoužívají. Zavedením metody „bootstrappingu“ (naučení z chyb) byla tato technika začleněna do systému pro sledování obličeje v reálném čase. [31]

Jiné metody detekce obličeje, jako jsou metody lineárních podprostorů nebo neuronové sítě, mohou být také použity pro rozpoznávání obličeje. Tyto techniky budou diskutovány v části věnované rozpoznávání obličejů. [31]

5.3 Metody rozpoznávání obličeje

Během posledních 20 let bylo navrženo množství algoritmů pro rozpoznávání obličejů. Zdá se, že mezi několika technikami významně přispěly k rozvoji detekce a rozpoznávání obličejů metody podprostorů a metody založené na vzhledu. Na základě typu použité obrazové transformace lze metody podprostorů dále obecně rozdělit na lineární a nelineární metody. [31]

Všechny existující techniky rozpoznávání obličeje lze klasifikovat do pěti typů podle způsobu, jakým identifikují obličej. Jsou to:

1. Metody založené na vzhledu, které využívají úplné texturové rysy.
2. Rozpoznávání obličeje založené na podprostorových metodách.
3. Techniky využívající neuronové sítě.
4. Modelově založené metody, které pracují s tvarem a texturou obličeje, včetně 3D hloubkové informace.
5. Jiné techniky, jako jsou korelační metody a použití podpůrných vektorových strojů (SVM). [31]

5.3.1 Metoda založená na geometrických příznacích

Přístupy založené na geometrických příznacích patří mezi nejstarší metody rozpoznávání a detekce obličeje. V těchto systémech se detekují významné rysy obličeje a

vzdálenosti mezi nimi. Tyto a další geometrické charakteristiky se pak kombinují do vektorů příznaků. [31]

Pro rozpoznání obličeje se nejprve získá vektor příznaků z testovacího obrazu a obrazu v databázi. Poté se mezi těmito dvěma vektory vypočítá míra podobnosti, nejčastěji na základě minimální vzdálenosti, která určuje identitu obličeje.

Šablonové přístupy založené na geometrických příznacích často překonávají tyto rané metody. Nejpoužívanější technika pro rozpoznání a detekci obličejů je právě metoda založená na šablonách. Na rozdíl od přístupů založených na geometrických příznacích využívá šablonový přístup celý obraz obličeje jako vektor příznaků, nikoli pouze vybrané výrazné rysy. [31]

5.3.2 Rozpoznávání obličeje na základě podprostorů

Obecně platí, že metody založené na podprostorech používají trénovací sadu obrazů obličejů k výpočtu souřadného prostoru, ve kterém jsou obrazy obličejů komprimovány do méně rozměrů, přičemž je zachována maximální variabilita napříč jednotlivými směry. Obrázky obličejů jsou si celkově podobné a nejsou náhodně rozloženy v tomto velkém obrazovém prostoru – dají se tedy popsat pomocí podstatně ménědimenzionálního podprostoru. [31]

Hlavní myšlenkou je převést tyto obrazy do souboru vektorů, které co nejlépe reprezentují strukturu obličejů. Tyto zredukované vektory definují podprostor obličejových obrazů, označovaný jako face space. Po provedení linearizace se vypočítá průměrný vektor ze všech obrazů a odečte se od jednotlivých obrazů. Poté se vypočítá kovarianční matice a z ní se extrahuje omezený počet vlastních vektorů, odpovídajících největším vlastním hodnotám. Tyto eigenvektory – označované jako eigenfaces – tvoří základ pro prostor s nízkou dimenzionalitou. [31]

Když se má testovat nový obraz, vypočítá se jeho projekce (expanze do eigenface prostoru) a porovná se s databází podle určité míry vzdálenosti (obvykle Eukleidovské). [31]

5.3.3 Rozpoznávání obličeje založené na neuronových sítích

Další nelineární řešení problému rozpoznávání obličeje je založeno na neuronových sítích. Výhodou neuronových sítí při klasifikaci oproti lineárním metodám je schopnost snížit chybné zařazení mezi sousedními třídami. [31]

Základní myšlenkou je použít síť, ve které je jeden neuron pro každý pixel v obraze. Nicméně, kvůli vysoké rozměrovosti obrazových vzorů nejsou neuronové sítě trénovány přímo na vstupních obrazech – místo toho se používá technika redukce dimenzionality, kterou doplňuje další neuronový model fungující v režimu autoasociace. Obraz obličeje je nejprve převeden na vektor s menšími rozměry pomocí první sítě (auto-asociace) a tento vektor se pak použije jako vstup do klasifikační sítě. [31]

Obecně je struktura neuronové sítě silně závislá na aplikační oblasti, a proto různé kontexty mohou vyžadovat odlišné sítě. Třída neuronových sítí známá jako samo-organizující mapy se také používá v rozpoznávání obličejů, aby se využily jejich specifické vlastnosti – například invariance vůči drobným změnám v obraze, jako jsou rotace, posuny a změny měřítka. [31]

Pravděpodobnostní rozhodovací neuronové sítě se rovněž používají v detekci a rozpoznávání obličeje. Jejich výhodou je hierarchická struktura s nelineárními bázovými funkcemi a soutěživým systémem přiřazování. Za zmínku stojí také hybridní přístup, při kterém jsou nejvíce diskriminující příznaky extrahovány pomocí PCA a následně použity jako vstup do neuronové sítě s radiální bázovou funkcí (RBF). RBF sítě se osvědčily při úlohách rozpoznávání obličejů, protože mají kompaktní topologii a vysokou rychlost učení. [31]

Nicméně, obecně mají neuronové sítě problémy, když se zvyšuje počet tříd. Navíc nejsou vhodné pro úlohy rozpoznávání obličeje s jediným modelem, protože pro trénink systému je třeba více obrázků jedné osoby. [31]

5.3.4 Metoda založená na korelaci

Metody detekce obličeje založené na korelaci vycházejí z výpočtu normalizovaného součinitele křížové korelace. Prvním krokem těchto metod je určení polohy významných obličejových rysů, jako jsou oči, nos nebo ústa. Význam robustní detekce těchto rysů jak pro detekci, tak pro rozpoznávání obličeje vedl k vývoji řady algoritmů pro detekci příznaků. Algoritmy pro detekci obličejových rysů používají sadu šablon k určení polohy očí v obraze tak, že vyhledávají body s maximální absolutní hodnotou normalizovaného korelačního součinitele mezi těmito šablonami a oblastmi testovacího obrazu. Aby se algoritmus vyrovnal s rozdíly v měřítku, používají se šablony v různých velikostech. Problémy spojené s variacemi měřítka lze výrazně snížit pomocí hierarchické korelace. Pro rozpoznávání obličeje se šablony odpovídající významnému rysu obličeje z testovacího obrazu

porovnávají s odpovídajícími šablonami všech obrazů v databázi. To vede k vytvoření vektoru skóre shody, který je vypočítán pomocí normalizovaného křížového korelačního koeficientu. Skóre podobnosti různých rysů se integrují do globálního skóre, které se použije pro rozpoznání. Jiné podobné metody, které využívají korelaci nebo statistiky vyššího řádu, ukázaly přesnost těchto metod, ale také jejich složitost. [31]

Pro zvládnutí rotací se používají šablony z různých pohledů. Jakmile je určen postoj, úloha rozpoznání se zjednoduší na klasickou korelaci, při níž se příznakové šablony porovnávají s odpovídajícími šablonami modelů z příslušného pohledu pomocí korelačního koeficientu. Tento výpočetně náročný přístup je však citlivý na světelné podmínky. [31]

5.3.5 Přístup pomocí podpůrných vektorových strojů (SVM)

Rozpoznávání obličeje je problém typu **K tříd**, kde **K** je počet známých osob. Podpůrné vektorové stroje (SVM), které pracují s binární klasifikací, lze tedy aplikovat na tento problém přeformulováním úlohy rozpoznávání obličeje a reinterpetací výstupu SVM klasifikátoru. [31]

Problém je formulován jako úloha v rozdílovém prostoru, kde model vyhodnocuje rozdíly mezi dvěma obrazy obličejů. V tomto rozdílovém prostoru se rozpoznávání obličeje chápe jako problém dvou tříd: rozdíly mezi obrazy stejné osoby a rozdíly mezi obrazy různých lidí. [31]

5.4 Techniky rekonstrukce obličeje

Generování syntetických obličejů pro účely rozpoznávání obličeje bylo v posledních letech intenzivně zkoumáno. Úspěšně bylo dosaženo přechodu z **2D** do **3D** rekonstrukce a generování nových obličejů s různými tvary a vzhledy. Techniky rekonstrukce z **2D do 3D** a **aktivní modely vzhledu** generované z 2D obrazů obličeje jsou výkonné metody. [31]

Doposud modelování zahrnuje čtyři hlavní přístupy:

- **Active appearance models**
- **manifolds**
- **geometry-driven face synthesis methods** včetně animace obličeje
- **techniky mapování výrazu**. 3D modely zahrnují obličejové síťové rámce, morfovateľné modely a modely založené na hloubkových mapách. Tyto modely vyžadují začlenění grafiky ve vysoké kvalitě a složité animační algoritmy. [31]

Polohy hlavy v 3D se odvozují z odpovídajících rysů mezi 2D a 3D. Detekce obličeje založená na 3D se také zkoumá použitím 3D morfovateľných modelů s přidáním statistické textury. Víceúhlová rekonstrukce ve 2D prostoru se provádí pomocí analýzy variet. Geometricky řízená syntéza obličeje a reflexní modely jsou rovněž navrhovány. Techniky mapování výrazu se ukázaly být užitečné při generování obličejů ve 2D. [31]

5.4.1 Třidimenzionální rozpoznávání obličeje

Většina výzkumu a komerčních systémů rozpoznávání obličeje se spoléhá na typické obrazové snímky obličeje, které jsou označovány jako dvourozměrné (2D) obrazy. V procesu rozpoznávání se v žádném bodě nevyužívá vytvořený třidimenzionální (3D) model obličeje, ani algoritmy výslovně nevyužívají skutečnosti, že obrazy jsou výsledkem pozorování 3D obličeje. Na rozdíl od 2D obrazů je 3D povrch obličeje necitlivý na osvětlení, polohu hlavy a kosmetické úpravy. Navíc lze 3D data využít ke kompenzaci omezení 2D dat. [31]

Zatímco v 2D rozpoznávání obličeje lze použít běžnou kameru, 3D rozpoznávání vyžaduje sofistikovanější senzor, schopný získávat hloubkové informace, často označovaný jako hloubková nebo 3D kamera či skener. Pro rozpoznávání obličeje je 3D tvar obličeje obvykle zachycen společně s 2D intenzitním obrazem. V tomto případě lze 2D obraz považovat za texturovou mapu překrytou na 3D tvaru. Hloubkový obraz – někdy také nazývaný obraz vzdálenosti – je obraz, ve kterém hodnota pixelu odráží vzdálenost od senzoru k zobrazovanému povrchu. Hloubkový obraz, stínovaný model a model drátového rámu jsou běžné alternativy pro zobrazení 3D dat obličeje. [31]

V jiném přístupu se jako prostředník používá generický, morfovateľný 3D model obličeje pro sladění dvou 2D obrazů pro účely rozpoznání. Tento přístup nezahrnuje snímání nebo porovnávání 3D popisů, místo toho je 2D obraz mapován na deformovateľný 3D model a 3D model s texturou se používá k vytvoření sady syntetických 2D obrazů pro porovnávání. Variace tohoto přístupu se již dnes používají v mnoha komerčních systémech pro rozpoznávání obličeje. [31]

Typický systém 3D rozpoznávání obličeje se skládá z následujících částí: jednotka pro pořízení a předzpracování obrazu, jednotka pro extrakci příznaků a jednotka pro měření podobnosti a klasifikaci. V následujících oddílech jsou tyto jednotky podrobně popsány s příklady implementací, které se objevily v literatuře. Výstupem běžného 3D senzoru je sada 3D bodů skenovaného povrchu, s hodnotami souřadnic x , y a z v každém bodě. 3D data jsou

obvykle reprezentována jako bodový mrak, nebo jako hloubkový obraz. Hloubkový obraz vzniká promítnutím skenovaných 3D bodů z objektu na rovinu $x-y$. [31]

Hloubkový obraz má podobný formát jako běžný 2D intenzitní obraz, avšak s tím rozdílem, že v hloubkovém obraze intenzita pixelu odpovídá hloubkové složce snímaného objektu. [31]

Ve snímaném 3D obraze jsou tedy intenzity pixelů úměrné hloubce jednotlivých bodů. Detekce označuje proces, při kterém se zjišťuje přítomnost a počet tváří v obraze. Za předpokladu, že obraz obsahuje pouze jeden obličej, je úlohou lokalizace určit polohu a velikost oblasti obličeje. Většina metod pro lokalizaci obličeje ve 3D obrazech je založena na analýze lokálních zakřivení povrchu obličeje. Tím se vytvoří množina možných bodů pro určení umístění charakteristických částí obličeje, jako je poloha nosu, očí a úst, ze které lze určit přesnou polohu, velikost a orientaci oblasti obličeje. [31]

Na základě umístění těchto bodů může být obličej vyříznut ze zbytku obrazu a případně přeměřitkován a natočen do normální polohy. [31]

5.4.2 Extrakce příznaků

Stejně jako v 2D rozpoznávání obličeje je účelem extrakce příznaků kompaktně získat informace z obrazu, které jsou relevantní pro rozlišení mezi obličejí různých lidí a zároveň stabilní vůči fotometrickým a geometrickým variacím v obrazech. Jeden nebo více příznakových vektorů se extrahuje z oblasti obličeje. Stávající metody extrakce příznaků lze rozdělit na globální a lokální. [31]

5.4.3 Globální extrakce příznaků

V metodách globální extrakce příznaků se vektory příznaků získávají z celého obličeje. Většina globálních metod pro 3D extrakci obličejových příznaků je odvozena z metod, které byly původně vyvinuty pro 2D obrazy obličejů, kde se šedotónové obrazy nahrazují hloubkovými obrazy. Globální metody vyžadují přesnou lokalizaci a normalizaci orientace, měřítka a osvětlení pro spolehlivé rozpoznávání. [31]

Analýza hlavních komponent je nejrozšířenější metodou globální extrakce příznaků a používá se jak pro 2D obrazy, tak pro hloubkové obrazy. Další oblíbené globální metody, jako jsou lineární diskriminační analýza a nezávislá komponentová analýza, se rovněž používají pro hloubkové obrazy. Globální metody nejen snižují rozměrnost dat, ale zároveň zachovávají prostorové vztahy mezi různými částmi obličeje. [31]

Použití globálních příznaků je běžné v systémech rozpoznávání obličejů, které pracují s obrazy získanými v kontrolovaném prostředí. V systémech založených na globálních příznacích je lokalizace a normalizace často prováděna manuálně pomocí označení charakteristických bodů na obličeji. Automatická lokalizace a normalizace se obvykle provádí pomocí iterativního algoritmu nejbližšího bodu. [31]

Metody lokální extrakce příznaků extrahují sadu vektorů z různých oblastí obličeje, přičemž každý vektor nese charakteristiky konkrétní obličejové oblasti. Tyto lokální metody mají výhodu nad globálními v nekontrolovaných podmínkách, kde se v obrazech vyskytují změny v osvětlení, rotaci, výrazu a měřítku. Proces místní funkce extrakce může být rozdělen do dvou částí. V první části jsou detekovány zájmové body v oblasti obličeje. Ve druhé části jsou tyto body použity jako místa, ve kterých se vypočítávají lokální příznakové vektory. Zájmové body lze detekovat jako extrémy v tzv. prostorově-škálové doméně, což vede k škálové invariantnosti příznaků. Zájmové body lze také detekovat analýzou zakřivení rysů obličeje nebo pomocí elastic bunch graph method, kde uzly pravoúhlé mřížky pokrývají oblast obličeje. [31]

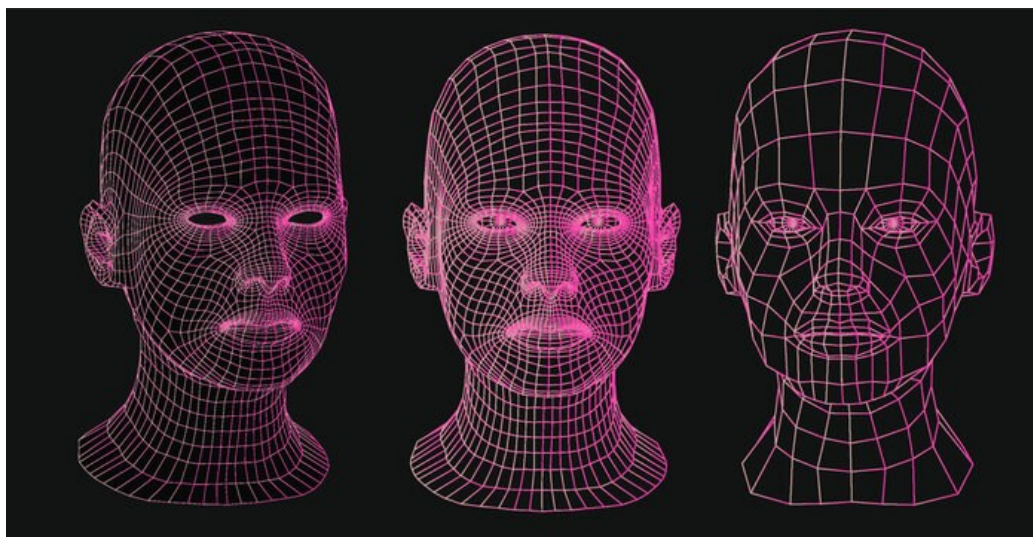
5.4.4 Třídimenzionální morfovateľný model

Morfovateľný model je třídimenzionální reprezentace, která umožňuje přesné modelování libovolného osvětlení a polohy hlavy, stejně jako oddělení těchto variací od ostatních aspektů, jako jsou identita a výraz. Jedná se o generativní model složený z lineárního 3D tvaru a modelu vzhledu, a modelu snímání, který mapuje 3D povrch na obraz.

Tvar a vzhled jsou modelovány jako lineární kombinace trénovací sady vzorových obličejů. [31]

Hlavním krokem konstrukce modelu je vytvořit odpovídající body mezi množinou 3D skenů obličejů. Při zpracování jednoho obličeje algoritmus automaticky odhaduje 3D tvar, texturu a všechny relevantní 3D scénické parametry, jako jsou poloha, osvětlení a výraz. V druhém kroku jsou odpovídající body mezi skeny a referenční sítí obličeje vypočítány. Registrované skeny obličejů jsou zarovnány tak, aby neobsahovaly žádnou globální rigidní transformaci. Poté se provádí analýza hlavních komponent pro odhad statistických údajů o tvaru a barvě obličejů. [31]

Úloha rozpoznávání je poté provedena měřením Mahalanobisovy vzdálenosti mezi tvarem a texturovými parametry modelu z galerie a přizpůsobeným modelem. [31]



Obrázek 26 3D obraz rozpoznávání obličeje

(zdroj: [35])

II PRAKTICKÁ ČÁST

6 SOFTWARE PRO IDENTIFIKACI OSOB

Identifikace osob na základě rozpoznávání obličejů se v posledních letech stala klíčovou technologií v oblasti moderní bezpečnosti, biometrie a automatizace přístupových systémů. Díky zásadním pokrokům v oblasti umělé inteligence, zejména v oblasti hlubokého učení a neuronových sítí, se tyto technologie rozvinuly do podoby sofistikovaných softwarových řešení, která jsou schopna realizovat přesné a rychlé rozpoznání obličejů v reálném čase.

Jedním z klíčových aspektů těchto technologií je jejich schopnost efektivně pracovat s velkým objemem obrazových dat, přičemž musí být zajištěna vysoká míra přesnosti i v případech proměnlivých podmínek, jako je variabilní osvětlení, změna úhlu snímání či zakrytí části obličeje. Mezi nejvýznamnější dodavatele technologií pro rozpoznávání obličejů patří společnosti jako **Hikvision**, **Dahua Technology**, **Axis Communications**, **Bosch Security Systems**, **AxxonSoft**, **Panasonic**, **Hanwha Techwin (Wisenet)**, **Avigilon (Motorola Solutions)**, **FaceFirst**, **Cognitec Systems**, **NEC Corporation**, **Ayonix**, **FacePhi** a **Visage Technologies**.

V rámci současného technologického diskurzu je zásadní otázkou také přesnost a spolehlivost těchto systémů. Výrobci pravidelně publikují výsledky testování přesnosti na standardizovaných databázích, přičemž hodnoty přesnosti se běžně pohybují nad 99 %. Významný podíl na zvyšující se přesnosti mají moderní algoritmy hlubokého učení a konvoluční neuronové sítě, které umožňují nejen detekci obličejů, ale i jejich autentifikaci s vysokou mírou spolehlivosti.

Technologická řešení jsou obvykle implementována buď přímo v hardwaru kamer, nebo jako samostatný serverový software. Například společnosti **Hikvision** a **Dahua** nabízejí pokročilé kamery s integrovaným rozpoznáváním obličejů, zatímco **AxxonSoft**, **NEC** či **Cognitec Systems** poskytují softwarové platformy, které se integrují s různými kamerovými systémy a zajišťují centrální správu dat. Tento přístup umožňuje flexibilitu při volbě hardwaru a zohledňuje požadavky na výkon a přesnost detekce.

Mezi základní kritéria pro výběr vhodného softwaru patří nejen jeho přesnost a rychlost detekce, ale i schopnost integrace s jinými systémy a dodržování zásad ochrany osobních údajů. Technologie pro rozpoznávání obličejů musí respektovat platné právní předpisy, včetně GDPR, a proto jsou moderní softwarové platformy navrženy s ohledem na šifrování dat a řízení přístupových práv.

6.1 Vybrané softwary

Tabulka 2 Softwary na rozpoznání obličeje

Software	Země původu	Implementace	Přesnost
Hikvision MinMoe	Čína	Integrovaný v kamerách	≥ 99 %
Dahua Face Recognition	Čína	Integrovaný v kamerách	99,9 %
Axis (SAFR Inside)	Švédsko	Externí software (SAFR)	99,87 %
Bosch IVA	Německo	Integrovaná analytika	> 95 %
AxxonSoft Axxon One	Rusko	Serverový software	≥ 90 %
Panasonic FacePRO	Japonsko	Serverový software	≥ 90 %
Hanwha Wisenet AI	Jižní Korea	Integrovaný v AI kamerách	99,83 %
Avigilon Control Center	USA	Serverový software	Není veřejná
NEC NeoFace	Japonsko	Serverový software	99,88 %
Ayonix Face Recognition	Japonsko	Serverový software	Vysoká (NIST)
FaceFirst Platform	USA	Cloudový software	99,8 %
FacePhi	Španělsko	Biometrická platforma	Vysoká (NIST)
Vivotek Face Recognition	Tchaj-wan	Integrovaný v kamerách	≥ 98 %
Cognitec FaceVACS	Německo	Serverový software	Vysoká (NIST)
VisageSDK	Švédsko	Vývojová sada (SDK)	Vysoká

(vlastní)

Tabulka 2 prezentuje komplexní přehled 14 softwarových řešení pro rozpoznávání obličejů. Každý záznam v tabulce se zaměřuje na specifický software, přičemž poskytuje zásadní informace o jeho původu, implementačních možnostech, přesnosti detekce, výhodách, slabinách a rovněž uvádí odkazy na relevantní zdroje.

Jedním z kritérií při analýze softwarových řešení je geografický původ technologie. V tomto směru dominují zejména společnosti pocházející z Číny (Hikvision, Dahua), Japonska (Panasonic, NEC, Ayonix), Německa (Bosch, Cognitec), Švédska (Axis, Visage Technologies), Jižní Koreje (Hanwha), Ruska (AxxonSoft), Spojených států (Avigilon, FaceFirst), Španělska (FacePhi) a Tchaj-wanu (Vivotek). Geopolitický a technologický kontext těchto výrobců často reflektuje rozdílné přístupy k problematice biometrického rozpoznávání, a proto je vhodné zohlednit nejen technické parametry, ale i legislativní rámec v příslušných regionech.

Důležitým aspektem je také způsob implementace softwaru. V tomto ohledu lze rozlišit několik přístupů:

1. **Integrovaný software v kamerách:** tento přístup je typický pro výrobce, jako jsou Hikvision a Dahua, kteří vyvíjejí kamery s integrovanou funkcí rozpoznávání

obličejů. Tyto systémy jsou schopné provádět detekci v reálném čase přímo na zařízení, což snižuje nároky na centrální serverovou infrastrukturu. [36] [37]

2. **Serverový software:** tento model, typický pro systémy jako AxxonSoft Axxon One nebo NEC NeoFace, se vyznačuje tím, že rozpoznávání probíhá na serveru, což umožňuje zpracování rozsáhlých databází a vysokou výpočetní kapacitu. [38] [39]
3. **Cloudové řešení:** platformy jako FaceFirst využívají cloudovou architekturu pro vzdálené zpracování dat, což umožňuje snadné škálování, ale zároveň zvyšuje nároky na přenos a zabezpečení dat. [40]
4. **SDK pro integraci:** vývojové sady, jako je VisageSDK, poskytují flexibilitu pro integraci rozpoznávání obličejů do stávajících aplikací, což je vhodné zejména pro vývojářské projekty s potřebou přizpůsobení. [41]

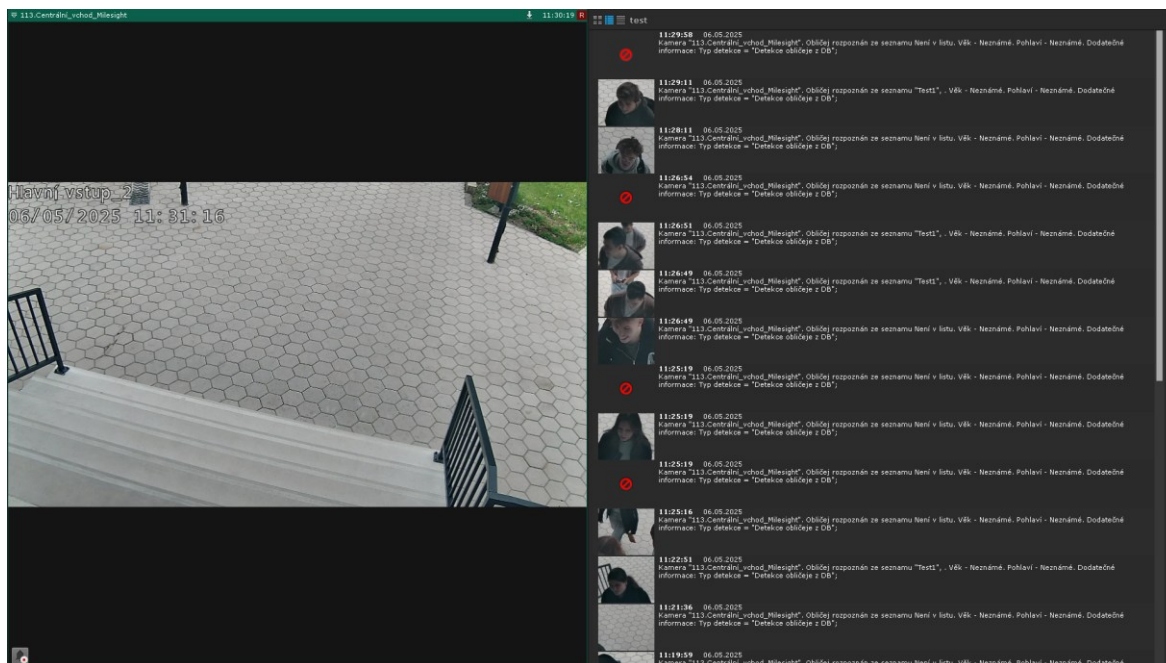
Přesnost rozpoznávání obličejů je klíčovým parametrem pro hodnocení kvality softwaru. Většina analyzovaných systémů dosahuje přesnosti nad 99 %, přičemž nejvyšší hodnoty (až 99,9 %) vykazují systémy Dahua a NEC, které využívají pokročilé algoritmy hlubokého učení a konvolučních neuronových sítí. Naopak systémy s širší analytickou funkcionalitou, jako je Bosch IVA, mají přesnost o něco nižší, avšak kompenzují to schopností detekce širšího spektra událostí. [37] [39]

Výhody jednotlivých systémů se různí podle aplikačního zaměření. Například Hikvision se vyznačuje rychlostí detekce v reálném čase, zatímco Axis se SAFR Inside nabízí flexibilní modulární přístup s možností integrace do různých bezpečnostních systémů. Naopak FacePhi se specializuje na digitální autentizaci v bankovním sektoru a poskytuje robustní ochranu uživatelských dat. Takto specializované přístupy zajišťují vysokou přidanou hodnotu v konkrétních segmentech trhu. [36][42]

Mezi slabiny jednotlivých softwarových řešení patří zejména technologické a finanční nároky. Například Hikvision nabízí omezené možnosti přizpůsobení algoritmů, zatímco Dahua může při komplexnějších úlohách vyžadovat výkonné servery. U systémů závislých na cloudových službách, jako je FaceFirst, mohou být vyšší provozní náklady, zatímco řešení typu SDK (VisageSDK) vyžadují značné programátorské znalosti. Závislost na softwaru třetí strany (např. SAFR u Axis) také přináší rizika spojená s kompatibilitou a licencováním. [36][37][40][41]

Posledním bodem je dostupnost ověřených údajů o výkonnosti a přesnosti. Většina softwarů deklaruje své výsledky na základě nezávislého testování, zejména prostřednictvím NIST

(National Institute of Standards and Technology), jehož výsledky potvrzují vysokou přesnost například u produktů NEC a Cognitec. U jiných systémů, jako je Avigilon, nejsou konkrétní hodnoty veřejně dostupné, což může komplikovat srovnání.



Obrázek 27 Ukázka detekce

(vlastní)

7 DETEKCE OSOB POMOCÍ VYBRANÉHO SOFTWARE

Pro tuto práci byl vybrán software AxxonOne, a to z důvodu zájmu o prozkoumání nové technologie, tak i dostupnosti pro praktické nastavování a testování. Tento software byl testován a nastavován na pražské střední škole, která byla autorovi známá z předchozího studia. Jako testovací subjekty byly využity fotografie studentů prvních ročníků z roku 2024/2025. Subjekty měly podepsaný souhlas se zpracováním osobních údajů, takže nedošlo k porušení žádných předpisů.

7.1 AxxonOne software

V současné době představuje software **Axxon One** jedno z nejpokročilejších řešení pro správu videa (Video Management Software – VMS), které je široce využíváno v oblasti bezpečnosti a monitoringu. Tento systém, vyvinutý ruskou společností **AxxonSoft**, je navržen tak, aby poskytoval vysokou úroveň přesnosti a spolehlivosti v aplikacích vyžadujících pokročilou analýzu videozáznamů a identifikaci osob na základě rozpoznávání obličejů. [38]

Jednou z klíčových vlastností systému Axxon One je jeho schopnost přesného rozpoznávání obličejů v reálném čase. Tento systém využívá moderní algoritmy hlubokého učení, které umožňují identifikovat osoby i za obtížných podmínek, jako je nedostatečné osvětlení nebo částečné zakrytí obličeje, například rouškami nebo brýlemi. Díky tomu je možné využít systém i v prostředích s proměnlivými podmínkami osvětlení, jako jsou letiště, nádraží či veřejné prostory. [38]

Systém Axxon One rovněž disponuje pokročilou analytikou na bázi umělé inteligence, která zahrnuje nejen rozpoznávání obličejů, ale také detekci podezřelého chování, jako je náhlé shlukování osob nebo pohyb v zakázaných zónách. Tato analytická vrstva umožňuje uživatelům efektivně spravovat bezpečnostní incidenty a přijímat okamžitá opatření. [38]

Mezi hlavní výhody Axxon One patří vysoká přesnost rozpoznávání obličejů (přes 90%), což je umožněno využitím pokročilých algoritmů strojového učení. Real-time detekce a možnost multi-kanálového zpracování výrazně zvyšují efektivitu monitorování rozsáhlých ploch. Další výhodou je škálovatelnost systému, díky níž lze snadno rozšiřovat kapacitu podle rostoucích potřeb bezpečnostního projektu. [38]

Na druhé straně je třeba zmínit i určitá omezení. Vzhledem k robustnosti systému jsou kladeny vyšší nároky na hardwarovou infrastrukturu, zejména na výkonné servery a grafické

jednotky, které zajišťují rychlé a efektivní zpracování velkého objemu dat. Dalším potenciálním omezením je složitost konfigurace, zejména při nasazení ve velkých bezpečnostních sítích, kde je nutná technická podpora při nastavování a optimalizaci systému AxxonOne. [38]

7.2 Používané prvky

Pro provádění detekce je zapotřebí kamerový systém. Pro naši detekci využijeme nainstalovanou kameru u vchodových dveří do budovy od výrobce Milesight. Konkrétně se jedná o IP kameru MS-C2966-X12RPE. Napájení máme řešené pomocí POE.



Obrázek 28 Milesight IP kamera

(zdroj: [43])

Tabulka 3 Vybrané důležité parametry kamery

Parametr	Hodnota
Obrazový senzor	CMOS SONY Progressive scan 1/2.8" (Starlight)
Min. osvětlení	0.002 Lux (barva) @ F1.6, 0 Lux (čb s IR)
WDR	Super WDR až 140dB
ZOOM objektiv	motor AF Zoom objektiv f=5.3-64mm F1.6-2.8, autofocus, Autoiris
Snímací úhel	61°-5° (horizontální), 36°-2° (vertikální), 69°-5° (diagonální)
IR přesvětlení	Smart IR LED II (180m)
DAy/Night	automatické přepínání pomocí IR cut filtru (ICR)
Max. rozlišení	1920 x 1080 / 60fps
Videokomprese	H.265+/H.265(HEVC)/H.264+/H.264/MJPEG
Datový tok	CBR (konstantní) / VBR (variabilní), 16kbps - 16Mbps
Obrazové parametry	jas / kontrast / saturace / ostrost

Audiokomprese	G.711/AAC/G.722/G.726
Ethernet	1x RJ45 port (10/100Mbit Ethernet)
Protokoly	IPv4/IPv6, ARP, TCP, UDP, RTP, RTSP, RTMP, RTCP, HTTP, HTTPS, DNS, DDNS, DHCP, FTP, NTP, SMTP, UPnP, Bonjour, SIP, SNMP, PPPoE, VLAN, 802.1x, QoS, IGMP, ICMP, SSL
NAS	podpora NAS (NFS, SMB/CIFS), ANR
Webové rozhraní	podpora webových prohlížečů Internet Explorer, Chrome, Firefox, Safari
Mobilní aplikace	aplikace Mobile APP pro Android, iPhone (iOS), podpora P2P
MicroSD slot	kompatibilní s MicroSD/SDHC/SDXC kartou (max. 1 TB, paměťová karta není v ceně)
Funkce	videodetekce pohybu, externí alarm. (alarm. vstup), maskování privátní zóny, BLC, HLC, 2D-DNR, 3D-DNR, Defog, ROI
VCA analýza	podpora video analytických funkcí VCA s podporou AI (Deep Learning): detekce osob a vozidel, detekce vstupu do zóny, detekce vystoupení ze zóny, pokročilá detekce pohybu, detekce neoprávněné manipulace s kamerou, detekce překročení linie, detekce podezřelého pohybu v zóně, ztráta objektu, odložení objektu, počítání osob, detekce tváří, heat mapa
Alarmové události	detekce pohybu, audio detekce, odpojení od sítě, tamper alarm (narušení kamery), alarm vstup ad.
Alarmové akce	FTP záznam, SMTP odeslání e-mailové zprávy, SD záznam, SIP vytočení linky VoIP telefonu, sepnutí alarm. výstupu, HTTP notifikace
Časosběrná funkce	periodicky ukládá v nastaveném intervalu snímky z kamery na FTP nebo SD kartu
Kompatibilita	ONVIF Profile S & G & Q & T, API
Třída prostředí	-40° až +60°C
Napájení	POE nebo DC12V, max. 8W (14W s IR LED), přepětová ochrana 4kV
Krytí	venkovní krytí IP67
Hmotnost	1447g
Rozměry	134 x 126 x 320 mm

(upraveno z: [43])

Dalším prvkem je UTP kabeláž propojující kameru se serverem, na kterém běží dané kamery.

A nakonec server, na němž pracuje software na detekci obličejů. Zde jsem ale nebyl blíže seznámen s jeho specifikacemi.



Obrázek 29 Server pro software AxxonOne

(zdroj: [44])

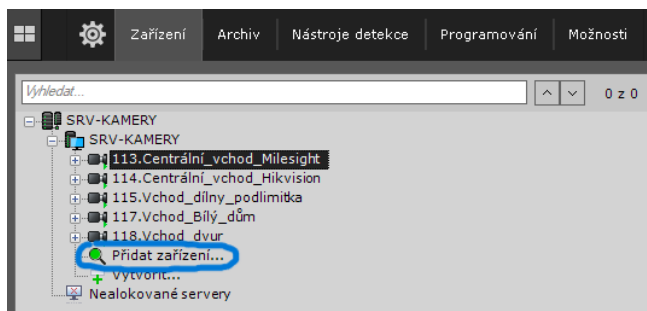


Obrázek 30 Server ve škole

(vlastní)

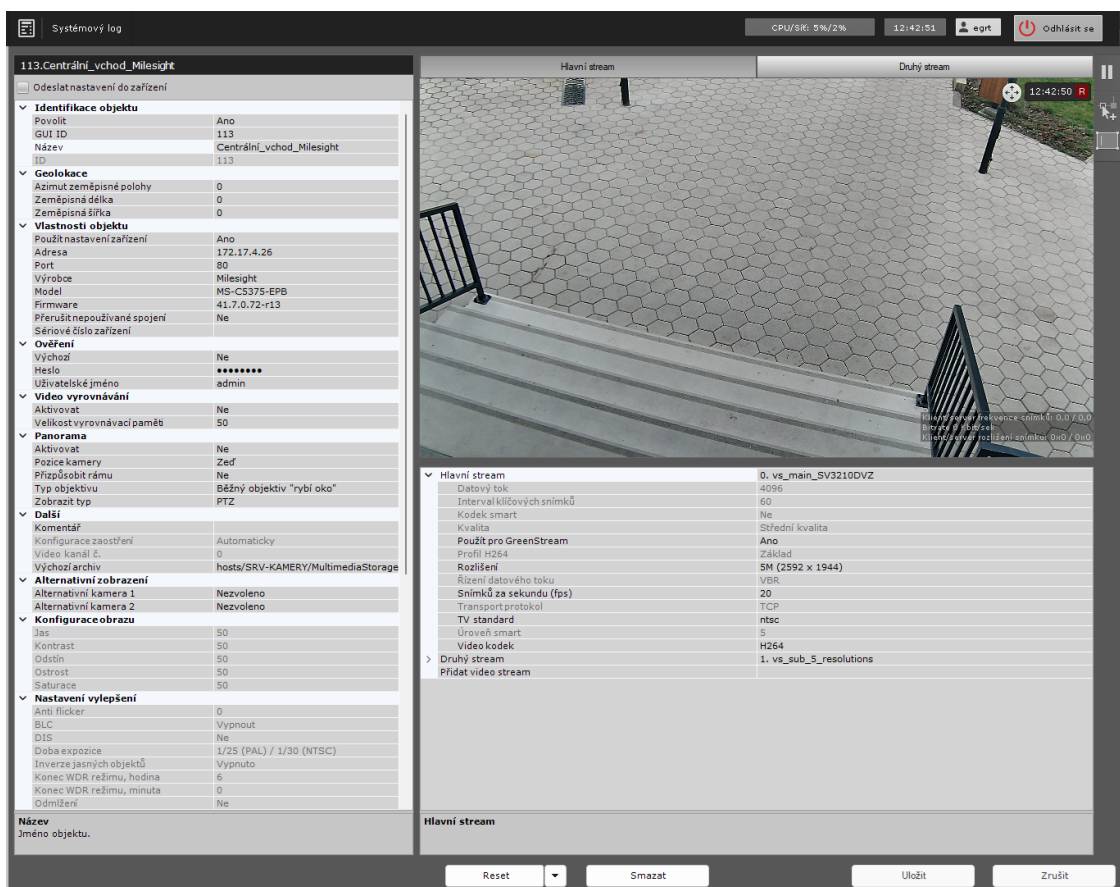
7.3 Proces nastavení a následné detekce

Po úspěšném nainstalování a zapojení prvků na svých místech se můžeme pustit do nastavování v aplikaci AxxonOne od společnosti AxxonSoft. Načte se server, ale nemáme tam žádnou kameru - tedy je musíme manuálně přidávat. Nejdříve je třeba připojit pomocí IP adresy kamery a přihlášení k ní si aktivovat kameru v softwaru. Na obrázku vidíme, že pomocí tlačítka „Přidat zařízení“ přidáme kameru (viz Obrázek 31 Přidání kamery).



Obrázek 31 Přidání kamery

(vlastní)



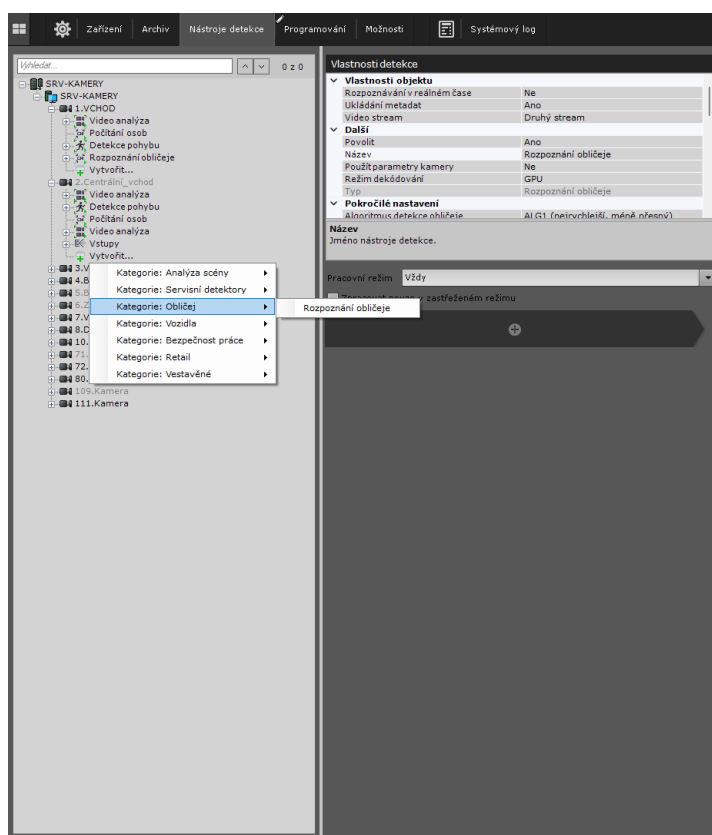
Obrázek 32 Vyplnění a ověření údajů

(vlastní)

Jak je vidět (Obrázek 32 Vyplnění a ověření údajů), ve „Vlastnosti objektu“ vyplníme IP adresu a port, který buď známe, anebo zjistíme na webovém rozhraní dané kamery. Určíme výrobce kamery a pak program nabízí výrobní typy od daného výrobce. Nejsou zde všechny modely, a tedy se orientujeme podle co nejbližšího modelu tomu, který používáme.

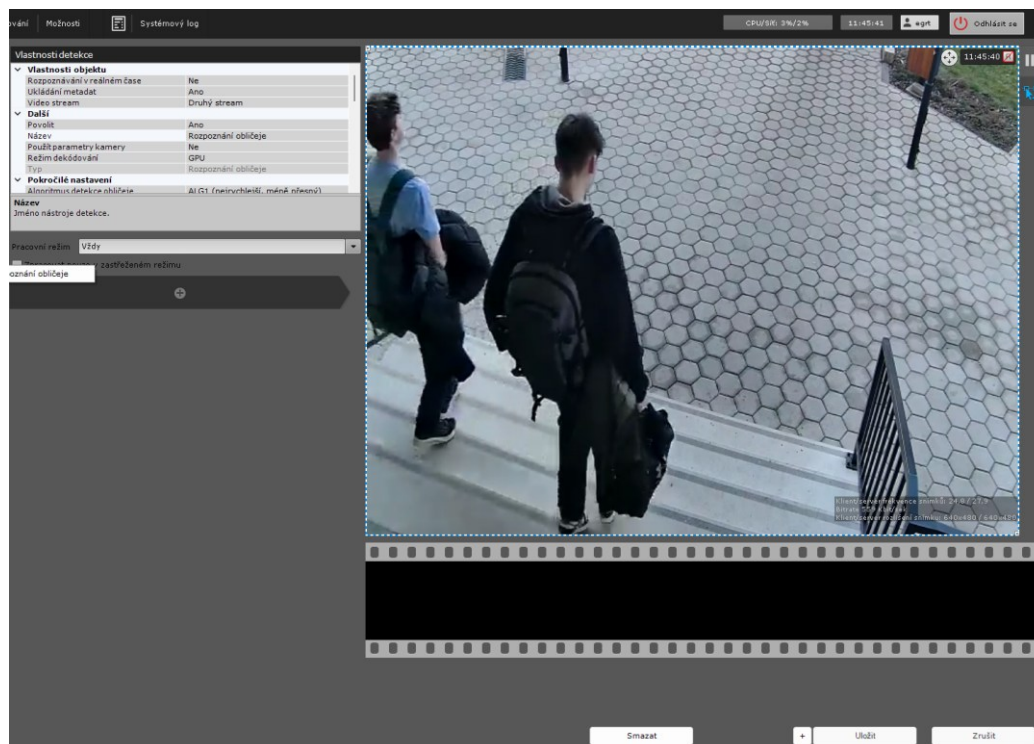
V „Ověření“ vyplníme uživatelské jméno, což bývá většinou od instalačních firem nastaveno na „admin“. Heslo, které jsme buď nastavovali my, anebo je od instalační firmy, a tedy si ho necháme od nich poslat. Poté by už měl naskočit stream kamery, kterou jsme přidali. Máme na výběr sledovat buď hlavní stream, který je v plné kvalitě, anebo druhý stream v horší kvalitě. Vždy pod streamem jsou vidět jeho parametry. Následně klikneme na tlačítko „uložit“ a první kamera je připravena.

Poté si v „Nástroje detekce“ (viz Obrázek 33 Nástroje detekce) vybereme naši kameru a klikneme na „Vytvořit“. Otevře se nabídka nástrojů detekce a my si vybereme „Obličej“ a ukáže se „Rozpoznání obličeje“. Poté se nám na streamu zobrazí modrobílý čtverec (viz Obrázek 34 Nastavení detekce), který udává místo detekce a můžeme jej zvětšovat a zmenšovat.



Obrázek 33 Nástroje detekce

(vlastní)



Obrázek 34 Nastavení detekce

(vlastní)

V „Základním nastavení“ (viz Obrázek 35 Parametry detekce) nastavíme Biometrická data na „Ano“. Můžeme si zde zapnout detekci maskování obličeje, kterou jsem ale v mojí práci nevyužil. To, co je dle mého názoru z výběru parametrů důležité, je „Pravost obličeje“, která nám určuje míru shody s danou fotkou u nás v databázi. Ostatní parametry se nám automaticky nastaví při počátečním vytvoření detekce.

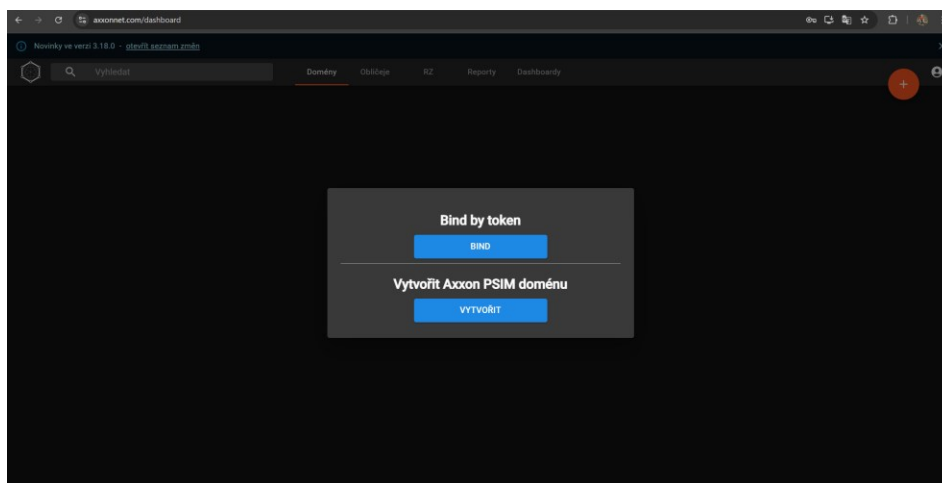
Vlastnosti detekce	
Zpracovat barevné snímky	Ne
▼ Základní nastavení	
Biometrická data	Ano
Detekovat maskování obličeje	Ne
HW pro nástroj detekce	CPU
Identify face attributes	Vypnuto
LivenessDetectionType	Vypnuto
Max. šířka obličeje	100
Maximální výška obličeje (%)	100
Min. výška obličeje	5
Minimální šířka obličeje (%)	5
Odhad věku a pohlaví	Ne
Pravost obličeje	90

Obrázek 35 Parametry detekce

(vlastní)

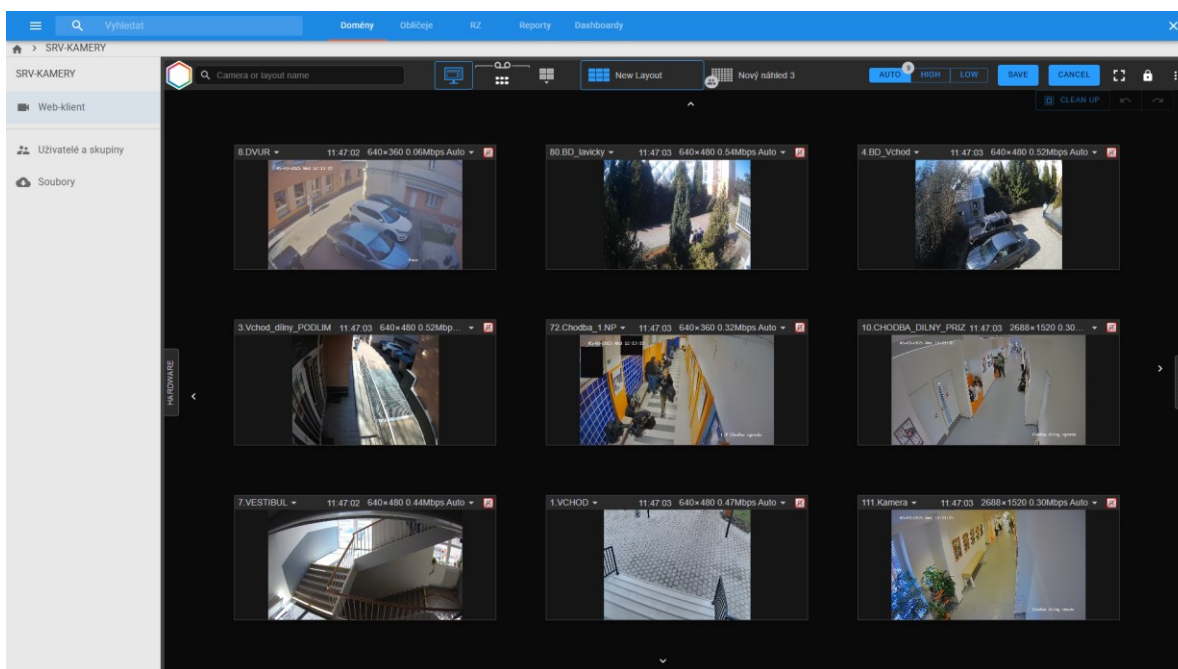
Poté je nutné vytvořit databázi fotek, které se budou využívat pro rozpoznávání obličejí. AxxonSoft vyvinul webové rozhraní AxxonNet pro tuto databázi. Sice si zde musíme

vytvořit zase účet, ale to je maličkost. Pomocí tokenu (viz Obrázek 36 Token pro napojení AxxonNetu) je propojen AxxonOne s AxxoNetem, v AxxonOne je na to kolonka v „Systémový log“. Poté by se měly zobrazit kamery (viz Obrázek 37 Naše kamery). Následně v sekci „Obličeje“ je třeba vytvořit databázi fotografií (viz Obrázek 38 Naše databáze fotek). Když se to podaří, už jen napojíme daný seznam na náš systém (viz Obrázek 39 Napojení seznamu na náš systém). Poté bychom ho měli vidět v AxxonOne softwaru (viz Obrázek 40 Viditelný seznam obličejů).



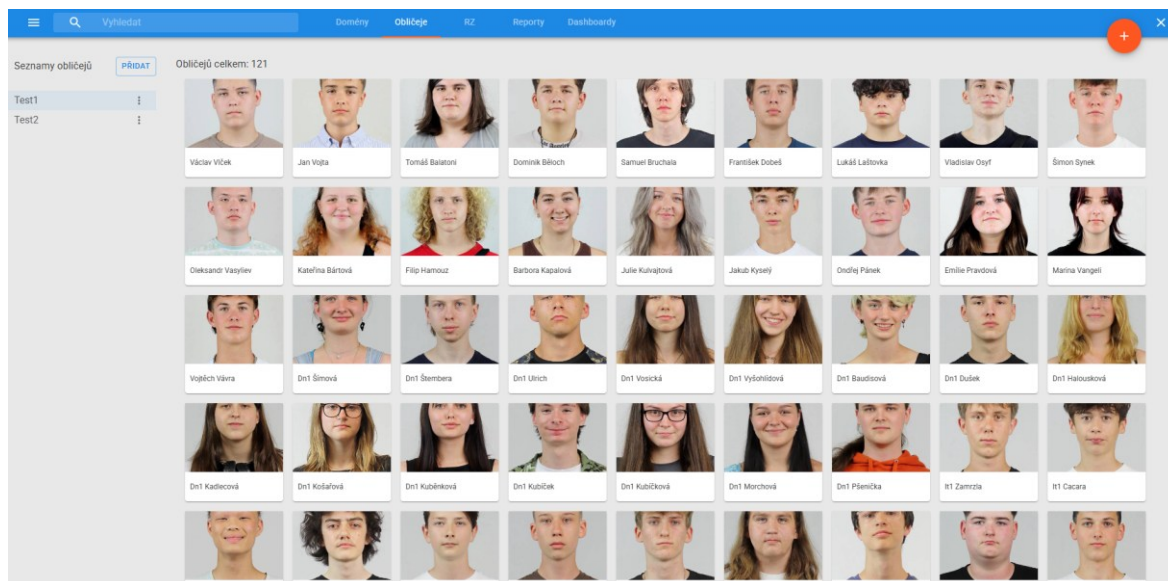
Obrázek 36 Token pro napojení AxxonNetu

(vlastní)

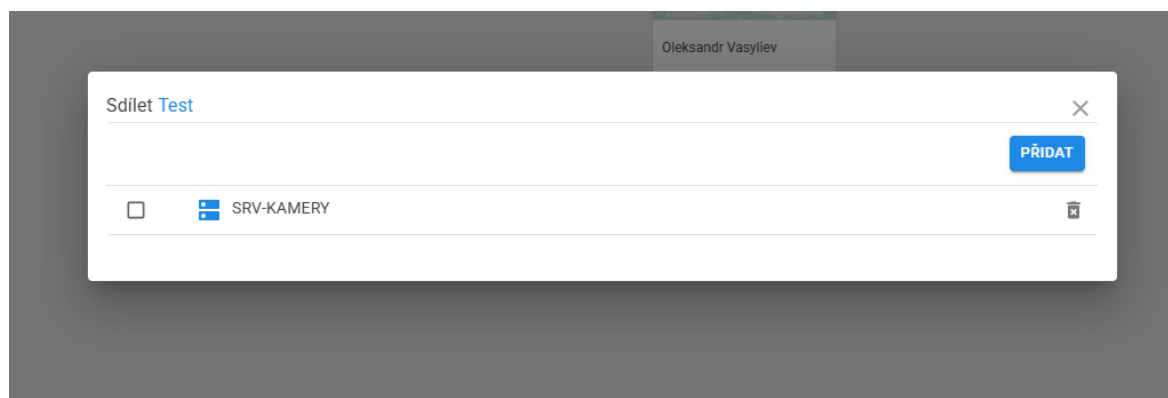


Obrázek 37 Naše kamery

(vlastní)



Obrázek 38 Naše databáze fotek

(vlastní)

Obrázek 39 Napojení seznamu na náš systém

(vlastní)

Seznam obličejů			
Smazat	Seznam obličejů	%	Nastavení seznamu
	Test1	85	

Obrázek 40 Viditelný seznam obličejů

(vlastní)

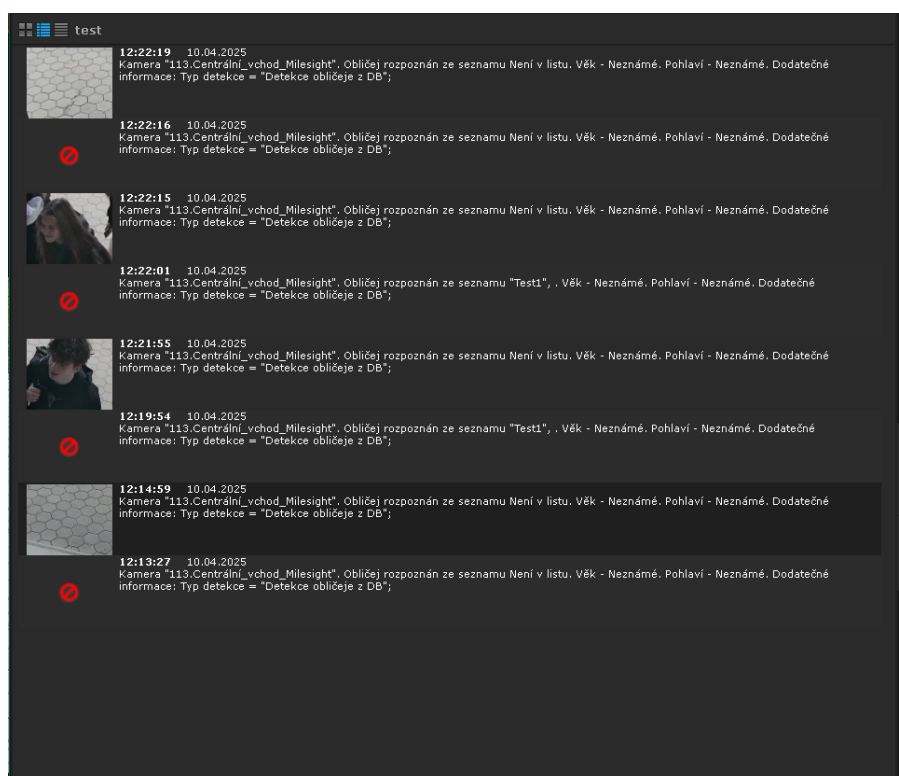
Při napojování našeho seznamu se přes mou snahu nedařilo dostat ho do softwaru AxxonOne. Musel jsem se obrátit na technickou podporu, která se tím začala zabývat.

Nejdříve technik zkontroloval nastavení našeho systému detekce a poté zkoušel hledat chybu na jejich webovém rozhraní na AxxonNetu.

Nemohl ale přijít na příčinu, a tak se musel poradit s kolegy v práci. Po pár dnech se vrátil a chtěl přístup na server, kde máme náš program. Našel nějaké nesrovnalosti, které opravil, a nakonec se zobrazil seznam tak, jak je vidět (Obrázek 40 Viditelný seznam obličejů).

7.4 Provedení detekce a následné vyhodnocení

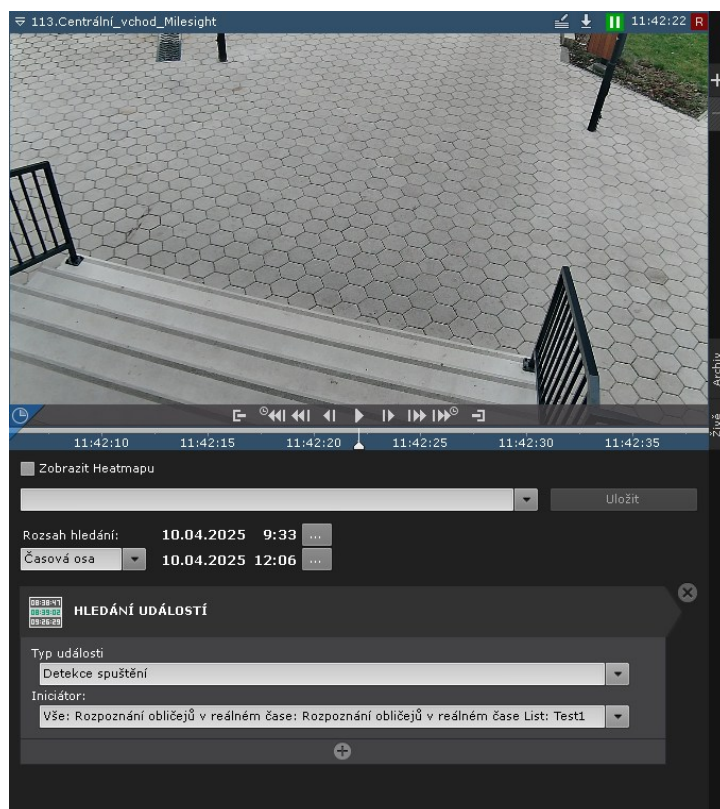
V školní den, kdy do školy chodí nejvíce studentů prvního ročníku, byla prováděna detekce. Byl jsem ve škole vždy alespoň 2 hodiny, abych mohl nějak porovnávat data. Jak je vidět na obrázku, vždy se načtou data podle toho, na jakou kameru se díváme. Jak je vidět na obrázku, sice ne vždy se zobrazí v obrázku daný obličej, důležité ale je, že se detekce provede. V popisku máme napsáno, jestli se obličej dané osoby v našem seznamu nachází nebo nikoli (viz Obrázek 41 Rozpoznávání obličejů).



Obrázek 41 Rozpoznávání obličejů

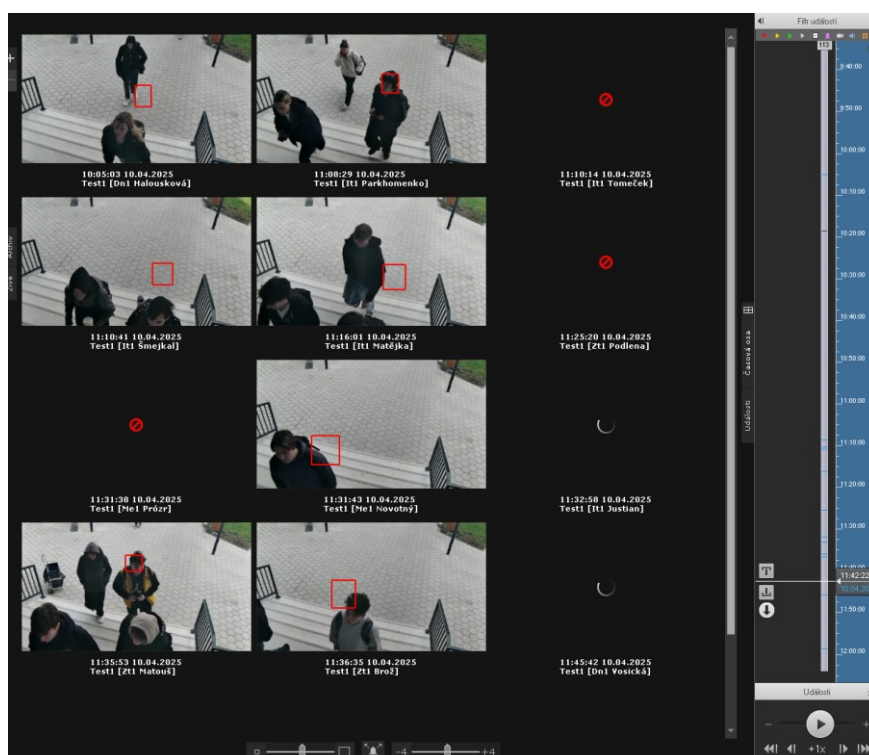
(vlastní)

Dále si můžeme otevřít v aplikaci archiv, který máme nastavený na 24 hodin, abychom dodržovali zákon. Je nutné si tedy zvolit „Detekci spuštění“ a dále najít iniciátor, což je zde „Vše“ (viz Obrázek 42 Hledání událostí). Zde si můžeme zobrazit proběhlé detekce. Z obrázku je vidět, že je jich dost, ale zase se nám některé bohužel nezobrazí, i když je na záznamu vidíme, pak na výsledku nejsou. V názvu je náš zvolený seznam, třída a pak příjmení pro identifikace. Máme zde i časovou osu, kde si můžeme projíždět daný záznam a měla by se nám zde zobrazit zaznamenaná detekce (viz Obrázek 43 Rozpoznání obličejů).



Obrázek 42 Hledání událostí

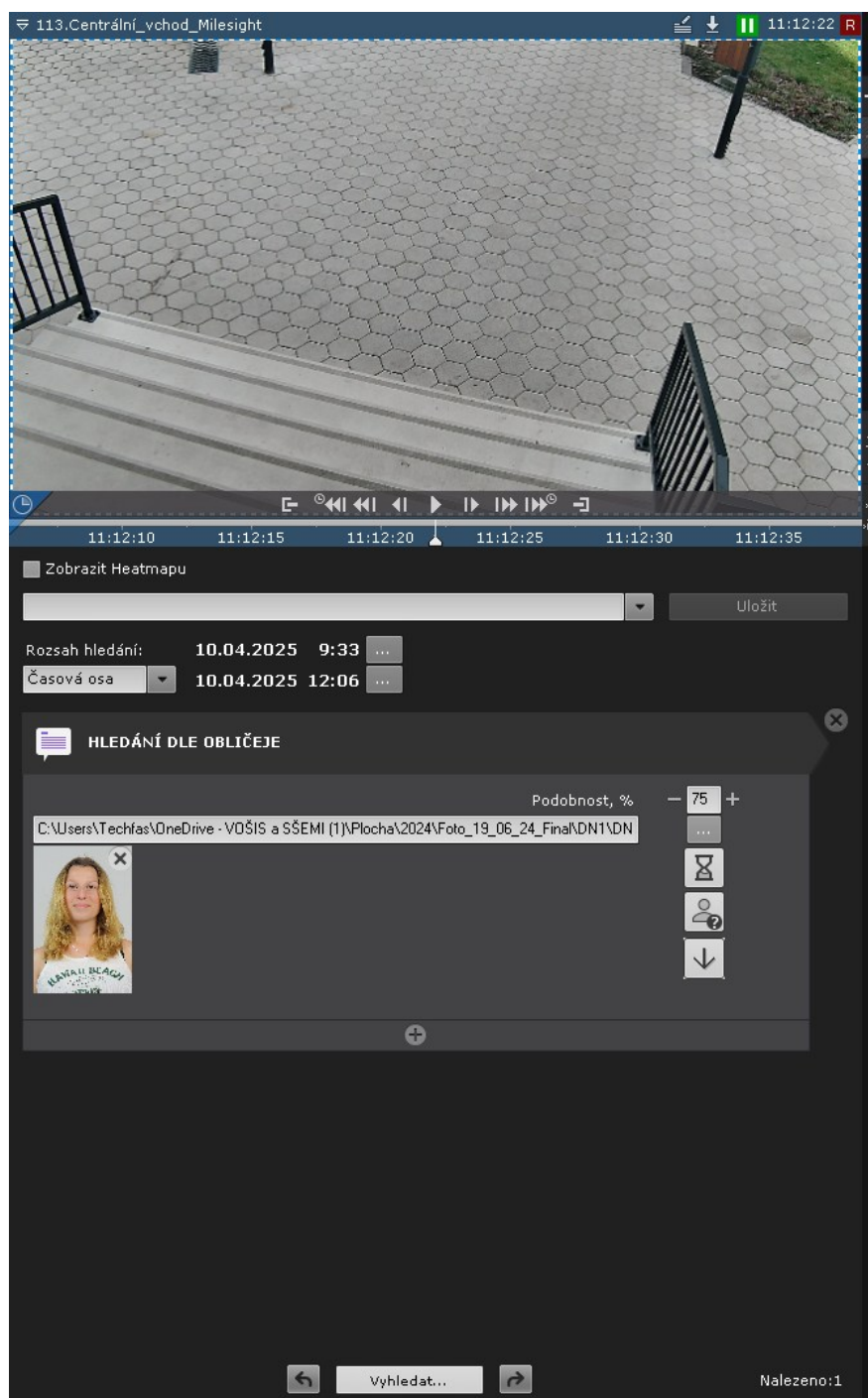
(vlastní)



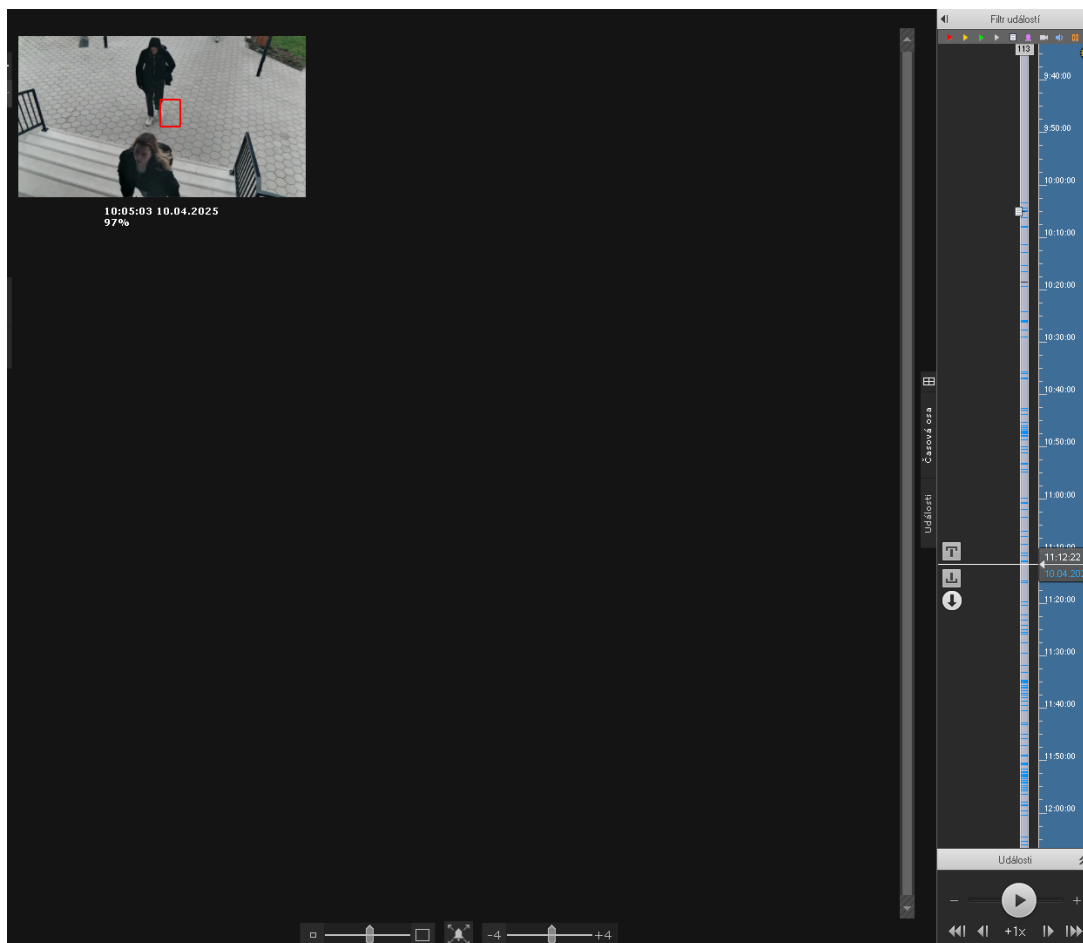
Obrázek 43 Rozpoznání obličejů

(vlastní)

V aplikaci v archivu můžeme hledat dle obličeje. Je nutné tedy mít dostupnou fotku dotyčné osoby, kterou chceme hledat, potom vytyčit čas na ose, který se nám má zobrazit, a prohledávat záznam. Jak je vidět na obrázku (Obrázek 44 Vyhledávání pomocí fotky), máme osobu na záznamu a ještě víme, který den a v kolik hodin byla provedena detekce. Dalším údajem je zde v procentech míra shody s fotkou obličeje z našeho seznamu. My zde máme 97 %, což je poměrně velká shoda, tedy je uvedená detekce úspěšná (Obrázek 45 Viditelná shoda).



Obrázek 44 Vyhledávání pomocí fotky

(vlastní)

Obrázek 45 Viditelná shoda

(vlastní)

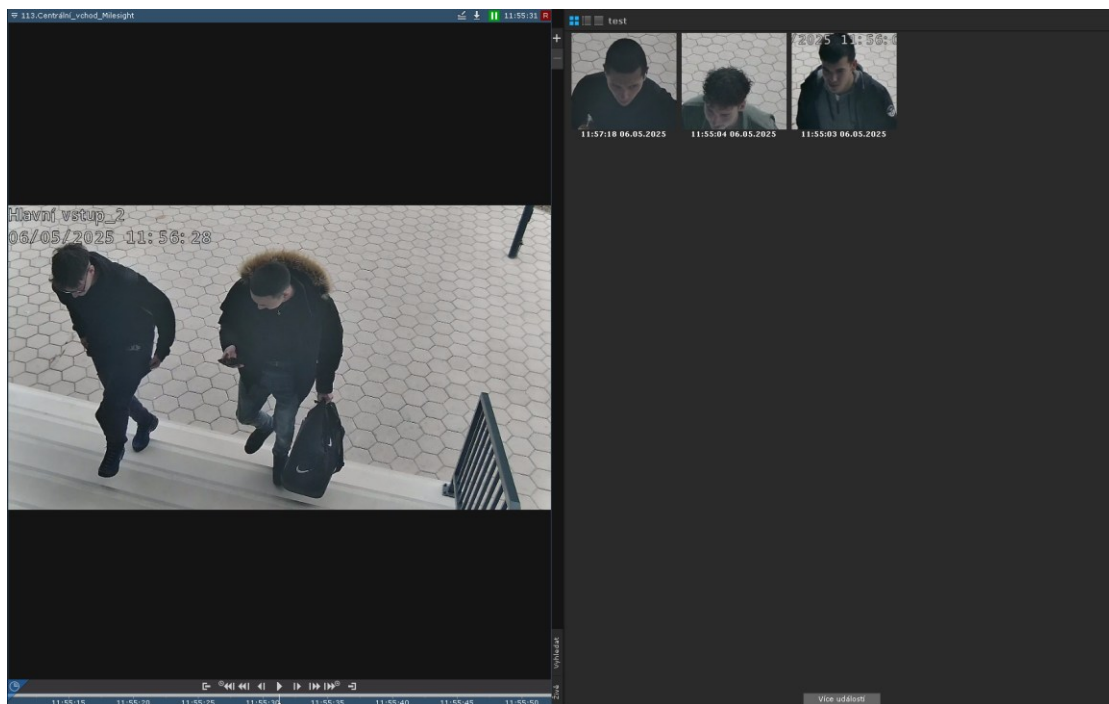
Je zde ale také dostupný seznam rozpoznaných obličejů na AxxonNetu. Obrázků je hodně a vidíme i informace, jestli byli nebo nebyli v seznamu, který máme v našem softwaru. Jak je vidět (viz Obrázek 46 AxxonNet seznam událostí), máme dostupný detekovaný obličej. Bohužel se zase stává, že zde buď úplně chybí, anebo je zde třeba jen chodník. Poté nám systém nabídne foto z našeho listu pro porovnání. Následují procenta shody. Uvedeno je také jméno seznamu, kdybychom jich náhodou měli více. Je patrné, na jaké kameře se pohyboval daný člověk. A nakonec je zde i jeho jméno a do jaké třídy patří. Tím, že je to byla jen testovací verze, se nám rozhodily třídy do jmen a naopak.

Snapshot	Original Image	Datetime	Accuracy	List Name	Camera Name	Name and Surname	Department	Comment
		2025-04-10 11:38:01	0	Not in any list	Vchod_Bílý_dům			
		2025-04-10 11:37:57	0	Not in any list	Centrální_vchod_Mile sight			
		2025-04-10 11:37:56	0	Not in any list	Centrální_vchod_Mile sight			
		2025-04-10 11:37:47	0	Not in any list	Vchod_Bílý_dům			
		2025-04-10 11:37:22	0	Not in any list	Centrální_vchod_Mile sight			
		2025-04-10 11:36:35	97,06	Test1	Centrální_vchod_Mile sight	Zt1 Brož	Filip	
		2025-04-10 11:36:29	88,66	Test1	Vchod_Bílý_dům	Vojtěch Vávra	MT	
		2025-04-10 11:36:25	91,93	Test1	Vchod_Bílý_dům	Mt1 Němcová	Nikola	

Obrázek 46 AxxonNet seznam událostí

(vlastní)

Bohužel zde není zaznamenána detekce (viz Obrázek 47 Neprovedená detekce), která je dle mého názoru nejspíš způsobena nastavením kamery a také úhlu obličeje pro detekci. Rozpoznání neproběhlo, což jde vidět v událostech napravo, podle času se provedla až pozdější detekce někoho jiného. Větší zoom už nastavit nelze, tudíž bude nutné lepší nastavení kamery a detekce.



Obrázek 47 Neprovedená detekce

(vlastní)

7.5 Shrnutí výsledků

V rámci této práce byl testován pokročilý software pro správu videa AxxonOne, a to v prostředí pražské střední školy. Výběr tohoto konkrétního softwaru byl motivován zájmem o nové technologie a dostupností pro praktické testování. Základní testovací materiál tvořily fotografie studentů prvních ročníků ze školního roku 2024/2025, přičemž všichni účastníci disponovali podepsaným souhlasem se zpracováním osobních údajů, což zajistilo soulad testování s příslušnými předpisy.

Software AxxonOne od společnosti AxxonSoft je významný především svou schopností provádět přesné rozpoznávání obličejů v reálném čase, což je umožněno pokročilými algoritmy hlubokého učení. Tato technologie zvládá detekovat obličeje i v komplikovaných podmínkách včetně nedostatečného osvětlení nebo částečného zakrytí obličeje. Mezi další výhody patří vysoká přesnost detekce obličejů přesahující 90 %.

Pro testování byla využita IP kamera Mileight MS-C2966-X12RPE, která poskytovala náležitou obrazovou kvalitu a podporu analytických funkcí potřebných pro software AxxonOne.

Proces implementace zahrnoval konfiguraci kamerového systému v softwaru AxxonOne. Nastavení probíhalo v několika krocích, od přidání kamery pomocí IP adresy

přes definování parametrů detekční zóny až po vytvoření a propojení databáze fotografií s webovým rozhraním AxxonNet. V průběhu implementace bylo nutné konzultovat technickou podporu kvůli potížím s propojením databáze, které se nakonec podařilo vyřešit zásahy technického týmu.

Samotná detekce obličejů byla provedena během vybraných školních dnů s cílem získat relevantní výsledky. Data ukazují, že ačkoliv systém úspěšně detekoval a identifikoval většinu obličejů s vysokou přesností shody (typicky nad 90 %), vyskytovaly se případy neúspěšné detekce.

Pro analýzu výsledků bylo využito nejen rozhraní softwaru AxxonOne, ale také webového rozhraní AxxonNet, které umožňovalo detailní přehled rozpoznaných obličejů včetně procentuální shody s databází. Výsledky jasně prokazují funkčnost a praktickou využitelnost softwaru, zároveň však poukazují na důležitost pečlivého technického nastavení, zejména optimalizace kamerových parametrů pro dosažení maximální efektivity a spolehlivosti detekce.

Celkově tato studie demonstrovala značný potenciál softwaru AxxonOne pro využití v bezpečnostních a monitorovacích aplikacích, zároveň však také identifikovala oblasti, které vyžadují další optimalizaci a důkladné technické nastavení.

ZÁVĚR

Na základě provedeného výzkumu a testování kamerového systému Axxon lze konstatovat, že tento systém představuje účinný nástroj pro identifikaci osob v kontrolovaných podmínkách. V rámci testů bylo prokázáno, že systém dosahuje vysoké přesnosti identifikace při standardních podmínkách vstupu do budovy. Nicméně výsledky rovněž ukázaly, že při proměnlivých světelných podmínkách nebo při zvýšené koncentraci osob v monitorovaném prostoru může docházet k poklesu přesnosti detekce.

Identifikace osob pomocí kamerových systémů je náročná na kvalitu záznamu a stabilitu prostředí, což vyžaduje precizní nastavení kamer i detekčních algoritmů.

Kromě technických aspektů je rovněž důležité dbát na legislativní rámec související s ochranou osobních údajů, neboť implementace kamerových systémů s identifikací osob představuje zásah do soukromí jednotlivců.

Celkově lze uzavřít, že kamerové systémy, jako je Axxon, představují významný přínos pro moderní bezpečnostní řešení, avšak jejich účinnost je podmíněna nejen kvalitním technickým zpracováním, ale i citlivým přístupem k ochraně osobních údajů.

SEZNAM POUŽITÉ LITERATURY

- [1] ADÁMEK, Milan; BARČOVÁ, Karla; BITALA, Petr; MACH, Václav a ŠEVČÍK, Jiří. *Dohledové videosystémy v bezpečnostních technologiích*. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2022. ISBN 978-80-7385-263-4.
- [2] Loveček, Tomáš a Nagy, Peter. *Bezpečnostné systémy:kamerové bezpečnostné systémy*. Žilina : Žilinská univerzita, 2008. ISBN 978-80-8070-893-1
- [3] *AHD kamerový systém*. Online. Kamerak.cz. Dostupné z: <https://www.kamerak.cz/clanek-2/ahd-kamerovy-system.html>. [cit. 2025-01-05].
- [4] *Analogová kamera*. Online. In: Absolon. -. Dostupné z: https://www.absolon.cz/katalog/kamerove-systemy--cctv_73/analogove-kamery_2808. [cit. 2025-03-07].
- [5] *Základní rozdělení kamerových systémů - rozdíly mezi AHD a IP*. Online. Securia Pro. 2020. Dostupné z: <https://www.securiapro.cz/clanek/zakladni-rozdeleni-kamerovych-systemu/>. [cit. 2024-12-31].
- [6] *Schéma IP kamera*. Online. In: TZBinfo. 2013. Dostupné z: <https://elektro.tzb-info.cz/10480-princip-cinnosti-typy-a-komunikacni-rozhrani-ip-kamer>. [cit. 2025-03-07].
- [7] *Základní rozdělení kamerových systémů - rozdíly mezi AHD a IP*. Online. Securia Pro. 2020. Dostupné z: <https://www.securiapro.cz/clanek/zakladni-rozdeleni-kamerovych-systemu/>. [cit. 2024-12-31].
- [8] *IP kamera*. Online. In: Escad Trade. -. Dostupné z: <https://www.escadtrade.cz/ip-kamerove-systemy/ip-kamery-a-nvr-milesight/>. [cit. 2025-03-07].
- [9] Lukáš, Luděk. *Bezpečnostní technologie, systémy a management II*. Zlín : VeR-BuM, 2012. ISBN 978-80-87500-19-4.
- [10] KŘEČEK, Stanislav. *Příručka zabezpečovací techniky*. 3. Praha: Cricetus, 2006. ISBN 80-902938-2-4.
- [11] *Ohnisková vzdálenost*. Online. In: Moje tajemno. 2015. Dostupné z: <https://moje.tajemno.net/ohniskova-vzdalenost/>. [cit. 2025-02-12].

- [12] *Clona objektivu.* Online. In: Fotoulita. -. Dostupné z: <http://www.fotoulita.cz/content/clona>. [cit. 2025-03-07].
- [13] *Hloubka ostrosti.* Online. In: Blogfotografa. -. Dostupné z: <https://www.blogfotografa.cz/hloubka-ostrosti-jak-na-ni/>. [cit. 2025-03-07].
- [14] *Super CCD.* Online. In: Digimanie. 2003. Dostupné z: <https://www.digimanie.cz/digitalni-fotoaparát-v-svetlocitlive-snimaci-prvky/7>. [cit. 2025-03-07].
- [15] *CMOS.* Online. In: Aldebaran. -. Dostupné z: https://www.aldebaran.cz/bulletin/2017_21_kub.php. [cit. 2025-03-07].
- [16] *Koaxiální kabel.* Online. In: Fyzmatik. 2010. Dostupné z: <https://fyzmatik.pise.cz/235-koaxial-a-terminator.html>. [cit. 2025-03-13].
- [17] *Kroucená dvojlinka.* Online. In: Ijs. -. Dostupné z: https://ijs2.8u.cz/index.php?option=com_content&view=article&id=19&Itemid=0. [cit. 2025-03-13].
- [18] *Optické vlákno.* Online. In: Techpedia. -. Dostupné z: [zdroj: https://techpedia.fel.cvut.cz/browse/?fileId=370&objectId=68&currPage=1021](https://techpedia.fel.cvut.cz/browse/?fileId=370&objectId=68&currPage=1021). [cit. 2025-03-13].
- [19] *DVR.* Online. In: CCTVSG. -. Dostupné z: <https://www.cctvsg.net/types-of-dvr-an-overview/>. [cit. 2025-03-13].
- [20] *NVR.* Online. In: Kamerak.cz. -. Dostupné z: <https://www.kamerak.cz/detail-193-1-D0814090/poe-nvr-7416-16ch-5mpx-h265-rekorder-pro-16-ip-kamer-cz-menu.html>. [cit. 2025-03-13].
- [21] *Box kamera.* Online. In: Flickr. 2011. Dostupné z: <https://www.flickr.com/photos/cctvsecuritysurveillance/5578479217>. [cit. 2025-02-26].
- [22] *Dome kamera.* Online. In: Hikvision. -. Dostupné z: <https://www.hikvision.com/cz/products/Turbo-HD-Products/PTZ-Cameras/Pro-Series/ds-2ae4225t-d/>. [cit. 2025-02-26].
- [23] *Bullet kamera.* Online. In: Hikvision. -. Dostupné z: <https://www.hikvision.com/en/products/IP-Products/Network-Cameras/Pro->

Series-EasyIP-/DS-2CD2025FWD-I/?subName=DS-2CD2025FWD-I+%28Black%29. [cit. 2025-02-26].

- [24] *Turret kamera*. Online. In: Hikvision. -. Dostupné z: <https://www.hikvision.com/ar/products/IP-Products/Network-Cameras/Pro-Series-EasyIP-/DS-2CD2385G1-I/?subName=DS-2CD2385G1-I>. [cit. 2025-02-26].
- [25] *Cube kamera*. Online. In: Hikvision. -. Dostupné z: <https://www.hikvision.com/cz/products/IP-Products/Network-Cameras/Wi-Fi-Series/ds-2cd2421g0-i-d-w/>. [cit. 2025-02-26].
- [26] *Panoramatická kamera*. Online. In: Hikvision. -. Dostupné z: <https://www.hikvision.com/ca-fr/products/IP-Products/Network-Cameras/Panoramic-Series/DS-2CD6D54FWD--I--Z--H--S---NFC-/>. [cit. 2025-02-26].
- [27] *PTZ kamera*. Online. In: Hikvision. -. Dostupné z: <https://www.hikvision.com/cz/products/Turbo-HD-Products/PTZ-Cameras/Pro-Series/ds-2ae4225t-d/>. [cit. 2025-02-26].
- [28] JANEČKOVÁ, Eva a BARTÍK, Václav. *Kamerové systémy v praxi*. Praha: Linde Praha, 2011. ISBN 978-80-7201-850-5.
- [29] ADÁMEK, Milan. *7. přednáška z předmětu Kamerové systémy*. Prezentace. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2018.
- [30] Dvořák, Pavel. Diplomová práce. *Popis objektů v obraze*. Brno : Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2011
- [31] DATTA, Asit Kumar; DATTA, Madhura a BANERJEE, Pradipta. *Face detection and recognition : Theory and Practice*. London, New York: CRC Press, 2016. ISBN 9781482226546.
- [32] *Detekce hran*. Online. In: Wikipedia. 2025. Dostupné z: https://en.wikipedia.org/wiki/Edge_detection#/media/File:%C3%84%C3%A4retuvastuse_n%C3%A4ide.png. [cit. 2025-04-30].
- [33] *Úroveň šedi*. Online. In: Scikit-image. Dostupné z: https://scikit-image.org/docs/stable/auto_examples/features_detection/plot_glm.html. [cit. 2025-04-30].

- [34] *Analýza příznaků.* Online. In: Ibug. Dostupné z: <https://ibug.doc.ic.ac.uk/research/detection-static-geometric-facial-features/>. [cit. 2025-04-30].
- [35] *3D obraz.* Online. Adobe Stock. Dostupné z: <https://stock.adobe.com/search?k=3d+facial+recognition>. [cit. 2025-05-10].
- [36] *Hikvision.* Online. Dostupné z: <https://www.hikvision.com/en/core-technologies/see-smarter-technology/acusense/?q=acusense&pageNum=1&position=1&hiksearch=true>. [cit. 2025-05-09].
- [37] *Dahua.* Online. Dahua. Dostupné z: <https://software.dahuasecurity.com/en/dss>. [cit. 2025-05-09].
- [38] *AxxonOne.* Online. AxxonSoft. Dostupné z: <https://cz.axxonsoft.com/>. [cit. 2025-05-09].
- [39] *NEC.* Online. NEC. Dostupné z: <https://www.nec.com/en/global/solutions/biometrics/face/index.html>. [cit. 2025-05-09].
- [40] *Facefirst.* Online. Facefirst. Dostupné z: <https://www.facefirst.com/>. [cit. 2025-05-09].
- [41] *VisageSDK.* Online. Dostupné z: <https://visagetechologies.com/face-recognition/>. [cit. 2025-05-09].
- [42] *Axis.* Online. Axis. Dostupné z: <https://www.axis.com/products/axis-face-detector>. [cit. 2025-05-09].
- [43] *Milesight IP kamera.* Online. ESCAD Trade. Dostupné z: <https://www.escadtrade.cz/2mp-venkovni-profi-bullet-plus-ai-ip-kamera-12x-zoom-5-3-64mm-60fps-wdr-140db-ir-smart-led-180m-poe-splnuje-ndaa-p21851/>. [cit. 2025-05-10].
- [44] *Server.* Online. Senetic. Dostupné z: <https://www.senetic.cz/product/P55280-421>. [cit. 2025-05-11].

SEZNAM OBRÁZKŮ

Obrázek 1 Analogová kamera.....	15
Obrázek 2 IP kamera - schéma	15
Obrázek 3 IP kamera.....	16
Obrázek 4 Ohnisková vzdálenost u objektivu	17
Obrázek 5 Clona objektivu	18
Obrázek 6 Hloubka ostrosti – příklad	19
Obrázek 7 Super CCD	21
Obrázek 8 Princip CMOS snímače	22
Obrázek 9 Koaxiální kabel	24
Obrázek 10 Kroucená dvojlinka	26
Obrázek 11 Optické vlákno	27
Obrázek 12 Ukázka DVR	28
Obrázek 13 Ukázka NVR	29
Obrázek 14 Ukázka kamer: vlevo kamera Box, vpravo kamera Dome.....	31
Obrázek 15 Ukázka kamer: vlevo Bullet kamera, vpravo Turret kamera	32
Obrázek 16 Ukázka kamer: vlevo Cube kamera, vpravo panoramatická kamera	32
Obrázek 17 Ukázka kamery: PTZ kamera.....	32
Obrázek 18 Funkční bloky VSS	39
Obrázek 19 Rozpoznání obličeje	41
Obrázek 20 Přístupy k technikám detekce obličeje	45
Obrázek 21 Typické obrázky pro klasifikaci obličejů	45
Obrázek 22 Detekční problém	46
Obrázek 23 Detekce hran.....	47
Obrázek 24 Úroveň šedi	48
Obrázek 25 Analýza příznaků.....	51
Obrázek 26 3D obraz rozpoznávání obličeje	59
Obrázek 27 Ukázka detekce	64
Obrázek 28 Milesight IP kamera	66
Obrázek 29 Server pro software AxxonOne	68
Obrázek 30 Server ve škole	68
Obrázek 31 Přidání kamery	69
Obrázek 32 Vyplnění a ověření údajů	69
Obrázek 33 Nástroje detekce	70
Obrázek 34 Nastavení detekce.....	71

Obrázek 35 Parametry detekce	71
Obrázek 36 Token pro napojení AxxonNetu	72
Obrázek 37 Naše kamery	72
Obrázek 38 Naše databáze fotek	73
Obrázek 39 Napojení seznamu na náš systém	73
Obrázek 40 Viditelný seznam obličejů	74
Obrázek 41 Rozpoznávání obličejů	75
Obrázek 42 Hledání událostí	76
Obrázek 43 Rozpoznání obličejů	76
Obrázek 44 Vyhledávání pomocí fotky	77
Obrázek 45 Viditelná shoda	78
Obrázek 46 AxxonNet seznam událostí	79
Obrázek 47 Neprovedená detekce	80

SEZNAM TABULEK

Tabulka 1 Třídy prostředí	39
Tabulka 2 Softwary na rozpoznání obličeje	62
Tabulka 3 Vybrané důležité parametry kamery	66

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AHD	Analog High Definition
ANN	Artificial Neural Network
CCD	Charge Couple Device
CCTV	Uzavřený televizní okruh
Cm	Centimetr
CMOS	Complementary Metal Oxide Semiconductor
CMY	Cyan, Magenta, Yellow
CNN	Convolutional Neural Networks
CPU	Central Processing Unit
ČR	Česká republika
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOF	Deep of Field
DRAM	Dynamic Random Access Memory
DSP	Digital Pixel System
DVR	Digital Video Recorder
EMI	Elektromagnetické rušení/interference
EMS	Elektromagnetická susceptibilita
FTP	File Transfer Protocol
Gb/s	Gigabit za sekundu
HDD	Hard Disk Drive
HD	High Definition
HDMI	High-Definition Multimedia Interface
HTTP	HyperText Transfer Protocol
IPv4	Internet Protocol version 4

IPv6	Internet Protocol version 6
IP	Internet Protocol
Km	Kilometr
Mb/s	Megabit za sekundu
MHz	Mega Hertz
MFT	Master File Table
MMF	Multimode Fibre
Mpix	Mega Pixel
MTCNN	Multi-Task Cascaded Convolutional Networks
NIST	Národní institut standardů a technologie
NVR	Network Video Recorder
ONVIF	Open Network Video Interface Forum
OSN	Organizace Spojených Národů
P	Progressive Scan - neprokládaný obraz
PCI	Peripheral Component Interconnect
PC	Počítač
PoE	Power over Ethernet
PSIA	Physical Security Interoperability Alliance
PVC	Polyvinylchlorid
RGB	Red, Green, Blue
RJ – 45	Zakončení ethernetového konektoru
ScTP/FTP	Screened/Foil Twisted Pair
SMF	Single Mode Fibre
STP	Shielded Twisted Pair
SVM	Support Vector Machines
Tb/s	Terabit za sekundu

TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
VGA	Video Graphics Array
VSS	Video Surveillance Systém – Dohledový videosystém
Wi-Fi	Wireless Fidelity
ZOOÚ	Zákon o ochraně osobních údajů
ZP	Zákoník práce
ÚOOÚ	Úřad pro ochranu osobních údajů
2D	Dvoudimenzionální
3D	Třidimenzionální