



Diplomová práce

Dálkově ovládaná fotopast s rozpoznáváním obrazu

Studijní program:

N0714A270010 Mechatronika

Autor práce:

Bc. Pavel Filjač

Vedoucí práce:

Ing. Lenka Kosková Třísková, Ph.D.

Ústav nových technologií a aplikované informatiky

Liberec 2024



Zadání diplomové práce

Dálkově ovládaná fotopast s rozpoznáváním obrazu

Jméno a příjmení:

Bc. Pavel Filjač

Osobní číslo:

M22000036

Studijní program:

N0714A270010 Mechatronika

Zadávací katedra:

Ústav nových technologií a aplikované informatiky

Akademický rok:

2024/2025

Zásady pro vypracování:

1. Definujte základní požadavky na vlastnosti cílového řešení.
2. Proveďte rešerši existujících řešení a srovnajte je s definovanými požadavky.
3. Navrhněte a realizujte HW prototyp fotopasti.
4. Navrhněte a realizujte SW fotopasti dle požadavků na zařízení včetně dovednosti rozpoznání tváře.
5. Navrhněte a realizujte backendovou část aplikace sloužící k ukládání fotografií a jejich zobrazování.
6. Realizované řešení otestujte.

<i>Rozsah grafických prací:</i>	dle potřeby dokumentace
<i>Rozsah pracovní zprávy:</i>	40 – 50 stran
<i>Forma zpracování práce:</i>	tištěná/elektronická
<i>Jazyk práce:</i>	čeština

Seznam odborné literatury:

- [1] LEA, Perry. IoT and edge computing for architects: implementing edge and IoT systems from sensors to clouds with communication systems, analytics, and security. Second edition. Birmingham: Packt, 2020. ISBN 978-1-83921-480-6.
- [2] SIMMONDS, Chris. Mastering embedded Linux programming: harness the power of Linux to create versatile and robust embedded solutions. Community experience distilled. Birmingham: Packt Publishing, 2015. ISBN 978-1-78439-253-6.
- [3] MONK, Simon. Raspberry Pi cookbook. Second edition. Beijing: O'Reilly, 2016. ISBN 978-1-491-93910-9.
- [4] GONZALEZ, Rafael C. a WOODS, Richard E. Digital image processing. Global edition. New York: Pearson, [2017]. ISBN 978-1-292-22304-9.

<i>Vedoucí práce:</i>	Ing. Lenka Kosková Třísková, Ph.D. Ústav nových technologií a aplikované informatiky
-----------------------	--

<i>Datum zadání práce:</i>	21. října 2024
<i>Předpokládaný termín odevzdání:</i>	9. května 2025

doc. Ing. Josef Černohorský, Ph.D.
děkan

L.S.

doc. Dr. Ing. Jaroslav Hlava
garant studijního programu

Prohlášení

Prohlašuji, že svou diplomovou práci jsem vypracoval samostatně jako původní dílo s použitím uvedené literatury a na základě konzultací s vedoucím mé diplomové práce a konzultantem.

Jsem si vědom toho, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci nezasahuje do mých autorských práv užitím mé diplomové práce pro vnitřní potřebu Technické univerzity v Liberci.

Užiji-li diplomovou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti Technickou univerzitu v Liberci; v tomto případě má Technická univerzita v Liberci právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Současně čestně prohlašuji, že text elektronické podoby práce vložený do IS STAG se shoduje s textem tištěné podoby práce.

Beru na vědomí, že má diplomová práce bude zveřejněna Technickou univerzitou v Liberci v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů.

Jsem si vědom/a následků, které podle zákona o vysokých školách mohou vyplývat z porušení tohoto prohlášení.

6. ledna 2025

Bc. Pavel Filjač

Dálkově ovládaná fotopast s rozpoznáváním obrazu

Abstrakt

Tato diplomová práce se zabývá kompletním zprovozněním fotopasti s nočním viděním se záložním zdrojem napájení a s možností jejího dálkového ovládání, včetně aplikování rozpoznání známých osob na základě jejich obličejových rysů. Pro rozpoznání obličejů bylo využito pokročilých algoritmů strojového učení, které umožňují rychlé a přesné vyhodnocení obrazu za různých světelných podmínek, včetně úplné tmy díky infračervenému nočnímu vidění.

V práci se analyzují požadavky na vlastnosti zařízení, podle kterých se následně volí vhodný hardware a jeho struktura zapojení. Součástí práce je také vývoj webového rozhraní, které umožňuje vzdálené ovládání zařízení, přístup k uloženým záznamům a správu přístupu.

Navrhované řešení předkládá komplexní nástroje pro zajištění objektu s možností dalšího rozšíření funkcí v budoucnosti. Výkon a stabilita systému byly ověřovány v reálném prostředí, kdy byla ověřena požadovaná spolehlivost i funkčnost celého zařízení.

Klíčová slova

fotopast, rozpoznání obličeje, vzdálený přístup, záložní zdroj, noční vidění, cloudové úložiště, webové rozhraní

Remote control camera trap using image recognition

Abstract

This diploma thesis deals with the complete operation of the camera trap with night vision with a backup power source and with the possibility of its remote control, including applying recognition of known persons based on their facial features. Advanced machine learning algorithms were used for face recognition, enabling fast and accurate image evaluation under various lighting conditions, including total darkness, thanks to infrared night vision.

The work analyzes the requirements for the properties of the target device, according to which appropriate hardware and its structure are subsequently selected engagement. The work also includes the development of a web interface, which allows remote device control, access to saved recordings and access management.

The proposed solution presents complex tools for securing the object with the possibility of further expansion of functions in the future. The performance and stability of the system were verified in a real environment, where the required reliability and functionality of the entire device were verified.

Keywords

camera trap, face recognition, remote control, backup power supply, night vision, cloud storage, web interface

Poděkování

Rád bych poděkoval za odborné vedení a cenné rady při realizaci této diplomové práce Ing. Lence Koskové Třískové, Ph.D.

Obsah

Seznam obrázků.....	11
Seznam grafů	11
Seznam tabulek.....	11
Seznam zdrojových kódů	11
Seznam zkratk.....	12
1 Úvod	14
1.1 Cíle práce	14
2 Specifikace funkce zařízení	16
2.1 Definice požadavků	16
2.1.1 Fotografování scén	16
2.1.2 Funkce rozeznávání	16
2.1.3 Organizace fotografií	17
2.1.4 Požadavky na hardware	17
2.2 Aktuálně dostupné produkty	17
2.2.1 Klíčové parametry fotopastí	18
2.2.2 Porovnání vybraných fotopastí	19
2.3 Obecný návrh k realizaci na základě požadavků	20
2.3.1 Zachytávání fotek ve dne i v noci	20
2.3.2 Uspořádání a propojení	20
2.3.3 Technické zázemí	22
2.4 Legislativa	22
3 Hardware a zapojení	23
3.1 Hardware uvnitř technického zázemí	23
3.1.1 Automatický přepínač baterie – UPS modul YX850	23
3.1.2 MOSFET IRLZ44N	23
3.1.3 Hardware pro podporu funkce UPS	24
3.1.4 Step-down měnič napětí M398F	25
3.1.5 Raspberry Pi 5	25
3.1.6 Další hardwarové komponenty	25
3.2 Hardware mimo technické zázemí	26
3.2.1 Arducam 8MP Sony IMX219	26
3.2.2 IR přísvit	27
3.2.3 Modul Zámku	28

3.2.4	Ovládací panel.....	28
3.2.5	PIR senzor	29
3.3	Zapojení.....	29
3.3.1	Zapojení dle schématu	30
3.3.2	Vstupy a výstupy z mikrokontroleru Raspberry	31
4	Software v Raspberry Pi 5.....	33
4.1	Obecná architektura vytvořených skriptů	33
4.1.1	Podpůrné nástroje Systemd a AutoSSH.....	34
4.2	Hlavní skript	34
4.2.1	Funkce foceni_fce	36
4.2.2	Funkce pro zjištění překrytí kamery	37
4.2.3	Funkce pro přidání známých tváří	38
4.2.4	Funkce pro nahrávání fotek do cloudového úložiště	39
4.2.5	Ostatní funkce	39
4.3	Skript pro rozpoznání osob	39
4.3.1	Face-recognition a dlib.....	39
4.3.2	Virtuální prostředí	40
4.3.3	Praktické použití	40
4.4	Skript pro přidání nových známých tváří	41
4.5	Skript pro komunikaci	42
4.5.1	SFTP přenos	42
4.5.2	Princip činnosti.....	42
5	Amazon S3	43
5.1	AWS Identity and Access Management a využití úložiště	43
6	Amazon EC2	44
6.1	Konfigurace serveru	44
6.1.1	Amazon Linux 2.....	44
6.1.2	Webový server	45
6.2	Webové rozhraní	45
6.2.1	Django a CSRF	45
6.2.2	Hlavní stránka a přihlášení	46
6.2.3	Kontrolní panel	48
6.2.4	Znamé tváře a další	48
6.2.5	Správa a odesílání e-mailů	50

7	Testování fotopasti	51
7.1	Z hlediska funkčnosti se zaměřením na rozpoznání	51
7.1.1	Rozpoznání s IR přísvitem	52
7.1.2	Rozpoznání v denním režimu a zátěžový test	53
7.2	Z hlediska bezpečnosti	56
7.2.1	Na straně serveru	56
7.2.2	Na straně Raspberry	56
8	Závěr	57
	Použitá literatura	58
	Přílohy	61
A	Obsah přiloženého souboru	61
B	Fotografie technického zázemí fotopasti	62

Seznam obrázků

Obrázek 1 Ukázka designu fotopasti (4).....	18
Obrázek 2 Možné uspořádání v cílovém umístění.....	21
Obrázek 3 Automatický přepínač baterie - UPS modul YX850 (5)	23
Obrázek 4 Schottky dioda SR540 (7).....	24
Obrázek 5 Přijímač EV1527 (11).....	26
Obrázek 6 Arducam 8MP Sony IMX219.....	26
Obrázek 7 Modul IR přísvitu.....	27
Obrázek 8 Ovládací panel.....	28
Obrázek 9 Schéma zapojení napájení v technickém zázemí	29
Obrázek 10 Zapojení na mikrokontroleru	31
Obrázek 11 Diagram připojení.....	33
Obrázek 12 UML diagram	35
Obrázek 13 Amazon EC2 (28)	44
Obrázek 14 Přihlašovací stránka.....	46
Obrázek 15 Hlavní stránka	47
Obrázek 16 Kontrolní panel.....	48
Obrázek 17 Známé tváře.....	49
Obrázek 18 Přidání známé tváře	49
Obrázek 19 Stránka se správou přístupu	50
Obrázek 20 Testovací umístění.....	51
Obrázek 21 Noční rozpoznání	53
Obrázek 22 Snímek ve dne s nasazenou čepicí	55
Obrázek B.1 Fotografie technického zázemí.....	62

Seznam grafů

Graf 1 Vývoj teploty CPU	55
--------------------------------	----

Seznam tabulek

Tabulka 1 Porovnání vybraných fotopastí	19
Tabulka 2 Zjištěná data (první polovina intervalu)	53
Tabulka 3 Zjištěná data (druhá polovina intervalu)	53
Tabulka 4 Souhrnné hodnoty	54

Seznam zdrojových kódů

Zdrojový kód 1 Příkaz pro kameru	36
Zdrojový kód 2 Ukázka porovnání tváří	41

Seznam zkratek

4K – Rozlišení, přibližně 4000 pixelů horizontálně

AC - Alternating Current

AWS – Amazon Web Services

BAT-/BAT+ - Kladný nebo záporný pól baterie

CPU – Central Processing Unit

CSI - Camera Serial Interface

CSRF - Cross-Site Request Forgery

CSS - Cascading Style Sheets

DSI - Display Serial Interface

EC2 - Elastic Compute Cloud

GND - Ground

GPIO - General-Purpose Input/Output

GSM - Global System for Mobile Communications

HDMI - High-Definition Multimedia Interface

HTML - HyperText Markup Language

I/O – Input / output

IAM - Identity and Access Management

IMAP- Internet Message Access Protocol

IoT – Internet of Things

IR- InfraRed

JPEG - Joint Photographic Experts Group

JSON - JavaScript Object Notation

LED - Light Emitting Diode

MIPI - Mobile Industry Processor Interface

MOSFET - Metal-Oxide-Semiconductor Field-Effect Transistor

PHP - Hypertext Processor

PIR - Passive Infrared Sensor

POP3 - Post Office Protocol 3

SFTP - Secure File Transfer Protocol

SMTP - Simple Mail Transfer Protocol

SQL - Structured Query Language

SSH – Secure Shell

TCP/IP - Transmission Control Protocol/Internet Protocol

UPS - Uninterruptible Power Supply

URL - Uniform Resource Locator

Wi-Fi - Wireless Fidelity(místní bezdrátová síť, často pro připojení k internetu)

1 Úvod

Sledování pohybů osob a související bezpečnostní opatření jsou oblastmi, které se díky technologickému pokroku v poslední době velmi rychle rozšiřují. Fotopasti jsou jedním z nástrojů využívaných v bezpečnostním odvětví, a nejen v něm – jde o nenápadné zařízení s autonomními funkcemi, určené k automatickému fotografování nebo natáčení videí s detekcí pohybu. Díky své univerzálnosti nacházejí své místo v monitoringu v různých oblastech – od divoké přírody po zabezpečení majetku. Jejich použití je širokospektrální. V divoké přírodě jsou cenným pomocníkem pro sledování zvěře. Naopak v urbanizovaných oblastech dobře slouží pro ochranu majetku, ať už před nedovoleným vniknutím, poškozením, nebo jinými nelegálními aktivitami. Dražší typy fotopastí obvykle nabízejí rozšiřující funkce. Jednou z nich může být například i možnost nastavení takzvaných chráněných zón, které umožňují zasílat pověřeným osobám informace o případném narušení takové zóny, nebo různými I/O rozšiřujícími porty. U takových zařízení je ale třeba dbát na jejich správné umístění a na jejich vlastní ochranu, protože vzhledem k jejich vyšší hodnotě se mohou samy stát cílem odcizení.

Fotopast je obvykle kompaktní zařízení spojující několik klíčových prvků do jednoho celku. Centrálním prvkem je kamera schopná pořizovat fotografie nebo videa ve vysoké kvalitě a je aktivována pohybovým senzorem – typicky infračervený senzor PIR – který reaguje na změny teploty v okolí a detekuje pohybující se objekty jako jsou lidé nebo živočichové. Důležitou součástí je také osvětlující systém, který umožňuje zachytit snímky i za tmy – moderní fotopasti k tomuto účelu využívají infračervené osvětlení nepozorovatelné lidským okem, a tak vizuálně nezasahující do přirozeného prostředí. Obvyklá technická infrastruktura se skládá z čipu (procesoru), paměťových komponent a energetických prostředků nezbytných pro správnou funkci zařízení (1).

1.1 Cíle práce

Tato diplomová práce se zabývá návrhem a realizací systému pro dálkově ovládanou fotopast s možností detekce a rozpoznávání obličejů. V úvodních fázích se práce zaměřuje na analýzu a definici požadavků na zařízení, včetně požadavků na spolehlivost detekce za různých provozních podmínek.

Následně se práce věnuje návrhu vhodného hardwarového a softwarového řešení. Součástí je výběr technologií pro technické zázemí fotopasti i její periferie a implementace algoritmů, které zajistí funkčnost systému. Při návrhu je brán zřetel na optimalizaci zařízení s ohledem na minimalizaci datového toku a celkovou spolehlivost

Další část této práce se soustředí na vytvoření uživatelsky přívětivého webového rozhraní pro snadné prohlížení pořízených snímků a jednoduché ovládaní zařízení. Webové rozhraní bude navrženo takový způsobem, aby poskytovalo intuitivní přístup k funkcím systému, včetně ovládaní základních funkcí zařízení. Systém bude také schopen provádět specifické akce na základě rozpoznání obličeje, jako je například odemknutí zámku, což rozšíří jeho praktické využití. Při návrhu webového rozhraní a komunikace fotopasti bude brán zřetel na použití zabezpečených technologií.

2 Specifikace funkce zařízení

Každý technický projekt začíná definováním požadavků jako základu pro následné navrhování řešení. Tento proces zahrnuje shromažďování a analýzu technických a uživatelsky orientovaných požadavků na zařízení, před jeho vytvořením. Správné stanovení požadavků je klíčové pro úspěšnost projektu a umožní tak vytvoření efektivního a bezpečného systému, jehož funkce budou plně v souladu s požadavky. Po stanovení požadavků následuje fáze vytvoření funkčního návrhu. Je třeba navrhnout takový systém, který bude v korelaci s aktuálními technologiemi a standardy. Funkční návrh se zaměřuje na strukturu systému, volbu vhodného hardwarového vybavení a zajištění dostatečné bezpečnosti. Je klíčové mít jasnou představu o požadovaných vlastnostech a cílech zařízení pro optimalizaci technických řešení. Výsledné řešení by také mělo zohlednit možná rizika a definovat postupy ke snížení nebo minimalizaci těchto rizik (2).

2.1 Definice požadavků

Fotopast bude zařízení navržené pro zachycení fotografií za různých světelných podmínek a s širokými funkcemi umožňujícími její všestranné využití. Umístěna bude na místě s dostupností elektrické sítě a internetového připojení, pomocí Wi-Fi nebo kabelovým připojením.

2.1.1 Fotografování scén

Funkce fotopasti musí zahrnovat schopnost pořizovat kvalitní fotografie za různých světelných podmínek, ve dne i v noci, s rozlišením vyšším než 3 megapixely, aby zachytila dostatečné množství detailů. Fotopast by měla být schopna spouštění snímání buď detekcí pohybu nebo v předem pevně nastavených intervalech (periodicky), nebo na základě vzdáleného příkazu od uživatele.

2.1.2 Funkce rozeznávání

Na základě pořízených fotografií je schopna zjistit, zda se na fotografii nachází tvář člověka. Pokud se na fotografii bude nacházet tvář člověka, tak ji fotopast bude schopna porovnat se známými tvářemi, které bude mít k dispozici a určit, zda se na fotografii nenachází známá osoba. Pokud fotopast identifikuje shodu se známou osobou, tak ji otevře elektronický zámek umístěný na dveřích a umožní jí tak přístup. Z důvodu předcházení možnému problému spojeného s případným výpadkem internetového spojení, není žádoucí, aby byla tato dovednost dislokována mimo místní zařízení.

2.1.3 Organizace fotografií

Fotografie pořízené zařízením budou automaticky nahrány do cloudové databáze pro další zpracování a uchování. Pro úsporu přenosové kapacity, především s ohledem na účtování dat podle objemu, mohou být tyto fotografie odeslány v nižším rozlišení, než v jakém byly vytvořeny. Přesto budou v plné kvalitě uloženy na interním úložišti zařízení, aby je bylo možné v případě potřeby do určité doby získat i v plném rozlišení.

2.1.4 Požadavky na hardware

Fotopast se bude skládat z několika hlavních částí. Modulu, ve kterém bude zakomponováno snímací zařízení, chráněné proti vnějším vlivům. Druhou částí bude technické zázemí fotopasti, které bude obstarávat nepřetržité napájení, zároveň zde bude i „mozek“ celého systému. Technické zázemí bude umístěno uvnitř objektu, což znamená, že nebude třeba zvláštní ochrany vůči vnějším povětrnostním vlivům. Dále zde bude modul pro detekci pohybu, zámek na dveře a jednoduchý ovládací panel, který bude sloužit pouze pro vypnutí, zapnutí a restartování systému.

2.2 Aktuálně dostupné produkty

Když je dnes zapotřebí opatřit si zařízení typu fotopasti, obvykle se využije internetových vyhledávačů. Po zadání klíčového slova „fotopast“ se zobrazí hlavně internetové obchody bez žádného velkého množství materiálů, které by se daly použít pro rešeršní činnost. Praktické rady a testy fotopastí jsou v českém online prostředí zatím poměrně málo dostupné. Stejně to platí i pro výsledky hledání v databázích technických knihoven (například Národní technická knihovna, Moravská zemská knihovna).

Pro účely rešerše produktů fotopastí bylo nutné procházet různé online obchody, aby bylo možné identifikovat opakující se texty a popisy, které se obvykle vyskytují u prodejců tohoto typu zařízení. Z přehledu těchto obchodů vyplývá, že většina z nich se zaměřuje na vybavení pro myslivost, zatímco menší část nabízí fotopasti určené pro zabezpečovací účely.

Ze zmíněného lze usoudit, že fotopasti se v dnešní době často využívají zejména k myslivosti, k ověření biodiverzity nebo sledování chování divokých zvířat a pro další účely.

Při studiu informací o použití fotopastí k jiným účelům než k monitorování zvířat se lze setkat pouze se strohými informacemi – například s možností jejich využití pro ochranu majetku (3).



Obrázek 1 Ukázka designu fotopasti (4)

2.2.1 Klíčové parametry fotopastí

- Rozlišení – Vyšší rozlišení fotoaparátu zajišťuje detailnější a kvalitnější snímky, což je zvláště důležité pro identifikaci zvířat nebo osob. Například fotopasti značky BUNATY nabízejí modely s rozlišením až 32 MP, což zajišťuje vysokou kvalitu obrazu (5).
- Detekční rozsah – Detekční rozsah určuje, jak daleko a široko dokáže fotopast detekovat pohyb.
- Rychlost spouštění – Rychlost spouštění určuje, jak rychle fotopast reaguje na detekci pohybu.
- Odolnost proti povětrnostním vlivům a maskování – Fotopasti jsou navrženy tak, aby odolaly různým povětrnostním podmínkám, včetně deště, sněhu a prachu. Maskování a design jsou důležité pro nenápadnost zařízení v terénu (6).
- Noční vidění – Tato funkce je obvykle umožněna díky infračervenému přísvitu.
- Napájení a výdrž na baterii – Fotopasti obvykle fungují na baterie, což ovlivňuje jejich výdrž a frekvenci výměny. Některé modely umožňují použití solárních panelů, což prodlužuje životnost zařízení a eliminuje potřebu časté výměny baterií.

- Kapacita úložiště a formát záznamu – Fotopasti ukládají pořízené snímky a videa na paměťové karty (obvykle microSD). Větší kapacita karty umožňuje delší dobu sledování a ukládání. Některé modely podporují různé formáty záznamu, včetně fotografií a videí, což poskytuje flexibilitu v dokumentaci událostí.
- Konektivita a možnosti přenosu dat – pokročilé modely fotopastí podporují připojení přes Wi-Fi, Bluetooth nebo mobilní sítě (např. 3G, 4G), což umožňuje vzdálený přístup k pořízeným snímkům a videím. Například fotopast UOVision Home Guard W1 je speciálně navržena pro ostrahu majetku a umožňuje zasílání snímků a videí s minimální prodlevou (7).

2.2.2 Porovnání vybraných fotopastí

Model	BUNATY FULL HD (8)	UOVision Home Guard W1 (7)	FOXcam Wi-Fi (9)	KeepGuard KG698A (10)
Rozlišení [MP]	24	12	5	13 denní, 2 noční
Detekční rozsah [m]	-	15–20	25	25
Zorné pole [°]	52	58	55	55 denní, 50 noční
Rychlost spouště [s]	0,7	0,6	-	-
Noční vidění	ANO – až 20 m	ANO – až 16 m	ANO – až 30 m	ANO – až 30 m
Video	ANO	ANO	ANO	ANO
Výdrž na baterii	-	až 1 rok	až 1 rok	až 1 rok
Max. kapacita [GB]	až 32	až 32	až 256	až 256
Bezdrátová konektivita	NE	Wi-Fi, GSM	Wi-Fi	NE
Cena [Kč]	5290	7540	2790	3990

Tabulka 1 Porovnání vybraných fotopastí

Z nabídek internetových prodejců je zřejmé, že klasické fotopasti obvykle nedisponují pokročilými funkcemi, jakými jsou detekce obličeje nebo interakce s dalšími zařízeními. Klasické fotopasti se spíše soustředí na nepřetržitý provoz, maskovaný hardware a zachytávání fotek na SD kartu, nebo jejich odesílání přes GSM síť.

Pokročilé funkce rozpoznávání objektů, interakce s dalšími zařízeními jsou v odvětví zabezpečení spíše přenechány dražším modelům IP kamer, které na rozdíl od fotopastí bývají velmi dobře viditelné.

2.3 Obecný návrh k realizaci na základě požadavků

Fotopast, sloužící pro zabezpečení majetku, by měla být takovým zařízením, které je schopné zachytávat snímky ve dne i v noci, reagovat na různé podněty, odesílat data do cloudového úložiště a zároveň umožňovat další funkcionality, jako je rozpoznávání obličejů či ovládání zámku. V následujícím textu bude postupně navrženo řešení jednotlivých požadavků, přičemž jádrem zařízení bude Raspberry Pi 5 a to především z důvodu vysoké kompatibility a možnosti snadného připojení až dvou kamer, pro možnost budoucího rozšíření, díky dvěma integrovaným kamerovým vstupům.

2.3.1 Zachytávání fotek ve dne i v noci

Pro zachytávání snímků ve dne i v noci je klíčové zvolit vhodný kamerový modul. Na trhu existuje široká nabídka kamerových modulů. Kromě zásadní dovednosti focení ve dne i v noci při výběru vhodného kamerového modulu hrálo důležitou roli také rozlišení kamery, kompatibilita, zorný úhel, kompaktnost a v neposlední řadě i pořizovací cena. Tyto požadavky vyselektovaly pouze kamery od dvou výrobců – Arducam a Waveshare. Od výrobce Waveshare se jedná například o model Waveshare RPi IR-CUT Camera nebo Waveshare IMX290-83 IR-CUT Starlight kamera. Vzhledem k tomu, že jedny ze stěžejních parametrů pro výběr kamery jsou její rozlišení a zorný úhel, tak jako možné nejlepší řešení byl vybrán kamerový modul Arducam 8MP Sony IMX219 s motorizovaným IR filtrem. Kamerové moduly od výrobce Waveshare nabízí buď mnohem nižší rozlišení (2 megapixels), nebo malý zorný úhel (75,7°). Vybraný kamerový modul je detailněji popsán v kapitole 3.2.1. Noční snímání bude doplněno o infračervený přísvit. Kamera i infračervený přísvit budou chráněny v odolném krytu, který je ochrání před vlivy počasí.

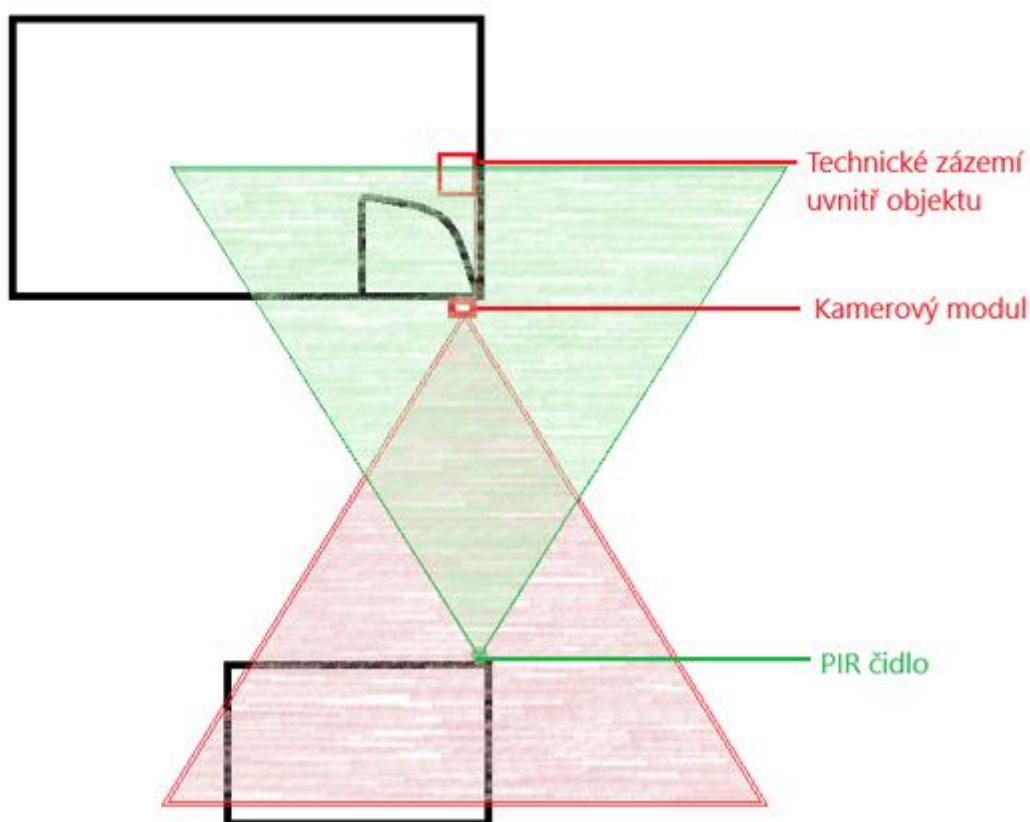
2.3.2 Uspořádání a propojení

Očekává se, že kamerový modul s IR přísvitem budou mimo budovu a technické zázemí bude uvnitř budovy. Díky tomuto uspořádání v případě potenciálního fyzického poškození či odcizení nedojde okamžitě ke ztrátě celého zařízení, ale pouze kamery a IR přísvitu. Škoda na majetku bude tedy mnohem nižší. Spolu s tímto uspořádáním však vzniká nutnost vyřešit kvalitní spojení modulu kamery s IR přísvitem a technického zázemí. Daná kamera disponuje pro přenos obrazu plochým 15 pinovým kabelem, který je více náchylný k poškození.

Takové spojení by nebylo dostatečně kvalitní a spolehlivé, což je jeden z cílů práce. Bylo proto vybráno řešení, které aplikuje převodník CSI-HDMI (a v technickém zázemí obráceně HDMI-CSI) a díky tomu bude komunikace fungovat na spolehlivějším fyzickém spojení, jakým je HDMI kabel.

IR přísvit bude připojen kulatým 3linkovým kabelem. Dva vodiče mu poskytnou zdroj napájení a jeden bude navíc sloužit pro potřeby zabezpečení, které je detailněji popsáno v kapitole 7.

Dále bude vyvinut ovládací panel, který bude disponovat 1 tlačítkem, 1 přepínačem a nějakým typem signalizace stavu. Tento panel bude s technickým zázemím propojen 6 linkovým kabelem. Nakonec je třeba zmínit i zámek, který bude spojen s technickým zázemím běžným dvojlinkovým vodičem.



Obrázek 2 Možné uspořádání v cílovém umístění

Na obrázku 2 je načrtnuto jedno z možných budoucích umístění důležitých modulů v cílovém umístění. Větší černý objekt představuje budovu, zatímco menší objekt je pouze přístřešek na dříví. Úhly zorných polí a některé další aspekty jsou vyobrazeny pouze ilustrativně a neodpovídají přesně realitě. Přesto lze dle obrázku posoudit, že takové řešení má velkou výhodu v tom, že PIR čidlo není umístěno v okolí kamery a díky tomu je systém méně nápadný. Z funkčního hlediska bude ale PIR čidlo při takovém umístění vždy snímat i pohyb v „mrtvých“ úhlech zorného pole kamery, a naopak kamera by měla potenciál snímat i v „mrtvých“ úhlech umístění PIR čidla, které jí v případě pohybu v této oblasti nedá signál pro zahájení snímání.

Na druhou stranu kamera má poměrně široké zorné pole (viz kapitola 3.2.1), také je nutné, aby byla umístěna v blízkosti dveří a protilehlý objekt není třeba, aby byl perfektně sledován, takže by v tomto případě mohla výhoda lepšího skrytí převážet před nevýhodami takového uspořádání.

2.3.3 Technické zázemí

V technickém zázemí bude muset být kromě „mozku“ celého zařízení, kterým bude Raspberry Pi 5 také mnoho dalších modulů. Především modul pro zajištění funkce UPS, napájecí modul nebo přijímač na frekvenci 433 MHz. Detailně je technické zázemí popsáno v kapitole 3.

2.4 Legislativa

Na fotopasti se dle Úřadu pro ochranu osobních údajů nahlíží stejně jako na ostatní kamerová zařízení. Vztahují se na ně veškeré právní podmínky jako u jiných technický prostředků ke zpracování osobních údajů. Dále cituji vyjádření ÚOOÚ (11).

Pokud je fotopast instalována např. pro potřeby monitorování zvěře a zároveň dochází k zaznamenávání náhodných snímků procházejících osob, jedná se o nahodilé shromažďování osobních údajů. Nejsou-li tyto údaje dále cíleně zpracovávány, pak se ve smyslu ustanovení § 3 odst. 4 zákona č. 101/2000 Sb. tento zákon aplikovat nebude. Ochranu soukromí lze v případě zveřejnění těchto náhodných snímků řešit podle občanského zákoníku.

Naopak, pokud je záměrem provozovatele využití fotopasti jako nástroje pro zabezpečení objektů, resp. obecně k ochraně majetku před škodou způsobenou jinými osobami, jde o zcela záměrné zpracovávání osobních údajů, na něž se uplatňuje zákon č. 101/2000 Sb. v celém svém rozsahu. Ten, kdo se rozhodne provozovat takové zařízení, tedy musí respektovat základní principy ochrany soukromí a osobní údaje může zpracovávat jen za podmínek, které zákon stanoví, zejména všech povinností týkajících se zabezpečení uchovávaných informací podle § 13 citovaného zákona.

3 Hardware a zapojení

Hardwarová část je jednou ze stěžejních oblastí této práce. V této části budou detailně popsány hardwarové prvky a jejich zapojení.

3.1 Hardware uvnitř technického zázemí

3.1.1 Automatický přepínač baterie – UPS modul YX850

Modul YX850 automaticky přepne zdroj napájení při výpadku energie. Za normálních okolností je zařízení napájeno síťovým zdrojem, který je připojen ke svorkám DC+ a DC-. V případě výpadku hlavního zdroje napájení modul přepne napájení zařízení na baterii, která je připojena ke svorkám BAT+ a BAT-. Baterii lze, při použití tohoto modulu, zároveň nabíjet ze síťového zdroje (12).

Specifikace:

Provozní napětí: 5–48 V DC

Max. zátěžový proud: 10 A

Rozměry: 61×29×18 mm (12)



Obrázek 3 Automatický přepínač
baterie - UPS modul YX850 (12)

3.1.2 MOSFET IRLZ44N

IRLZ44N je logický N-kanálový MOSFET v balení TO-220 určený pro spínání při zatížení s nízkými hradlovými napěťovými signály. Jeho plné otevření nastává již při 3,3 V, což jej činí vhodným pro řízení pomocí mikrokontrolerů. Dokáže pracovat s proudem až 47 A. Je ideálním kandidátem pro rychlé spínání zátěžových prvků jako jsou motory, relé nebo LED světla. Maximální povolené napětí mezi „drainem“ („odvod“ nebo „kolektor“ u bipolárních tranzistorů) a sourcem („zdrojem“) dosahuje 55 V (13).

3.1.3 Hardware pro podporu funkce UPS

První komponentou pro spolehlivou funkci UPS je Schottkyho dioda SR540 s nízkým úbytkem napětí. Tato dioda je určena pro aplikace, kde je potřeba rychlé spínání a vysoká účinnost. Má maximální napětí 40 V a maximální proud 5 A. Tato dioda je ideální pro použití v napájecích obvodech, spínacích zdrojích, ochranných obvodech proti zpětnému proudu nebo v regulátorech napětí (14).



Obrázek 4 Schottky dioda SR540 (14)

Druhou nepostradatelnou komponentou je superkondenzátor. Superkondenzátory jsou pasivní součástky schopné uchovávat velké množství elektrické energie. Vynikají svou vysokou kapacitou násobně větší než u běžných elektrolytických kondenzátorů. Na rozdíl od klasických kondenzátorů určených pro okamžité uvolnění energie, superkondenzátory mají schopnost uchovat a uvolnit energii v podstatně vyšších kvantech a navýšit tak dodanou úroveň výkonu. Díky tomu jsou vhodné pro širokospektrální aplikace vyžadující rychlé dodání většího množství energie. Tato součástka by se dala popsat jako něco mezi baterií a běžným kondenzátorem. Nedokáže zadržet tolik energie jako baterie podobné velikosti, ale její výhodou je rychlé nabíjení a vybíjení, což umožňuje dodání velkého množství energie během krátké doby.

Kromě toho superkondenzátory dobře pracují v širokém rozsahu teplot a jsou vhodné pro používání i v extrémních klimatických podmínkách. Jsou využívány v mnoha různých oblastech aplikací, kde je potřeba okamžitého dodání energie. Například bývají často používány v záložních zdrojích energie nebo při regulaci napětí a také v systémech pro obnovu energie v autech (například během rekuperace energie) a ve spotřební elektronice. Díky schopnosti poskytnout energii rychle a opakovaně jsou také vhodné pro systémy čelící náhlým špičkovým spotřebám energie. Superkondenzátory mají tu nevýhodu, že mají nižší energetickou hustotu ve srovnání s běžnými bateriemi. To znamená, že nejsou vhodné pro dlouhodobé uchovávání energie. Nicméně v aplikacích, které vyžadují krátkodobé, ale silné dodávání energie, se stávají nepostradatelnými (15).

Hlavní parametry tohoto konkrétního typu superkondenzátoru SC2V7L106MLR jsou maximální napětí, které činí 2,7 V a jeho kapacita, která činí 10 F.

3.1.4 Step-down měnič napětí M398F

M398F je výkonný step-down napěťový měnič, který dokáže převést vstupní napětí v rozsahu 9–35 V na stabilní výstupní napětí 5 V s maximálním proudem až 5 A. Díky své vysoké účinnosti dosahující až 95 %, se skvěle hodí pro dodávání energie zařízením potřebujícím stabilní 5 V napájení z různých zdrojů s vyšším napětím, jako jsou automobilové systémy či průmyslové aplikace a mnohé další projekty. Modul disponuje svorkovnicí usnadňující připojení kabelů spolu s LED diodou signalizující provozní režim. Kompaktní rozměry o velikosti 45×30×15 mm umožňují jednoduchou integraci do různých projektů (16).

3.1.5 Raspberry Pi 5

Model Raspberry Pi 5 je aktuálně nejvýkonnějším modelem ze série Raspberry Pi a kromě již zmíněného vysokého výkonu disponuje jako první model z této série 2 CSI rozhraními.

Díky tomu, že toto zařízení obsahuje dva 4linkové MIPI CSI/DSI konektory, je možné pracovat se dvěma displeji s rozlišeními až 4k a se dvěma kamerami. Tato variabilita otevírá nové perspektivy pro multimediální aplikace i projekty potřebující vícero kamerových modulů. Raspberry Pi 5 má i dostačující možnosti pro komunikaci, disponuje dual-band Wi-Fi (na 2,4 GHz i 5 GHz) dle normy 802ac a Bluetooth ve verzi 5. Tyto vlastnosti zajistí rychlé a stabilní bezdrátové připojení pro celou řadu aplikací od jednoduchých IoT zařízení po sofistikované síťové systémy.

CPU v Raspberry Pi 5 tvoří 64bitový čtyř-jádrový procesor Arm Cortex-A76 s frekvencí 2,4 GHz, poskytuje výkon zhruba 2 až 3krát vyšší než předchozí generace procesorů této řady. Tento nárůst výkonu umožní plynuleji provozovat více úloh najednou (multitasking), rychleji zpracovávat data a efektivněji spouštět náročné aplikace, což je dobrým předpokladem pro jeho využití v rámci rychlého rozpoznání obličejů (17).

Jako úložiště pro operační systém i data byla zvolena MicroSDHC karta Kingston 16GB Industrial, která by měla vynikat svou dlouhou životností.

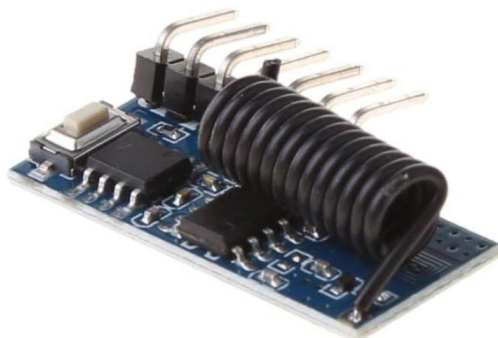
S těmito vlastnostmi je tento model skvělou volbou pro projekty potřebující vysoký výkon, flexibilní možnosti rozhraní a spolehlivé bezdrátové připojení.

3.1.6 Další hardwarové komponenty

Vzhledem ke komplexnosti a obsáhlosti celé práce tvoří technické zázemí samozřejmě i mnoho dalších částí, jakými jsou vodiče, rezistory, aktivní chladič CPU, wago svorky nebo i další typ rychlospojek. Celý systém je dimenzován tak, aby poskytoval spolehlivý přenos energie i informací. Tomu odpovídá i použitý napájecí síťový zdroj, poskytující 12 V a 8 A.

Zdroj je dostatečně předimenzovaný, aby mohl poskytovat dostatek energie nejen samotnému Raspberry (pro které je od výrobce doporučen zdroj s výkonem 27 W), nabíječe pro olověné baterie s funkcí udržování stavu nabité baterie a maximálním výkonem 9,6 W, IR přísvitu o výkonu 2,28 W, ale počítá i s určitými ztrátami, například v měniči napětí a dovoľoval by i integraci napájení pro Wi-Fi router, aby i pro něj mohlo být zajištěno bezproblémové napájení i v případě výpadku elektrické sítě.

V poslední řadě je třeba neopomenout také 4kanálový 433Mhz přijímač EV1527, který slouží k příjmu signálu z bezdrátového PIR čidla.



Obrázek 5 Přijímač EV1527 (18)

3.2 Hardware mimo technické zázemí

V této části bude popsáno, jakým hardware disponuje navržené řešení fotopasti mimo technické zázemí. Jedná se o modul kamery, IR přísvitu, zámku a ovládacího panelu, které jsou k technickému zázemí připojeny kabelovými vodiči. Navíc sem také patří bezdrátový PIR detektor pohybu.

3.2.1 Arducam 8MP Sony IMX219

Kamerový modul je stěžejní komponentou celého systému. Tento modul disponuje rozlišením 8 megapixelů, motorizovaným IR filtrem a širokým zorným polem, které činí 100°. Díky takto širokému záběru dokáže zachytávat tak velkou oblast, pro kterou by jinak bylo třeba více běžných kamer s užším zorným polem. Senzor Sony IMX219 navíc zajišťuje svým rozlišením dostatek detailů i pro náročnější účely.



Obrázek 6 Arducam 8MP Sony IMX219

Na obrázku lze vidět, že kamerový modul disponuje vlastním fotorezistorem. Běžně je tento fotorezistor umístěn přímo na desce plošného spoje kamery, ale v tomto případě byl odpájen a připájen na krátké vodiče, dál od desky plošného spoje, ale zato blíže k průhledné části krytu. Je to z toho důvodu, aby dokázal fotorezistor lépe určovat aktuální světelné podmínky, protože kdyby zůstal „utopen“ v krabici na desce plošného spoje, tak by obzvlášť na přelomu dne a noci, nedokázal přesně určovat intenzitu světla, protože by byl ve více tmavém prostředí a dopadalo by na něj tak méně světla.

3.2.2 IR přísvit

Vybraný IR přísvit obsahuje 24 tmavých IR LED diod, které emitují záření o vlnové délce 850 nm. Jeho 90 – ti stupňový rozptyl záření téměř odpovídá zornému poli použité kamery. Má vlastní fotorezistor, který při trvalém napájení rozsvítí diody pouze při nízké intenzitě světla. Původně byl tento modul vybrán díky své malé velikosti (44 mm vnější průměr) tak, aby mohl být instalován přímo na kamerovém modulu s kamerovým objektivem uprostřed. Toto umístění se při testování ukázalo jako nevhodné a byl tak umístěn samostatně. Napětí pro jeho napájení je 12 V a jeho spotřeba je 2,28 W.



Obrázek 7 Modul IR přísvitu

3.2.3 Modul Zámku

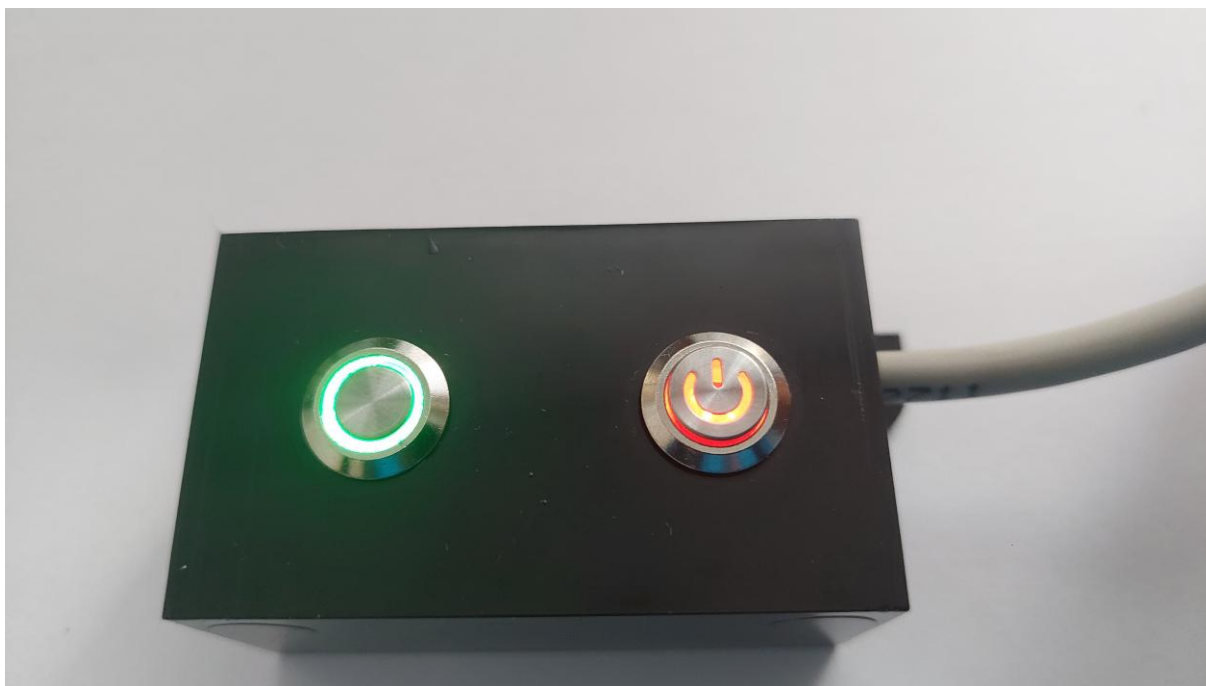
Jako zámek byl zvolen obyčejný 12 V elektromagnetický zámek. Je z kovového materiálu a jeho kulatá západka má průměr 1 cm, což jej činí dostatečně fyzicky odolným pro danou aplikaci.

3.2.4 Ovládací panel

Ovládací panel byl vyvinutý přímo pro tuto práci. Je velmi jednoduchý, skládá se pouze ze dvou komponent – z jednoho tlačítka a jednoho přepínače. Jeho účelem bude umožnit uživateli restart, zapnutí nebo vypnutí fotopasti, nebude-li chtít být focen. Jak tlačítko, tak přepínač mají v sobě integrované LED osvětlení, které je připojeno tak, aby signalizovalo stav toho, co daná komponenta ovládá.

Pro tlačítko platí, že při jeho krátkém stisku se fotopast vypne a při stisku delším než 3 s se restartuje. Svítí-li jeho integrovaná dioda, tak to znamená, že je fotopast zapnutá. Pokud nesvítí, tak to znamená, že je vypnutá, nebo se restartuje.

Pro přepínač platí, že pokud je ve své dolní poloze, tak je fotopast napájena, pokud je ve své horní poloze, tak je přerušena velká část obvodu fotopasti. Pokud se z horní polohy přepínač přepne do dolní, tak automaticky dojde k zapnutí fotopasti. Svítí-li jeho integrovaná dioda, reaguje přesně podle stavu přepínače. Rozpojí-li se obvod jeho přepnutím do horní polohy, tak tím zároveň dojde i k přerušení napájení pro jeho integrovanou diodu.

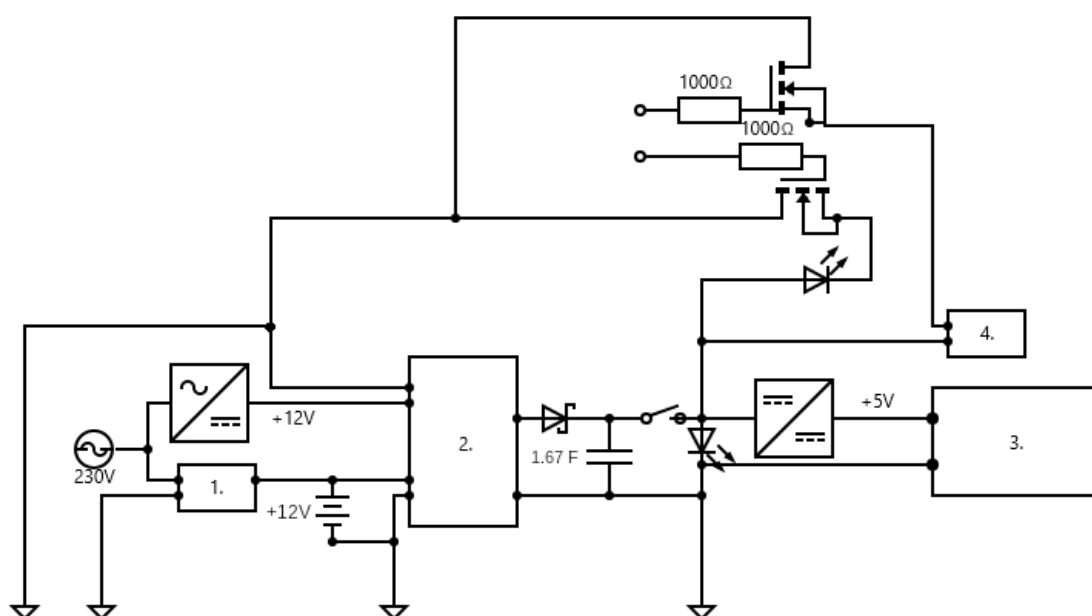


Obrázek 8 Ovládací panel

3.2.5 PIR senzor

Jedná se o jedno z nejjednodušších zařízení tohoto druhu. Použitý PIR senzor komunikuje bezdrátově na frekvenci 433 MHz pomocí protokolu eV1527. Tento protokol je podporovaný použitým přijímačem. Rozsah snímání je 120° na 8–12 m a ve volném prostoru dokáže přenášet signál až na 80 m. Napájen je dvěma bateriemi typu AAA.

3.3 Zapojení



Obrázek 9 Schéma zapojení napájení v technickém zázemí

Vysvětlivky:

1. Nabíječka
2. UPS modul YX850
3. Raspberry Pi 5
4. Zámek

3.3.1 Zapojení dle schématu

Schéma zapojení napájení na obrázku 9 se zaměřuje převážně jen na napájení uvnitř technického zázemí až po Raspberry Pi 5. Některé další komponenty jsou napájeny přímo z tohoto mikropočítače a nejsou tak v tomto schématu zohledněny.

Ze schématu je zřejmé, že je technické zázemí napájeno přímo ze síťového zdroje (230 V AC). Zdrojové napětí se dále dělí do dvou větví, do AC-DC měniče s transformátorem a do nabíječky baterie. Tím je zajištěno, že za těmito komponenty se dále v obvodu vyskytuje pouze bezpečné DC napětí do 15 V.

Původně bylo zamýšleno, že k přepínání zdroje napájení bude plně stačit UPS modul. Při následném testování ale bylo zjištěno, že UPS modul nereaguje přímo na výpadek hlavního zdroje napájení, ale na pokles napětí na jeho výstupu, což by bylo zcela nedostatečné, protože by docházelo k restartu fotopasti při změně zdroje napájení. Za účelem eliminace tohoto problému byla na výstup z UPS modulu přidána Schottkyho dioda a šest sériově spojených superkondenzátorů.

$$n = \frac{V_{Celk}}{V_i} \quad (3.30)$$

$$n = \frac{14,7}{2,7} = 5,4 \quad (3.31)$$

Na základě vztahu 3.31 bylo vypočteno, proč je zapotřebí právě 6 superkondenzátorů. Pokud by bylo v obvodu stabilní napětí činící maximálně 12 V, tak by stačilo 5 superkondenzátorů, ale vzhledem k tomu, že při nabíjení baterie a při přepnutí obvodu na napájení z baterie může být krátkodobá špička napětí až 14,7 V, tak z toho důvodu jich bylo použito právě 6.

Nicméně obecně při sériovém zapojení kondenzátorů klesá jejich kapacita. Použité superkondenzátory sice mají kapacitu velmi vysokou, přesto bylo na základě výpočtu ze vztahu 3.42 ověřeno, že jejich celková kapacita zůstane dostatečně vysoká i při jejich sériovém zapojení.

$$\frac{1}{C_{Celk}} = \sum_{k=1}^6 \frac{1}{C_i} \quad (3.40)$$

$$\frac{1}{C_{Celk}} = \frac{6}{10} = 0,6 F \quad (3.41)$$

$$C_{Celk} = 1,67 F \quad (3.42)$$

Bude-li se počítat s tím, že může přepnutí UPS modulu trvat až 1 s a napětí je 12 V, poté se může vypočítat výkon, který po tuto dobu dokáže superkondenzátory dodat.

Energie kondenzátoru:

$$E = \frac{1}{2} CV^2 \quad (3.50)$$

$$E = \frac{1}{2} * 1,67 * 144 = 120.24 \text{ J} \quad (3.51)$$

Výkon při čase $t = 1 \text{ s}$:

$$P = \frac{E}{t} \quad (3.60)$$

$$P = \frac{120.24}{1} = 120.24 \text{ W} \quad (3.61)$$

Dle vypočteného výkonu převyšujícího 120 W lze usoudit, že kapacita je zcela dostatečná pro spolehlivé dodávání výkonu ve stavu, kdy dojde k přepínání mezi zdroji.

3.3.2 Vstupy a výstupy z mikrokontroleru Raspberry

Kromě připojení kamery na dedikovaný kamerový (CSI) vstup, byly na mikrokontroleru využity i některé další piny.

Napájení přijímače	3v3 Power	1	2	5v Power	Napájení teplotního čidla
	GPIO 2 (I2C1 SDA)	3	4	5v Power	
	GPIO 3 (I2C1 SCL)	5	6	Ground	
1-WIRE	GPIO 4 (GPCLK0)	7	8	GPIO 14 (UART TX)	
	Ground	9	10	GPIO 15 (UART RX)	
Výstup ovládání IR přísvitu	GPIO 17	11	12	GPIO 18 (PCM CLK)	
Výstup LED tlačítko	GPIO 27	13	14	Ground	
Vstup tlačítko	GPIO 22	15	16	GPIO 23	
	3v3 Power	17	18	GPIO 24	
	GPIO 10 (SPI0 MOSI)	19	20	Ground	
	GPIO 9 (SPI0 MISO)	21	22	GPIO 25	
	GPIO 11 (SPI0 SCLK)	23	24	GPIO 8 (SPI0 CE0)	
	Ground	25	26	GPIO 7 (SPI0 CE1)	
	GPIO 0 (EEPROM SDA)	27	28	GPIO 1 (EEPROM SCL)	
	GPIO 5	29	30	Ground	
Vstup ochrany	GPIO 6	31	32	GPIO 12 (PWM0)	
	GPIO 13 (PWM1)	33	34	Ground	
	GPIO 19 (PCM FS)	35	36	GPIO 16	Výstup pro ovládání zámku
Vstup z přijímače PIR čidla	GPIO 26	37	38	GPIO 20 (PCM DIN)	
	Ground	39	40	GPIO 21 (PCM DOUT)	

Obrázek 10 Zapojení na mikrokontroleru

GPIO 4 je využitý pro 1-WIRE, což je komunikační protokol, který umožňuje připojení více zařízení k jediné datové sběrnici. Běžně se používá v aplikacích, kde je potřeba jednoduché a levné řešení pro připojení periférií, například pro senzory, paměťová zařízení nebo teplotní čidla. V této práci je tato sběrnice použita pro připojení teplotního čidla, které bude moci být použito v rámci testování pro zjištění teploty okolí, nebo uvnitř technického zázemí.

GPIO 17 slouží jako výstupní pin ovládání IR přísvitu přes 1 k Ω rezistor je napojen na gate mosfetu.

GPIO 27 slouží přímo (pouze přes rezistor) jako výstup pro integrovanou LED diodu tlačítka. Tento pin je softwarově nastaven na vysokou hodnotu při spuštění hlavního programu. Do nízké hodnoty přejde až po vypnutí mikrokontroleru. Přestože tento pin poskytuje pouze 3,3 V a 16 mA, tak je to plně dostačující pro signalizační osvětlení tlačítka.

GPIO 22 je využitý jako vstupní pin do mikrokontroleru z tlačítka. V hlavním programu je hodnota tohoto pinu neustále skenována. Podle délky stisku tlačítka program rozhodne, zda bude mikrokontroler vypnut, nebo restartován.

GPIO 6 slouží jako vstupní pin zabezpečení proti násilnému odejmutí kamery. Více v kapitole 7, která se věnuje zabezpečení.

GPIO 26 - tento pin slouží jako vstupní pin z přijímače eV1527. V případě zjištění aktivity na tomto pinu dojde k okamžitému zahájení snímkování podle přednastavených parametrů.

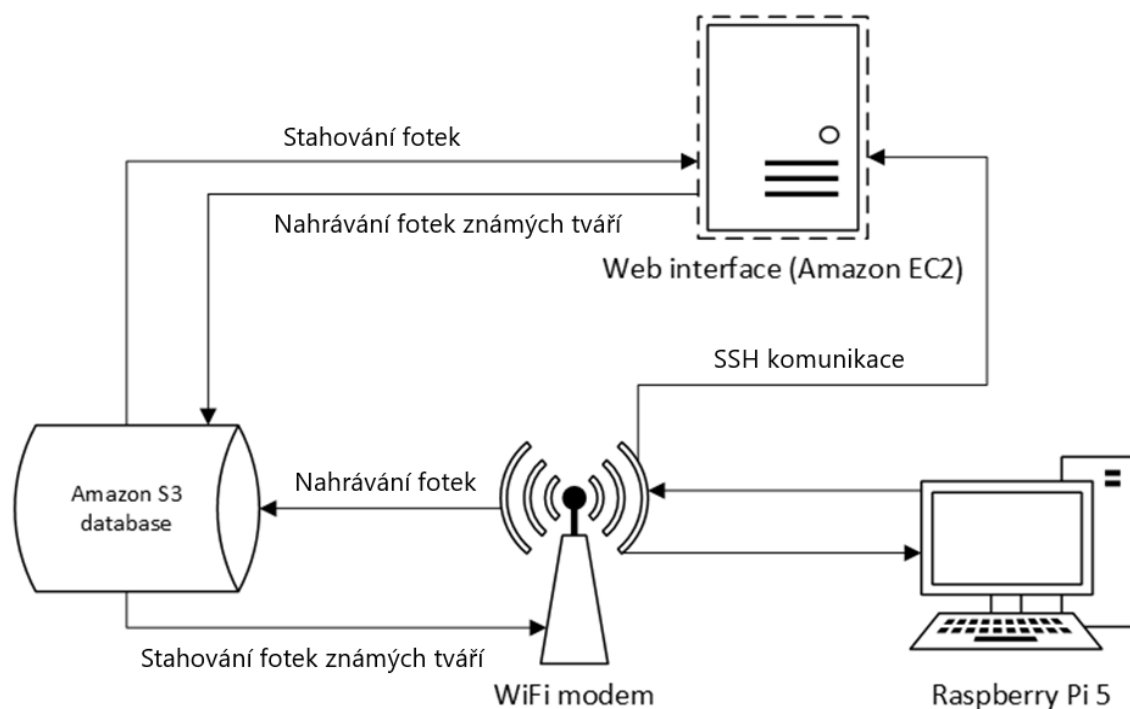
GPIO 16 slouží podobně jako GPIO 17 k ovládání zámku přes 1 k Ω rezistor, napojený na gate mosfetu.

4 Software v Raspberry Pi 5

Dříve, než se zde začne rozebírat konkrétní vytvořený software, tak je třeba uvést, na čem celý systém stojí, respektive operační systém, kterým je Debian Je to volně dostupný operační systém založený na Linuxu. Byl vybrán především proto, že podporuje široký sortiment hardwaru, včetně Raspberry Pi 5. Je ideální volbou při IoT projekty, především díky své bezpečnosti a stabilitě. Konkrétně byla použita jeho verze Bookworm. Pro vytváření skriptů byl zvolen programovací jazyk Python, a to především kvůli možnosti jeho univerzálního a flexibilního využití (19).

4.1 Obecná architektura vytvořených skriptů

Obecná struktura vytvořených skriptů je navržena tak, aby zařízení spolehlivě vytvářelo fotografie dle nastavených scénářů, rozpoznávalo obličeje a pořízené fotografie následně bezpečně nahrálo do cloudového úložiště. Zároveň se software připojuje bezpečným způsobem na webový server, aby mohlo zařízení reagovat na příkazy uživatele nebo informovat o nastalé krizové situaci. Vzhledem k nutnosti izolovaného prostředí pro specifické funkce a knihovny, jejichž instalace v rámci hostitelského operačního systému by mohla vést k nežádoucím interakcím a potenciální destabilizaci, byla implementována sada pomocných skriptů. Tři pomocné skripty se spouští ve virtuálním prostředí, naopak hlavní program není spouštěn ve virtuálním prostředí, kvůli snazšímu přístupu k GPIO pinům. Na obrázku 11 je přibližně vyobrazen diagram datových toků. Wi-fi modem zde slouží pouze pro poukázání na to, že fotopast ke svému chodu využívá dostupnou Wi-Fi síť.



Obrázek 11 Diagram připojení

Důležitými programy v zařízení jsou:

- Main.py – hlavní program, řídí veškerý chod
- Rozpoznani4.py – v tomto programu probíhá rozpoznání obličejů
- Check_face_encoding.py – tento program se používá při přidávání nových známých tváří
- Ssh.py – zprostředkovává komunikaci se serverem

4.1.1 Podpůrné nástroje Systemd a AutoSSH

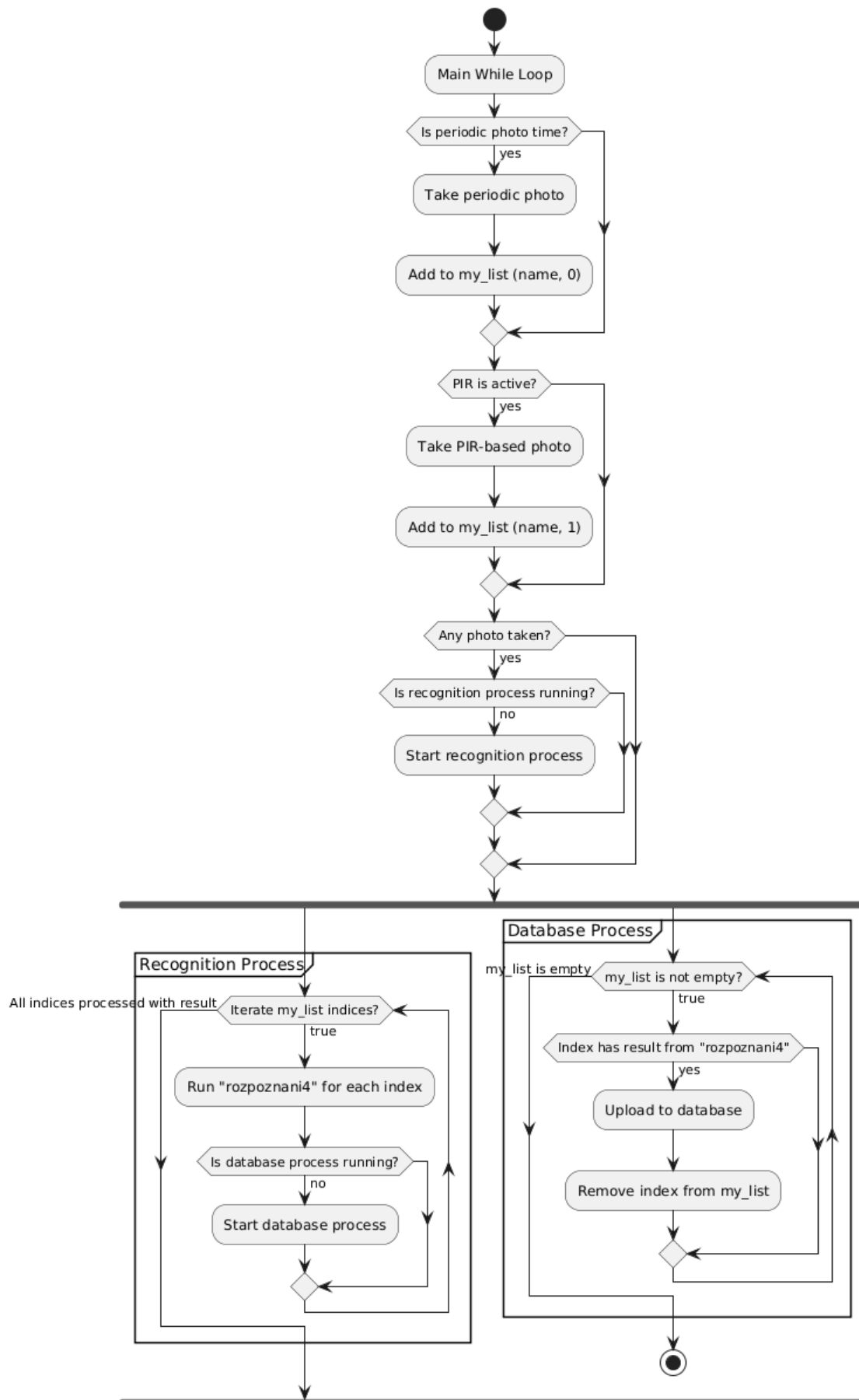
Systemd je systém pro spouštění služeb a jedním ze základních kamenů Linuxových operačních systémů, který funguje jako správce služeb. Tento systém nahrazuje tradiční SysVInit, přináší možnost paralelního spouštění služeb a podporuje transakční řízení závislostí. Obsahuje komponenty pro spravování síťového času, základního nastavení systému a protokolování informací. SystemD je navržen s důrazem na efektivitu a flexibilitu. Tím se stal standardem pro správu Linuxových služeb (20). V této konkrétní práci je SystemD využitý k automatickému spouštění hlavního programu po startu zařízení a také k automatizovanému spouštění AutoSSH.

AutoSSH je nástroj navržený pro automatické opětovné vybudování SSH relací a tunelů s cílem zajistit jejich nepřetržitou dostupnost pro uživatele. Tato aplikace je koncipována takovým způsobem, aby sledovala probíhající SSH spojení a v případě jeho výpadku provedla automatickou obnovu tohoto spojení. Takové funkce jsou obzvláště užitečné při dlouhodobém nebo stabilním připojení k síti. AutoSSH je kompatibilní s různými operačními systémy včetně použitého Debianu a lze jej snadno integrovat s nástroji jako například výše popsáním SystemD pro správu služeb (21).

4.2 Hlavní skript

Jak už bylo psáno, tak tento program řídí veškerou naprogramovanou funkcionalitu zařízení. Po startu zařízení je spuštěn pomocí systemd. Tento program při svém spuštění nejdříve vykoná několik operací, které se vykonávají pouze při jeho spuštění.

Mezi tyto operace patří: uvolnění všech linek na I/O portech, inicializace proměnných, které se posléze sdílí mezi procesy nebo spuštění samostatného procesu monitoringu tlačítka z ovládacího panelu. Program také nastaví zámek do zamknutého stavu, ale předtím počká 10 s, aby měl uživatel po zapnutí dostatek času na zavření dveří. Informaci o stavu zámku program také pošle do webového rozhraní. Dále proběhne synchronizace známých tváří dle dat z cloudového úložiště. Nakonec spustí funkci focení_fce, ve které je nekonečná smyčka a udržuje tak program v chodu. Na následujícím diagramu na obrázku 12 je velmi stručně naznačen proces pořízení fotografie až po její uložení do cloudového úložiště.



Obrázek 12 UML diagram

4.2.1 Funkce foceni_fce

Tato funkce je nepostradatelná pro chod celého systému. Při jejím spuštění si tato funkce, kromě inicializace několika proměnných, nastavuje v systému prioritu na 2, aby ji i při vyšším zatížení věnoval systém dostatek prostředků, například pro včasnou aktivaci kamery při příchodu informace o pohybu.

Funkce obsahuje nekonečný cyklus. V tomto cyklu se ovládá chod zámku, podle sdílené proměnné „unlock“, která když nabývá hodnoty „True“, tak je zámek otevřen po dobu 10 s, aby měl uživatel dostatek času na otevření dveří. Dále zde dochází k periodickému vytváření fotek. Perioda snímkování je nastavena zhruba na 40 minut. Na přesnost tohoto snímkování nejsou kladeny velké nároky, toto snímkování slouží jen k tomu, aby si uživatel mohl kdykoliv ověřit, že fotopast funguje a zjistit si například jaké je počasí v destinaci umístění fotopasti. Periodické snímkování tedy nemusí mít přesnou periodu, protože je inicializováno podle počtu průchodů ve smyčce. Periodické snímkování také funguje pouze v čase od 7:00-18:30, protože noční snímky nejsou z tohoto hlediska zajímavé, ani žádoucí kvůli zbytečnému zaplňování úložiště.

```
capture_command = f"libcamera-still -o {photo_path}  
-t 2500 --tuning-file pi5_imx219_100d.json"
```

Zdrojový kód 1 Příkaz pro kameru

Výše uvedený kód je příkaz, jehož spuštěním je vytvořen periodický snímek. Pro vytvoření jakéhokoliv typu snímku (periodický, na základě aktivity PIR senzoru, nebo příkazem uživatele) je vždy použit příkaz z volně dostupné knihovny libcamera a konfigurační soubor „pi5_imx219_100d.json“. Konfigurační soubor byl vyžádán přímo od výrobce kamery, protože bez něj byly na pořízených snímcích špatné barvy.

Libcamera je otevřené dostupné softwarové řešení, zaměřující se na usnadnění práce s kamerovými systémy na různých platformách, včetně Linuxu Androidu či ChromeOS. Poskytuje jednotné programovací rozhraní pro vývojáře, které abstrahuje od složitostí spojených s různými hardwarovými komponentami, jako jsou kamerové senzory, obrazové procesory či přijímače. Tato knihovna komunikuje s mediálním subsystémem jádra Linuxu, usnadňuje konfiguraci kamer a umožňuje vývojáři zaměřit se na vývoj aplikací, místo aby ztrácel čas na ovládání zařízení na nízké úrovni (22).

Při každém focení je také aktivován IR přísvit, který nemusí být reálně zapnutý, protože při dostatečném světle jeho fotorezistor zajistí, že zůstane vypnutý.

Je-li focení vyvoláno na základě aktivity PIR čidla, tak jsou pořízeny 3 snímky za sebou v přibližném rozmezí 2, 4 nebo 8 s. Volba intervalu mezi snímky závisí na počtu vykonání této akce během posledních 3 minut. Pokud bylo toto snímkování provedeno maximálně 4krát, zůstává interval na 2 s, pokud 4 – 7x tak je interval nastaven na 4 s a pokud víc jak 7krát, tak je interval nastaven na 8 s.

Tento přístup je zvolen z důvodu snížení frekvence snímkování v případě nepřetržité aktivity PIR čidla. Původně bylo zamýšleno, že tato funkce bude implementována pomocí knihovny libcamera, která umožňuje i tvorbu příkazu pro sekvenční snímání. Bylo by tím dosaženo lepší přesnosti snímkování v určeném intervalu. Tato varianta se ale ukázala jako nevhodná z toho důvodu, že proces rozpoznávání tváře mohl být následně spuštěn až po skončení celé sekvence, což prodlužovalo dobu potřebnou k odemknutí zámku při identifikaci známé tváře.

Ať už je snímek vytvořen periodicky, nebo kvůli aktivitě PIR čidla, tak je vždy uložen do složky Pictures s názvem, který reprezentuje aktuální datum a čas. Tento název kromě jiného zajišťuje jedinečnost názvu souboru. Dále je v proměnné typu seznam založen nový řádek s prvním prvkem, který reprezentuje název souboru, druhým prvkem, jenž indikuje, zda byl snímek pořízen periodicky, nebo na základě aktivity PIR čidla, a třetím prvkem, který je inicializován jako prázdný, protože později bude sloužit jako výsledek rozpoznání.

V hlavním cyklu je také obvykle každých 60 s, volána funkce, která zjišťuje, zda nebyla kamera překryta a každých 10 s se obvykle navazuje SSH komunikace s webovým serverem. Časy uvedené v předchozí větě odpovídají, pokud během jejich trvání nedošlo k focení, které jejich periodu vždy prodlouží o dobu svého trvání, nebo k otevření zámku, což má stejný efekt jako focení. Vliv má i samotná doba pro vykonávání funkce. Prodloužení těchto period způsobí i příkazy uživatele z webového rozhraní.

Pokud právě neprobíhá focení, tak je v hlavním cyklu také implementována reakce v případě přerušení vedení ke kameře, což okamžitě vyvolá spojení s webovým serverem, který tuto informaci dále zpracuje.

4.2.2 Funkce pro zjištění překrytí kamery

Funkce pro zjištění, zda nebyla kamera překryta, je volána periodicky, obvykle každých 60 s, pokud nedochází k focení z jiného důvodu nebo k odemknutí zámku. Jedinou záležitostí, která by mohla spuštění této funkce po delší dobu blokovat, by tedy bylo focení z důvodu aktivity PIR čidla. Z toho důvodu je tato funkce volána i při každé prostřední fotce ze sekvence 3 fotek. Pokud byla zvolána periodicky, tak je vytvořený snímek po posouzení touto funkcí smazán, aby zbytečně nezabíral místo v úložišti.

Funkce funguje na tom principu, že si načte vytvořený snímek (cesta k němu je funkci předána jako parametr při jejím volání) a převede ho do stupňů šedi. Dále obrázek normalizuje do pole hodnot 0–1 a rozdělí na dlaždice o velikosti 32x32. Poté zvolí centrální oblast obrázku (střed podle jeho výšky a šířky) a analyzuje pole dlaždic o velikosti 15 x 15. Z tohoto pole se vypočítá průměrná směrodatná odchylka všech dlaždic. Je-li směrodatná odchylka dostatečně velká, tak to indikuje, že je obrázek v této části dostatečně rozmanitý. V opačném případě, při nízké průměrné směrodatné odchylce to znamená, že je pole příliš

homogenní, což by odpovídalo překrytí kamery lepící páskou. Pokud tedy průměrná směrodatná odchylka nepřekročí určitou, pevně definovanou mez, tak funkce vrátí tuto informaci do hlavního cyklu, ze kterého byla volána a následně je tato informace předána webovému serveru.

Směrodatná odchylka je druhá odmocnina rozptylu a je to jedna ze základních měr variability. Značí průměrnou vzdálenost hodnot od středu. Čím je hodnota směrodatné odchylky vyšší, tím rozptýlenější data budou.

4.2.3 Funkce pro přidání známých tváří

Vzhledem k tomu, že se neočekává časté přidávání známých tváří (protože většinou budou jednou nahrány a poté už se jen málokdy budou přidávat další), tak je tato funkce spuštěna pouze při zapnutí fotopasti.

Funkce se připojuje k Amazon S3 bucketu (bucket by se dal česky nazvat jako oddíl cloudového úložiště, podobně jako tabulka v Microsoft Server SQL databázi) a načítá z něj všechny objekty. Každý objekt v tomto bucketu má 3 metadata.

Metadata „result“ označují, zda byl daný objekt už zpracován fotopastí, nebo ne. Pokud už byl zpracován, tak tento objekt funkce přeskočí.

Metadata „directory“ určují budoucí možné umístění pro obsah (samotný binární obsah objektu). Tyto metadata by měla obsahovat název známé osoby, pro kterou odpovídá fotografie v obsah.

Metadata „povolen“ definují, zda je nebo není daná osoba povolená pro otevření zámku. Podle toho funkce upravuje lokální JSON soubor, ve kterém jsou tyto data udržována.

Pokud tedy není nastaven „result“, tak se obsah dočasně stáhne a uloží jako JPEG soubor do kořenové složky skriptu. Pokud je nastaven „directory“, tak tato funkce spustí v před vytvořeném virtuálním prostředí skript `check_face_encoding.py` postupně pro všechny objekty v této složce. Pokud je pro aktuální objekt výstup z této funkce roven 0, tak je daný soubor přesunut do složky dle jeho „directory“, odkud je už připravený pro použití při rozpoznávání. Pokud není výstup z této funkce roven 0, tak je soubor z místního úložiště zase odstraněn. Na základě tohoto zpracování je pro daný objekt změněn „result“ jako součást metadat. Pokud byly na obrázku detekovány charakteristické obličejové rysy, tak je nastaveno „Successful“, pokud ne, tak „Undetected face“. Pokud by se stalo, že by se jeho název shodoval s již existujícím obrázkem v dané složce, tak je nastaveno „Exists“.

4.2.4 Funkce pro nahrávání fotek do cloudového úložiště

Tato funkce je spuštěna z funkce rozpoznání jako samostatný proces. Postupně prochází sdílený seznam, na který se při focení ukládají názvy snímků. Pokud aktuální řádek seznamu obsahuje vyhodnocení z rozpoznání snímku, tak se tento snímek zmenší na velikost 820 x 616 pixelů (v tu chvíli má zhruba 100 kB) a nahraje do cloudového úložiště spolu s metadaty, která jsou obsažena na daném řádku (informace, zda snímek pochází z periodického focení a výsledek rozpoznání). Dále funkce přidá metadata časového razítka, která extrahuje z názvu snímku. Je-li snímek úspěšně nahrán, tak daný řádek ze seznamu odstraní.

K seznamu se stejně jako kdekoliv jinde přistupuje pomocí zámku, aby bylo předcházeno případným problémům, pokud by ke sdílenému seznamu zároveň přistupoval i nějaký další proces.

4.2.5 Ostatní funkce

V hlavním skriptu se nachází i další méně sofistikované funkce, ale přesto neméně důležité. Jednou z nich je například hlídání zaplnění úložiště. Tato funkce v pravidelných intervalech hlídá velikost složky, kam se ukládají pořízené snímky a přesáhne-li tato velikost určitou mez, tak dojde k odstranění poloviny nejstarších snímků, aby nedošlo k přeplnění úložiště.

Nachází se zde také několik podpůrných funkcí, které zprostředkovávají spouštění dalších skriptů ve virtuálním prostředí a organizují jejich vstupy a výstupy.

4.3 Skript pro rozpoznání osob

Tento skript je volán vždy z hlavního skriptu viz. předchozí kapitola 4.2. Z důvodu použití knihovny face-recognition, kterou bylo nutné nainstalovat ve virtuálním prostředí je i tento samotný skript spouštěn ve virtuálním prostředí.

4.3.1 Face-recognition a dlib

Nástroj na rozpoznání obličejů nazvaný face-recognition je postaven na knihovně dlib a poskytuje snadno použitelné prostředky pro identifikaci a detekci tváří. Tato knihovna nabízí širokou škálu funkcí včetně hledání tváří na obrázku, či identifikace konkrétních osob podle rysů jejich obličeje a lokalizaci klíčových bodů, jako jsou oči, ústa nebo nos. Díky těmto vlastnostem může být knihovna využívána pro různorodé aplikace, jako je třídění fotografií, ověřování identity nebo i interaktivní aplikace reagující na přítomnost obličeje.

Knihovna využívá spojení technik, založených na hlubokých neuronových sítích (CNN) a model histogramů orientovaných gradientů (HOG). Model založený na HOG je rychlý a nenáročný algoritmus. Na druhou stranu model CNN poskytuje vyšší přesnost, ale na úkor většího výpočetního zatížení. Úspěšnost knihovny v rozpoznávání obličejů byla demonstrována pomocí modelu dlib, dosahujícím úspěšnosti 99.38 % ve standardním benchmarkovém datasetu Benchmark Labeled Faces in Wild (LFW).

Knihovna face-recognition je zaměřena na identifikaci obličejů, a to především takových, které jsou orientovány čelním pohledem. Pokud je pozorovaný obličej pozorován pod úhlem, nebo viditelný z profilu místo čelního pohledu, může to negativně ovlivnit detekci. Toto omezení je dáno použitým typem trénovacích dat a algoritmů optimalizovaných pro čelní pohled (23)(24).

4.3.2 Virtuální prostředí

Virtuální prostředí je oddělený pracovní prostor, který umožňuje programátorům spravovat závislosti a konfigurace jednotlivých projektů nezávisle na globálním systému. Tato oddělenost zaručuje, že knihovny a jejich verze použité v jednom projektu nebudou mít vliv na ostatní projekty na stejném zařízení. V Pythonu se virtuální prostředí vytvoří pomocí modulu „venv“, který je součástí standardní knihovny. Tímto postupem lze pohodlně řídit konkrétní verze knihoven pro různé projekty, což usnadní vývoj a testování aplikací.

4.3.3 Praktické použití

Vstupem do toho skriptu je cesta k pořízenému snímku. Tento skript si pořízený snímek načte a pokusí se v něm vyhledat tváře a jejich rysy. Pokud žádnou tvář nenajde, tak se ukončí. Pokud najde jednu nebo více tváří, tak si uloží jejich rysy.

Následně skript ze složek známých tváří začne načítat jejich rysy. Kód využívá paralelní zpracování pro efektivní načítání a zpracování známých tváří. Jakmile má tyto rysy načtené, tak spustí jejich porovnávání. Toto porovnávání funguje na tom principu, že jsou postupně vybírány rysy tváří z pořízeného snímku a každý z těchto rysů je porovnáván postupně se všemi rysy známých tváří.


```
for unknown_encoding in unknown_face_encodings:
    for name, encodings in known_encodings:

results=face_recognition.compare_faces(encodings,
unknown_encoding, tolerance=0.5)

    if any(results):
        print(name)
        sys.exit(0)
```

Zdrojový kód 2 Ukázka porovnání tváří

Zdrojový kód 2 aplikuje poslední část výše popsané logiky. Navíc je v tomto kódu zohledněna tolerance, která defaultně bývá nastavena na 0,6. Hodnota 0,5 je přísnější kritérium, které se vztahuje ke vzdálenosti mezi vektory charakteristik obličejů. Je-li tolerance podobným způsobem snížena, tak to znamená, že je vyšší pravděpodobnost, že nedojde k záměně osoby s jinou osobou, na druhou stranu ale algoritmus s nižší tolerancí nemusí rozpoznat známou osobu i když by měl. Snížení tolerance by se tedy dalo označit jako bezpečnější rozpoznání, ale za cenu možného většího počtu nerozpoznání známé osoby.

Zobrazený kód je zakončen ukázkou jednoho z možných ukončení skriptu. V tomto případě se kód ukončí, dojde-li k nalezení první shody mezi tvářemi z pořízeného snímku a známými tvářemi. Není třeba plýtvat výpočetní prostředky pro případné zkoumání dalších tváří, protože cílem není identifikovat všechny osoby, ale umožnit přístup do objektu, je-li identifikována známá osoba.

Z technického hlediska „sys.exit(0)“ předá skriptu, ze kterého byl tento skript spuštěn, informaci, že vše proběhlo v pořádku a zároveň je získána i informace o posledním výpisu do konzole, ve kterém se nachází jméno nalezené osoby.

4.4 Skript pro přidání nových známých tváří

Tento skript slouží k tomu, aby uživateli umožňoval uživatelsky přívětivé přidání snímků známých osob. Skript je volán z hlavního skriptu při jeho startu a pracuje opět ve virtuálním prostředí.

Pracuje tím způsobem, že načte obrázek, ke kterému mu byla předána cesta, upraví jeho velikost na šířku 640 pixelů při zachování poměru stran z důvodu menší výpočetní náročnosti a pokusí se detekovat obličejové rysy na daném obrázku. Vzhledem k tomu, že od uživatele může očekávat obrázek, který je pořízen různými metodami (třeba focen na výšku nebo na šířku), tak i tento skript používá různé metody pro detekci tváří. Patří mezi ně například otáčení obrázku a detekování v různých velikostech (64x64 nebo 128x128 pixelů). Poté vybere nejlepší získanou obličejovou charakteristiku a vyříznutý obličej uloží pro budoucí použití při rozpoznávání.

Skript také vrací různé chybové hodnoty, pokud nedošlo k nalezení tváře nebo její charakteristiky, nebo pokud bylo naopak na obrázku nalezeno více tváří, tak i v tomto případě neuloží žádnou tvář, protože by nedokázal určit, která z identifikovaných tváří patří zadané známé osobě.

4.5 Skript pro komunikaci

Tento skript je v pravidelných intervalech volán v hlavním programu a slouží pro komunikaci mezi fotopastí a webovým serverem.

4.5.1 SFTP přenos

SFTP (Secure File Transfer Protocol) je standardní způsob pro bezpečné přenosy dat mezi zařízeními pomocí šifrované komunikace přes SSH tunel pro ochranu dat během jejich přenosů v síti, či mezi zařízeními a infrastrukturou sítě. Mimo samotné přenosy umožňuje SFTP také správu funkcí jako je třeba vytvoření složek nebo nastavení oprávnění k souborům. SFTP se často používá tam, kde je nutné zaručit bezpečné sdílení citlivých informací (25).

4.5.2 Princip činnosti

Skript nejprve kontroluje, zda byl spuštěn se vstupním argumentem nebo bez něj. Fungování by se dalo popsat jako práce se souborem, protože ve skutečnosti je princip komunikace založen na čtením a zápisu do JSON souborů dostupných na serveru. Pokud byl spuštěn se vstupním argumentem, tak to znamená, že bude předávat serveru data. Tato operace by se tedy dala zjednodušeně označit za zápis a má přednost před čtením, protože fotopast předává serveru touto komunikací pouze kritická data, která znamenají, že byla narušena ochrana fotopasti, proto je žádoucí, aby tato data byla neprodleně předána. Není-li nastaven vstupní argument, tak skript předává do hlavního programu příkazy z webového rozhraní a vrací informaci, zda příkazy přijal.

5 Amazon S3

Amazon S3 je služba pro ukládání objektů, která ukládá data jako objekty v segmentech. Objektem je zamýšlen soubor a jakákoli metadata, která soubor popisují. Poskytuje vysokou škálovatelnost, dostupnost a výkon. Díky svému designu umožňuje zákazníkům různých velikostí a odvětví ukládat a chránit rozličné objemy dat.

Přestože S3 nabízí několik funkcí podobných práci s databázemi, jako například vyhledávání objektů pomocí klíčů, nebylo vyvinuto pro složité dotazy, indexování nebo transakční operace, které jsou obvyklé u databází. V S3 není možné přistupovat k datům přímými dotazovacími jazyky (např. SQL) a chybí zde relace mezi daty nebo schopnost zpracovávat složité dotazy.

Shrnutím lze říct, že Amazon S3 by nemělo být chápáno jako databáze, spíše jako velmi flexibilní a škálovatelné úložiště dat schopné spolupráce s dalšími technologiemi, za účelem poskytnutí několika funkcionalit, podobných těm u databází (26).

5.1 AWS Identity and Access Management a využití úložiště

AWS Identity and Access Management (IAM) je nástrojem pro bezpečné budování přístupů ke zdrojům AWS. Umožňuje vytvoření uživatele s různými oprávněními ke službám AWS pomocí rolí. Tato služba umožňuje podrobné řízení přístupových práv a využití bezpečnostních funkcí jako je například dvou faktorová autentifikace (2FA) (27).

V tomto úložišti byly vytvořeny dva buckety, neboli oddíly. Jeden slouží pro ukládání snímků z fotopasti a druhý k ukládání známých tváří, které se sem nahrávají pomocí webového rozhraní. Buckety jsou designované na maximálně 1000 objektů, při překročení je sice možné přidávat další, ale databáze už neumožňuje jejich seřazení. K přetečení tohoto maxima by ale běžně nemělo docházet, protože je nastaven čas expirace objektu na jeden měsíc a není očekáváno, že by fotopast pořídila za toto časové období více snímků.

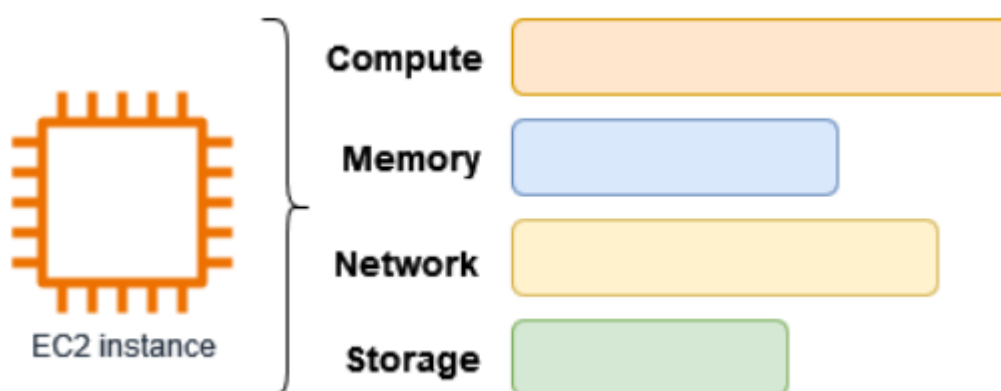
Pomocí IAM byl vytvořen uživatel „raspberry“, kterému byla přiřazena práva právě pouze k přístupu k S3 úložišti. Přestože uživatel nedisponuje žádnými přihlašovacími údaji typu „jméno a heslo“ tak se dokáže k úložišti bezpečně připojit pomocí vytvořeného přístupového klíče, který je uložen v souboru, nacházejícím se v adresářích uživatele v Raspberry. Díky tomu je zajištěn spolehlivý a bezpečný přístup zařízení k úložišti a celkově je lokalita uložení přístupového klíče bezpečnější, než kdyby byl tento klíč obsažen například ve zdrojovém kódu.

Pro přístup k úložišti z webového rozhraní byla vytvořena pouze role, která umožňuje tento přístup a která byla následně přiřazena k instanci, na které je webové rozhraní spuštěno. Díky AWS ekosystému je tedy tímto způsobem dosaženo ještě vyšší úrovně zabezpečení než pomocí přístupového klíče, protože neexistující přístupový klíč nemůže být zneužit.

6 Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) poskytuje na vyžádání škálovatelnou výpočetní kapacitu v cloudu Amazon Web Services (AWS). Pomocí Amazon EC2 je možné spustit jeden nebo více virtuálních serverů podle toho, kolik jich je právě potřeba, nakonfigurovat zabezpečení sítě a spravovat úložiště. Je možné přidat kapacitu pro zvládnutí výpočetně náročných úkolů. Když se využití sníží, je možné kapacitu opět snížit.

EC2 se používá pro širokou škálu scénářů, jako je hostování webových aplikací, výpočty, analýzy dat nebo testování nových aplikací. Je to robustní a flexibilní platforma pro správu výpočetních prostředků v cloudu (28).



Obrázek 13 Amazon EC2 (28)

Tento poskytovatel virtuálního serveru byl vybrán pro tuto práci z toho důvodu, že představuje nejlepší možné řešení z hlediska kompatibility a bezpečnosti se zvoleným S3 úložištěm v rámci ekosystému AWS.

6.1 Konfigurace serveru

Jak už bylo naznačeno, tak na platformě AWS EC2 byla spuštěna instance virtuálního serveru. Jako operační systém byl zvolen Amazon Linux 2 z důvodu nejlepší optimalizace, zabezpečení a podpory ze strany poskytovatele.

6.1.1 Amazon Linux 2

Amazon Linux 2 je operační systém Linux od společnosti AWS. Poskytuje stabilní a vysoce výkonné spouštěcí prostředí zaměřené na zabezpečení pro vývoj a provoz cloudových aplikací. Amazon Linux 2 je poskytován bez dalších poplatků. AWS poskytuje průběžné aktualizace zabezpečení a údržby pro Amazon Linux 2 (29).

6.1.2 Webový server

Vhodný webový server byl vybírán mezi dvěma z jedněch největších hráčů na trhu. Mezi webovým serverem od Apache a Nginx. Jako vhodnější kandidát se ukázal Nginx, protože je 2,5x rychlejší než Apache a protože nemá tak rozsáhlý kód a díky tomu je snáze udržitelný a to i z hlediska bezpečnosti (30).

Dříve než bylo přistoupeno k samotnému nastavení webového serveru, tak byla zakoupena internetová doména fotopastweb.cz a byl opatřen TLS certifikát, který umožňuje bezpečné připojení pomocí šifrování přenášených dat.

V dalších krocích byl webový server nastaven tak, aby implementoval současné standardy zabezpečení, například zde byl instalován Certbot, který se stará o automatickou aktualizaci TLS certifikátu. Dále byl Nginx nastaven jako reverzní proxy server, aby přesměroval požadavky na port, na kterém běží webové rozhraní.

6.2 Webové rozhraní

Dle jasně definovaných požadavků musí webové rozhraní umožňovat zprostředkování pro několik úloh.

- Zobrazovat pořízené snímky z fotopasti s možností filtrování dle data a času.
- Poskytovat rozhraní pro jednoduché ovládání fotopasti
- Umožňovat přidávání známých tváří

Pro tyto účely byl zvolen framework Django, pomocí kterého byly vytvořeny 4, respektive 5 webových stránek, pokud se sem zahrne i stránka pro přihlášení. Při tvorbě webového frontendu (část webové stránky, která je viditelná uživateli) byly použity 4 druhy prostředků.

- HTML – struktura stránky a formuláře
- CSS – vzhled stránky a formulářů
- JavaScript – přidává interaktivitu a další
- Django Template Language – poskytuje CSRF ochranu

Backend (pozadí webové stránky, které se stará o celkovou funkčnost) zde zajišťuje programovací jazyk Python.

6.2.1 Django a CSRF

Django je framework pro vývoj webových aplikací v jazyce Python, navržený k usnadnění rychlého vytváření a snadné údržbě webů. Tento framework umožňuje programátorům jednoduché vytvoření stabilních a bezpečných aplikací s integrovanými nástroji pro správu databází a směrování URL.

Další funkce zahrnují formuláře pro ověření uživatele a dále také kromě jiného Django podporuje například princip „Don't Repeat Yourself“, což znamená snížení duplikace kódu a usnadnění údržby aplikace. Je postaveno pro škálovatelnost a bezpečnost, což ho činí oblíbenou volbou pro profesionální vývoj webových aplikací (31).

CSRF ochranu poskytují specifické tokeny, přidávané do formulářů a požadavků, pro ověření serverem, před zasláním požadavku. Slouží k prevenci neoprávněných akcí z jiných webových stránek (32).

6.2.2 Hlavní stránka a přihlášení

Přístup na tuto stránku, stejně jako na všechny další je podmíněn úspěšným přihlášením. Pro samotné přihlášení byla vytvořena pouze webová šablona pro stránku, na které dochází k přihlášení. O ostatní záležitosti, které jsou spojeny s přístupem a správou uživatelů, se stará framework Django, který poskytuje uživateli s dostatečnými právy možnost přidávání nebo odebírání uživatelů, správu jejich práv atd. v uživatelsky přívětivém prostředí webového rozhraní.



The image shows a web form for login. At the top, the title "Přihlášení" is centered in a bold, dark blue font. Below the title, there are two labels: "Uživatelské jméno:" and "Heslo:", both in a bold, dark blue font. Each label is followed by a white rectangular input field with a thin grey border. At the bottom of the form, there is a solid green rectangular button with the text "Přihlásit se" in white, centered on it.

Obrázek 14 Přihlašovací stránka

Na výše zobrazeném obrázku 14 lze vidět design formuláře pro přihlášení. Po vložení správných přihlašovacích údajů se změní název tlačítka na „Přihlašuji...“ a pokud na něj uživatel v této fázi znovu klikne, tak tím neprovede žádnou akci.

Je to tak nastaveno z toho důvodu, že přihlašování na hlavní stránku trvá několik sekund (záleží na kvalitě připojení) a uživatel by tak někdy mohl mít tendenci zkusit kliknout podruhé na přihlašovací tlačítko. Tento krok by ale způsobil chybu kvůli chybnému, nebo neaktuálnímu CSRF tokenu.

The image shows the top section of a web application. At the top, there is a green navigation bar with three white buttons: 'Vítej Pavel!', 'Přejít na kontrolní panel', and 'Přejít na známé tváře'. To the right of these buttons is a red button with white text that says 'Odhlásit se'. Below the navigation bar is a light gray search form. It contains two date input fields, one labeled 'Od:' and one labeled 'Do:'. Each input field has a placeholder 'dd.mm.rrrr --:--' and a small calendar icon on the right. Below the date fields is a green button with white text that says 'Filtrovat'.

Obrázek 15 Hlavní stránka

Na obrázku 15 je zobrazen design hlavní stránky. V horní liště jsou 3 tlačítka. Tlačítka „Přejít na kontrolní panel“ a „Přejít na známé tváře“ se zobrazí pouze uživateli, který má oprávnění k jejich zobrazení a použití. Tato tlačítka slouží k přesměrování uživatele na další stránky webové aplikace. Tlačítko „Odhlásit se“ uživatele odhlásí a přesměruje ho na přihlašovací stránku.

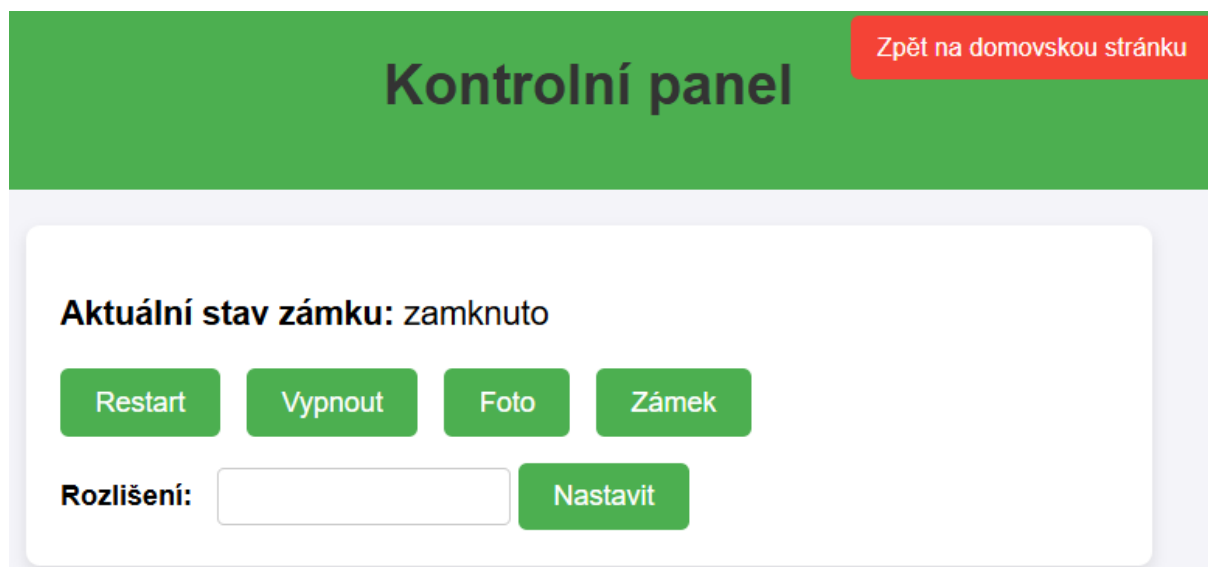
Vzhledem k tomu, že nebylo žádoucí, aby všichni registrovaní uživatelé měli přístup ke všem dovednostem webového rozhraní (mezi které patří třeba i vypnutí fotopasti), tak bylo vytvořeno přístupové právo, které mohou mít jen někteří uživatelé a jediné uživatelé s tímto přístupovým právem mají tyto rozšířené možnosti. Toto přístupové právo neovlivňuje pouze vzhled hlavní stránky, ale je implementováno i v kódu backendu. Tato implementace zajistí, že uživatelé bez tohoto práva se opravdu nedostanou na nedostupné stránky i kdyby například zkusili do adresního řádku dopsat „/control“, což je odkaz na jednu ze stránek, kam nemají přístup.

Pod horní lištou jsou už jen 2 pole pro vložení datumu a času. Tyto pole umožňují komfortní zadání datumu a času a po stisku tlačítka „Filtrovat“ se uživateli zobrazí snímky z fotopasti, které byly vytvořeny ve vloženém časovém intervalu. Pokud jsou pole nevyplněna, tak se uživateli zobrazí 10 posledních snímků, které byly fotopastí pořízeny. To je také příčinou, proč přihlašování trvá několik sekund, protože webová aplikace musí poslat žádost do databáze, snímky se musí seřadit a stáhnout. Fotky se zobrazují spolu s vybranými metadaty pod daným formulářem. Struktura vyobrazení fotek je zobrazena na vybraných obrázcích v kapitole 7.

Fotky se načítají pomocí vygenerované podepsané URL s pevně nastavenou dobou expirace. Podepsaná URL obsahuje jedinečný token, bez kterého není umožněn vzdálený přístup k fotkám v databázi.

6.2.3 Kontrolní panel

Jako kontrolní panel je pojmenována stránka, ze které je možné posílat příkazy fotopasti.



Obrázek 16 Kontrolní panel

Na této stránce je zobrazen aktuální stav zámku. Z této stránky je možné také fotopast ovládat, a to intuitivně dle vyobrazených tlačítek. Tlačítka předávají fotopasti povely pomocí přepsání JSON souboru, který si fotopast pravidelně skenuje pomocí SSH připojení.

Ať je stav zámku jakýkoliv, tak stiskem tlačítka „Zámek“ vždy dojde k přepnutí zámku do opačného stavu, než v jakém se právě nachází. Textové pole pro rozlišení slouží k tomu, aby se po vložení přesného názvu snímku předal fotopasti příkaz k tomu, aby se daný snímek pokusila nahrát v plném rozlišení, pokud má daný snímek stále k dispozici ve svém interním úložišti. Jakmile je zadán jakýkoliv příkaz a fotopast ho přijme, tak je na stránce vyobrazena informace o úspěšném přijetí příkazu.

6.2.4 Známé tváře a další

Na této stránce webové aplikace je možné zobrazovat aktuálně používané snímky známých tváří a přidávat další. Ke každému názvu snímku tu jsou také informace o tom, které osobě patří, stanovisko fotopasti k danému snímku a informace, zda je daná osoba povolena pro otevření zámku.

V horní liště jsou tlačítka, která přesměrovávají buď na hlavní stránku, nebo na další stránku, kde je možné udělovat nebo odebírat přístupy daným osobám.

Známé tváře Přejít na správu Návrat na domovskou stránku			
Název souboru	Osoba	Stanovisko	Povolen
Clipboard01.jpg	jiri	Succesful	ano
detected_face_4.jpg	jiri	Succesful	ano
img_20241218164418.jpg	jiri	Succesful	ano
img_20241223113907.jpg	pavel	Undetected face.	ano
img_20241223114059.jpg	pavel	Succesful	ano
img_20241223190649.jpg	pavel	Succesful	ano
img_20241224170915.jpg	pavel	Exists	ano

Obrázek 17 Známé tváře

V tabulce na obrázku 17 jsou viditelné 4 sloupce. V prvním je název souboru a ve druhém název osoby. Ve třetím sloupci je stanovisko fotopasti k danému souboru. Toto stanovisko může nabývat 4 hodnot. „Successful“ znamená, že byl na snímku úspěšně detekován obličej a fotopast ho bude používat při rozpoznávání. „Undetected face“ znamená, že na snímku buď nebyla nalezena žádná tvář, nebo jich bylo nalezeno více, což neumožňuje správné přiřazení obličejového rysu k požadované osobě. „Exists“ znamená, že snímek s tímto názvem už pro danou osobu existuje. Pro úspěšné přidání by bylo tedy třeba přejmenovat název souboru. Poslední typ stanoviska, který není vyobrazen na obrázku, je stanovisko, které informuje o dosud neznámém stavu. Znamená to, že daný soubor ještě nebyl zpracován.

Náhled obrázku

Klikněte na název souboru pro zobrazení obrázku.

Nahrát nový soubor

Vybrat soubor

Soubor nevybrán

Zadejte název osoby

Nahrát soubor

Obrázek 18 Přidání známé tváře

Pod tabulkou z obrázku 17 je část stránky vyobrazená na obrázku 18. Po kliknutí na název souboru v tabulce se zobrazí fotografie, kterou tento soubor představuje. Její velikost je omezena pevně danou šířkou (a výška se dopočítá podle poměru stran), tak aby fotografie nezabírala na stránce příliš prostoru.

Pod tím je zde možnost nahrání nových souborů, respektive fotek s tváří osoby, která má být přidána. Po kliknutí na „Vybrat soubor“ se otevře dialogové okno, které umožňuje výběr souborů ze zařízení uživatele. Je zde vepsáno omezení, že soubory mohou být pouze typu JPEG. Jakmile se do textového pole zadá název osoby a stiskne se tlačítko „Nahrát soubor“, tak dojde k přidání tohoto souboru do databáze známých tváří.

6.2.5 Správa a odesílání e-mailů

Ze stránky se správou je možné řídit pravomoci známých osob k otevření zámku. Je tu také log, který obsahuje až 100 posledních zpráv z fotopasti, které jsou odesílány v případě možné sabotáže. Pod logy se nachází tlačítko pro návrat na předchozí stránku.



Čas	Zpráva
2024-12-27 15:20:01	Zjistena_mozna_sabotaz,_kamera_prekryta!

Obrázek 19 Stránka se správou přístupu

Tyto logy jsou zde nejen zobrazeny, ale také jakmile server obdrží od fotopasti novou zprávu tohoto typu, tak ji do jedné minuty (bez započtení prodlení přenosu) odešle na přednastavenou e-mailovou adresu. Tento způsob zajištění rychlé notifikace uživatele byl upřednostněn, například před zasláním textové zprávy, z důvodu nižších provozních nákladů. E-maily jsou odesílány prostřednictvím SMTP.

SMTP je internetový protokol sloužící k přenosu elektronických zpráv mezi servery a klienty za účelem jejich doručení a funguje na aplikační vrstvě modelu TCP/IP (port 25). Elektronické zprávy jsou ukládány do schránek, ke kterým je možné přistupovat prostřednictvím protokolů POP3 nebo IMAP (33).

7 Testování fotopasti

Testování mělo za účel otestovat vlastnosti fotopasti za plného provozu v aktuálních klimatických podmínkách a v umístění podobnému budoucímu cílovému umístění. Při testování se dbalo nejen na správnou funkčnost fotopasti, ale i na dostačující zabezpečení. Fotopast byla v jednom kuse zapnutá (jen s krátkými výpadky, kdy se ověřovala třeba její reakce na vypnutí) po dobu delší jak 14 dní, aby byla dostatečně otestována její stabilita. Během jednoho dne byla také po dobu jedné hodiny podrobena intenzivnímu zatížení.

Osoby na případně dostupných obrázcích z testování vyjádřily souhlas se zveřejněním snímků.

7.1 Z hlediska funkčnosti se zaměřením na rozpoznání

Ještě dříve, než bylo zahájení testování zařízení v reálných podmínkách, tak bylo zjištěno, že IR přísvit nemůže být ve společném pouzdře s kamerou, jak bylo původně zamýšleno, a to kvůli odrazu infračerveného světla od průhledného krytu. Z toho důvodu byl IR přísvit instalován zvlášť.



Obrázek 20 Testovací umístění

Na obrázku 20 lze vidět testovací umístění fotopasti. Je to ve venkovním prostředí a jak kamerový modul, tak PIR čidlo jsou místo pevného uchycení vruty uchyceny pouze pomocí stahovacích pásek, aby nedošlo k poškození testovacího umístění.

7.1.1 Rozpoznání s IR přísvitem

Při dlouhodobém testování bylo zjištěno, že je algoritmus rozpoznání poměrně citlivý na intenzitu osvětlení. V běžných denních hodinách (zhruba od 7:00-16:00) bylo rozpoznávání velmi úspěšné. V nočních hodinách při osvětlení IR přísvitem fotopast ze začátku nebyla schopná detekovat známou tvář. Bylo potřeba doplnit do známých tváří testované osoby 3 noční snímky, které byly fotopastí pořízeny. Poté se úspěšnost detekce výrazně zvýšila (osoba byla rozpoznána v 28 případech z 30 detekcí), dalo by se říct, že se blížila úspěšnosti v denním režimu, ale toho není v noci možné dosáhnout, protože snímky nasvícené pouze IR přísvitem nejsou tak ostré, jako kdyby byly pořízeny ve dne a úspěšné rozpoznání je možné pouze ve vzdálenosti zhruba 0,5 – 3 m od kamerového modulu. Rozhodně lze ale konstatovat, že by testovaná osoba byla do objektu vpuštěna během prvních několika pořízených fotografií (obvykle do druhé fotografie).

Obecně je někdy obtížné objektivně posoudit, zda na některém snímku měla být osoba rozpoznána, nebo ne. Dost záleží například na úhlu pohledu, který by měl být vždy přímý vůči kamerovému modulu – viz kapitola 4.3.1. Toto omezení není vyloženě problematické, protože osoba, která se chce dostat do objektu, se ve vlastním zájmu postaví tak, aby mohla být rozpoznána.

Problematické rozpoznávání bylo pozorováno na přelomu dne a noci, kdy ještě bylo dostatek světla, takže se v kameře nevypnul IR filtr, ale zároveň snímaná tvář byla nedostatečně osvětlena, aby detekční algoritmus mohl detekovat její rysy. Výrobce kamery prozatím neumožňuje softwarové ovládání IR filtru, jeho vypínání probíhá automaticky. Díky možnosti ovládání zámku vzdáleně přes webové rozhraní je možné i v této mimořádné situaci umožnit osobě přístup do objektu. Navíc v cílovém umístění je instalováno venkovní osvětlení, jehož použití by umožnilo dostatečné nasvícení tváře i časovém období, kdy dochází k východu nebo západu slunce.

Na obrázku 21 jsou 2 snímky obrazovky webového rozhraní. Běžně se ve webovém rozhraní zobrazují snímky pouze pod sebou, pro tento účel ale byly snímky spojeny vedle sebe, aby na nich šlo dobře demonstrovat to, že kamera dokáže správně přidanou osobu v noci úspěšně rozpoznat i v různých vzdálenostech od kamerového modulu.



Čas: 2024-12-27 17:37:32 - PIR

Rozpoznání: pavel



Čas: 2024-12-27 17:37:15 - PIR

Rozpoznání: pavel

Obrázek 21 Noční rozpoznání

7.1.2 Rozpoznání v denním režimu a zátěžový test

Jednoho dne v denních hodinách v časovém rozmezí 11:24-12:24 proběhlo intenzivní testování funkčnosti fotopasti i při vyšším zatížení, než jaké je obvyklé. Z tohoto důvodu bylo dočasně zrušeno zvětšování intervalu, který jindy prodlužuje dobu mezi jednotlivými snímky, viz kapitola 4.2.1. Snímkování tedy probíhalo v návaznosti na aktivitu PIR čidla vždy po třech snímcích v rozmezí 2 s. Při tomto testování bylo před kameru neustále vstupováno a byly tak pořízeny nižší stovky snímků. Zároveň byla zaznamenávána teplota CPU (s periodou 10 s) a okolní teplota (s periodou 30 min). Jak už bylo řečeno v kapitole 7.1.1, tak není vždy jednoduché posoudit, jestli osoba měla tvář nastavenou dostatečně přímo, aby ji fotopast mohla rozpoznat. Z tohoto důvodu se následující rozbor bude zabývat pouze těmi snímky, na kterých rozpoznávání fotopasti detekovalo obličej.

	Osoba 1	Osoba 2	Osoba 3	Osoba 4	Osoba 5
Známa osoba	NE	ANO	NE	NE	NE
Počet celkových detekcí tváře	33	30	12	6	5
Počet správných detekcí známé osoby	-	23	-	-	-
Počet záměn za jinou známou osobu	1	-	-	-	-

Tabulka 2 Zjištěná data (první polovina intervalu)

	Osoba 1
Známa osoba	ANO
Počet celkových detekcí tváře	50
Počet správných detekcí známé osoby	46
Počet záměn za jinou známou osobu	1

Tabulka 3 Zjištěná data (druhá polovina intervalu)

V tabulce 1 jsou data z rozpoznávání detekovaných tváří 6 různých osob během 30 minut testování. V tabulce 3 jsou data z druhých 30 minut testování, kdy byla osoba 1 nastavena jako známá osoba, tím že se do databáze přidaly její fotky a fotopast se restartovala.

Celkem detekcí obličejů	136
Nerozpoznání známé osoby	11
Počet kritických chyb	2
Úspěšnost rozpoznání známých osob	86,25 %
Kritická chybovost	1,47 %

Tabulka 4 Souhrnné hodnoty

Z tabulky 4 vyplývá, že fotopast dokáže ve většině případů úspěšně rozpoznat známé osoby. Její úspěšnost by nejspíše mohla být ještě zvýšena přidáním většího počtu fotek ke známým tvářím, které v době testování měly vždy pouze nižší jednotky nahraných fotek.

Zároveň byla při rozpoznávání vykázána poměrně nízká kritická chybovost, která byla definována jako poměr počtu kritických chyb (tedy záměn detekované tváře za známou tvář jiné osoby) k celkovému počtu detekcí tváře. Přestože 1,47 % je nízká hodnota, tak je to pořád kritická chyba, která by v některých případech mohla způsobit neoprávněné umožnění přístupu do objektu. Na druhou stranu lze přihlídnout k tomu, že se to stalo pouze u osoby 1 a 2. Tyto osoby jsou stejného pohlaví a jsou si blízké příbuzné, takže mají podobné obličejové rysy a u cizích osob by tento případ neměl nastat. Přesto byla kvůli tomu upravena mez pro rozpoznávání, aby byl algoritmus o něco přísnější.

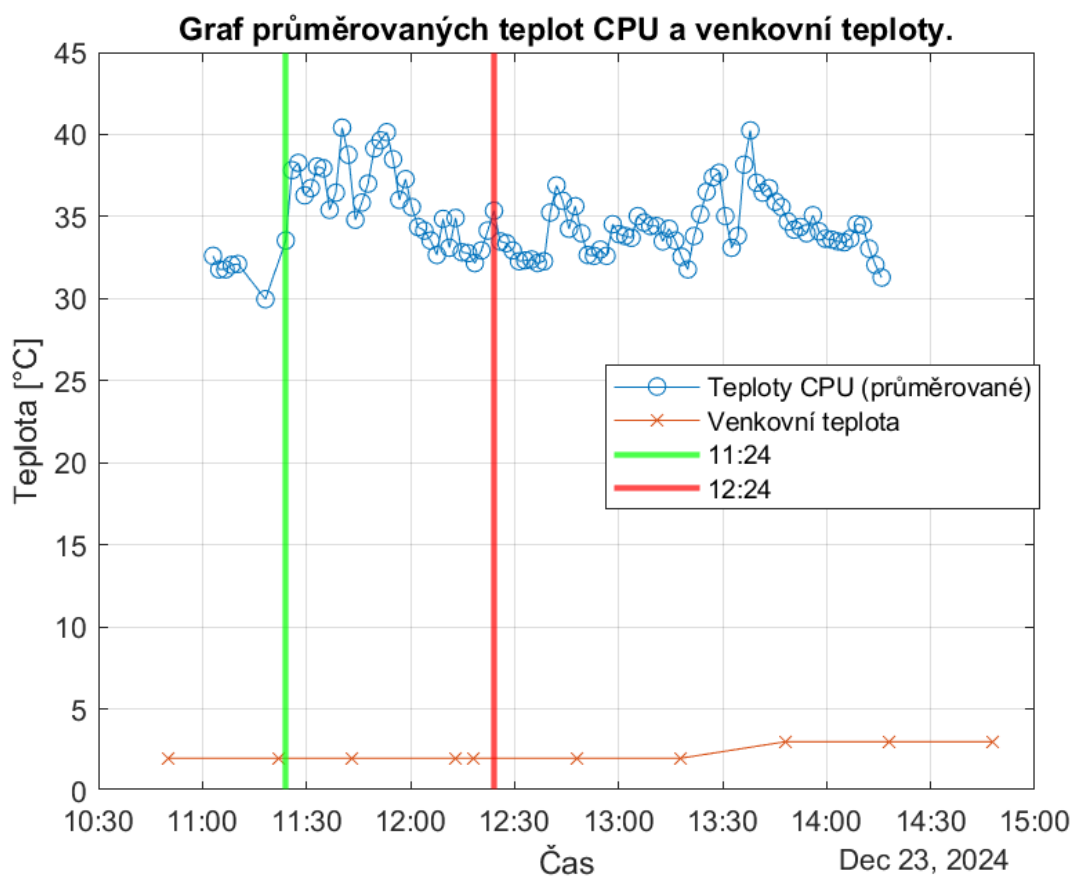
Jak bylo uvedeno na začátku podkapitoly, tak byly při tomto testu pořízeny nižší stovky fotek, přesto bylo dle souhrnné tabulky 4 detekováno pouze 136 tváří. Není to jen z toho důvodu, že někdy měly osoby nepřímo natočené tváře, ale i kvůli tomu, že bylo zároveň testováno, jak rozpoznávací algoritmus reaguje na to, když osoby mají na sobě čepici, brýle, nebo nasazenou kapuci. Na základě tohoto testování nebyly vykázány žádné konkrétní data z toho důvodu, že se jednalo o ne zcela objektivní záležitosti (například výška umístění čepice) a vstupovalo do toho více dalších faktorů. Obecně lze ale říct, že nasazená čepice neměla téměř žádný vliv, pokud nebyla nasazena příliš nízkou (algoritmus zpracovává obličej zhruba po obočí). I s nasazenými brýlemi bylo rozpoznávání podobně úspěšné jako bez nich (testovány byly průhledné dioptrické brýle, ne tmavé). Je třeba podotknout, že osoba měla i v databázi známých tváří nahranou fotku, na které má na sobě brýle.



Čas: 2024-12-27 10:21:25 - PIR

Rozpoznání: pavel

Obrázek 22 Snímek ve dne s nasazenou čepicí



Graf 1 Vývoj teploty CPU

Aktuální klimatické podmínky umožnily provést testování fotopasti v reálném (venkovním) prostředí pouze při okolních teplotách blízkých nule. Je to jeden z důvodů, proč teplota CPU dle grafu 1 nedosahuje nijak vysokých hodnot. V tomto grafu si lze také všimnout toho, že ani ve vyznačeném čase intenzivního testování teploty CPU o moc nenarostly. Z toho důvodu by postrádalo smysl měřit teplotu i uvnitř technického zázemí, protože by se při porovnání své velikosti vůči velikosti CPU, měnila spíše jen vzhledem k okolní teplotě, než kvůli zvýšení teploty CPU.

7.2 Z hlediska bezpečnosti

Fotopast byla vystavena dvěma různým druhům možné sabotáže. V prvním případě byl odpojován vodič, který slouží pro fyzickou kontrolu toho, zda nebyl kamerový modul odpojen. Tento vodič vede do kamerového modulu jako GND v rámci HDMI kabelu, vstupujícího přes redukci do kamery. Z kamery je vyveden zpět do technického zázemí pomocí 1 volného vodiče ze 3 vodičů 3linkového kabelu, sloužícího pro napájení IR přísvitu. Tím je zajištěna reakce jak na poškození HDMI kabelu, tak i na poškození napájení IR přísvitu.

Druhým typem sabotáže bylo překrývání kamery lepicí páskou, viz obrázek 20. Při obou typech sabotáže došlo k úspěšnému rozpoznání sabotáže. V obou případech přišel e-mail na cílovou adresu do 2 minut.

7.2.1 Na straně serveru

V serverovém logu byly zaznamenány 2 různé typy útoků, které se úspěšně podařilo odrazit. Prvním typem útoků bylo několik příkazů, kterými se útočník snažil získat informace o cestě ke knihovně, kterou by se posléze mohl pokusit zneužít. Jednalo se například o příkaz:

`„/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php“` Na který server odpověděl „404 Not Found“. Tato odpověď je optimální, protože neumožnila útočníkovi zjistit žádné informace o serveru, ani potvrdit, zda je server zranitelný.

Druhý typ útoku se snažil zneužít funkci „`call_user_func_array`“, která může být použita v některých PHP aplikacích. I na tento typ útoku odpověděl server stejně, jako na první typ útoku. Pro zajištění ještě vyšší bezpečnosti byla upravena konfigurace Nginx tak, aby byl do složky „/vendor“ blokován veškerý přístup. Ještě vyšší úroveň zabezpečení by mohla být zajištěna například použitím Web Application Firewall (WAF).

7.2.2 Na straně Raspberry

Vzhledem k tomu, že Raspberry nemá veřejnou IP adresu, tak není tak jednoduché k němu získat přístup. Pro uživatele bylo vytvořeno silné heslo a doporučuje se pravidelně provádět bezpečností aktualizace operačního systému. To lze provádět i jednoduše pomocí vzdáleného připojení Raspberry Pi Connect.

8 Závěr

Cílem práce bylo definovat požadavky pro dálkově ovládanou fotopast se schopností rozpoznání obličeje a příslušnou reakcí na tuto událost. Poté bylo zapotřebí vybrat vhodný hardware, správně ho pospojovat a naprogramovat softwarovou část, která se dělila na 2 velké celky. Na část v Raspberry a na část softwaru na webovém serveru. Tyto 2 celky spolu musely umět dobře interagovat, aby byl zajištěn bezchybný a bezpečný chod.

V práci je popsáno jak definování požadavků pro cílové zařízení, tak i postupný proces, ve kterém je popisován jak použitý hardware, tak i detailně jeho softwarová část. Fotopast byla sestavena a úspěšně otestována v reálném prostředí, kdy ve většině ohledů dosahovala uspokojivých výsledků.

Fotopast je nyní stále aktivní na místě testovacího umístění. Očekává se, že instalace zařízení v cílovém umístění bude provedena v příhodnějším klimatickém období, kdy teplotní podmínky umožní bezpečnou a efektivní realizaci montáže.

Na zařízení fotopasti by bylo možné v budoucnu implementovat různá vylepšení. Především v oblasti webového rozhraní by bylo možné přidat více filtrů, které by umožnily filtrování snímků podle typu zachycení snímku, nebo podle výsledku rozpoznání snímku, konkrétně třeba podle jména známé osoby. Dále by bylo možné i rozšířit komunikaci mezi fotopastí a webovým serverem, případně i navazující e-mailová upozornění, aby docházelo k informování, například při změně stavu zámku.

Použitá literatura

- 1) MAREK, Ondřej. Vestavná fotopast se záznamem snímků na SD kartu. Online, Bakalářská práce, vedoucí Václav Šimek. Brno: Vysoké učení technické v Brně. Fakulta informačních technologií. Ústav počítačových systémů, 2019. Dostupné z: <http://hdl.handle.net/11012/180153>. [cit. 2024-12-18].
- 2) ŽÁČEK, Jaroslav, 2014. *SOFTWARE INŽENÝRSTVÍ* [online]. Ostrava, Dostupné z: https://web.osu.cz/~Zacek/sweng/skripta_sweng.pdf. Ostravská univerzita [cit. 2024-12-18].
- 3) Ochrana majetku a osob v exteriérech pomocí fotopastí. Online, Bakalářská. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/25157/kukula_2013_bp.pdf [cit. 2024-12-26].
- 4) KOWALCZYK, Dariusz. *File:Camera trap, fotopułapka, kamera leśna, kamera obserwacyjna.jpg*. Online. In: . 2020-11-17. Dostupné z: https://commons.wikimedia.org/wiki/File:Camera_trap_fotopu%C5%82a_pka_kamera_le%C5%9Bna_kamera_obserwacyjna.jpg. [cit. 2025-01-05].
- 5) *Nejprodávanější fotopasti*. Online. E-fotopast.cz. 2025. Dostupné z: <https://www.e-fotopast.cz/nejprodavanejsi-fotopasti.html>. [cit. 2025-01-05].
- 6) *Fotopast na zloděje*. Online. AGRON.cz. 2025. Dostupné z: https://www.agron.cz/blog/fotopast-na-zlodeje/?srsltid=AfmBOoqymu5itzo4yaxdmQk_Rabi8tYJ5fzvjXYQ9t74oA7BPvG6-ZZJ. [cit. 2025-01-05].
- 7) *Fotopast WIFI UOVision Home Guard W1*. Online. FOTOPAST.CZ s.r.o. Dostupné z: <https://www.fotopast.cz/fotopasti/131-fotopast-wifi-uovision-home-guard-w1.html>. [cit. 2025-01-05].
- 8) *Fotopast BUNATY FULL HD*. Online. E-fotopast.cz. 2025. Dostupné z: <https://www.e-fotopast.cz/fotopast-bunaty-full-hd.html>. [cit. 2025-01-05].
- 9) *Fotopast FOXcam Wi-Fi*. Online. FOXcam, s.r.o. Dostupné z: <https://www.eshop-fotopasti.cz/produkt/fotopast-foxcam-wifi/>. [cit. 2025-01-06].
- 10) *Fotopast KeepGuard KG698A*. Online. FOXcam, s.r.o. Dostupné z: <https://www.eshop-fotopasti.cz/produkt/fotopast-keepguard-kg698a/>. [cit. 2025-01-06].
- 11) VÝBORNÝ, Filip. *KONFIGUROVATELNÁ VESTAVNÁ FOTO/VIDEOPAST SE ZÁZNAMEM DAT A SAMOČINNOU ADAPTACÍ NA OKOLÍ*. Online, Diplomová. Brno: VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ, 2015. Dostupné z: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=115067. [cit. 2024-12-20].
- 12) HADEx. Online. Dostupné z: <https://www.hadex.cz/m523-automaticky-prepinac-baterie---ups-modul-yx850>. [cit. 2024-12-16].
- 13) Infineon. Online. 1999 - 2024 Infineon Technologies AG. Dostupné z: <https://www.infineon.com/dgdl/irlz44npbf.pdf?fileId=5546d462533600a40153567217c32725>. [cit. 2024-12-17].

- 14) 2020 Rectron Semiconductor. Online. Dostupné z: <https://eu.mouser.com/datasheet/2/345/sr520-sr5200-34059.pdf>. [cit. 2024-12-17].
- 15) WIKIPEDIA CONTRIBUTORS. Supercapacitor. Online. In: Wikipedia: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2001-, 2024-11-12. Dostupné z: <https://en.wikipedia.org/w/index.php?title=Supercapacitor&oldid=1256882093> [cit. 2024-12-17].
- 16) Hadex.cz. Napájecí modul step-down měnič 9-35V na 5V/5A, svorkovnice – M398F [online]. Dostupné z: <https://www.hadex.cz/m398f-napajeci-modul-step-down-menic-9-35v-na-5v5a-svorkovnice/> [cit. 2024-12-17].
- 17) Peška, Robert. Raspberry Pi 5 odhalena [online]. 29. září 2023. Dostupné z: <https://vyvoj.hw.cz/raspberry-pi-5-odhalena.html> [cit. 2024-12-18].
- 18) LaskaKit. Online. Copyright 2024 LaskaKit. Dostupné z: <https://www.laskakit.cz/prijimac-433mhz-ev1527-4-kanaly/>. [cit. 2024-12-21].
- 19) Reasons to use Debian. Online. Debian. 2022-02-11. Dostupné z: https://www.debian.org/intro/why_debian. [cit. 2024-12-26].
- 20) Systemd. Online. In: Freedesktop: the free encyclopedia. San Francisco (CA): Wikimedia Foundation, 2024-02-22. Dostupné z: <https://www.freedesktop.org/wiki/Software/systemd/>. [cit. 2024-12-27].
- 21) AutoSSH. Online. Harding.motd. 2019-01-09. Dostupné z: <https://www.harding.motd.ca/autossh>. [cit. 2024-12-27].
- 22) Introduction. Online. The libcamera documentation authors. 2023. Dostupné z: <https://libcamera.org/introduction.html>. [cit. 2025-01-06].
- 23) GEITGEY, Adam. Modern Face Recognition with Deep Learning. Online. Medium. 2016. Dostupné z: <https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78>. [cit. 2024-12-28].
- 24) ANDERSON, Martin. Facial Detection and Recognition With Dlib. Online. Width LLC. 2021-09-29. Dostupné z: <https://www.width.ai/post/facial-detection-and-recognition-with-dlib>. [cit. 2024-12-28].
- 25) Co je to SFTP a proč bych ho měl používat pro přenos souborů? Online. MyDreams. Dostupné z: <https://www.mydreams.cz/cz/wiki/7821-co-je-to-sftp-a-proc-bych-ho-mel-pouzivat-pro-prenos-souboru.html>. [cit. 2024-12-28].
- 26) How Amazon S3 works. Online. Amazon Web Services. Dostupné z: <https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html>. [cit. 2024-12-28].
- 27) What is IAM? Online. Amazon Web Services. Dostupné z: <https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>. [cit. 2024-12-28].
- 28) What is Amazon EC2? Online. Amazon Web Services. Dostupné z: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html>. [cit. 2024-12-28].

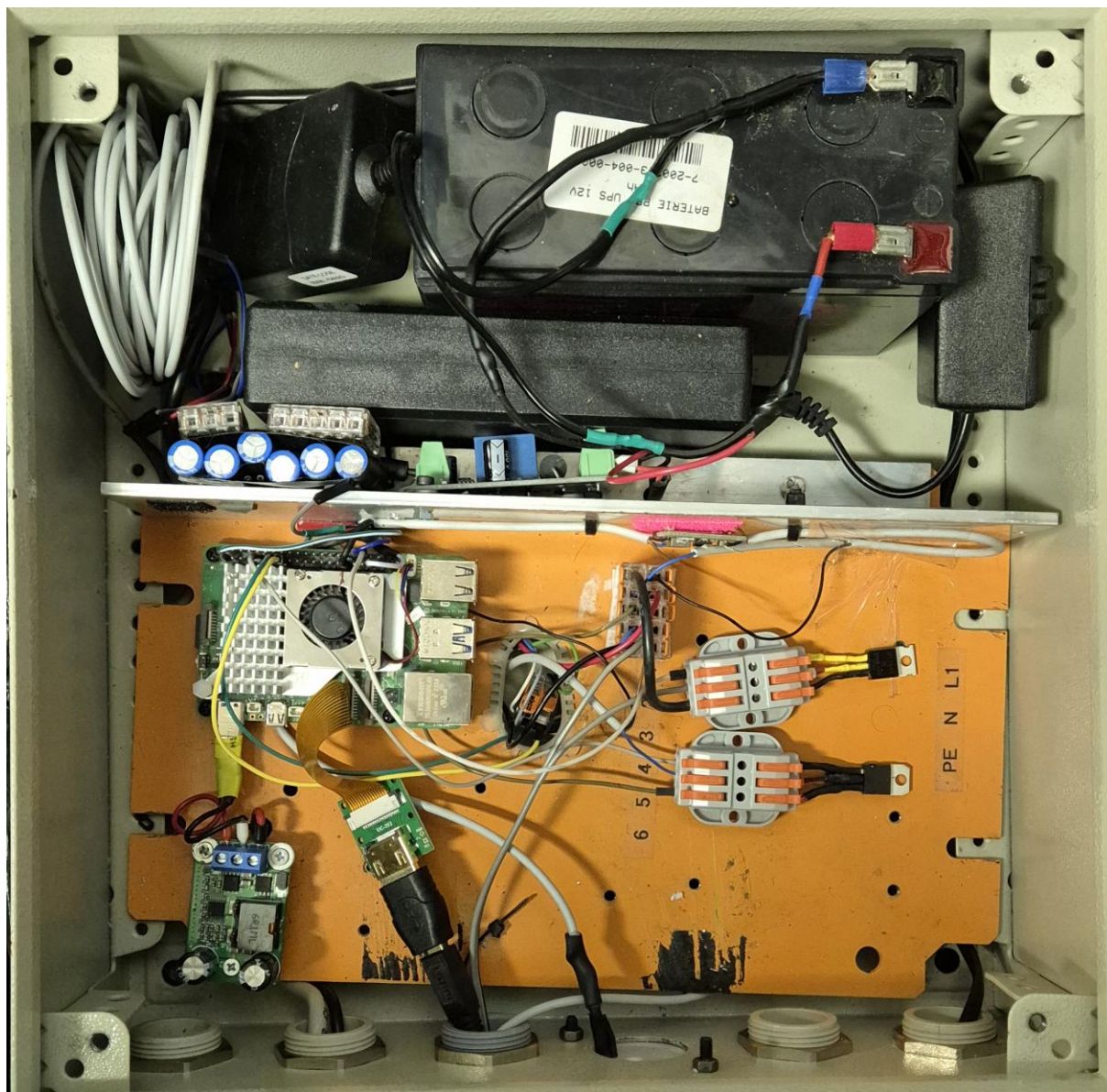
- 29) Amazon Linux 2. Online. Amazon Web Services. Dostupné z: <https://aws.amazon.com/amazon-linux-2/>. [cit. 2024-12-28].
- 30) JANÍK, David. Apache vs Nginx. Online. Váš Hosting s.r.o. 2024, 2023-10-24. Dostupné z: <https://www.vas-hosting.cz/blog-apache-vs-nginx>. [cit. 2024-12-28].
- 31) Django documentation. Online. Django Software Foundation. Dostupné z: <https://docs.djangoproject.com/en/5.1/>. [cit. 2024-12-28].
- 32) *Co je token CSRF a jak pomáhá zmírňovat útoky CSRF?* Online. Evropský institut pro certifikaci IT. 2023. Dostupné z: <https://cs.eitca.org/cybersecurity/eitc-is-wasf-web-applications-security-fundamentals/same-origin-policy/cross-site-request-forgery/examination-review-cross-site-request-forgery/what-is-a-csrf-token-and-how-does-it-help-mitigate-csrf-attacks/>. [cit. 2024-12-29].
- 33) Co je SMTP. Online. Aira GROUP. 2022. Dostupné z: <https://www.sprava-site.eu/smtp/>. [cit. 2024-12-29].

Přílohy

A Obsah přiloženého souboru

- RPI_software.zip – Vytvořené skripty v Raspberry
- Rozhrani.zip – Zdrojové kódy webového rozhraní
- DP_Filjac.pdf – Diplomová práce v elektronické podobě

B Fotografie technického zázemí fotopasti



Obrázek B.1 Fotografie technického zázemí