

ŽILINSKÁ UNIVERZITA V ŽILINE

FAKULTA RIADENIA A INFORMATIKY

DIPLOMOVÁ PRÁCA

Študijný odbor: **Informatika**

Bc. Lucia Piatriková

**Vizuálna detekcia falšovaných ochranných prvkov
na občianskom preukaze**

Vedúci práce: **Ing. Peter Tarábek, PhD.**

Reg.č. 1738/2021

Apríl 2022

ŽILINSKÁ UNIVERZITA V ŽILINE

FAKULTA RIADENIA A INFORMATIKY

VIZUÁLNA DETEKCIA
FALŠOVANÝCH OCHRANNÝCH PRVKOV
NA OBČIANSKOM PREUKAZE

DIPLOMOVÁ PRÁCA

Študijný odbor: Informatika

Pracovisko: Katedra Matematických Metód a Operačnej Analýzy

Fakulta riadenia a informatiky

Žilinská univerzita v Žiline

Školiteľ: Ing. Peter Tarábek, PhD.

Žilina, 2022

Bc. Lucia Piatriková

ZADANIE TÉMY DIPLOMOVEJ PRÁCE.

Študijný program: Inteligentné informačné systémy

Meno a priezvisko

Lucia Piatriková

Osobné číslo

558736

Názov práce v slovenskom aj anglickom jazyku

Vizuálna detekcia falšovaných ochranných prvkov na občianskom preukaze

Visual detection of counterfeit security features on an identity card

Zadanie úlohy, ciele, pokyny pre vypracovanie

(Ak je málo miesta, použite opačnú stranu)

Cieľ diplomovej práce:

V súčasnosti je preferovaná vzdialená forma autentifikácie osoby pomocou elektronických kanálov. Doklad je snímaný v nekontrolovanom prostredí, čo môže predstavovať bezpečnostné riziko. Cieľom práce je preskúmať možnosti detekcie falošného dokladu na základe analýzy jeho ochranných prvkov. Súčasťou práce je preskúmať vplyv snímania dokladu na vizuálnu podobu ochranných prvkov a vytvorenie vhodného datasetu.

Obsah:

1. Analýza ochranných prvkov dokladu a vplyvu snímania na jeho vizuálne vlastnosti
2. Návrh postupu snímania dokladu
3. Vytvorenie datasetu pre vývoj a testovanie metód verifikácie
4. Návrh vhodnej metódy/metód a jej/ich implementácia
5. Vyhodnotenie metód a záver

Meno a pracovisko vedúceho DP: Ing. Peter Tarábek, PhD., KMMOA, ŽU

Meno a pracovisko tútora DP:

8.2.2022 

vedúci katedry
(dátum a podpis)

- 3 MAR. 2022

Zadanie zaregistrované dňa pod číslom 1738/2021 podpis 

Čestné vyhlásenie

Prehlasujem, že som diplomovú prácu *Vizuálna detekcia falšovaných ochranných prvkov na občianskom preukaze* vypracovala samostatne pod vedením Ing. Petra Tarábeka, PhD., a uviedla v nej všetky použité literárne a iné odborné zdroje v súlade s právnymi predpismi, vnútornými predpismi Žilinskej univerzity a vnútornými aktmi riadenia Žilinskej univerzity a Fakulty riadenia a informatiky.

V Žiline, dňa

.....

Bc. Lucia Piatriková

Podakovanie

Chcela by som sa poďakovať svojmu vedúcemu diplomovej práce Ing. Petrovi Tarábekovi, PhD., za odborné rady, ochotu a cenné pripomienky, ktoré mi poskytol pri písaní diplomovej práce. Zároveň ďakujem Ing. Lucii Centárovej a Ing. Jánovi Zázrivcovi zo spoločnosti SOFTEC za odborné konzultácie a užitočné pripomienky.

ABSTRAKT V ŠTÁTNOM JAZYKU

PIATRIKOVÁ, Lucia, Bc.: *Vizuálna detekcia falšovaných ochranných prvkov na občianskom preukaze*. [Diplomová práca]. – Žilinská Univerzita v Žiline. Fakulta riadenia a informatiky; Katedra Matematických Metód a Operačnej Analýzy. – Vedúci: Ing. Peter Tarábek, PhD. – Stupeň odbornej kvalifikácie: inžinier. – Žilina: FRI UNIZA, 2022 – 92 s.

Digitálne overenie identity je novým trendom, ktorý umožňuje klientom prístup ku službám a produktom na diaľku, zjednodušuje interakciu klienta a spoločnosti, a šetrí ich náklady. Digitálne overenie nesie so sebou mnohé bezpečnostné riziká. Systém musí byť schopný odhaliť falošné doklady. Cieľom diplomovej práce je preskúmať možnosti detekcie falošného dokladu na základe analýzy jeho ochranných prvkov. Práca sa zameriava na detekciu a overenie vizuálnych vlastností ochranného prvku s opticky variabilnou farbou (OVI), ktorému sa zatiaľ žiadne iné práce nevenovali. OVI je typ farby, ktorá mení svoj odtieň pri nakláňaní, zmene uhla pohľadu alebo osvetlenia. V práci je navrhnutý postup detekcie občianskeho preukazu a ochranného prvku, ktorý dokáže veľmi presne nájsť ochranný prvok na snímkach videa. Okrem toho sú rozobraté vizuálne vlastnosti OVI ochranného prvku a aspekty, ktoré je potrebné overiť. Práca ponúka rôzne odporúčania a návrhy na riešenie viacerých čiastkových problémom týkajúcich sa vizuálneho overenie ochranného prvku. Niektoré postupy sú aj prakticky preskúmané, pričom sa používajú metódy digitálneho spracovania obrazu a niektoré metódy strojového učenia. V práci sa uvádzajú úspešné metódy a aj tie, ktoré sa ukázali ako nevhodné. Práca sa tiež venuje analýze vplyvu snímania na vizuálne vlastnosti objektu a limitáciám snímania ochranných prvkov. Prináša základné znalosti do danej problematiky a je východiskom pre sofistikovanejšie riešenie. Navrhovaný postup dokáže odhaliť falošný občiansky preukaz na videu na základe OVI ochranného prvku, ale má svoje limitácie.

Kľúčové slová: digitálne overenie identity, digitálne spracovanie obrazu, občiansky preukaz, OVI, počítačové videnie, strojové učenie

ABSTRAKT V CUDZOM JAZYKU

Nowadays, electronic identity verification is popular in the world. It allows clients to access services and products remotely, simplifies the interaction between client and institution, and saves their expenses. Digital verification suffers many security risks. The system must be able to reveal fake identity cards. The goal of the diploma thesis is to research the potential for detection of fake identity cards based on an analysis of its security features. The study is focused on the detection and visual verification of security feature with Optically variable ink (OVI). No other work has studied OVI till now. OVI is a type of ink whose colour varies with rotation, or a change in observer or light source position. In the diploma thesis, there is proposed a method that successfully detects an identity card and a security feature on video frames. Furthermore, OVI visual characteristics are analysed along with desired verification aspects. There are written several recommendations and suggestions for solving various partial problems related to visual OVI verification. A few practical experiments were realized by applying digital image processing and machine learning methods. There are mentioned both results, successful and also not suitable methods. Additionally, recording impact on object colour is reviewed together with security features recording limitations. The diploma thesis gives fundamental knowledge to the topic and can be the basis for more sophisticated solutions. Proposed methods can reveal fake identity card on video by analysing the OVI security feature. But it still has limitations.

Key words: computer vision, digital image processing, electronic identity verification, identity card, machine learning, OVI

Obsah

Úvod	1
1 Občiansky preukaz a jeho ochranné prvky	4
1.1 Pravosť občianskeho preukazu	4
1.2 Ochranné prvky občianskeho preukazu	6
1.2.1 Limitácie snímania ochranných prvkov	9
2 Vybrané metódy počítačového videnia	11
2.1 Farebné počítačové videnie	11
2.1.1 Vznik farebného obrazu	11
2.1.2 Vplyv snímania na vizuálne vlastnosti objektu	13
2.1.3 Farebné modely	14
2.2 Metódy digitálneho spracovania obrazu	16
2.2.1 Histogram	16
2.2.2 Prahovanie	17
2.2.3 Template Matching	17
2.2.4 Detekcia hrán	18
2.2.5 Detekcia keypointov	21
2.3 Metódy strojového učenie	23
2.3.1 Regresia a klasifikácia	23
2.3.2 Detekcia anomálií	27
2.3.3 Zhlukovanie	29

3	Návrh a implementácia metód analýzy ochranného prvku	32
3.1	Vplyv snímania na vizuálne vlastnosti ochranného prvku s opticky variabilnou farbou	33
3.1.1	Skúmanie vplyvu snímania na vizuálne vlastnosti ochranného prvku . .	35
3.2	Návrh postupu snímania a overenia pravosti občianskeho preukazu	37
3.3	Dataset občianskych preukazov	39
3.4	Návrh metód nájdenia občianskeho preukazu na snímke	43
3.4.1	Detekcia hrán občianskeho preukazu	43
3.4.2	Detekcia pomocou keypointov	44
3.5	Návrh metód nájdenia ochranného prvku na občianskom preukaze	47
3.5.1	Hľadanie ochranného prvku v celej scéne	47
3.5.2	Hľadanie ochranného prvku vo výreze občianskeho preukazu	54
3.6	Návrh metód kontroly vizuálnych vlastností ochranného prvku	57
3.6.1	Analýza farebnosti ochranného prvku	59
3.6.2	Reprezentácia farebnosti ochranného prvku na snímke	62
3.6.3	Overenie odlesku ochranného prvku	65
3.6.4	Overenie farby vzhľadom na polohu občianskeho preukazu	69
3.6.5	Overenie dostatočnej zmeny farby ochranného prvku	76
3.7	Výsledný navrhovaný postup overenia pravosti ochranného prvku s opticky variabilnou farbou	81
	Záver	85
	Zoznam použitej literatúry	88
	Prílohy	
	Príloha A: Obsah CD disku	I

Zoznam obrázkov

1.1	Ochranné prvky prednej strany občianskeho preukazu	8
1.2	Ochranné prvky zadnej strany občianskeho preukazu	8
2.1	Rozdelenie zdrojov svetla	12
2.2	Vplyv pozadia na vnímanie farby[12]	13
2.3	RGB model[1]	15
2.4	HSV model[1]	15
2.5	HSV farebný kruh[32]	15
2.6	Template Matching[34]	17
2.7	Výber hrán Canny detektorom	19
2.8	Reprezentácia priamky používaná v Houghovej transformácii	20
2.9	Výstup Houghovej transformácie[22]	20
2.10	SIFT škálový priestor[17]	21
2.11	SIFT lokálny extrém[17]	21
2.12	SIFT deskriptor[3]	22
2.13	Lineárna regresia	24
2.14	Support Vector Regression[42]	26
2.15	One Class SVM[40]	27
2.16	Isolation Forest[40]	28
2.17	Local Outlier Factor[40]	29
2.18	Algoritmus K-means[43]	30
2.19	Porovnanie algoritmov K-means a DBSCAN[52]	31
3.1	SK symbol	32
3.2	Starší lipový lístok	32

3.3	Novší lipový lístok	32
3.4	Ochranný prvok osvetlený zdrojmi svetla s rôznou teplotou	36
3.5	Biela papierová maska	36
3.6	Čierna plastová maska	36
3.7	Čierna papierová maska	36
3.8	Postup overenia pravosti občianskeho preukazu	39
3.9	Scéna	40
3.10	Detekcia hrán - scéna 1	43
3.11	Detekcia hrán - scéna 2	43
3.12	Detekcia hrán - scéna 2 (iné parametre)	43
3.13	Spárované keypointy	44
3.14	SIFT vs ORB	45
3.15	Normalizácia občianskeho preukazu	46
3.16	RGB histogramy	48
3.17	RGB prahovanie	49
3.18	HSV prahovanie	49
3.19	Výsledok Template Matching	49
3.20	Výstupná matica so skóre Template Matching	50
3.21	Výsledok Template Matching s originálnym rozlíšením	50
3.22	Výsledok Template Matching s prispôbeným rozlíšením	51
3.23	Výsledok Template Matching pre súčet skóre viacerých vzorov	51
3.24	Výsledok Template Matching pre 4 typy čiernobielych snímok	52
3.25	Výstupná matica Template Matching na celom občianskom preukaze	52
3.26	One Class SVM	53
3.27	Isolation Forest	53
3.28	Local Outlier Factor	53
3.30	Keypointy ochranného prvku	54
3.29	Keypointy na výrezoch s rôznou farbou ochranného prvku	54
3.31	Spôsoby overenia vizuálnych vlastností OVI ochranného prvku	58
3.32	RGB histogramy dvoch rôznych sérií obrázkov staršieho ochranného prvku	59

3.33 HSV heatmapy sérií obrázkov ochranných prvkov	60
3.34 HSV histogramey sérií obrázkov ochranných prvkov	61
3.35 Dominantné farby pre rôzny počet zhlukov	63
3.36 Dominantné farby sérií snímok	63
3.37 Vplyv veľkosti filtra na dominantné farby	64
3.38 Histogram rozdielov za sebou nasledujúcich snímok videa	64
3.39 Hranové filtre	65
3.40 Porovnanie skóre správnych a chybných výrezov snímok	66
3.41 Porovnanie skóre reálnych a falošných občianskych preukazov	66
3.42 Vysoké hranové skóre - chybný výrez	68
3.43 Nízke hranové skóre - chybný výrez	68
3.44 Nízke hranové skóre - správny výrez	68
3.45 Chyba regresie pre každú snímku	72
3.46 Priemerná chyba regresie videí	72
3.47 Pomer snímok vo videu označených ako reálne	75
3.48 Zmena jasů videí (hodnoty V)	77
3.49 Vzťah priemernej chyby regresie a maximálnej zmeny hodnoty V	77
3.50 Reprezentanti K-means podľa rôznych komponentov HSV (k=5)	78
3.51 Reprezentanti DBSCAN podľa rôznych komponentov HSV	79
3.52 Postup detekcie ochranného prvku	82
3.53 Výsledný navrhovaný postup overenia pravosti OVI ochranného prvku	84

Zoznam tabuliek

1.1	Porovnanie ochranných prvkov rôznych typov občianskych preukazov	9
3.1	Prehľad datasetov	42
3.2	Úspešnosť detekcie občianskeho preukazu	46
3.3	Úspešnosť metrík Template Matching	56
3.4	Úspešnosť detekcie pomocou keypointov a metódy Template Matching	57
3.5	Úspešnosť detekcie ochranného prvku	68
3.6	Porovnanie regresných modelov	71
3.7	Porovnanie detektorov anomálií	74
3.8	Matica zámen detektora anomálií Local Outlier Factor	74
3.9	Výsledky detektora anomálií Local Outlier Factor	74
3.10	Matica zámen navrhovaného postupu verifikácie	83
3.11	Výsledky navrhovaného postupu verifikácie	83

Zoznam príloh

Príloha A : Obsah CD disku

Zoznam skratiek

2D Dvojmerný z angl. two-dimensional

3D Trojmerný z angl. three-dimensional

CIE Medzinárodná komisia pre osvetľovanie francúzsky Commission
Internationale de l'Eclairage

CMYK Azúrová, purpurová, žltá a čierna farebná zložka z angl. Cyan, Magenta,
Yellow, Key Black

CRI Index podania farieb z angl. Color Rendering Index

DBSCAN angl. Density-based spatial clustering of applications with noise

DID Difrakčný identifikačný prvok® z angl. Diffractive Identification Device

eIDV Elektronické overenie totožnosti z angl. electronic IDentity Verification

FPS Počet snímok za sekundu z angl. frames per second

HSB Odtieň, saturácia, jas z angl. Hue, Saturation, Brightness

HSL Odtieň, saturácia, svetlosť z angl. Hue, Saturation, Lightness

HSV Odtieň, saturácia, jas z angl. Hue, Saturation, Value

MRZ Strojovo čitateľná zóna z angl. Machine Readable Zone

OCR Optické rozpoznávanie znakov z angl. Optical Character Recognition

ORB angl. Oriented FAST and Rotated BRIEF

OVD Opticky variabilný prvok z angl. Optically Variable Device

OVI Opticky variabilná farba z angl. Optically Variable Ink

RANSAC Náhodný výberový konsenzus angl. Random Sample Consensus

RGB Červená, zelená a modrá farebná zložka z angl. Red, Green, Blue

SIFT angl. Scale-invariant feature transform

SR Slovenská republika

SVM Metóda podporných vektorov z angl. Support Vector Machines

TM_SQDIFF štvorcová vzdialenosť z angl. Template Matching Square Difference

UV Ultrafialové žiarenie z angl. ultraviolet

Zoznam pojmov

achromatický bezfarebný

autenticita pravosť, hodnovernosť

chromatický farebný

duplexový dvojitý

giloš jemný čiarový vzor

heatmapa teplotná mapa

keypoint zaujímavý bod obrázka

makroskop prístroj na pozorovanie objektov s malým zväčšením

mikrotext rozmerovo veľmi malé písmená

negatívny obraz biele písmo je umiestnené na farebnom pozadí

normalizovaný občiansky preukaz snímka občianskeho preukazu umiestneného rovno
oproti kamere s orezaným pozadím

občiansky preukaz občiansky preukaz vydaný po roku 2007 Slovenskou republikou

outlier príliš odlišný bod

pozitívny obraz farebné písmo je umiestnené na bielom pozadí

reliéfny plastický, vypuklý

Template Matching metóda hľadajúca pozíciu šablóny (angl. template) v obrázku

Úvod

V súčasnosti je preferovaná vzdialená forma autentifikácie osoby pomocou elektronických kanálov. Digitálne overenie identity je novým trendom v oblasti bankovníctva, telekomunikácií a iných služieb. Nahrádza osobnú identifikáciu a overenie klienta pracovníkom spoločnosti. Umožňuje klientom prístup ku všetkým službám a produktom, ktoré môže organizácia ponúknuť, jednoduchým a rýchlym spôsobom na diaľku bez potreby návštevy pobočky alebo predajne, a to prostredníctvom internetu a mobilného telefónu. Digitálne overenie všeobecne zjednodušuje interakciu klienta a spoločnosti, a šetrí ich náklady. Aktuálne existujú softvérové riešenia, ktoré overujú identitu na základe fotografie občianskeho preukazu a "selfie" fotografie klienta.

Digitálne overenie nesie so sebou mnohé bezpečnostné riziká, pretože časť procesu je v nekontrolovanom prostredí v rukách klienta. Systém musí byť odolný voči falšovaným dokladom, ktoré by pri fyzickej kontrole dokladu boli zjavné, napríklad vytlačený občiansky preukaz. Dôležitou súčasťou overenia pravosti občianskeho preukazu je kontrola jeho ochranných prvkov. Každý ochranný prvok je unikátny a má špecifické vlastnosti. Niektoré ochranné prvky sa nedajú kontrolovať vizuálne alebo iba za určitých podmienok, napr. pod UV svetlom. V práci sa pod pojmom občiansky preukaz myslí občiansky preukaz vydaný po roku 2007 Slovenskou republikou.

Cieľom diplomovej práce je preskúmať možnosti detekcie falošného dokladu na základe analýzy jeho ochranných prvkov. V práci sa skúma, či má elektronické overenie ochranných prvkov potenciál, či sa dá riešiť a akými postupmi a metódami, a ako k nemu celkovo pristupovať. Diplomová práca je základným výskumom v danej problematike ochranných prvkov.

Pri riešení je vhodné postupovať od jednoduchších ochranných prvkov po zložitejšie. Diplomová práca sa zameriava na detekciu a overenie vizuálnych vlastností ochranného prvku s opticky variabilnou farbou OVI. Ochranný prvok je umiestnený v pravom hornom rohu prednej strany občianskeho preukazu. OVI je typ farby, ktorá mení svoj odtieň pri nakláňaní, zmene uhla pohľadu alebo osvetlenia. Vizuálna zmena farby je vlastnosť potenciálne využiteľná

pri vizuálnej detekcii. Hlavnou výhodou je, že prvok nekoliduje so žiadnymi osobnými údajmi, čím je zachovaná anonymita dokladu a je ľahšie detekovateľný. Analýze a digitálnemu overeniu pravosti OVI ochranného prvku sa zatiaľ žiadne práce nevenovali.

Prvá časť práce sa zaoberá občianskym preukazom a jeho ochrannými prvkami. Popisuje, kedy je občiansky preukaz pravý, a akým spôsobom je pravosť možné overiť. Detailne sú v nej popísané všetky jeho ochranné prvky a uvažuje sa, aké sú ich limitácie snímania.

Náplňou druhej časti práce je oboznámenie sa s problematikou farebného počítačového videnia. Rozoberá, ako vzniká farebný obraz, ako vplýva snímanie na vizuálne vlastnosti objektu a aké farebné modely na popísanie farby existujú. Druhá kapitola sa tiež venuje vybraným metódam digitálneho spracovania obrazu a strojového učenia. Popisuje všeobecne metódy a prístupy, a tiež konkrétne algoritmy a modely, ktoré boli použité v rámci analýzy OVI ochranného prvku.

Tretia časť práce sa venuje analýze a návrhu metód detekcie a verifikácie vizuálnych vlastností OVI ochranného prvku. Na začiatku je podrobnejšie popísaný vplyv snímania na vizuálne vlastnosti OVI ochranného prvku. Ďalej je navrhnutý celý postup snímania a overenia pravosti občianskeho preukazu, v rámci ktorého je niekoľko krokov zameraných na kontrolu ochranných prvkov. Následne sú popísané datasety, ako vznikli a za akým účelom. Ďalej sú navrhnuté a preskúmané metódy, ktoré sú rozdelené do troch skupín, a to metódy na nájdenie občianskeho preukazu na snímke, metódy nájdenia ochranného prvku a metódy kontroly vizuálnych vlastností ochranného prvku. Navrhnutý postup detekcie občianskeho preukazu a ochranného prvku dokáže veľmi presne nájsť ochranný prvok na snímkach videa. Čo sa týka overenia vizuálnych vlastností ochranného prvku, v práci sú popísané tri aspekty overenia, a to overenie odlesku, overenie farby prvku vzhľadom na polohu občianskeho preukazu a overenie dostatočnej zmeny farby. Uvádzajú sa úspešné metódy a aj tie, ktoré sa ukázali ako nevhodné, a súčasne rôzne odporúčania a návrhy na riešenie viacerých čiastkových problémom. V závere kapitoly je zhrnutý výsledný navrhovaný postup overenia pravosti ochranného prvku.

Výstupom práce je tiež testovacia aplikácia, ktorá dokáže detekovať občiansky preukaz a ochranný prvok na videu, a overiť niektoré vizuálne vlastnosti ochranného prvku. Cieľom práce nie je finálna funkčná aplikácia, ktorá rieši úlohu detekcie a overenia ochranných prvkov občianskeho preukazu. Aplikácia vznikla hlavne za účelom testovania metód detekcie a verifikácie vizuálnych vlastností ochranného prvku. Vyskúšali sa rôzne prístupy, z ktorých niektoré sa v práci označili ako neodporúčané.

V práci sú preskúmané základné metódy digitálneho spracovania obrazu a niektoré metódy strojového učenia. Práca prináša základné znalosti do danej problematiky a je východiskom pre sofistikovanejšie riešenie, pre ktoré je ale nutné mať k dispozícii väčšie množstvo dát.

1 Občiansky preukaz a jeho ochranné prvky

Podľa zákona č. 395/2019 Z. z. o občianskych preukazoch, je občiansky preukaz verejná listina, ktorou občan Slovenskej republiky preukazuje svoju totožnosť a štátne občianstvo. Je povinný ho vlastniť každý občan s trvalým pobytom na území Slovenskej republiky, ktorý dovŕšil vek pätnásť rokov.

V Slovenskej republike sú aktuálne platné tri typy občianskych preukazov vydaných po roku 2007. Prvý typ bol vydávaný v rokoch 2008-2013, druhý typ 2013-2015 a tretí od 2015 do dnešného dňa. Jednotlivé typy občianskych preukazov sa líšia v prevedení určitých ochranných prvkoch, v ich tvare, veľkosti alebo farbe.[31]

1.1 Pravosť občianskeho preukazu

Občiansky preukaz vydáva príslušný útvar Policajného zboru, obvykle s platnosťou na desať rokov. Ako je uvedené v §3 zákona č. 395/2019 Z. z. o občianskych preukazoch, občiansky preukaz obsahuje nasledujúce údaje o občanovi: meno a priezvisko, rodné priezvisko, deň, mesiac, rok a miesto narodenia, rodné číslo, pohlavie, štátne občianstvo, adresu trvalého pobytu na území Slovenskej republiky alebo miesto jeho pobytu v zahraničí, fotografiu tváre, podpis, číslo občianskeho preukazu, deň, mesiac, rok a miesto vydania občianskeho preukazu a deň, mesiac a rok uplynutia jeho platnosti.

Každý slovenský občiansky preukaz je verejná listina, ktorá je majetkom Slovenskej republiky. “Kto verejnú listinu, úradnú pečať, úradnú uzáveru, úradný znak, úradnú značku alebo ciachu falšuje, podstatne pozmení ich obsah v úmysle, aby sa použili ako pravé, alebo ich použije ako pravé, alebo si ich nechá vyhotoviť s úmyslom použiť ich ako pravé, dopustí sa podľa § 352 trestného zákona č. 300/2005 Z. z. v znení neskorších predpisov trestného činu

falšovania a pozmeňovania verejnej listiny, úradnej pečate, úradnej uzávery, úradného znaku a úradnej značky.”[44] Falšovaním občianskeho preukazu sa rozumie jeho úplné vyhotovenie skopírovaním textu a grafických prvkov tak, aby vyzeral ako vydaný príslušným orgánom.

Všetky materiály a technológie použité pri tvorbe občianskeho preukazu sú jedinečné. Každý typ tlače zanecháva špecifické stopy, ako je napríklad nedokonalosť tlače alebo špecifické opotrebenie tlačiarne. Na dokladoch sa môžu nachádzať aj menšie chyby v pravopise, ktoré sú identifikačným prvkom určitej série.[33]

Na overenie pravosti dokladu používajú experti makroskop. Overenie znamená kontrolu a porovnanie všetkých ochranných prvkov. Čím je doklad cennejší, tým má viac ochranných prvkov a vo viacerých vrstvách[33].

Verifikácia osoby je overenie, či osoba skutočne existuje. Elektronické overenie totožnosti z angl. electronic IDentity Verification (eIDV) najčastejšie pozostáva z elektronickej kontroly občianskeho preukazu prostredníctvom fotografie alebo videa. eIDV je nevyhnutnou súčasťou digitálneho onboarding, ktorý umožňuje klientovi inštitúcie, napríklad banky, využívať jej služby bez návštevy pobočky, iba pomocou mobilného telefónu alebo iného smart zariadenia.

Digitálne overenie totožnosti so sebou nesie mnohé bezpečnostné riziká, pretože časť procesu je v nekontrolovanom prostredí v rukách klienta. Systém musí vedieť odhaliť pokusy o falšovanie, ktoré by pri fyzickej kontrole dokladu boli zjavné, napríklad vytlačený občiansky preukaz, prelepená fotografia, snímka obrazovky namiesto skutočného občianskeho preukazu a pod. Ďalším krokom je kontrola ochranných prvkov občianskeho preukazu. Každý ochranný prvok je unikátny a má špecifické vlastnosti, a nie všetky sa dajú kontrolovať vizuálne. Preto problematika ochranných prvkov digitálneho overenia ešte nie je podrobne preskúmaná.

1.2 Ochranné prvky občianskeho preukazu

Ochranné prvky občianskeho preukazu slúžia na overenie jeho pravosti. Nachádzajú sa na prednej aj na zadnej strane. Sú navrhnuté tak, aby znemožnili kopírovanie alebo iné falšovanie občianskeho preukazu, a súčasne ich bolo možné jednoducho skontrolovať. Ochranné prvky sú detailne popísané v oficiálnych dokumentoch [46, 47, 45], ktoré sú vydané Ministerstvom vnútra SR.

Občiansky preukaz je vyrobený z viacvrstvého polykarbonátu. Veľkosť a tvar sú vo formáte ID-1 podľa normy ISO/IEC 7810. Osobné informácie o občanovi a jeho podoba sú na občiansky preukaz dorobené technológiou laserového gravírovania. Na zadnej strane preukazu sa nachádza strojovo čitateľná zóna z angl. Machine readable zone (MRZ). Obsahuje údaje o doklade a jeho držiteľovi vo forme opticky rozoznatelných znakov. Od roku 2013 je občiansky preukaz vydávaný s elektronickým kontaktným čipom, na ktorom sú uložené dáta o jeho držiteľovi.[45]

Z obidvoch strán občianskeho preukazu je farebné pozadie, ktoré je zložené z viacerých bezpečnostných prvkov. Farebné prechody v pozadí sú plynulé, čo je dosiahnuté pomocou irisovej (dúhovej) líniovej tlače.

Gilošovaná ochranná podtlač na pozadí občianskeho preukazu je jedným z hlavných prostriedkov ochrany proti kopírovaniu. Tvoria ju jemné čiary usporiadané do komplexných vzorov v kombinácii s päťcípimi hviezdami. V rokoch 2008-2015 bola podtlač zostavená z duplexových prvkov a 3D motívov lipového listu. Od roku 2015 ju tvoria pravidelné šesťuholníky.[46, 47, 45]

Mikrotext sú rozmerovo veľmi malé písmená, ktoré sú viditeľné len pri zväčšení, napr. lupou. Na občianskom preukaze je umiestnený pozitívny a negatívny mikrotext. Pozitívny mikrotext je vytlačený v pozitívnom obraze, čiže farebné písmo je umiestnené na bielom pozadí. Negatívny mikrotext v negatívnom obraze je zostavený opačne.[46, 47, 45]

UV grafika na občianskom preukaze je fluorescenčná potlač, ktorá vykresľuje symboly Slovenskej republiky viditeľné len v UV svetle. Pri bežnom svetle je bezfarebná. V rokoch 2008-2015 bola charakteristická viacerými motívmi s plynulým farebným prechodom medzi dvomi farbami, cez celú prednú a zadnú stranu občianskeho preukazu. Od roku 2015 sa na prednej strane zmenila na červený útvar zložený z päťcípich hviezd a nachádzajúci sa len

v strednej časti preukazu, a na zadnej strane je vykreslený štátny znak SR.[46, 47, 45]

Reliéfny prvok je razba na fólii vo forme obrazcov alebo textu razených pri vysokom tlaku[31]. Na občianskych preukazoch vydávaných v rokoch 2008-2015 je na zadnej strane a obsahuje text a obrys lipového listu. Od roku 2015 je umiestnený na prednej strane s textom “Slovenská republika” a skratkou “SVK”. [46, 47, 45]

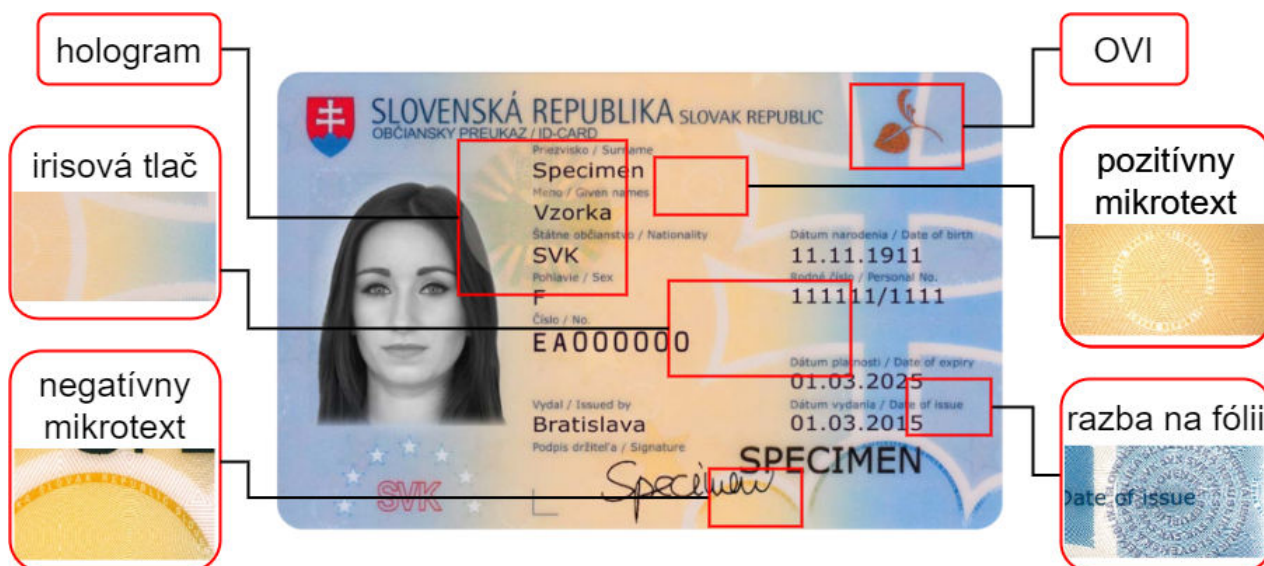
Opticky variabilný prvok z angl. Optically Variable Device (OVD) je ochranný prvok, ktorého podoba a informácie, ktoré poskytuje, sa menia v závislosti od aktuálnych pozorovacích a svetelných podmienok[31].

Na občianskych preukazoch z rokov 2008-2015 je umiestnený priehľadný Kinegram®, druh OVD. Kinegram® je počítačovo vytvorený hologram, ktorý vie zobrazit viacnásobné obrazy[31]. Na preukaze vytvára efekt pohybu a farebnej zmeny, a čiastočne prekrýva fotografiu držiteľa. Od roku 2015 je namiesto Kinegramu® použitá technológia Difrakčný identifikačný prvok z angl. Diffractive Identification Device (DID®) s podobnými vlastnosťami. Na občianskych preukazoch z rokov 2008-2013 je ešte navyše umiestnený holografický ochranný príložok. Tento vodorovný metalizovaný príložok obsahuje mikrotxt spolu s motívom lipového listu.[46, 47, 45] V holograme je uložené veľké množstvo informácií, niektoré viditeľné iba pri viacnásobnom zväčšení.

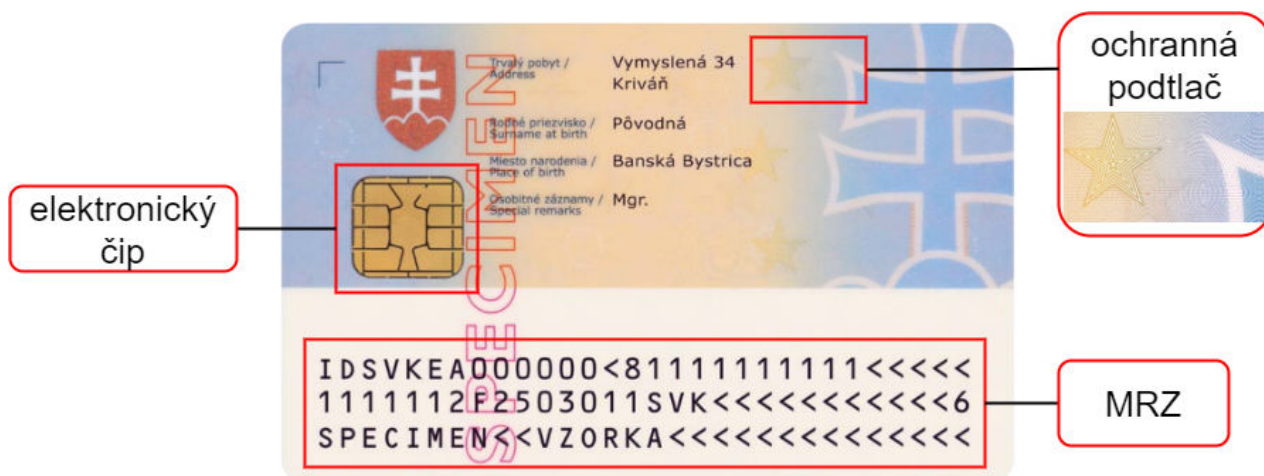
Ďalším druhom OVD je Opticky variabilná farba z angl. Optically Variable Ink (OVI). OVI je typ farby, ktorá mení svoj odtieň pri nakláňaní, zmene uhla pohľadu alebo osvetlenia, čím bráni jeho farebnému kopírovaniu. Na občianskom preukaze prechádza z purpurovej až do zelenej farby. Na prednej strane občianskych preukazov vydaných v rokoch 2008-2013 sú touto farbou vytlačené v pravom hornom rohu písmena SK. Od roku 2013 sa vymenili za obrázok lipového lístku a na zadnej strane v ľavej hornej časti pribudla OVI farbou tlačená mapa Slovenskej republiky. Mapa bola v roku 2015 zamenená za štátny znak SR.[46, 47, 45]

Farba OVI obsahuje mikroskopické pigmenty, ktoré pôsobia ako interferenčné filtre a spôsobujú farebné zmeny pri zmene uhla zdroja svetla alebo pozorovateľa. Pri falšovaní je možné zachytiť farbu platnú iba pre konkrétny uhol, ktorá po jeho zmene zostáva konštantná. OVI je na občiansky preukaz nanosená technikou sieťotlače. Farba je pomocou stierky pretláčaná cez priepustné miesta šablóny (sieťky) na občiansky preukaz, pričom vzniká hrubá a husto pokrytá vrstva farby.[31]

Rozdiely medzi ochrannými prvkami rôznych typov občianskych preukazov sú prehľadne porovnané v tabuľke 1.1. Na obrázkoch 1.1 a 1.2 sú vyznačené jednotlivé ochranné prvky. Občiansky preukaz na obrázkoch je tretieho typu z roku 2015 a je použitý zo zdroja[45].



Obr. 1.1: Ochranné prvky prednej strany občianskeho preukazu



Obr. 1.2: Ochranné prvky zadnej strany občianskeho preukazu

Tabuľka 1.1: Porovnanie ochranných prvkov rôznych typov občianskych preukazov

	typ 2008	typ 2013	typ 2015
OVI-predná strana	SK	lipový lístok typu 1	lipový lístok typu 2
OVI-zadná strana	-	mapa SR	štátny znak SR
pozitívny mikrotexť, negatívny mikrotexť, irisová tlač, MRZ	áno	áno	áno
ochranná podtlač	duplexové a 3D prvky	duplexové a 3D prvky	prevažne šesťuholníky
UV grafika	dvojfarebné motívy	dvojfarebné motívy	jednofarebný motív
hologram	Kinegram®	Kinegram®	DID®
elektronický čip	nie	áno	áno
reliéfny prvok	zadná strana	zadná strana	predná strana

1.2.1 Limitácie snímania ochranných prvkov

Pri vizuálnej detekcii je možné kontrolovať iba vizuálne vlastnosti ochranných prvkov. Ostatné vlastnosti, ako napríklad hmatové, sa len pomocou snímky overiť nedajú. Snímanie občianskeho preukazu so sebou prináša isté obmedzenia a limitácie, ktoré sťažujú alebo vôbec neumožňujú kontrolu niektorých ochranných prvkov.

Preskúvanie miniatúrnych ochranných prvkov vyžaduje kvalitnú fotografiu s vysokým rozlíšením, čo je v bežných podmienkach nerealizovateľné, za predpokladu, že systém budú používať bežný používatelia s rôznymi snímacími zariadeniami. To platí hlavne pre pozadie občianskeho preukazu, kde je potrebné kontrolovať plynulé farebné prechody, a pre jemnú gilošovanú ochrannú podtlač. Ďalším príliš detailným ochranným prvkom je mikrotexť. Aj vo fyzickej praxi vyžaduje kontrola spomenutých ochranných prvkov použitie vhodného zväčšovacieho nástroja.

Fluorescenčná potlač je pozorovateľná len pri UV svetle a pri bežnom osvetlení nie je viditeľná. Ochranné prvky s touto vlastnosťou je komplikované kontrolovať v bežných podmienkach, pretože to vyžaduje zdroj UV svetla.

Reliéfny prvok je bezfarebný, ale viditeľný pri bežnom osvetlení[31]. Keďže ho tvorí mikro-text, vizuálny spôsob kontroly vyžaduje kvalitnú fotografiu s vysokým rozlíšením. Prvok je tiež možné overiť hmatom, ale tento spôsob nespadá do vizuálneho skúmania ochranných prvkov.

Na občianskom preukaze sa nachádzajú citlivé osobné údaje, ktoré musia byť chránené. Niektoré ochranné prvky sú umiestnené v blízkosti osobných údajov, t. j. textu alebo fotografie, alebo sa s nimi prekrývajú. To komplikuje ich detekciu a overenie platnosti. Aj samotná príprava tréningových a testovacích dát je náročná, keďže je potrebné dodržiavať ochranu osobných údajov.

Ochranné prvky, ktoré nezasahujú do textovej časti s osobnými údajmi alebo do fotografie, umožňujú preskočiť riešenie ochrany osobných údajov, pretože na ich detekciu nie sú potrebné, a tak zachovávajú anonymitu občianskeho preukazu. Vďaka tomu pri príprave dát postačuje menší počet reálnych občianskych preukazov.

Práca sa zameriava na detekciu a overenie ochranného prvku s opticky variabilnou farbou OVI. Prvok sa nachádza v pravom hornom rohu občianskeho preukazu, pričom nekoliduje so žiadnymi osobnými údajmi. Je viditeľný pri ľubovoľných svetelných podmienkach, bez potreby zväčšovacieho nástroja. Jeho typickou vlastnosťou je zmena farby, ktorá je potenciálne využiteľná pri vizuálnej detekcii.

2 Vybrané metódy počítačového videnia

Počítačové videnie, angl. computer vision, je oblasť umelej inteligencie, kde počítače získavajú zmysluplné informácie z vizuálnych dát, napríklad digitálnych obrázkov alebo videí. Medzi úlohy, ktoré rieši počítačové videnie, patria napríklad rozpoznávanie objektov, vizuálna detekcia alebo sledovanie objektu, ktorý bol detekovaný.[13] V kapitole sú popísané základy farebného videnia a farebného počítačového videnia, a vybrané metódy digitálneho spracovania obrazu a strojového učenia.

2.1 Farebné počítačové videnie

Svetlo vyžarované svetelným zdrojom sa šíri prostredím. Po odraze od povrchu objektu je zachytené ľudským okom alebo snímačom. Vlastnosti zdroja svetla, prostredia, materiálu na povrchu objektu, scény, v ktorej sa objekt nachádza, a mnoho ďalších faktorov má vplyv na farby, ktoré vidíme. Ak je obraz zachytený snímačom, farba ďalej závisí od fyzických vlastností a nastavenia snímača, a jeho následného spracovania.

2.1.1 Vznik farebného obrazu

Proces vnímania farby sa skladá z troch častí: osvetlenie, odraz svetla od povrchu a jeho zachytenie. Výsledná pozorovaná farba je ovplyvnená všetkými tromi aspektami.[12] Ďalším pôsobiacim faktorom je prostredie, cez ktoré sa svetlo šíri, ale tomu sa kapitola podrobnejšie nevenuje.

Svetlo je elektromagnetické žiarenie, pozostávajúce z fotónov s určitou vlnovou dĺžkou. Svetlo, ktoré osvetľuje pozorovanú scénu, je vyžarované prirodzeným alebo umelým zdrojom svetla, respektíve ich kombináciou. Svetelné zdroje sú charakterizované emitovaným spektrom



Obr. 2.1: Rozdelenie zdrojov svetla

vlnových dĺžok a spôsobom smerovania fotónov. Spektrum je možné popísať pomocou teploty čierneho telesa, angl. black body radiator. Teplé farebné odtiene majú nižšiu teplotu ako studené odtiene. Bodový zdroj svetla vyžaruje lúč tvorený fotónmi pohybujúcimi sa rovnakým smerom. Ak sa fotóny pohybujú náhodnými smermi, svetlo je rozptýlené a svetelný zdroj sa nazýva plošný.[12] Jednotlivé typy zdrojov svetla sú znázornené na obrázku 2.1.

Pri odraze svetla interaguje materiál povrchu s dopadajúcim svetlom. V závislosti od materiálu, fotóny určitej vlnovej dĺžky sú absorbované a ostatné sú odrazené. Biele materiály väčšinu fotónov odrážajú a čierne naopak absorbujú.[12]

Odrazené svetlo je pozorované ľudským okom alebo zachytené obrazovým senzorom. Pri pozorovaní je energia fotónov zoskupená do určitých vlnových pásiem v určitom priestore za určitý časový interval. Na sietnici ľudského oka sa nachádzajú tri typy fotoreceptorov, pre krátke, stredne dlhé a dlhé vlnové dĺžky. Preto je naše farebné videnie trichromatické. Aby kamera imitovala ľudské oko, musí mať tri kanály s rôznou citlivosťou svetelného senzora.[12]

Farebná konštancia, angl. color constancy, je jav, pri ktorom je obraz explicitne upravený vzhľadom na farbu svetelného zdroja. Aj napriek tomu, že sa spektrum denného svetla mení počas dňa, človek vidí stále skoro rovnaké farby nezávisle od farby zdroja svetla. Ľudské oko dokáže tieto efekty prirodzene eliminovať a automaticky balansovať bielu farbu. Pri počítačovom spracovaní obrazu je potrebné v prvom kroku odhadnúť farebnosť zdroja svetla. Až druhým krokom je chromatická adaptácia, ktorá transformuje farby obrázka tak, aby vyzerali ako po osvetlení bielym zdrojom svetla. Chromatická adaptácia je významným aspektom vnímania farieb, aj keď nie je taká očividná, ako adaptácia na svetlo alebo tmu.[12]

Farba objektu je významne ovplyvnená okolitou scénou, čiže spektrálnym kontextom objektu. Tento jav sa nazýva farebný kontrast a jeho dôsledkom je, že vnímaná farba dvoch spektrálne identických objektov s rôznym farebným spektrom pozadia je rozdielna. Keď

je objekt umiestnený na takom pozadí, ktoré spôsobuje jeho skreslené vnímanie odtieňa farby, tak vnímaná farba objektu je posunutá smerom ku farbe ležiacej oproti farbe pozadia na Newtonovom farebnom kruhu.[16] Tento jav je znázornený na obrázku 2.2.



Obr. 2.2: Vplyv pozadia na vnímanie farby[12]

2.1.2 Vplyv snímania na vizuálne vlastnosti objektu

Vizuálne vlastnosti objektu na fotografii, hlavne jeho farba a tvar, sú ovplyvnené vlastnosťami a nastavením kamery. Pri vzniku snímky sa na určitý čas otvorí uzávierka, čím vystaví obrazový senzor svetlu. Senzor zaznamenáva množstvo dopadnutého svetla, ktoré je po uzavretí uzávierky zmerané a uložené do pamäte.[49]

Obrazový senzor (snímač obrazu) je elektronický čip pokrytý veľkým množstvom obrazových bodov (fotodetektorov), ktorých počet hovorí o jeho rozlíšení. Fotodetektory vedia zachytiť len úroveň intenzity svetla. Pre vznik farebnej snímky sa používajú farebné filtre, červený, zelený a modrý, ktoré filtrujú svetlo pred dopadom na fotodetektor. Na základe princípu, akým senzor separuje jednotlivé farby, sa rozlišujú rôzne typy farebných obrazových senzorov. V súčasnosti najpoužívanejší sa nazýva Bayerov filter. Ďalším faktorom, ktorý má vplyv na kvalitu snímky, je veľkosť senzora. Malé senzory s vysokým rozlíšením musia mať menšie fotodetektory a sú preto zrnitejšie ako väčšie senzory s rovnakým rozlíšením.[49]

Dynamický rozsah senzora je pomer medzi minimálnym požadovaným množstvom svetla a maximálnym množstvom svetla bez straty detailov, a tiež pomer medzi najtmavším a najsvetlejším pixelom fotografie. Farby scény musia byť vnútri dynamického rozsahu. To znamená, že čím vyšší je dynamický rozsah scény, k tým väčšiemu skresleniu dochádza. Vďaka

väčšiemu dynamickému rozsahu senzora majú snímky menší šum a sú detailnejšie v tieni alebo svetlých častiach. Pre väčšinu senzorov platí, že čím väčšie sú fotodetektory, tým väčší je aj ich dynamický rozsah.[49]

Ak na senzor dopadá príliš málo svetla, tak je fotografia podexponovaná a obsahuje veľa tmavých tieňov. Preexponovaná fotografia má naopak tzv. "prepálené" čisto biele oblasti. Množstvo svetla pôsobiaceho na snímací senzor je možné regulovať pomocou troch parametrov expozície: rýchlosť uzávierky, clona a ISO, ktoré majú veľký vplyv na farby fotografie. Rýchlosť uzávierky je dĺžka otvorenia uzávierky, tiež nazývaná expozičný čas. Kontroluje, ako dlho je senzor vystavený prichádzajúcemu svetlu. ISO vyjadruje citlivosť na svetlo. Určuje, ako veľmi bude svetelný signál zo senzora zosilnený. Čím viac je signál zosilnený, tým má snímka viac šumu. Clona je variabilný otvor v objektíve, ktorý reguluje, koľko svetla cezeň prechádza. Cez väčšiu clonu prenikne menej svetla a fotografia má vyššiu hĺbku ostrosti.[49]

Kamera premieta skutočný 3-rozmerný svet do 2-rozmernej roviny fotografie, čo môže spôsobiť skreslenie tvaru objektov na snímke. Existujú dva typy skreslenia: optické a perspektívne. Skoro všetky šošovky trpia optickým skreslením, ktoré spôsobuje zakrivenie rovných čiar fotografie. Závisí od viacerých faktorov, ako napríklad od dĺžky šošovky alebo ohniskovej vzdialenosti. Perspektívne skreslenie vôbec nesúvisí so šošovkou, ale s umiestnením objektu voči kamere. Jeho dôsledkom je, že objekt sa môže na fotografii javiť väčší, ako v skutočnosti je.[7]

2.1.3 Farebné modely

Svetlo, ktoré je zachytené senzorom, je výsledkom interakcie spektra svetelného zdroja a odrazového spektra povrchu videného objektu. To, ako senzor zachytí svetlo, závisí od jeho citlivosti (senzitivity). Ľudské videnie je trichromatické, preto sú potrebné tri kanály na zachytenie všetkých človekom viditeľných farieb. To znamená, že musí byť definovaná trojrozmerná reprezentácia farby a tri úrovne citlivosti senzora, ktoré ju zachytia. Nastavenie citlivosti sa medzi kamerami líši a má vplyv na farby fotografie.[12]

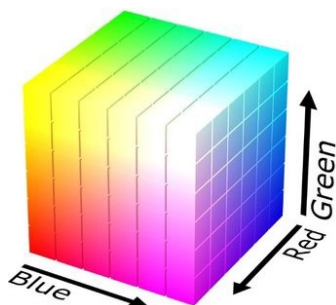
Farebný model je matematická reprezentácia farieb. Farba uložená v počítači musí byť kvantizovaná. To znamená, že spektrálna informácia pixela je zhustená do diskretných čísiel

z konečného rozsahu hodnôt, a tým sa redukuje počet možných farieb obrázka. Existujú rôzne farebné modely, ktoré kódujú rovnakú farbu na základe rôznych princípov, pričom zdôrazňujú jej určité vlastnosti.

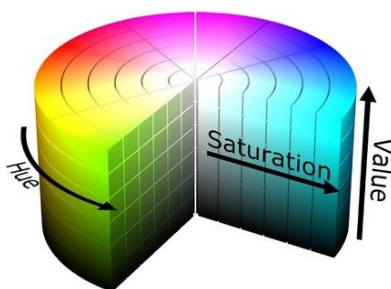
RGB z angl. Red, Green, Blue (Červená, zelená a modrá zložka) je farebný model založený na podobnom princípe, akým farbu vníma ľudské oko. Geometricky sa znázorňuje v tvare kocky, ako je ukázané na obrázku 2.3. RGB model je primárne používaný pre kamery a displeje. Vzhľadom na rôznorodosť senzorov sa rovnaké RGB farby medzi zariadeniami líšia. Obrázok vyzerá odlišne na rôznych displejoch alebo na vytlačenej fotografii. Hodnoty RGB kanálov sú vysoko korelované. Ich dekorelovaním vznikajú tzv. oponentské farebné modely, kde sú definované tri páry protihľých farieb: červená-zelená, žltá-modrá a biela-čierna.[12]

Ďalším typom sú intuitívne farebné modely, ktoré vyjadrujú farbu pomocou odtieňa, sýtosti a intenzity. Tieto pojmy ale nie sú presne definované, a preto existuje pre každú definíciu samostatný farebný model. Farebný odtieň, angl. hue, popisuje dominantnú vlnovú dĺžku vo farebnom spektre. Sýtosť (saturácia) vyjadruje čistotu farby. Poslednou zložkou je intenzita, definovaná ako jas alebo svetlosť. Informácia o intenzite je achromatická, čiže nezávislá od chromatickej informácie. Takto definované farebné modely sú HSL (angl. Hue, Saturation, Lightness) definujúci intenzitu ako svetlosť a HSV (angl. Hue, Saturation, Value), ktorý je tiež nazývaný HSB (angl. Hue, Saturation, Brightness), pracujúci s jasom.[12]

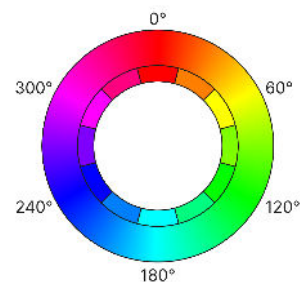
HSV farebný model je často zobrazovaný ako kužeľ alebo valec, ktorý je ilustrovaný na obrázku 2.4. Farebný odtieň H je určený hodnotou uhla (0° , 360°) HSV farebného kruhu, na obrázku 2.5. Kruh tvoria tri primárne farby, červená, zelená a modrá. Ostatné farby sú kombináciou dvoch primárnych farieb. Komponent H je cyklický, čiže červená farba má hodnoty



Obr. 2.3: RGB model[1]



Obr. 2.4: HSV model[1]



Obr. 2.5: HSV farebný kruh[32]

blízke 0° a súčasne 360° . Saturácia S znamená podiel chromatickej a achromatickej (sivej) zložky vo farbe, od úplne sivej 0% po jasnú sýtu farbu 100%. Hodnota jas V vyjadruje množstvo svetla dopadajúceho na objekt, od úplne čiernej 0% po najjasnejšiu farbu 100%.

Existuje veľa ďalších farebných modelov, napríklad CMYK (angl. Cyan, Magenta, Yellow, Key Black) používaný pri farebnej tlači. XYZ je jedným z najstarších modelov, ktorý vytvorila Medzinárodná komisia pre osvetľovanie CIE (francúzsky Commission Internationale de l'Eclairage). Pre väčšinu ostatných farebných modelov je referenčnou bázou, na základe ktorej sú odvodené, napríklad CIE $L^*u^*v^*$ alebo CIE $L^*a^*b^*$.

2.2 Metódy digitálneho spracovania obrazu

Digitálne spracovanie obrazu, angl. digital image processing, je algoritmické spracovanie digitálnych obrázkov v počítači. Vstupom do metód je digitálny obrázok a výstupom je modifikovaný vstupný obrázok alebo jeho extrahované príznaky. Čiernobiely obrázok je v počítači reprezentovaný maticou typu $M \times N$ a farebný maticou typu $M \times N \times 3$, s tromi farebnými kanálmi.

2.2.1 Histogram

Histogram obrázka je grafickou reprezentáciou rozdelenia intenzít jeho pixelov. Udáva relatívnu početnosť všetkých možných hodnôt intenzít daného obrazu[43], resp. relatívny počet pixelov v intervale intenzít, angl. bin. Počet histogramov opisujúcich jeden obrázok závisí od počtu jeho farebných kanálov. Čiernobiely obrázok charakterizuje jeden histogram, ale farebný RGB obrázok až tri, jeden histogram pre každú farebnú zložku.

Z tvaru histogramu je možné určiť niektoré vlastnosti obrazu, napr. kontrast alebo jas, ale bez zachytenia priestorovej informácie[43]. Pomocou metódy ekvalizácie (vyrovnania angl. equalization) histogramu je možné zosilniť kontrast obrázka. Metóda adaptívnej ekvalizácie histogramu, angl. adaptive histogram equalization, zachováva lokálne vlastnosti obrázka vďaka tomu, že pracuje s viacerými histogramami z rôznych jeho častí [28].

2.2.2 Prahovanie

Prahovanie, angl. thresholding, je jednoduchá metóda segmentácie obrazu. Segmentácia rozdeľuje obrázok na viacero segmentov, tiež nazývaných oblasti alebo objekty obrazu. Cieľom je zjednodušenie obrázka, aby sa dal ľahšie analyzovať.

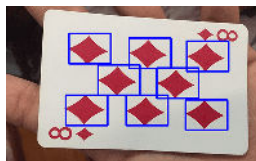
Vstupom do metódy je čiernobiely alebo farebný obrázok. Výstupom prahovania je binárny obrázok, ktorý oddeľuje objekty od pozadia. Globálne prahovanie používa len jednu prahovú hodnotu pre celý obrázok, resp. jednu pre každý farebný kanál. Sofistikovanejšie pracuje lokálne (adaptívne) prahovanie, kde sa prah mení na základe lokálnych charakteristík okolia bodu. Je mnoho postupov na určenie prahovej hodnoty, napríklad metódy pracujúce so štatistickými vlastnosťami obrázka, histogramom alebo Otsu binarizácia.[48]

2.2.3 Template Matching

Template Matching je technika, ktorá hľadá také oblasti obrázka, ktoré vyhovujú šablóne, angl. template. Cieľom je šablónu na obrázku nájsť. Šablóna je malý obrázok, postupne sa posúva po väčšom obrázku a na každej pozícii je vypočítané skóre. Skóre vyjadruje, na koľko daná oblasť zodpovedá šablóne.[27]

Metriky na výpočet skóre môžu byť rôzne, založené napríklad na vzájomnej korelácii alebo štvorcovej chybe. V závislosti od metriky sa hľadá minimálne alebo maximálne skóre. Ak sa na obrázku očakáva iba jeden výskyt šablóny, vyberie sa pozícia s najlepším skóre. V druhom prípade, sa vyberú všetky pozície, ktorých skóre je nad alebo pod definovanou hraničnou hodnotou, ako je ilustrované na obrázku 2.6.

Metóda sa zameriava na intenzitu alebo farbu oblasti. Nevýhodou je, že nie je invariantná voči rotácii ani škálovaniu. Aby bolo možné na obrázku oblasť so šablónou nájsť, musí mať rovnaké natočenie aj rozlíšenie ako šablóna.



Obr. 2.6: Template Matching[34]

2.2.4 Detekcia hrán

Operácia konvolúcie je základným nástrojom filtrácie. Hornopriepustný, angl. high-pass, filter prepúšťa iba vysokofrekvenčné zložky obrazu a jeho výstupom je hranový obraz. Opakom je dolnopriepustný, angl. low-pass, filter, tiež nazývaný vyhladzovací, ktorý obraz rozmazáva.[43]

Na detekciu hrán sa používajú hranové filtre, ktoré sú hornopriepustné. Výsledkom je aproximácia gradientu, ktorý popisuje orientovanú zmenu intenzity obrázka. Jedným z najpopulárnejších hranových filtrov je Sobelov filter. Vertikálny filter je definovaný v tvare 2.1 a horizontálny v tvare 2.2.

$$\begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \quad (2.1)$$

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & -1 \end{bmatrix} \quad (2.2)$$

Laplaceov filter je hranový filter, ktorý pracuje s druhou diferenciou. Zvyčajne je definovaný v nasledujúcom v tvare:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad (2.3)$$

Canny detektor hrán

Canny detektor hrán je populárny algoritmus detekcie hrán, ktorý navrhol John F. Canny[5]. Algoritmus sa skladá z viacerých krokov. Z dôvodu, že detekcia hrán je citlivá na šum, sa na začiatku obrázkov vyhladí aplikovaním Gaussovho filtra. Gaussov filter je dolnopriepustný, rozmazáva obraz a redukuje šum. Na výpočet používa dvojrozmernú Gaussovú funkciu.

V druhom kroku kroku sa použije Sobelov filter, ktorého výstupom sú derivácie 1. rádu v horizontálnom G_x a vertikálnom smere G_y . Z nich sa ďalej vypočíta veľkosť a smer gradientu nasledovne:

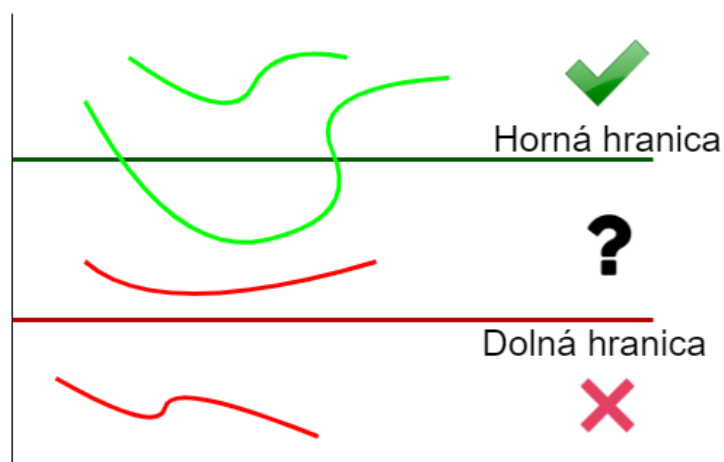
$$gradient(G) = \sqrt{G_x^2 + G_y^2} \quad (2.4)$$

$$\theta = \tan^{-1}\left(\frac{G_y}{G_x}\right) \quad (2.5)$$

Smer hrany je zaokrúhlený na uhol, ktorý reprezentuje jeden zo štyroch smerov: horizontálny, vertikálny a dva diagonálne.[19]

V ďalšom kroku sa robí stenčovanie hrán, angl. edge thinning, ktoré je založené na fakte, že gradient je kolmý na hranu. Pre každý pixel sa overí, či je lokálnym maximom z jeho okolia v smere a proti smeru gradientu. Touto operáciou sa ponechajú iba pixely s najprudšou zmenou intenzity, čiže tenké hrany, a ostatné sú potlačené.[19]

V poslednom kroku sa overuje, či sú vybrané pixely skutočne hranami alebo len šumom. K tomu sú použité dve prahové hodnoty: horná a dolná hranica. Všetky hrany s gradientom vyšším ako horná hranica sú považované za isté hrany. Naopak všetky hrany s nižšou hodnotou gradientu sú vylúčené. Hrany s gradientom medzi dolnou a hornou hranicou nie sú vyradené iba v tom prípade, ak sú spojené s niektorou zaručenou hranou. Výber hrán je znázornený na obrázku 2.7. Výstupom algoritmu je binárny obrázok s detekovanými hranami.[19]



Obr. 2.7: Výber hrán Canny detektorom

Houghova transformácia

Houghova transformácia je metóda, ktorá hľadá geometrické útvary na obrázku. Pôvodne bola navrhnutá pre priamky, ale dá sa zovšeobecniť pre ľubovoľný útvar, ktorý je popísateľný matematickou rovnicou.[27]

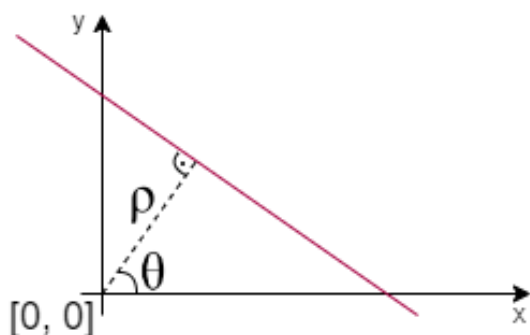
Priamku je možné popísať smernicovou rovnicou $y = ax + b$, kedy je priamka reprezentovaná bodom (a, b) . Nedostatkem tejto reprezentácie sú vertikálne hrany, pre ktoré je parameter a neohraničený. Preto sa používa nasledujúca rovnica priamky:

$$\rho = x \cos \theta + y \sin \theta \quad (2.6)$$

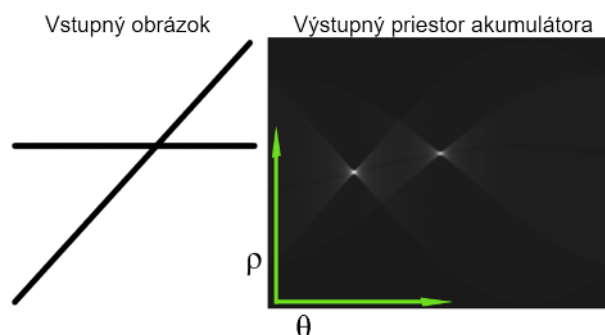
kde ρ je kolmá vzdialenosť priamky od začiatku súradnicovej sústavy a θ je uhol medzi súradnicovou osou x a touto kolmicou, ako je znázornené na obrázku 2.8. Každá priamka je potom reprezentovaná bodom v polárnych súradniciach (ρ, θ) v parametrickom Houghovom priestore.[22]

Vstupom do metódy je binárny napr. hranový obrázok. Na začiatku sa inicializuje 2D pole, nazývané akumulátor, kde je každý rozmer reprezentovaný jedným z parametrov priamky ρ a θ . Veľkosť poľa závisí od požadovanej presnosti. Posudzuje sa každý bod (x, y) vstupného obrázka, cez ktorý prechádza hrana. Pre jeden bod sa do rovnice 2.6 postupne dosadia všetky uvažované hodnoty uhla θ , napríklad $\theta = 0, 1, \dots, 180$. Na základe vypočítaných dvojíc (ρ, θ) , sa v akumulátore na ich pozíciách zvýši hodnota o 1. Číže body hlasujú za priamky, ktoré nimi prechádzajú. Čím viac hlasov priamka má, tým viac bodmi prechádza.[22]

Výstupom je akumulátor, kde súradnice každého bodu reprezentujú jednu priamku a hodnota vyjadruje počet bodov vstupného obrázka, ktorými priamka prechádza. Definovaním minimálnej hodnoty sa z akumulátora vyselektujú tie dvojice parametrov (ρ, θ) , ktoré sú považované za priamky. Ostatné sa pokladajú za šum.[22] Príklad výstupného priestoru akumulátora je na obrázku 2.9.



Obr. 2.8: Reprezentácia priamky používaná v Houghovej transformácii



Obr. 2.9: Výstup Houghovej transformácie[22]

2.2.5 Detekcia keypointov

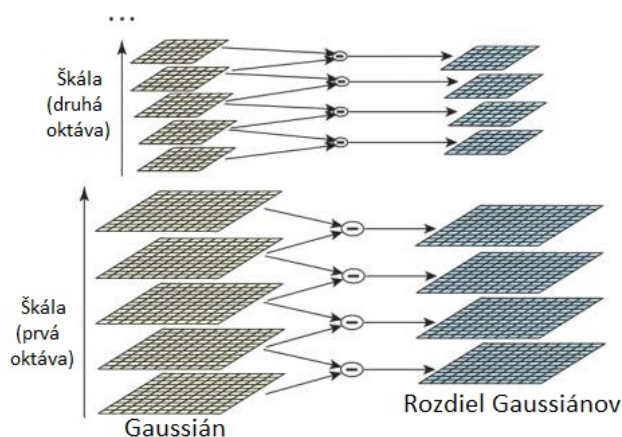
Keypointy sú zaujímavé body obrázka, z ktorých okolia sa extrahujú deskriptory (lokálne príznaky). Existujú viaceré algoritmy na detekciu a deskripciu keypointov, a jedným z prvých je algoritmus SIFT.[43]

Algoritmus SIFT

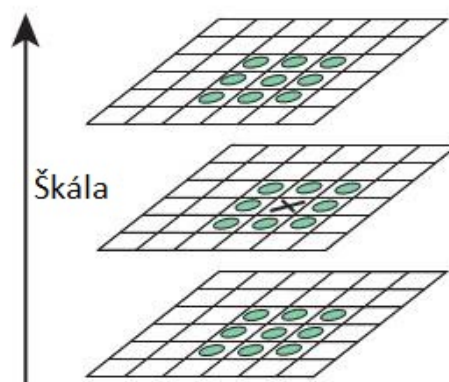
SIFT, z angl. Scale-invariant feature transform, je algoritmus detekcie a deskripcie keypointov, ktorý navrhol D. Lowe[17]. Je invariantný voči rotácii, posunu, škálovaniu, zmene osvetlenia a čiastočnému skresleniu objektu.

V prvom kroku je originálny obrázok zmenšený do k rôznych veľkostí, ktoré sa nazývajú oktávy. Pre každú oktávu je vytvorených n obrázkov rôznej úrovne rozmazania pomocou Gaussovho filtra. Na nerozmazaný obrázok sa aplikuje filter, následne sa na výsledok opäť aplikuje filter, a naň opäť atď, až vznikne n rôzne rozmazaných obrázkov. Úrovně rozmazania predstavujú rôzne úrovne škálovania obrázka. Týmto spôsobom sa vytvorí škálová pyramída s k oktávami a n obrazmi. Následne sa vypočíta rozdiel Gaussiánov tak, že sa odčítajú susedné obrázky v rámci jednej oktávy. V oktáve bude na konci už len $n - 1$ obrázkov.[43, 24] Vznik škálového priestoru je znázornený na obrázku 2.10.

Vo vzniknutom škálovom priestore sa hľadajú lokálne extrémny. Skúma sa okolie bodu na danom obraze a okolie toho istého bodu v dvoch susedných obrazoch rôznej škály, ako je



Obr. 2.10: SIFT škálový priestor[17]

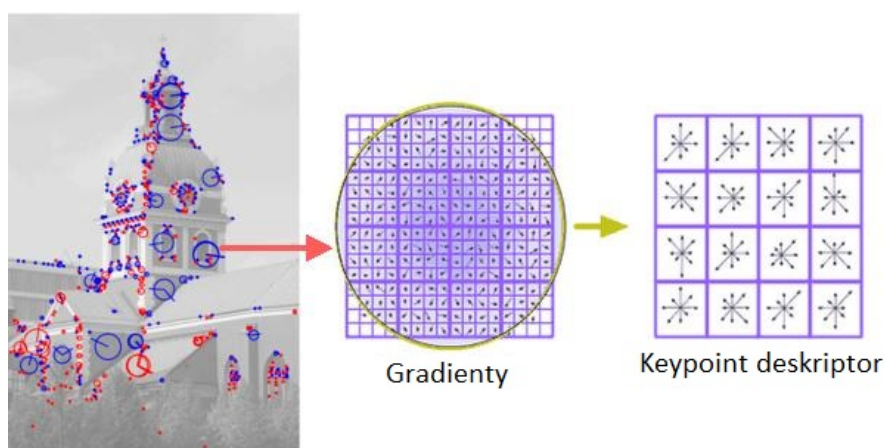


Obr. 2.11: SIFT lokálny extrém[17]

znázornené na obrázku 2.11. Bod je vybraný ako lokálny extrém vtedy, ak je väčší alebo menší ako všetky susedné body. Nájdené lokálne extrémny sú považované za potenciálne keypointy, ktoré sú najlepšie reprezentované v tej škále, v ktorej boli lokálnym extrémom. Následne sú odstránené tie keypointy, ktoré majú nízky kontrast alebo ležia na hrane. Ostatné sú považované za silné keypointy a ponechané pre výpočet deskriptorov.[17]

Aby boli keypointy invariantné voči rotácii, orientácia keypointu je vypočítaná na základe jeho lokálnych vlastností. Zoberie sa okolie keypointu, pričom veľkosť okolia závisí od jeho škály. Pre danú oblasť sa vypočíta veľkosť a smer gradientu. Následne sa vytvorí histogram smerov s 36 intervalmi, angl. bin, ktorý pokrýva všetky smery od 0° do 360° . Hodnoty histogramu pre jednotlivé smery sú vypočítané na základe veľkosti gradientu okolia. Vrcholy histogramu sa zhodujú dominantnými smermi lokálneho gradientu a najvyššie sú použité ako orientácie keypointov. Tým môžu vzniknúť viaceré keypointy, ktoré sú na rovnakej pozícii, s rovnakou škálou, ale odlišnou orientáciou.[17, 24]

Keypointy sú doteraz opísané pozíciou, škálou a orientáciou. Ďalší krok vytvorí deskriptory a zabezpečí ich invariantnosť voči 3D rotácii a zmene osvetlenia. Zoberie sa 16×16 okolie keypointu, ktoré sa rozdelí do 16 blokov o veľkosti 4×4 , čiže 16 štvorcových oblastí, ako je znázornené na strednej časti obrázka 2.12. Pre každý blok je vytvorený histogram smerov s 8 hodnotami, ktoré reprezentujú 8 rôznych orientácií. Smerové histogramy jednotlivých blokov sú znázornené na pravej časti obrázka 2.12. Dokopy majú všetky histogramy 128 hodnôt a sú uložené ako vektor, ktorý tvorí deskriptor keypointu. Invariancia rotácie je dosiahnutá



Obr. 2.12: SIFT deskriptor[3]

tým, že súradnice deskriptora a smerov gradientu sú otočené smerom ku orientácii keypointu. Na redukovanie vplyvu osvetlenia je vektor deskriptora normalizovaný na jednotkový vektor.[17]

Keypointy sa párujú s keypointami iného obrázka identifikovaním najbližších susedov. Najbližší sused je keypoint, ktorý má najkratšiu vzdialenosť deskriptora. Na eliminovanie falošných párov keypointov sa porovnávajú prvý a druhý najbližší sused. Ak je pomer vzdialenosti od najbližšieho a druhého najbližšieho keypointu väčší ako 0.8, potom je pár keypointov zahodený.[17, 24]

Homografia je transformácia medzi dvomi rovinami, ktorá je reprezentovaná maticou typu 3×3 . Zo spárovaných keypointov je možné extrahovať ich polohu, čím vzniknú dvojice súradníc bodov v jednej a druhej rovine. Ak existujú minimálne štyri spárované body, vypočíta sa z nich perspektívna transformácia medzi rovinami objektu na vzorovej a analyzovanej snímke. A tým sa na obrázku identifikoval hľadaný objekt. Vzhľadom na to, že nie všetky keypointy musia byť spárované správne, pri výpočte homografie sa používa metóda RANSAC[11], ktorá hľadá takú podmnožinu bodov, ktorá má čo najnižšiu chybu transformácie.

2.3 Metódy strojového učenie

Algoritmy strojového učenia automaticky vytvárajú modely na základe tréningových dát. Modely robia predikcie alebo rozhodnutia bez toho, aby na to boli explicitne naprogramované. Okrem tréningového datasetu používajú validačný dataset na hyperparametrizáciu modelu a testovacie dáta na jeho finálne overenie.

2.3.1 Regresia a klasifikácia

Regresná analýza je štatistická technika, ktorá skúma a modeluje vzťahy medzi premennými[18]. Cieľom je vytvoriť taký model, ktorý na základe vstupných príznakov objektu x_j dokáže odhadnúť výstup y . Výstup sa tiež nazýva závislá premenná a vstupy sú nezávislé premenné. Regresné modely predikujú spojité výstupy. Klasifikácia je iný typ úlohy, ktorý predikuje kategóriu vstupného objektu. Obidva typy modelov patria medzi metódy učenia učiteľom, čiže všetky vstupné objekty majú priradené očakávané výstupy.

Lineárna regresia

Lineárna regresia je lineárny model, ktorý hľadá nadrovinu reprezentujúcu trénovacie dáta. V dvojrozmernom modeli je to priamka, ako je znázornené na obrázku 2.13. Výstupom modelu je hodnota lineárnej kombinácie vstupných príznakov. Matematický zápis vyzerá nasledovne:

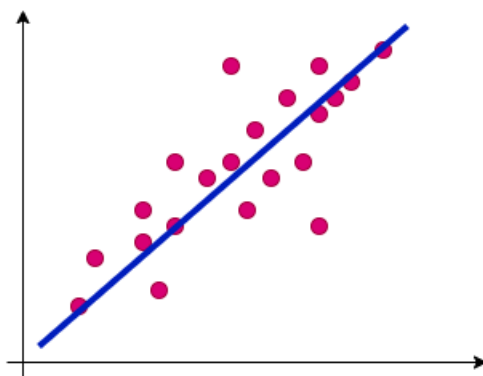
$$y(\vec{w}, \vec{x}) = w_0 + w_1x_1 + \dots + w_nx_n \quad (2.7)$$

kde vektor $\vec{w} = (w_0, \dots, w_n)$ sú koeficienty lineárnej kombinácie, $\vec{x} = (x_1, \dots, x_n)$ sú vstupné príznaky a y je výstupná predpovedaná hodnota.[39]

Koeficienty $\vec{w} = (w_0, \dots, w_n)$ sú parametre modelu lineárnej regresie, ktoré sa počas tréningu upravujú. Cieľom je nájsť také hodnoty parametrov, pre ktoré je rozdiel skutočnej a predpovedanej hodnoty minimálny. Existujú rôzne techniky odhadu parametrov modelu. V klasickej lineárnej regresii sa používa metóda najmenších štvorcov, kde sa minimalizuje suma štvorcových chýb, ktorá je matematicky zapísaná nasledovne:

$$\arg \min_{\vec{w}} \sum_{i=1}^k \left(\vec{w}^T \cdot \vec{x}_i - y_i \right)^2 \quad (2.8)$$

kde $\vec{w}$ sú hľadané parametre modelu, x_i je i -ty vstupný objekt s očakávaným výstupom y_i a k je počet objektov trénovacieho datasetu. Metóda najmenších štvorcov predpokladá, že všetky vstupné príznaky sú lineárne nezávislé.[18, 39]



Obr. 2.13: Lineárna regresia

SVM

SVM, angl. Support Vector Machine, je metóda, ktorá sa používa na klasifikáciu, regresiu alebo Outlier detekciu. Klasická verzia algoritmu SVM rieši klasifikačný problém. Cieľom pri klasifikácii je nájsť nadrovinu, ktorá je čo najviac vzdialená od trénovacích dát, a súčasne ich separuje do daných tried. Objekty, ktoré sú najbližšie k tejto nadrovine, sa nazývajú podporné vektory, angl. support vectors.[41, 43]

Rozšírenie pre regresiu má názov angl. Support Vector Regression a navrhli ho Drucker et al.[9] Podobne ako pri lineárnej regresii, je cieľom nájsť nadrovinu, ktorá reprezentuje dáta. V SVM sa neminimalizuje štvorcová chyba ako pri lineárnej regresii, ale koeficienty. Pôvodná chyba je presunutá do obmedzujúcich podmienok. Model vyzerá nasledovne:

$$\min_{\vec{w}} \frac{1}{2} \|\vec{w}\|^2 \quad (2.9)$$

za podmienky:

$$\forall i = 1, \dots, k: \quad |\vec{w}^T x_i - y_i| \leq \epsilon \quad (2.10)$$

kde $\vec{w}$ sú hľadané parametre modelu, x_i je i -ty vstupný objekt s očakávaným výstupom y_i a k je počet objektov trénovacieho datasetu. Metóda umožňuje definovať maximálnu akceptovateľnú chybu ϵ . Z podmienky modelu vyplýva, že absolútna chyba musí byť menšia ako špecifikovaná hraničná hodnota ϵ . [42]

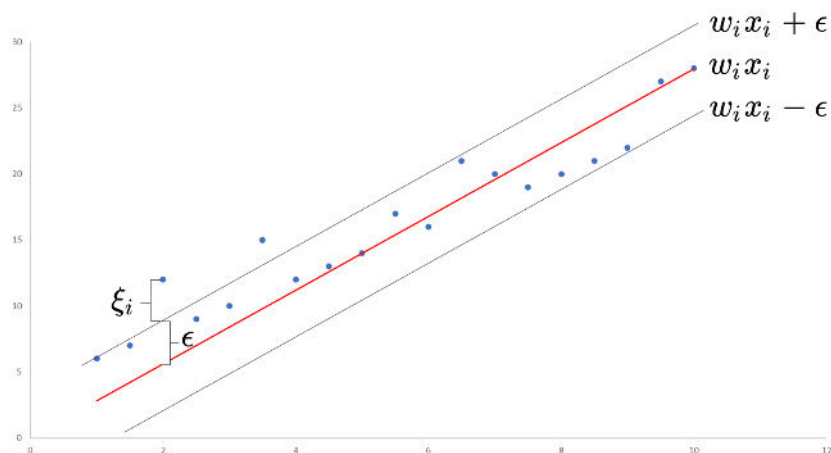
Keďže skoro v každom datasete existujú objekty, pre ktoré podmienka 2.10 nikdy nie je splnená, riešením sú doplnkové premenné. Doplnková premenná ξ vyjadruje, ako sa chyba líši od hranice ϵ . Doplnený model vyzerá nasledovne:

$$\min_{\vec{w}} \frac{1}{2} \|\vec{w}\|^2 + C \sum_{i=1}^k |\xi_i| \quad (2.11)$$

za podmienky:

$$\forall i = 1, \dots, k: \quad |\vec{w}^T x_i - y_i| \leq \epsilon + |\xi_i| \quad (2.12)$$

kde parameter C vyjadruje, ako je model tolerantný voči dátam mimo hranice ϵ . [42] Príklad nájdenej nadroviny a hranice je ilustrovaný na obrázku 2.14.



Obr. 2.14: Support Vector Regression[42]

Algoritmus CatBoost

CatBoost, z angl. categorical boosting, je relatívne nový algoritmus, ktorý efektívne spracúva kategorické vstupné dáta. Algoritmus je založený na gradientom posilnených rozhodovacích stromoch. Posilnenie, angl. boosting, kombinuje väčší počet slabých modelov, čím vznikne jeden oveľa silnejší model. CatBoost v rámci tréningu postupne vytvára rozhodovacie stromy, pričom každý ďalší strom má vďaka výpočtu gradientu menšiu chybu ako predchádzajúce stromy.[8, 30]

Posilňovacie algoritmy majú často problém s pretrénovaním, angl. overfitting, pretože sú postavené na rozhodovacích stromoch. Ďalším problémom je, že tréningový proces je ťažké paralelizovať, pretože stromy sa vytvárajú sekvenčne. CatBoost má implementované funkcie, ktoré pretrénovanie minimalizujú a ďalšie funkcie, ktoré zvyšujú rýchlosť učenia aj pre datasety s miliónmi dátových objektov.[29] Využíva tzv. zabúdacie, angl. oblivious, stromy. To znamená, že všetky vrcholy v rovnakej hĺbke stromu majú rovnaké rozdeľovacie kritérium. Vďaka tomu sú stromy vyvážené, menej náchylné na pretrénovanie a urýchľujú výpočet.[8, 30]

CatBoost dokáže riešiť regresiu, klasifikáciu a viacriednu klasifikáciu. Podľa článku [8] prekonáva najmodernejšie implementácie gradientom posilnených rozhodovacích stromov.

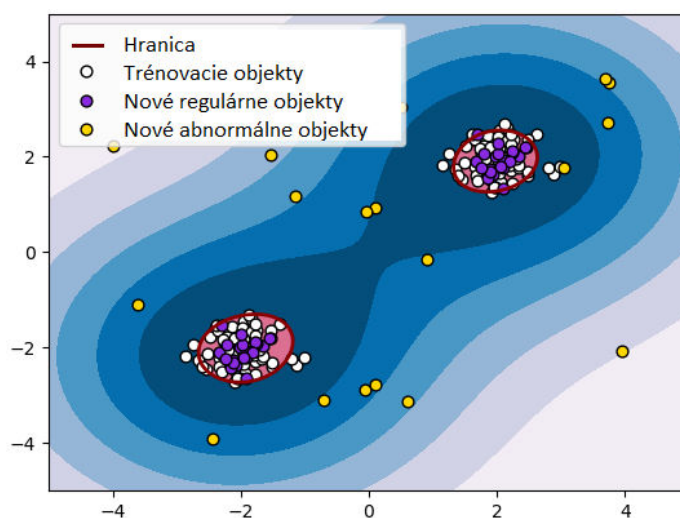
2.3.2 Detekcia anomálií

Detekcia anomálií je klasifikátor, ktorý sa snaží určiť, či objekt patrí do rovnakého rozdelenia ako ostatné objekty alebo je považovaný za príliš odlišný. Odlišný objekt sa nazýva outlier alebo anomália.[40]

Existujú dva typy detekcie anomálií, a to Outlier detekcia a Novelty detekcia. Pri Outlier detekcii trénovacie dáta obsahujú outliery, ktoré sú veľmi odlišné od ostatných objektov. Outlier detektor sa snaží odhadnúť oblasti, kde sú dáta najviac koncentrované, a odlíšiť vyčnievajúce objekty. Novelty detekcia v tréningu neočakáva outliery. Až následne sa snaží odhadnúť, či je novoprichádzajúci objekt regulárny alebo outlier.[40]

One Class SVM

One Class SVM je algoritmus Novelty detekcie. Algoritmus je modifikovaná verzia metódy SVM pre jednu triedu, angl. one class, ktorú navrhol Schölkopf et al.[35] Cieľom je nájsť čo najtesnejšiu hranicu, ktorá vymedzuje oblasť rozdelenia trénovacích dát vo viacrozmernom priestore, ako je znázornené na obrázku 2.15. Odhadne sa funkcia f , ktorá má kladné hodnoty pre regulárne objekty z rozdelenia a negatívne hodnoty pre ostatné objekty. Ak nový objekt leží mimo ohraničeného priestoru, považuje sa za abnormálny, funkcia f ho ohodnotí negatívnou hodnotou a je označený ako outlier.[40]

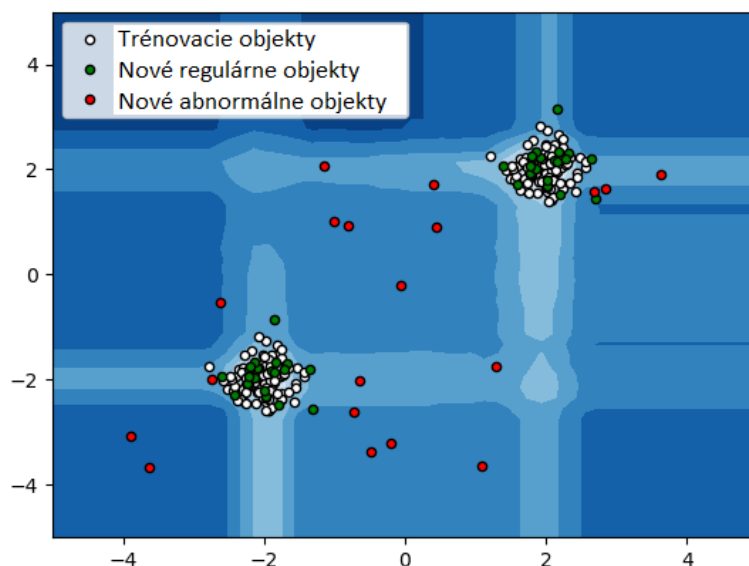


Obr. 2.15: One Class SVM[40]

Isolation Forest

Isolation Forest je metóda Outlier detekcie, ktorú navrhli Liu et al.[15]. Algoritmus explicitne izoluje anomálie, namiesto opisu normálnych objektov, a využíva k tomu náhodný les rozhodovacích stromov, angl. random forest. Stromy sa vytvárajú náhodne, v každom vrchole sa vyberie náhodný príznak a náhodná prahová hodnota. Strom sa už ďalej nedelí, ak je každý objekt sám "izolovaný" v liste stromu.[40]

Priemerná hĺbka objektu v rozhodovacích stromoch náhodného lesa predstavuje rozhodovaciu funkciu, ktorá kvantifikuje normálnosť objektu. Anomálie majú výrazne menšiu hĺbku ako regulárne objekty. Preto objekty, ktoré majú v stromoch náhodného lesa príliš malé hĺbky, sú označené za outliery.[40] Rozhodovací priestor je ilustrovaný na obrázku 2.16.

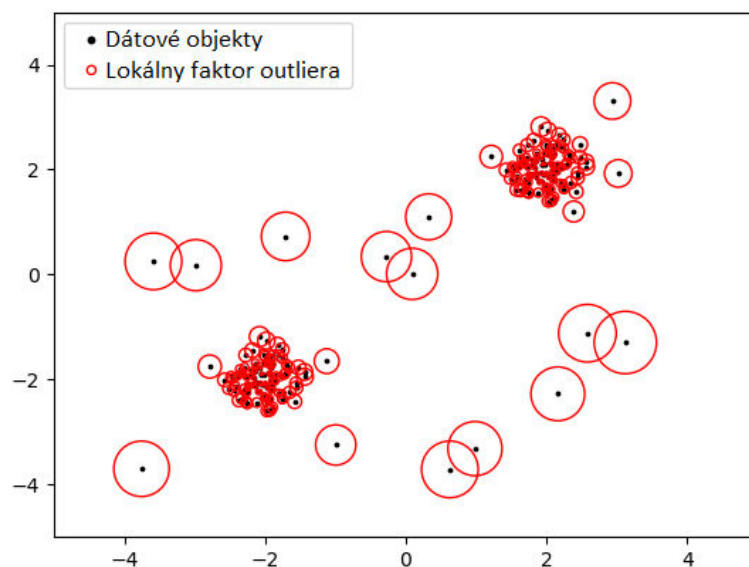


Obr. 2.16: Isolation Forest[40]

Local Outlier Factor

Local Outlier Factor je algoritmus Outlier detekcie, ktorý navrhol Breunig et al.[4] Algoritmus posudzuje lokálne vlastnosti objektu. Vypočíta sa skóre, nazývané lokálny faktor outliera, ktoré vyjadruje stupeň abnormálnosti objektu na základe odlišnosti voči susedným objektom.[40] Myšlienka je ilustrovaná na obrázku 2.17.

Cieľom je nájsť také objekty, ktoré majú výrazne nižšiu hustotu ako ich susedia a sú teda výrazne odlišné od okolitých objektov. Lokálna hustota sa získa s využitím metódy najbližších susedov. Skóre lokálny faktor outliera je vypočítané ako pomer priemernej lokálnej hustoty k najbližších susedov a lokálnej hustoty objektu. Za outlier sa považuje ten objekt, ktorý má lokálnu hustotu oveľa menšiu ako jeho susedia, čiže je osamotený vzhľadom na jeho okolie.[40]



Obr. 2.17: Local Outlier Factor[40]

2.3.3 Zhukovanie

Zhlukovanie, angl. clustering, je technika, pri ktorej sa rôznorodé dátové objekty rozdelia na základe podobnosti do neprázdnych disjunktných podmnožín, ktoré sa nazývajú zhľuky. Objekty pridelené do rovnakého zhľuku sú navzájom viac podobné ako s objektmi zaradenými do iných zhľukov. Zhľuky je možné zdefinovať ako oblasti s vysokou hustotou objektov oddelené oblasťami s nízkou hustotou. Zhlukovanie patrí medzi metódy učenia bez učiteľa, kedy učiaci sa model hľadá súvislosti medzi objektmi a nedostáva žiadnu spätnú väzbu.

Algoritmus K-means

Algoritmus K-means alebo algoritmus K-priemerov je jeden z najznámejších a najjednoduchších zhukovacích algoritmov. Zhuk je určený jeho centrom, čo je bod, ktorý je jeho priemerom a stredom. Počet zhukov k musí byť definovaný vopred. Algoritmus pracuje iteratívne v dvoch krokoch.

Na začiatku sa inicializuje k centier, náhodne alebo nejakou sofistikovanejšou metódou. Potom sa opakujú nasledujúce dva kroky, kým algoritmus nekonverguje alebo nie je splnené nejaké iné konečné kritérium.

Krok 1: Každý objekt je priradený do zhuku, ku ktorého centru má najkratšiu vzdialenosť.

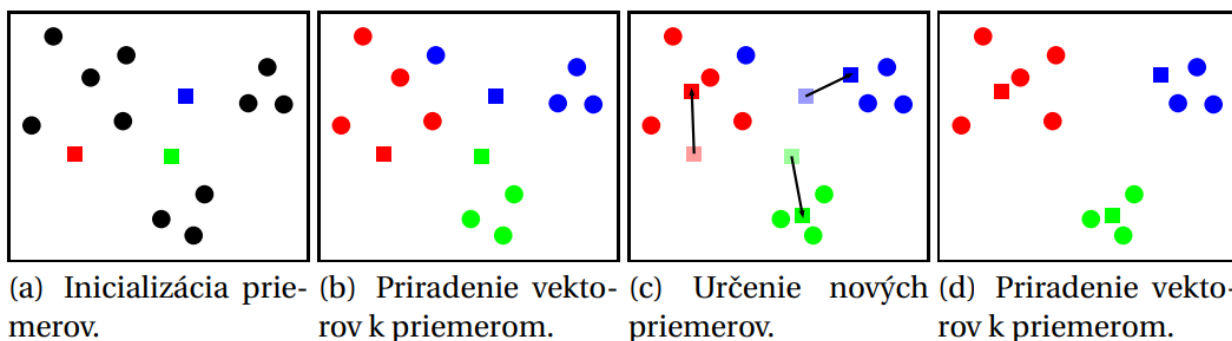
Krok 2: Centrá zhukov sú prepočítané na základe priradených objektov.

Nové centrum zhuku je vypočítané ako priemer jeho objektov, podľa nasledujúceho vzorca:

$$\vec{\mu}_j^{(t+1)} = \frac{1}{|C_j^{(t)}|} \sum_{\vec{x} \in C_j^{(t)}} \vec{x} \quad (2.13)$$

kde $\vec{\mu}_j$ je centrum j -teho zhuku C_j , $|C_j|$ je počet objektov j -teho zhuku C_j , $\vec{x}$ je dátový objekt a t je aktuálna iterácia algoritmu. Jednotlivé kroky algoritmu sú znázornené na obrázku 2.18.

Algoritmus K-means vždy konverguje k lokálnemu optimu. Ktoré lokálne optimum to bude, závisí od iniciačnej polohy centier. Preto nie je zaručené, že algoritmus nájde globálne optimum.[43]



Obr. 2.18: Algoritmus K-means[43]

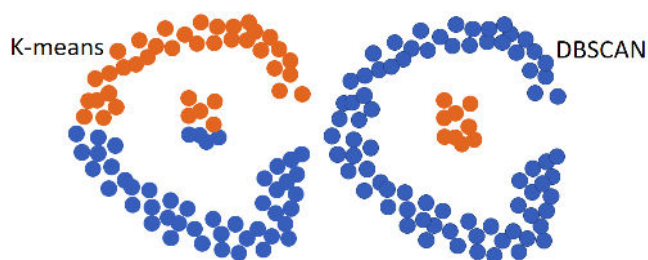
Algoritmus DBSCAN

DBSCAN, z angl. Density-based spatial clustering of applications with noise, je zhukovací algoritmus, ktorý navrhol Ester et al.[10]. Predpokladá sa, že zhuky sú oblasti s vysokou hustotou dátových objektov, ktoré sú oddelené oblasťami s nízkou hustotou. Algoritmus hľadá oblasti s vysokou hustotou a označí ich za zhuky. Najlepšie výsledky dosahuje na dátach, z ktorých vzniknú zhuky podobnej hustoty. Ak je v dátach šum, algoritmus odhalí a označí outliers.[36]

V oblastiach s vysokou hustotou sa nachádzajú tzv. jadrové body. Bod je jadrový, ak sa v jeho okolí nachádza dostatočný počet iných bodov. Minimálny počet susedných bodov v okolí vyjadruje, ako tolerantný je algoritmus voči šumu. Veľký vplyv na výsledok má tiež, ako je definované okolie bodu.[36]

Zhluk je množina jadrových bodov, ktoré sú dostatočne blízko seba, podľa definovanej metriky vzdialenosti. Okrem jadrových bodov sú v zhuku aj tzv. dosiahnuteľné alebo hraničné body. Dosiahnuteľný bod sa nachádza v okolí jadrového bodu, ale sám nie je jadrovým bodom, pretože nemá dostatočný počet susedných bodov vo svojom okolí. Všetky body, ktoré nemajú vo svojom okolí žiadny jadrový bod, sú považované za outliers alebo šum.[36]

DBSCAN nevyžaduje vopred definovaný počet zhukov, ale odvodí ho sám na základe dát. Zhluk vzniká tak, že sa zoberie jeden jadrový bod a vytvorí zhluk. Všetky susedné body v jeho okolí sa pripoja k zhuku. Následne sa pripoja susedia pripojených jadrových bodov atď. Algoritmus je deterministický pre rovnako usporiadané dáta. Zhuky môžu byť ľubovoľného tvaru, nielen konvexného.[36] Na obrázku 2.19 je porovnanie výsledkov algoritmov K-means a DBSCAN. Algoritmus K-means nedokáže takto usporiadané dáta správne rozdeliť, pretože očakávané zhuky nemajú konvexný tvar.



Obr. 2.19: Porovnanie algoritmov K-means a DBSCAN[52]

3 Návrh a implementácia metód analýzy ochranného prvku

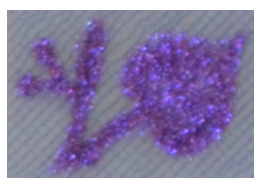
V práci sa rieši analýza jedného vybraného ochranného prvku ako parciálny problém analýzy ochranných prvkov. Analyzovaný prvok je opticky variabilná farba (OVI), ktorá mení svoj odtieň. Vizualna zmena farby je vlastnosť potenciálne využiteľná vo vizuálnej detekcii.

Skúmaný OVI ochranný prvok je umiestnený v pravom hornom rohu občianskeho preukazu. Výhodou je, že nekoliduje so žiadnymi osobnými údajmi, vďaka čomu je zachovaná anonymita, je ľahšie detekovateľný a na preskúmanie vlastností ochranného prvku postačuje menší počet reálnych občianskych preukazov, keďže jeho vzhľad nezávisí od konkrétneho občianskeho preukazu. Na každom z troch typov aktuálne platných občianskych preukazov má OVI prvok iný tvar, a to písmena SK alebo dva rôzne lipové lístky. Navrhované metódy analýzy ochranného prvku sú zamerané na overenie pravosti OVI symbolu dvoch typov lipových lístkov, pretože platnosť občianskych preukazov so SK symbolom končí tento rok.

Analýze a digitálnemu overeniu pravosti OVI ochranného prvku sa zatiaľ žiadne práce nevenovali. Práca je prvým úvodným výskumom v tejto oblasti, skúma rôzne prístupy, postupy a hľadiská. Hlavným cieľom je preskúmať, či má elektronické kontrolovanie ochranných prvkov potenciál. Navrhované metódy môžu byť rozšírené a výsledky analýzy môžu byť použité na tvorbu komplexnejších modelov. Niektoré metódy tiež môžu byť použité v časti postupu overenia iných ochranných prvkov s podobnými vlastnosťami.



Obr. 3.1: SK symbol



Obr. 3.2: Starší lipový lístok



Obr. 3.3: Novší lipový lístok

3.1 Vplyv snímania na vizuálne vlastnosti ochranného prvku s opticky variabilnou farbou

Analýzu vizuálnych vlastností ochranného prvku s opticky variabilnou farbou OVI komplikuje vysoká variácia svetelných podmienok, ktoré ovplyvňujú pozorovanú farbu. Preskúvanie všetkých možných kombinácií osvetlenia a vlastností snímacieho senzora spolu s nastaveniami kamery je náročné. V tejto podkapitole sú zhrnuté hlavné faktory ovplyvňujúce vizuálne vlastnosti OVI ochranného prvku v súvislosti s jeho snímaním.

Ešte pred samotným snímaním, významný vplyv na farbu ochranného prvku má zdroj svetla. Index podania farieb z angl. Color Rendering Index (CRI) vyjadruje, ako skutočne vyzerajú farby po osvetlení daným svetelným zdrojom. Hovorí o farbe osvetleného objektu v závislosti od zdroja svetla ešte pred snímaním fotoaparátom. Zachytená farba ochranného prvku závisí od teploty farby svetelného zdroja[12]. Teplota farby slnečného svetla sa mení v závislosti od počasia a časti dňa. Teplota farby blesku fotoaparátu je väčšinou statická, ale je možné ju zmeniť pomocou filtra. Ak na fotografii nie je vyvážená biela farba, čiže teplota zdroja svetla je vychýlená od neutrálnej bielej, potom je vychýlená aj farba zachyteného ochranného prvku[50].

Množstvo svetla dopadajúceho na povrch občianskeho preukazu súvisí s intenzitou osvetlenia, ktorá je spojená so vzdialenosťou od svetelného zdroja, napríklad blesku fotoaparátu. Množstvo odrazeného svetla závisí od mnohých faktorov, ako napríklad farba alebo drsnosť povrchu. Príliš veľa svetla zachyteného obrazovým snímačom, spôsobeného napríklad bleskom odrazeným od hladkého povrchu občianskeho preukazu, môže spôsobiť skreslenie. V takejto situácii vzniká preexponovaná fotografia. Svetlosť farby ochranného prvku OVI je možné ovplyvniť pomocou parametrov expozície, a tými sú rýchlosť uzávierky, clona a ISO. Významný vplyv má tiež dynamický rozsah snímacieho senzora. S tým súvisí scéna, v akej je občiansky preukaz umiestnený.

Nielen nastavenie, ale aj vlastnosti obrazového senzora fotoaparátu, ako je jeho veľkosť, rozlíšenie alebo citlivosť farebných kanálov, ovplyvňujú farbu ochranného prvku. Komplexnejší model by teoreticky mohol byť schopný odhadnúť tieto vlastnosti a odhaliť, akým senzorom

bola fotografia zhotovená.

Základným predpokladom digitálneho overenia pravosti ochranného prvku je kvalita a rozlíšenie fotografie. Pri nekvalitných snímkach je aj pre človeka ťažké určiť pravosť občianskeho preukazu. Hlavné faktory ovplyvňujúce kvalitu a farby fotografie sú podrobnejšie popísané v oddieli Vplyv snímania na vizuálne vlastnosti objektu.

Postup snímania OVI ochranného prvku je potrebné navrhnuť tak, aby bolo zachytených čo najviac farebných odtieňov ochranného prvku. Zmena farby OVI je spôsobená zmenou uhla zdroja alebo zdrojov svetla voči prvku. Zmena uhla nastane zmenou polohy alebo rotáciou občianskeho preukazu, alebo zmenou pozície zdroja svetla. 3D projekcia do 2-rozmernej roviny po rotácii občianskeho preukazu môže spôsobiť okrem zmeny farby aj zmenu tvaru ochranného prvku na snímke.

Farba OVI ochranného prvku závisí od pozície zdroja svetla a od pozície pozorovateľa. Pri digitálnom overení ochranného prvku je možné určiť polohu snímača voči občianskemu preukazu, ale problémom je určiť polohu zdroja svetla, jeho uhol a vzdialenosť od roviny občianskeho preukazu. Ďalším hľadiskom je, či je zdroj svetla bodový alebo plošný. Komplikovanejšia situácia nastane, ak je zdrojov svetla viac. Farba ochranného prvku je hlavne ovplyvnená primárnym zdrojom svetla, pričom ostatné zdroje spôsobujú skreslenie, tým väčšie, čím sú silnejšie. Pri podobne silných zdrojoch svetla môže vzniknúť viac odleskov ochranného prvku.

Pre vlastné navrhnuté metódy digitálneho overenia sa vybral ako primárny zdroj svetla blesk fotoaparátu, vďaka čomu má overovateľ pod kontrolou zdroj svetla. Spolu s polohou snímača sa mení aj poloha zdroja svetla. Okrem pozície občianskeho preukazu voči snímaču je teda možné určiť aj polohu zdroja svetla voči preukazu, a následne použiť vzťah medzi polohou a farbou ochranného prvku na overenie jeho pravosti. Komplikáciou je, ak je iný zdroj svetla, napríklad Slnko, silnejší ako blesk. Predpokladom na použitie postupu založeného na blesku ako primárnom zdroji svetla, je slabé okolité osvetlenie. Ideálne podmienky sú v tmavej miestnosti s jediným zdrojom svetla bleskom. Okrem toho v dôsledku statickej farby blesku, v bežných podmienkach môžu byť pozorované aj iné odtiene farby ochranného prvku. Z toho dôvodu takéto riešenie nie je úplne robustné, a nie je vhodné na použitie vo všetkých možných svetelných podmienkach.

Pri väčšom počte svetelných zdrojov je vhodnejšie sledovať celkovú charakteristiku zmeny farby, ako iba súvislosť medzi polohou a farbou ochranného prvku. Komplexnejší model by teoreticky mohol byť schopný odhadnúť počet zdrojov svetla v scéne, ich pozície, intenzitu, farbu a ďalšie vlastnosti, nájsť ich harmonické priebehy.

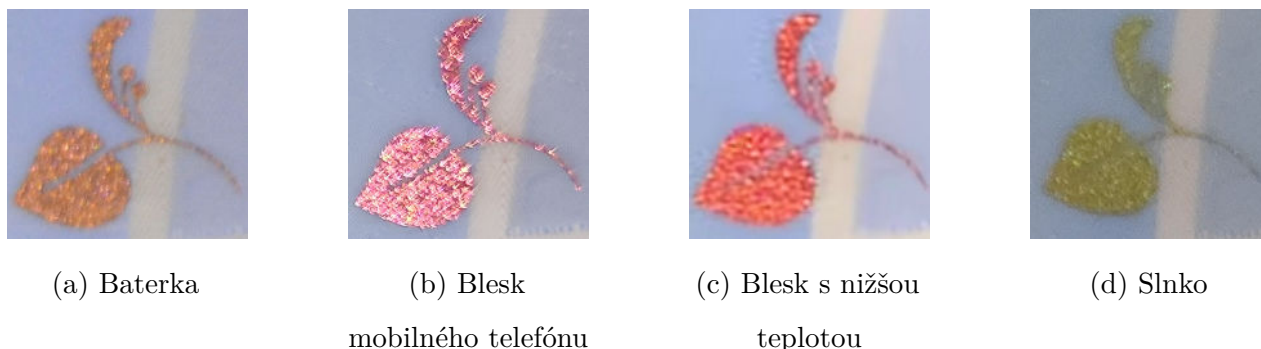
3.1.1 Skúmanie vplyvu snímania na vizuálne vlastnosti ochranného prvku

V rámci prvotnej analýzy sa pozorovala zmena farby ochranného prvku, jej závislosť od zdroja svetla, jeho intenzity a farby, ďalej sa skúmal vplyv snímania na farbu ochranného prvku na fotografii, ktorá sa porovnala s jeho skutočnou farbou. Zmenu farby ochranného prvku je možné dosiahnuť zmenou pozície snímača, občianskeho preukazu alebo zdroja svetla. Prostredníctvom praktických experimentov sa skúmalo, ktorý spôsob zmeny farby je vhodný pre digitálne overenie pravosti ochranného prvku.

Ak sa pohybuje občianskym preukazom alebo snímačom, mení sa poloha preukazu voči snímaču. Okrem farby ochranného prvku sa preto na snímke mení aj jeho tvar. To je možné vyriešiť transformáciou do normalizovaného tvaru s využitím homografie, ako je popísané v podkapitole 3.4. Snímka občianskeho preukazu je normalizovaná vtedy, keď je preukaz umiestnený priamo oproti kamere a pozadie je orezané. Príklad normalizácie je znázornený na obrázku 3.15.

Ak sa pohybuje zdrojom svetla, scéna je statická a vzájomná poloha preukazu a snímača zostáva rovnaká. Občiansky preukaz netreba normalizovať a mení sa iba farba ochranného prvku. Zmenou polohy zdroja svetla je možné pozorovať farebnosť prvku pri rôznej vzdialenosti a teda aj intenzite zdroja svetla.

V experimente sa tiež vizuálne porovnali zdroje svetla s rôznou teplotou, dva rôzne blesky, baterka a slnko. Na obrázku 3.4 sú ochranné prvky snímané v rovnakej pozícii voči rôznemu zdroju svetla. Farba je pri každom zdroji odlišná, a teda sa potvrdilo, že farba ochranného prvku na fotografii závisí od teploty zdroja svetla.

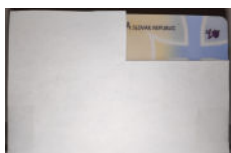


Obr. 3.4: Ochranný prvok osvetlený zdrojmi svetla s rôznou teplotou

Maska občianskeho preukazu

Pri vzniku niektorých datasetov je použitá maska z dôvodu ochrany osobných údajov. Má presný tvar občianskeho preukazu s výrezom v pravom hornom rohu, ktorý odkrýva ochranný prvok a časť občianskeho preukazu, ktorá neobsahuje osobné údaje. Porovnávali sa tri masky: biela papierová, čierna papierová a čierna hladká plastová maska.

Materiál a farba masky ovplyvňujú farebnosť ochranného prvku na fotografii. Biela farba odráža viac svetla a čierna ho viac pohlcuje. S ohľadom na dynamický rozsah senzora, biela maska môže spôsobiť, že farba ochranného prvku je tmavšia ako v skutočnosti. Vzhľadom na materiál masky, ale hlavne hladkosť jeho povrchu, drsnejší povrch papiera svetlo viac rozptýli ako hladká plastová maska. Ak sa svetlo od hladkej masky odrazí priamo do objektívu, môže vzniknúť prepálená fotografia. Výhodou použitia bielej masky je, že na jej základe je možné určiť vyváženie bielej farby na fotografii. Ale to je možné zaručiť aj bielym pozadím scény. Preto bola na vytvorenie jedného z datasetov, ktorý je primárne použitý na skúmanie farebnosti ochranného prvku, použitá čierna papierová maska. V počiatočných fázach analýzy bol vytvorený aj jeden menší dataset s bielou maskou.



Obr. 3.5: Biela
papierová maska



Obr. 3.6: Čierna
plastová maska



Obr. 3.7: Čierna
papierová maska

3.2 Návrh postupu snímania a overenia pravosti občianskeho preukazu

Pravý občiansky preukaz obsahuje všetky bezpečnostné prvky a všetky údaje v ňom uvedené sú pravdivé. Aby mohol byť občiansky preukaz považovaný za pravý, je potrebné overiť každý uvedený aspekt. Práca sa podrobnejšie venuje iba kontrole ochranného prvku OVI. Postup uvedený v tejto podkapitole je len návrh, ako by mohol vyzerat kompletný postup, kde jedným z krokov je overenie OVI prvku. Ostatným krokom, ktoré nesúvisia s OVI prvkom, sa práca nevenuje.

Vstupom do procesu digitálneho overenia pravosti občianskeho preukazu je snímka alebo video, ktoré natočí sám klient pomocou mobilného telefónu alebo iného smart zariadenia. Ďalej navrhnuté metódy overenia ochranného prvku s opticky variabilnou farbou OVI očakávajú na vstupe video. Predpokladá sa autenticita dát na úrovni senzora, čiže vstupné dáta nie sú pozmenené a prenos dát je vykonaný zabezpečeným kanálom. Na videu musí byť zachytený celý občiansky preukaz, ktorý mení svoj uhol natočenia vzhľadom na polohu snímacieho zariadenia a polohu zdroja svetla. Očakáva sa, že primárnym zdrojom osvetlenia je blesk fotoaparátu a ostatné zdroje pôsobia s minimálnou intenzitou. V tomto prípade je poloha snímača zhodná s polohou zdroja svetla, preto je zmenu farby na videu možné dosiahnuť rotovaním občianskeho preukazu alebo zmenou polohy fotoaparátu. Pohybovanie dokladom alebo fotoaparátom môže byť úplne náhodné, ale podmienkou je, aby bola na videu zachytená dostatočná zmena farby ochranného prvku. Výhodou použitia blesku je, že doklad nie je snímaný v úplne nekontrolovanom prostredí, ale scéna je z časti v rukách overovateľa. Komplexnejší model bez podmienky použitia blesku by mohol fungovať aj so zmenou polohy zdroja svetla.

V prvom kroku je overené, či sa na snímke nachádza občiansky preukaz a následne sú preskúvané jeho ochranné prvky. Kontroluje sa prítomnosť ochranného prvku a či spĺňa požadované vlastnosti. Samotné overenie ochranného prvku nie je postačujúce, pretože musí mať aj správny kontext, ako je jeho pozícia na doklade a aj v súvislosti k ostatným ochranným prvkom. Doteraz popísaná časť postupu je v nasledujúcich podkapitolách detailne rozobrať a prakticky preskúmaná. Ďalej spomenuté kroky sa podrobnejšie neriešia, ale sú uvedené

pre úplnosť riešenia.

Ďalším krokom by mala byť verifikácia občianskeho preukazu, čiže overenie existencie osoby a pravosti osobných údajov uvedených na občianskom preukaze porovnaním s dátami v externej databáze. Údaje sa načítajú pomocou metódy optického rozpoznávania znakov (OCR). Skontroluje sa ich konzistentnosť, zodpovedajúci typ dokladu, identifikačné číslo, fotografia a pod. Osobné údaje sú priradené ku konkrétnej osobe a je overená ich platnosť.

Posledným krokom by malo byť overenie voči rôznym typom podvodov, ako napríklad prelepenie fotografie alebo nasnímanie obrazovky namiesto reálneho občianskeho preukazu. Pre tento krok je vhodné použiť modely s využitím strojového učenia alebo hlbokého strojového učenia.

Navrhovaný kompletný postup overenia pravosti snímaného občianskeho preukazu je zhrnutý v nasledujúcich krokoch:

Vstup: Video s meniacou sa polohou a natočením občianskeho preukazu.

Krok 1: Nájdenie občianskeho preukazu. (podkapitola 3.4)

Krok 2: Overenie ochranných prvkov.

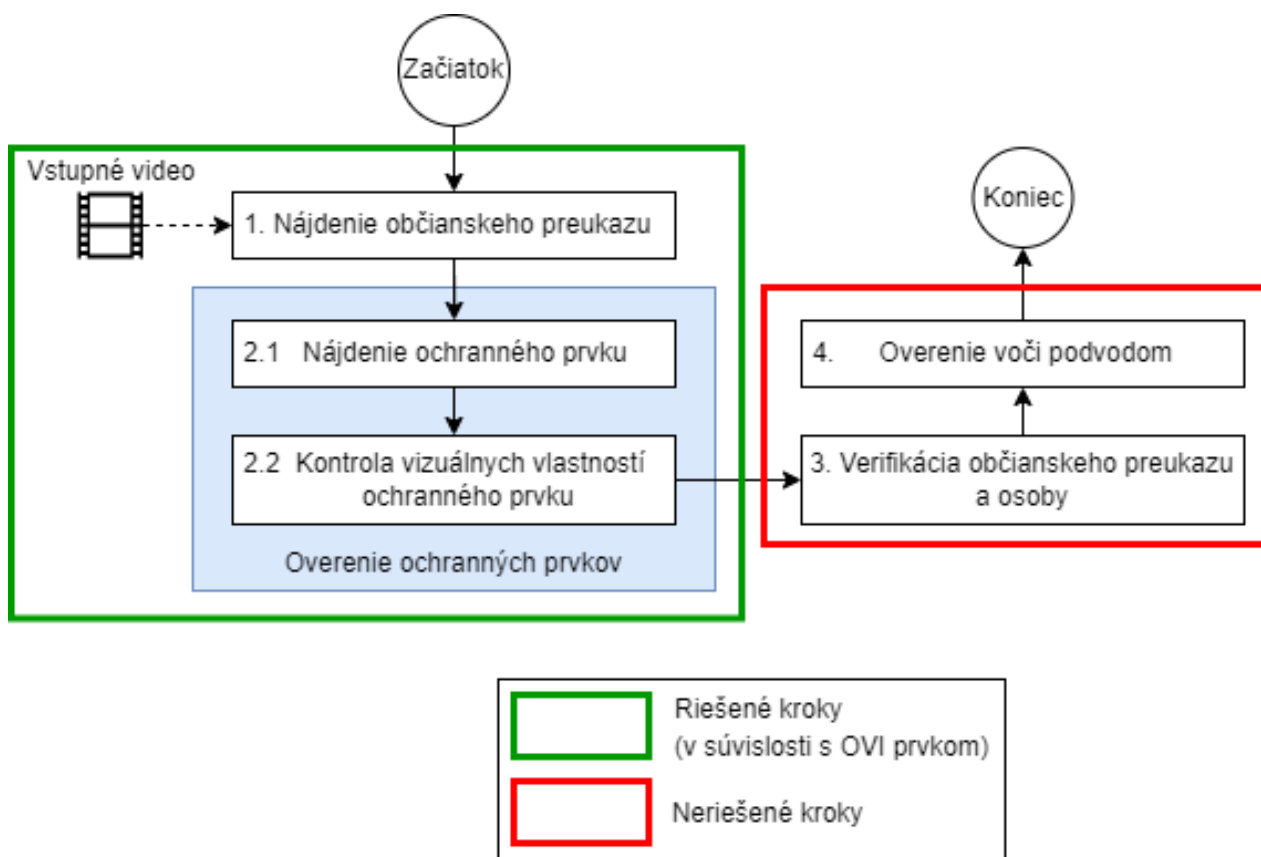
Krok 2.1: Nájdenie ochranného prvku. (podkapitola 3.5)

Krok 2.2: Kontrola vizuálnych vlastností ochranného prvku. (podkapitola 3.6)

Krok 3: Verifikácia občianskeho preukazu a osoby.

Krok 4: Overenie voči podvodom.

Navrhovaný postup je ilustrovaný na obrázku 3.8. Zelenou farbou je znázornené časť postupu, ktorej sa práca ďalej venuje. Nasledujúce podkapitoly podrobnejšie analyzujú iba kroky 1 a 2 v súvislosti s overením pravosti ochranného prvku s opticky variabilnou farbou OVI. Niektoré kroky digitálneho overenia sa môžu vykonávať paralelne a iné sekvenčne. Ak sú všetky kroky úspešné, občiansky preukaz je považovaný za pravý.



Obr. 3.8: Postup overenia pravosti občianskeho preukazu

3.3 Dataset občianskych preukazov

Pre skúmanie vybraného symbolu OVI bolo vytvorených päť typov datasetov, s rôznym účelom a využitím v inej časti postupu návrhu metód. Všetky datasety sú prehľadne popísané v tabuľke 3.1. Keďže je potrebné zachytiť prednú stranu občianskeho preukazu, s dátami je potrebné manipulovať opatrne a dbať na ochranu osobných údajov.

Prvý dataset vznikol experimentovaním s rôznymi druhmi osvetlenia, s rôznou teplotou a intenzitou zdrojov svetla, vzdialenosťou a pod. Tiež sa skúmal vplyv masky občianskeho preukazu na farbu ochranného prvku. Pre všetky skúmané kombinácie zdrojov svetla a masky vzniklo zopár snímok s rôznou polohou a natočením občianskeho preukazu.

Druhý dataset je tvorený niekoľkými fotografiami celých občianskych preukazov umiestnených v rozličnej vzdialenosti alebo uhle natočenia od snímača. Fotografie sú zhotovené v rôznorodom prostredí, s rôznym pozadím a za rôznych svetelných podmienok. Hlavným účelom je nájsť občianskeho preukazu a ochranného prvku na fotografii, a preskúmanie jeho umiestnenia a tvaru.

Predná strana občianskeho preukazu obsahuje citlivé osobné údaje, s ktorými je potrebné zaobchádzať opatrne a získanie súhlasu na zhotovenie takejto fotografie nie je jednoduché. Z dôvodu ochrany osobných údajov vznikol tretí dataset, kde sú citlivé dáta prekryté maskou. Takto anonymizovaný doklad umožňuje jednoduchšiu manipuláciu a spracovanie, a preto dataset obsahuje väčší počet snímok. Cieľom je preskúmať farebné vlastnosti ochranného prvku nasnímaného z rôznych uhlov alebo s rôznym uhlom osvetlenia. Preukazy sú odфотографované tak, aby zachytili všetky farby, ktoré môže v daných svetelných podmienkach ochranný prvok nadobudnúť.

Dataset s maskou obsahuje 440 fotografií, zachytáva 15 odlišných občianskych preukazov v 4 rôznych prostrediach. Preukazy sú fotené v sériách, kde jedna séria obsahuje fotografie jedného občianskeho preukazu foteného jedným fotoaparátom a v jednom prostredí, ale v rôznom uhle voči objektívu. Fotografie vznikli bez slnečného svetla a primárnym zdrojom osvetlenia je blesk fotoaparátu. Scéna je tvorená bielym pozadím, otáčajúcim sa stojanom s občianskym preukazom po vodorovnej osi a staticky na statíve umiestneným fotoaparátom. Na fotografovanie boli použité fotoaparáty mobilných zariadení Pocophone F1 a Poco X3 NFC, a kvalitnejší fotoaparát Nikon D5100. Stojan sa otáča po 10 stupňoch a v rámci jednej série je zhotovených 11 fotografií: základné umiestnenie priamo oproti objektívu ± 50 stupňov.



Obr. 3.9: Scéna

V rámci série je celá scéna statická, okrem rotácie občianskeho preukazu. Medzi sériami tretieho datasetu a aj fotografiami prvého a druhého datasetu je variabilnosť vzdialenosti a výšky fotoaparátu alebo typu blesku. Rôzna kvality fotografie je dosiahnutá použitím rôznych fotoaparátov. Medzi fotografiami sú občianske preukazy všetkých troch typov. Aj medzi preukazmi rovnakého typu sú rozdiely, a to v stupni fyzického poškodenia, ako napríklad škrabance.

Pre potreby detailnejšej analýzy vznikli dve ručne upravené verzie tretieho datasetu. Prvá obsahuje výrezy pravého horného rohu občianskeho preukazu v mieste, kde nie je prekrytý maskou. Druhá verzia je tvorená výrezmi ochranného prvku a je použitá hlavne na analýzu jeho farebnosti.

Štvrtý dataset je zložený z 92 videí, ktoré sú rôzne dlhé, nasnímané v mierne odlišných svetelných podmienkach a štyrmi rôznymi mobilnými telefónmi. Na videách sa striedajú štyri rôzne občianske preukazy, so starším aj novším symbolom. Pozadie občianskeho preukazu je buď jednofarebné, s textúrou alebo sa v pozadí objavuje komplexná scéna. Poloha preukazu voči mobilnému telefónu sa mení pohybom telefónu alebo občianskeho preukazu v ruke používateľa. Pri natáčaní videí bola snaha sa čo najviac priblížiť k bežným podmienkam, v ktorých by mohlo byť overenie používané.

Pre účely overenia úspešnosti navrhnutých metód je nevyhnutné vytvoriť piaty dataset falošných občianskych preukazov. Možností falšovania dokladov je veľa. Nepravý občiansky preukaz môže vzniknúť napríklad vytlačením na papier, kancelársky, fotografický, lesklý, alebo umelou transformáciou statickej snímky v počítači. V práci sú prakticky použité vytlačené občianske preukazy na klasický kancelársky papier a na fotografický papier. Dataset je tvorený 71 videami, ktoré sú použité pri testovaní metód verifikácie. Videá vznikli rovnakým spôsobom ako videá vo štvrtom datasete, ale namiesto reálnych občianskych preukazov sú použité falzifikáty.

Tabuľka 3.1: Prehľad datasetov

	Typ dát (počet)	Účel	Popis
Dataset 1	pravé snímky (72)	prvotná analýza farby prvku	experimentovanie s rôznou polohou dokladu, rôznym osvetlením a maskou, sledovanie vplyvu na farbu prvku
Dataset 2	pravé snímky (23)	detekcia občianskeho preukazu a ochranného prvku	rôzne osvetlenie, rôzne mobilné telefóny, rôzne scény
Dataset 3	pravé snímky (440)	analýza farby prvku v konkrétnych pozíciách	s bleskom, rôzne mobilné telefóny, preukaz s maskou, podobná scéna, fotené v sériách
Dataset 4	pravé videá (92)	testovanie metód	s bleskom, rôzne mobilné telefóny, rôzne scény
Dataset 5	falošné videá (71) papier + fotografia	testovanie metód	s bleskom, rôzne mobilné telefóny, rôzne scény

3.4 Návrh metód nájdania občianskeho preukazu na snímke

Prvým krokom navrhovaného postupu overenia pravosti občianskeho preukazu je nájdenie občianskeho preukazu na snímke, ako je znázornené na obrázku 3.8. V súvislosti s overením pravosti ochranného prvku s opticky variabilnou farbou OVI je nájdenie občianskeho preukazu na snímke použité na zúženie oblasti prehľadávania pri detekcii prvku. Z normalizovaného občianskeho preukazu sa použije výrez pravého horného rohu. Tým sa zaručí, že sa ochranný prvok nachádza na občianskom preukaze a na správnej pozícii. Okrem toho, normalizovaný občiansky preukaz je možné použiť na analýzu ďalších ochranných prvkov alebo osobných údajov.

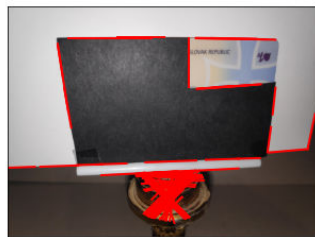
3.4.1 Detekcia hrán občianskeho preukazu

Cieľom skúmanej metódy je nájsť občiansky preukaz na snímke pomocou detekcie jeho hrán. V prvom kroku je na snímku aplikovaný Canny detektor hrán a následne Houghova transformácia na nájdenie hrán občianskeho preukazu. Uvedené metódy sú použité z Pythonovej knižnice OpenCV[22].

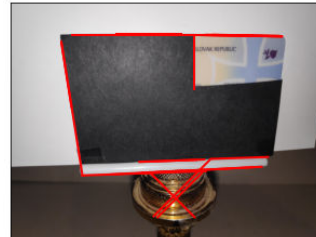
Tento postup vyžaduje, aby bolo pozadie občianskeho preukazu bez textúry, pretože inak by hrany pozadia mohli detektor pomýliť. Celá scéna a svetelné podmienky majú významný vplyv na výsledok, a preto toto riešenie nie je dostatočne robustné. Vplyv scény je možné pozorovať na obrázkoch 3.10 a 3.12, kde sú snímky z tretieho datasetu s čiernou maskou



Obr. 3.10: Detekcia hrán -
scéna 1



Obr. 3.11: Detekcia hrán -
scéna 2



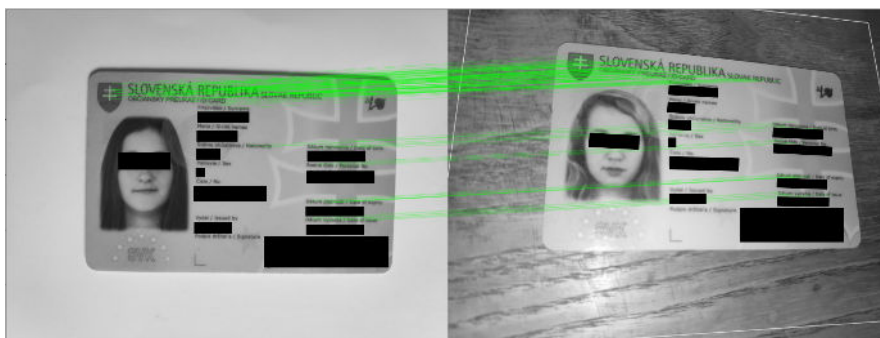
Obr. 3.12: Detekcia hrán -
scéna 2 (iné parametre)

občianskeho preukazu, na ktorých sú nájdené hrany označené červenou farbou. Na prvej snímke algoritmus nenašiel všetky hrany a na druhej označil aj hrany v pozadí. Na obrázku 3.11 sú zaznačené čiary po menšej úprave vstupných parametrov algoritmu oproti snímke 3.12. V tomto prípade algoritmus označil menej čiar v pozadí, ale aj menej hrán občianskeho preukazu. To znamená, že ani zmena vstupných parametrov algoritmu nepomohla nájsť všetky hrany občianskeho preukazu a redukovať hrany v pozadí. Z týchto dôvodov, metódu nie je vhodné použiť na nájdenie občianskeho preukazu na snímke.

3.4.2 Detekcia pomocou keypointov

Detekcia občianskeho preukazu pomocou keypointov používa ako vzor snímku normalizovaného občianskeho preukazu, ktorého keypointy sa párujú s keypointami analyzovanej snímky. Keď sa zistí dostatočná zhoda a dostatočný počet keypointov je spárovaný, občiansky preukaz sa na snímke úspešne našiel. Pre otestovanie danej metódy detekcie je použitý druhý dataset. Na obrázku 3.13 sú zelenými čiarami spojené spárované keypointy, pričom občiansky preukaz vľavo bol použitý ako vzor. Čierne útvary sú použité kvôli ochrane osobných údajov a boli doplnené až po aplikovaní metódy.

Porovnali sa viaceré algoritmy detekcie keypointov, ktoré sú implementované v knižnici OpenCV[21]. Na obrázku 3.14 je na rovnakých snímkach použitý v prvom riadku algoritmus SIFT a v druhom algoritmus ORB. Ružovou farbou sú znázornené spárované keypointy. Na základe spárovaných keypointov je možné vypočítať homografiu, čiže transformačnú maticu typu 3×3 , ktorá hovorí o pozícii občianskeho preukazu voči snímaču, a pomocou



Obr. 3.13: Spárované keypointy



Obr. 3.14: SIFT vs ORB

nej občiansky preukaz normalizovať. Normalizácia v tomto prípade znamená transformáciu do roviny normalizovaného občianskeho preukazu, čiže orezanie scény v pozadí a vyrovnanie občianskeho preukazu. Oblasť dokladu vypočítaná na základe homografie je na obrázkoch ohraničená žltou čiarou.

Najlepšie výsledky dosiahol algoritmus SIFT. ORB na snímkach nenašiel dostatočný počet keypointov pre výpočet správnej homografie. SIFT je invariantný voči rotácii, posunu, škálovaniu, zmene osvetlenia a čiastočnému skresleniu objektu, čo sa aj prakticky overilo pokusmi so zmenou polohy občianskeho preukazu, zmenou rozlíšenia, zdroja svetla a pod. Preto je metódu detekcie keypointov a algoritmus SIFT vhodné použiť na nájdenie občianskeho preukazu na snímke.

Ukážka normalizácie pomocou algoritmu SIFT je na obrázku 3.15. Na normalizovanom preukaze je následne možné skontrolovať, či obsahuje niektoré konkrétne časti alebo jednoduchšie ochranné prvky, napríklad štátny znak v ľavom hornom rohu spolu s nápisom SLOVENSKÁ REPUBLIKA. Na kontrolu môže byť opäť použitá detekcia keypointov a algoritmus SIFT, ale so vzorom pre konkrétnu kontrolovanú oblasť alebo prvok. Normalizovaný občiansky preukaz je spolu s transformačnou maticou vstupom do ďalšej analýzy ochranného prvku.



Obr. 3.15: Normalizácia občianskeho preukazu

Navrhovaná metóda nájdania občianskeho preukazu pomocou algoritmu SIFT sa otestovala na videách štvrtého a piateho datasetu. Jej úspešnosť je uvedená v tabuľke 3.2. Výsledky vyjadrujú, na koľkých snímkach algoritmus detekoval a nedetekoval občiansky preukaz. O niečo úspešnejší je na pravých občianskych preukazoch. Celkovo má na všetkých snímkach úspešnosť 91.24%.

V istých situáciách, občiansky preukaz na snímke nájdený nie je. Je to spôsobené nedostatočným počtom spárovaných keypointov. Dôvodom je úplná alebo čiastočná absencia preukazu na snímke, príliš veľký uhol rotácie voči snímaču, vizuálne poškodenie dokladu alebo pokrivenie roviny pri falošnom občianskom preukaze. Snímka, na ktorej nebol detekovaný občiansky preukaz, nepokračuje do ďalšieho kroku overenia.

Tabuľka 3.2: Úspešnosť detekcie občianskeho preukazu

	reálne	falošné	spolu
detekovaný	5747	3341	9088
nedetekovaný	388	484	872
úspešnosť	93,68%	87,35%	91,24%

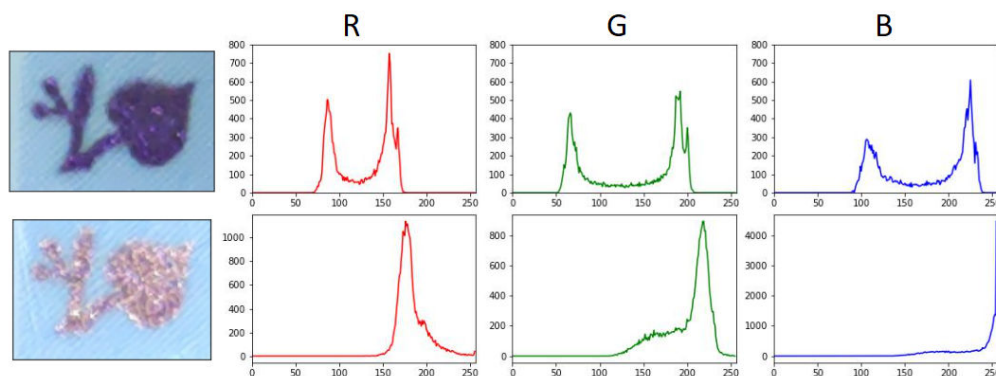
3.5 Návrh metód nájdania ochranného prvku na občianskom preukaze

Druhý krok overenia pravosti občianskeho preukazu, ako je znázornené na obrázku s postupom 3.8, je overenie jeho ochranných prvkov. Ešte pred kontrolou vizuálnych vlastností ochranného prvku je potrebné overiť, či sa na snímke vôbec nachádza a nájsť jeho pozíciu. Preskúmané metódy detekcie ochranného prvku je možné rozdeliť na dva typy, orientované na tvar alebo orientované na farbu. Na začiatku sa experimentovalo s hľadaním ochranného prvku v celej scéne. Následne sa usúdilo, že prehľadávanú oblasť je potrebné čo najviac zúžiť. Na to je použitý výrez pravého horného rohu normalizovaného občianskeho preukazu, ktorý bol získaný postupom opísaným v predchádzajúcej podkapitole 3.4.

3.5.1 Hľadanie ochranného prvku v celej scéne

V počiatočnej fáze analýzy boli vyskúšané metódy, ktoré sa pokúšali nájsť ochranný prvok v celej scéne, nie len vo výreze normalizovaného občianskeho preukazu. Bez normalizácie je tvar ochranného prvku na snímke veľmi rôznorodý a preto sa viac hodí zamerať na farbu. Ale hlavným cieľom analýzy farebnosti v tejto časti postupu je preskúmanie možnosti nájdania ochranného prvku v scéne prostredníctvom jeho farby, nie overenie jeho farebných charakteristík.

Na obrázku 3.16 sú histogramy hodnôt pixelov pre výrezy s ochranným prvkom. K jednému obrázku ochranného prvku sú priradené tri histogramy, jeden pre každú zložku RGB farebného modelu. Na obrázkoch ochranných prvkov je vidieť, že každý má inú farbu, takisto aj ich histogramy sú odlišné. Modrá farba v pozadí ochranného prvku sa tiež líši, čo znamená, že ochranné prvky boli snímané s rôznym osvetlením. Z týchto dôvodov je veľmi náročné nájsť metódu založenú na farbe, ktorá je schopná detekovať ochranný prvok v ľubovoľných svetelných podmienkach.



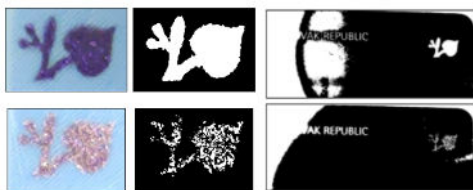
Obr. 3.16: RGB histogramy

Prahovanie

Prvým pokusom na nájdenie ochranného prvku v scéne bol experiment s prahovaním, angl. thresholding, ktorý je jednou z najjednoduchších metód segmentácie obrazu. Výstupom je čiernobiely obrázok, ktorý označuje, ktoré pixely patria a nepatria hľadanému objektu. Na začiatku bolo použité jednoduché prahovanie s jednou globálnou prahovou hodnotou, resp. jednou pre každý farebný kanál, ktorá je určená na základe histogramov snímok, podobných ako na obrázku 3.16. Preskúmala sa aj kombinácia s metódou normalizácie histogramu za účelom zvýšenia kontrastu vstupného obrázka. Na určenie globálnej prahovej hodnoty sa tiež skúsila použiť metóda Otsu prahovania. Všetky prahovacie metódy sú použité z knižnice OpenCV[23].

Na obrázkoch 3.17 a 3.18 je výstup prahovania použitého na výrez ochranného prvku a na väčšiu scénu. V riadku je tiež zobrazený originálny obrázok ochranného prvku. Všetky snímky patria do prvého datasetu. Na obrázku 3.17 je prahovanie aplikované na RGB farebný model, a na obrázku 3.18 na HSV model, presnejšie iba na komponent H, čiže samotný odtieň farby bez sýtosti a jas. HSV model dokáže lepšie izolovať samotnú farbu. Ale pre obidva farebné modely má prahovanie problém s odleskami a okrem prvku vyberá aj iné časti scény.

Okrem jednoduchého prahovania sa robili experimenty s adaptívnymi prahovacími metódami, kde je prahová hodnota pixela určená na základe jeho okolia. Boli preskúvané dva spôsoby adaptívneho určenia prahovej hodnoty, a to priemer a gaussovsky vážený súčet okolitých pixelov.



Obr. 3.17: RGB prahovanie



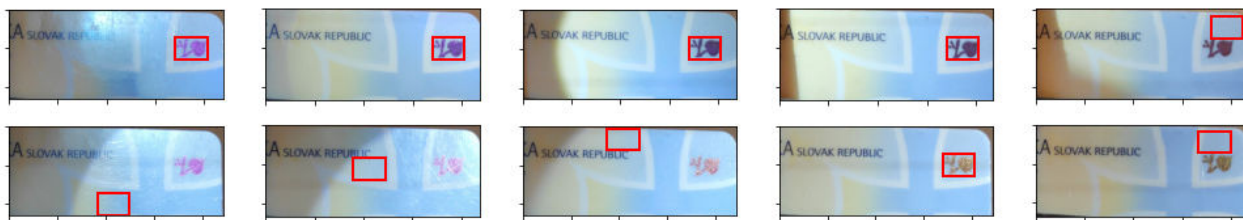
Obr. 3.18: HSV prahovanie

Prahovacie metódy sú závislé od svetelných podmienok a farebnosti ochranného prvku. Zmena jeho farby a odlesk zrníčok spôsobujú, že metóda často správne nevyberie všetky pixely ochranného prvku, niekedy skoro žiadne. Na druhej strane, zachytáva iné oblasti snímky s podobným farebným odtieňom. Z týchto dôvodov sa nedá jednoznačne určiť, kde sa ochranný prvok nachádza, a metóda sa samostatne nedá použiť na jeho nájdenie.

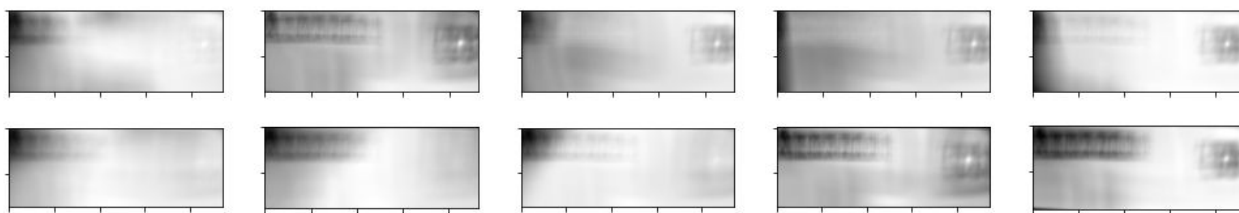
Detekcia pomocou metódy Template Matching

Metóda Template Matching používa šablónu ochranného prvku, ktorú posúva po obrázku a hľadá pozíciu s najväčšou zhodou, ktorá je vypočítaná podľa vybranej metriky. Výstupom je matica so skóre pre každú pozíciu fotografie. Metóda neberie do úvahy tvar ochranného prvku, ale iba jeho farbu. Výsledok závisí od farby vzoru na šablóne, ale značný vplyv má aj modrá farba v jeho pozadí. Snímky použité na testovanie metódy Template Matching sú súčasťou prvého datasetu. V experimentoch sa používa implementácie metódy z knižnice OpenCV[26].

Na obrázku 3.19 je 10 snímok výrezov občianskeho preukazu s rôznym odtieňom ochranného prvku. Červeným obdĺžnikom je určená pozícia, ktorú Template Matching označil za ochranný prvok. Metóda je aplikovaná na farebné vstupné snímky. Na obrázku 3.20 sú ich výstupné matice, kde svetlejšia farba znamená vyššie skóre danej pozície. Metóda na viacerých snímkach neurčila správnu pozíciu ochranného prvku.



Obr. 3.19: Výsledok Template Matching



Obr. 3.20: Výstupná matica so skóre Template Matching

Na obrázkoch 3.21, 3.22 a 3.23 je pozícia ochranného prvku hľadaná v rámci celej scény s občianskym preukazom prekrytým bielou maskou. Na obrázku 3.21 má ochranný prvok iné rozlíšenie ako na šablóne. Lepšie výsledky s prispôbeným rozlíšením na obrázku 3.22 potvrdzujú, že ochranný prvok na snímke musí mať rovnaké rozlíšenie ako vzor.

Pre rozšírenie metódy o symboly rôznych farieb je možné súčasne použiť viaceré šablóny s odlišnými farbami ochranného prvku. Boli preskúvané dva spôsoby agregácie výsledného skóre, a to súčet a minimum, resp. maximum podľa použitej metriky. Na obrázku 3.23 sú označené pozície ochranného prvku, ktoré sú výsledkom súčtu skóre piatich rôznych šablón. Tento typ agregácie je menej úspešný ako použitie iba jedného vzoru na obrázku 3.22. Dôvodom je, že pre rôzne farby ochranného prvku sa skóre veľmi líši. Preto je za pozíciu ochranného prvku lepšie vybrať takú, ktorej skóre je minimum alebo maximum zo skóre všetkých pozícií a šablón.



Obr. 3.21: Výsledok Template Matching s originálnym rozlíšením



Obr. 3.22: Výsledok Template Matching s prispôsobeným rozlíšením



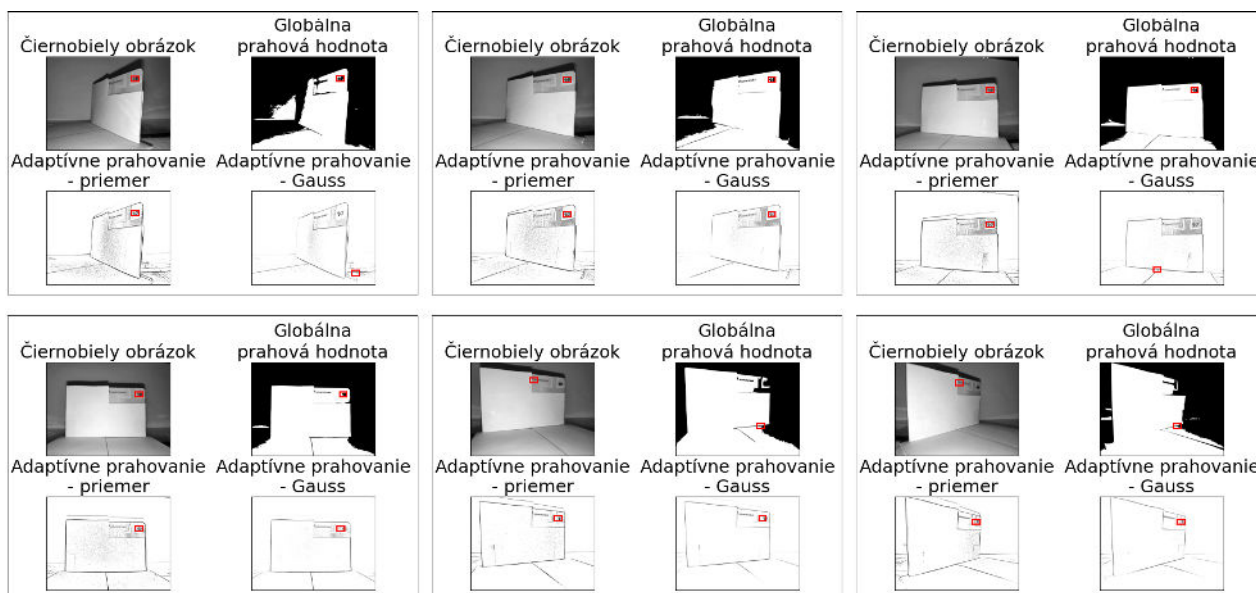
Obr. 3.23: Výsledok Template Matching pre súčet skóre viacerých vzorov

Ďalej sa preskúmali možnosti použitia Template Matching na čiernobielych snímkach a výstupoch z prahovania opísaného v predchádzajúcej časti o prahovaní. Otestovala sa kombinácia s farebným Template Matching, kde je výstupom súčet výstupných matíc farebného a čiernobieleho skóre. Analyzovali sa štyri typy čiernobielych variant snímky: klasická čiernobiela snímka a výstup globálneho, adaptívneho priemerového a adaptívneho gaussovského prahovania.

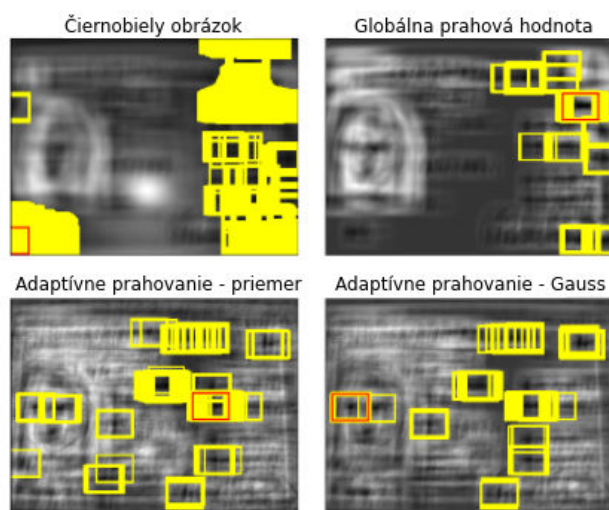
Na obrázku 3.24 sú pre jednu snímku výsledky všetkých štyroch typov jej čiernobielych modifikácií. Snímky sa líšia rôznym uhlom natočenia občianskeho preukazu. Kombinácia farebného a čiernobieleho Template Matching nepriniesla výrazné zlepšenie pri hľadaní ochranného prvku, preto je postačujúci samostatný farebný Template Matching.

Na obrázku 3.25 sú výstupné matice pre štyri typy čiernobielych variant snímky s celým občianskym preukazom bez masky. Žltou farbou sú znázornené pozície s vysokým skóre a červenou pozícia s najvyšším skóre. Na obrázku je vidieť, že Template Matching nachádza

ochranný prvok aj na mnohých iných miestach občianskeho preukazu, ktoré šablóny farebne vyhovujú, a preto je potrebné hľadať ochranný prvok v čo najmensej možnej oblasti, najlepšie vo výreze pravého horného rohu občianskeho preukazu.



Obr. 3.24: Výsledok Template Matching pre 4 typy čiernobielych snímok

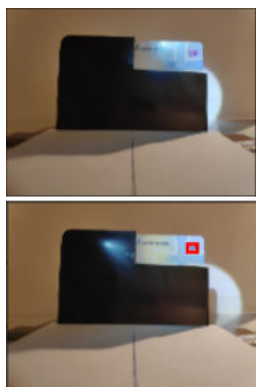


Obr. 3.25: Výstupná matica Template Matching na celom občianskom preukaze

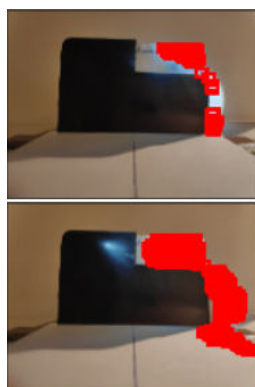
Detekcia anomálií

Prakticky sa preskúmali tri metódy detekcie anomálií: One Class SVM, Isolation Forest a Local Outlier Factor. Metódy sú použité z Pythonovej knižnice Scikit-learn[40]. Všetky výrezy zo snímky, okrem tých, ktoré obsahujú ochranný prvok, sú považované za nevyhovujúce prípady (anomálie). Na tréning detektora sú použité výrezy s ochranným prvkom, ktoré sú transformované do jednorozmerného vektora. Detektor sa postupne posúva po celej snímke a vyhodnocuje jednotlivé pozície, či sa na nich vzor nachádza alebo je pozícia nevyhovujúca.

Nevýhodou detektora je, že výsledok veľmi závisí od svetelných podmienok a rozlíšenia snímky. Na jednej snímke môže detektor označiť viac výrezov za ochranný prvok alebo aj žiadny. Výsledky algoritmov na dvoch rôznych snímkach z prvého datasetu sú znázornené na obrázkoch 3.26, 3.27 a 3.28. Pozície prehlásené za ochranný prvok sú vyznačené červeným obdĺžnikom. Algoritmus One Class SVM na väčšine testovacích snímok nevybral žiadnu pozíciu za ochranný prvok. Ale ak nejakú pozíciu označil, tak sa na nej skoro vždy ochranný prvok nachádzal. Na druhej strane, Isolation Forest a Local Outlier Factor často na jednej snímke označili oveľa viac pozícií, a pri hľadaní boli niekoľko násobne pomalšie ako One Class SVM. Z uvedených dôvodov sa detekcia anomálií nehodí na hľadanie OVI ochranného prvku na fotografii.



Obr. 3.26: One
Class SVM



Obr. 3.27:
Isolation Forest



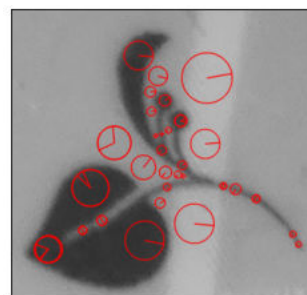
Obr. 3.28: Local
Outlier Factor

3.5.2 Hľadanie ochranného prvku vo výreze občianskeho preukazu

Ochranný prvok s opticky variabilnou farbou OVI je umiestnený v pravom hornom rohu občianskeho preukazu. Z normalizovaného občianskeho preukazu je pomerne jednoduché vyrezať oblasť, kde by sa mal ochranný prvok nachádzať. Pri normalizovaní občianskeho preukazu môžu nastať menšie chyby transformácie alebo posuny, preto je vyrezaná oblasť trochu väčšia. Okrem toho, na každom z dvoch skúmaných typov občianskych preukazov sa OVI ochranný prvok nachádza na inej pozícii.

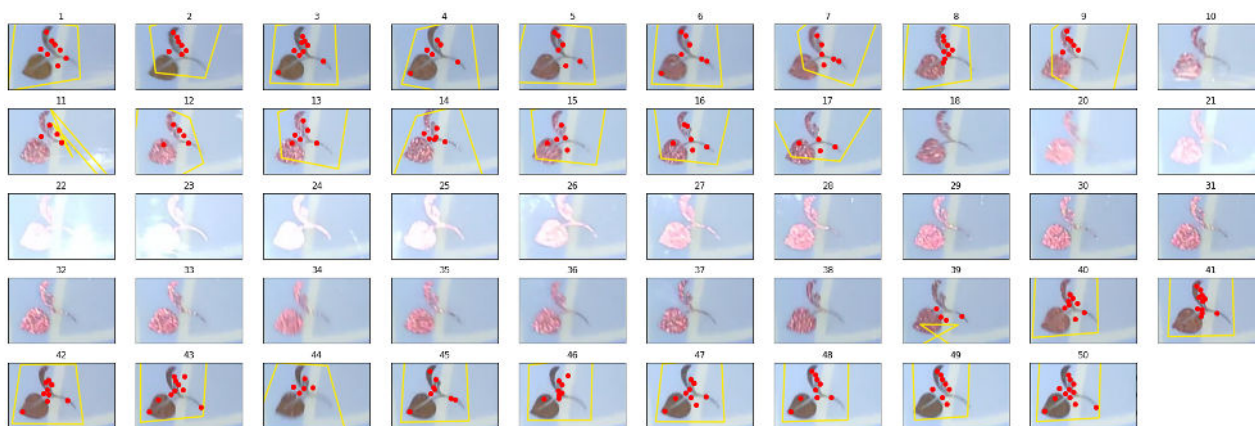
Detekcia pomocou keypointov

Algoritmus SIFT úspešne dokáže nájsť občiansky preukaz v scéne. Nájdenie ochranného prvku vo výreze je zložitejšie. Detekciu komplikuje zmena farby prvku, hlavne z tmavej farby na svetlú, ďalej odlesk samotného ochranného prvku alebo odraz blesku od povrchu občianskeho preukazu. Výhodou metódy je, že z výstupu algoritmu je jasné, či bol ochranný prvok nájdený alebo nebol.



Obr. 3.30: Keypointy ochranného prvku

Na obrázku 3.29 je vidieť, aké keypointy, znázornené červenou farbou, sú nájdené na ochranných prvkoch rôznej farby a s rôznym odleskom. Snímky vznikli výrezom z normalizovaného občianskeho preukazu pri spracovaní videa štvrtého datasetu. Ako vzor je použitý



Obr. 3.29: Keypointy na výrezoch s rôznou farbou ochranného prvku

výrez ochranného prvku zo snímky iného videa. Na snímkach so silným odleskom nie sú nájdené žiadne keypointy. Žltou čiarou je znázornená oblasť, kde by sa na základe nájdených keypointov a vypočítanej homografie mal prvok nachádzať. Na viacerých snímkach túto oblasť nie je možné identifikovať pre nedostatok keypointov, aj keď sa na snímke ochranný prvok nachádza. Keďže jednou z vlastností ochranného prvku je, že sa leskne, a teda ju je v ďalšom kroku v rámci vizuálnej kontroly potrebné overiť, tento prístup nájdenia ochranného prvku nie je dostačujúci.

Detekcia keypointov sa zameriava na tvar ochranného prvku, a preto môže byť vhodným doplnením inej farebne založenej metódy, napríklad Template Matching. Vzhľadom k tomu, že z výstupu algoritmu je zjavné, či bol na snímke ochranný prvok detekovaný, je túto metódu možné použiť na overenie, ktorý typ symbolu sa na snímanom občianskom preukaze nachádza. Vyhodnotenie môže byť spravené na základe výsledkov na snímkach, kde bol detektor schopný prvok nájsť. Keď je prvok nájdený na dostatočnom počte snímok, je pravdepodobné, že daný typ symbolu sa na občianskom preukaze naozaj nachádza. Ak boli na videu zachytené obidva typy ochranných prvkov, môže ísť o chybu detekcie alebo poškodenú snímku. Pokiaľ sa na videu pomocou keypointov overí typ symbolu, môžu sa z výstupu iných aplikovaných metód vyhodíť tie snímky, na ktorých bol chybné detekovaný iný typ ochranného prvku.

Detekcia pomocou metódy Template Matching

Na základe záverov z oddielu 3.5.1, navrhovaná metóda aplikuje Template Matching na farebný výrez snímky občianskeho preukazu. Pozícia ochranného prvku je vybraná tá, ktorá má najmenšie skóre spomedzi všetkých pozícií a všetkých šablón s ochranným prvkom, resp. najvyššie v závislosti od použitej metriky.

Pre správne nájdenie vzoru je nevyhnutné, aby mal ochranný prvok na prehľadávanej snímke rovnaké rozlíšenie ako šablóna. V implementovanej metóde sú pre každý vzor použité tri šablóny s rovnakým rozlíšením, ale rôznou farbou ochranného prvku. Normalizované občianske preukazy majú rovnaké rozlíšenie, vďaka čomu je jednoduché upraviť rozlíšenie výrezu, aby vyhovovalo rozlíšeniu šablóny ochranného prvku.

Kvôli výberu vhodnej metriky bol urobený experiment, v rámci ktorého sa porovnala úspešnosť nájdenia ochranného prvku s využitím rôznych metrík implementovaných v Pythonovej knižnici OpenCV[25]. V experimente sa použili snímky z tretieho datasetu, ktoré boli orezané na oblasť pravého horného rohu občianskeho preukazu bez zmeny rozlíšenia a normalizácie, pretože snímky boli zhotovené s maskou občianskeho preukazu, a tá neumožňuje urobiť prvý krok nájdenia občianskeho preukazu v scéne. Na základe výsledkov v tabuľke 3.3, kde je uvedená úspešnosť jednotlivých metrík, bola vybraná metrika TM_SQDIFF, čiže štvorcová vzdialenosť z angl. Template Matching Square Difference.

Metrika TM_SQDIFF je vypočítaná na základe nasledujúceho vzťahu:

$$R(x, y) = \sum_{x', y'} \left(T(x', y') - I(x + x', y + y') \right)^2 \quad (3.1)$$

kde $R(x, y)$ je výsledná matica so skóre pre jednotlivé pozície, T je obrázok šablóny a I je skúmaná fotografia.

Nevýhodou metódy Template Matching je, keďže pracuje s farbou, že pri rôznych svetelných podmienkach má pozícia s ochranným prvkom rôzne skóre. Metóda vždy vráti pozíciu, ktorá má najlepšie skóre. Z toho dôvodu nie je isté, či našla alebo nenašla ochranný prvok. Môže nastať situácia, kedy aj po nájdení občianskeho preukazu a jeho normalizácii nie je možné nájsť ochranný prvok, napríklad po priamom osvetlení bleskom fotoaparátu. Ďalším problémom vyplývajúcim z variabilných svetelných podmienok je, keď zachytená farba ochranného prvku nie je obsiahnutá v šablónach. Vtedy sa môže stať, že iná pozícia bez ochranného prvku má lepšie skóre ako pozícia s prvkom.

Tabuľka 3.3: Úspešnosť metrík Template Matching

CCOEFF	CCOEFF NORMED	CCORR	CCORR NORMED	SQDIFF	SQDIFF NORMED
85,9%	78,2%	23,6%	55,9%	87,5%	57,5%

Detekcia pomocou keypointov a metódy Template Matching

Finálny navrhovaný postup detekcie ochranného prvku je spojením metódy Template Matching a detekcie pomocou keypointov algoritmom SIFT na výreze občianskeho preukazu.

Postupne sa analyzujú snímky videa. Do metódy vstupuje výrez pravého horného rohu normalizovaného občianskeho preukazu aktuálne analyzovanej snímky. Metóda Template Matching vyreže ochranný prvok. Na výreze sa detekcia keypointov pokúsi nájsť ochranný prvok a tým určiť, aký typ prvku je na občianskom preukaze. Na záver, po prejdení všetkých snímok, sa vylúčia tie výrezy, na ktorých bol metódou Template Matching vyrezaný nesprávny typ ochranného prvku.

Úspešnosť finálneho navrhovaného postupu detekcie je otestovaná na snímkach videí štvrtého a piateho datasetu. Výsledky sú uvedené v tabuľke 3.4. Detekcia je menej úspešná na falošných občianskych preukazoch. Celkovo bolo správne nájdených 91,58% výrezov ochranného prvku.

Tabuľka 3.4: Úspešnosť detekcie pomocou keypointov a metódy Template Matching

	reálne	falošné	spolu
správna detekcia	5457	2749	8206
chybná detekcia	321	433	754
úspešnosť	94,44%	86,39%	91,58%

Kompletný navrhovaný postup detekcie ochranného prvku je doplnený kontrolou jednej z vizuálnych vlastností, ktorá vylúči hlavne chybné detekované výrezy. Táto vizuálna vlastnosť je odlesk ochranného prvku, ktorý je podrobne rozobratý v oddieli 3.6.3, a v tomto oddieli v časti Využitie detekcie odlesku pri hľadaní ochranného prvku je popísaná kompletná metóda detekcie ochranného prvku spolu s výsledkami na testovacích dátach štvrtého a piateho datasetu.

3.6 Návrh metód kontroly vizuálnych vlastností ochranného prvku

Ochranný prvok s opticky variabilnou farbou OVI je vizuálne charakterizovaný svojím tvarom a variabilnou farbou. Tvar prvku spolu s jeho pozíciou na občianskom preukaze je

overený v predchádzajúcej časti postupu. Táto podkapitola je zameraná na kontrolu farebnej charakteristiky ochranného prvku, ktorá je súčasťou kroku 2.2 postupu overenia pravosti občianskeho preukazu, znázorneného na obrázku 3.8.

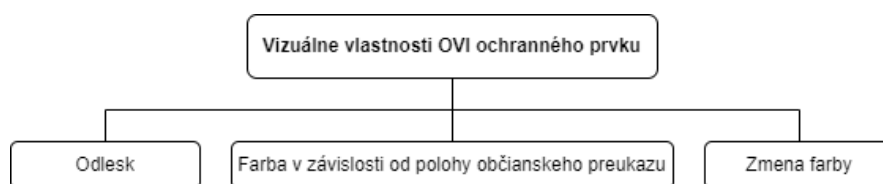
Vstupom do tejto časti postupu je séria snímok s výrezom ochranného prvku, ktorá vznikla zo sekvencie snímok videa štvrtého alebo piateho datasetu. Na určenie pozície ochranného prvku bol aplikovaný postup opísaný v predchádzajúcej podkapitole 3.5. V tejto podkapitole sa pracuje už len s výrezmi ochranných prvkov, kde každý výrez bol získaný vyrezaním z pôvodnej snímky zo sekvencie snímok videa.

Overenie farebnej charakteristiky ochranného prvku je zložitý problém, ku ktorému je možné pristupovať rôznymi spôsobmi. Prvým dôležitým rozhodnutím je výber reprezentácie farby ochranného prvku, od čoho sa odvíjajú všetky použité overovacie metódy. Tie by sa mali skladať z minimálne troch častí.

Prvou metódou je kontrola odlesku ochranného prvku na výreze snímky. Odleskom sa rozumie trblietanie sa zrníčok Opticky variabilnej farby. Ochranný prvok sa na snímke neleskne, ak je príliš "hladký". V oddieli, ktorý sa odlesku venuje, je navrhnutý spôsob merania odlesku, a jeho využitie na vylúčenie chybné detekovaných výrezov ochranného prvku.

Druhým aspektom je overenie farby vzhľadom na polohu občianskeho preukazu. To znamená, že sa na každom výreze snímky videa kontroluje, či pre danú polohu preukazu má ochranný prvok správnu farbu. Na modelovanie tohoto vzťahu sa skúsili použiť regresné modely a detekcia anomálií.

Aby sa odhalil prípad, kedy by používateľ občianskym preukazom vôbec nepohyboval, kontrola by mala zahŕňať tiež overenie, či bola na videu zachytená dostatočná zmena farby ochranného prvku. To znamená, že video obsahuje snímky a z nich zhotovené výrezy ochranného prvku, medzi ktorými sa farba prvku dostatočne odlišuje. Prakticky sa preskúmala zmena jasů ochranného prvku medzi výrezmi zo snímok videa.



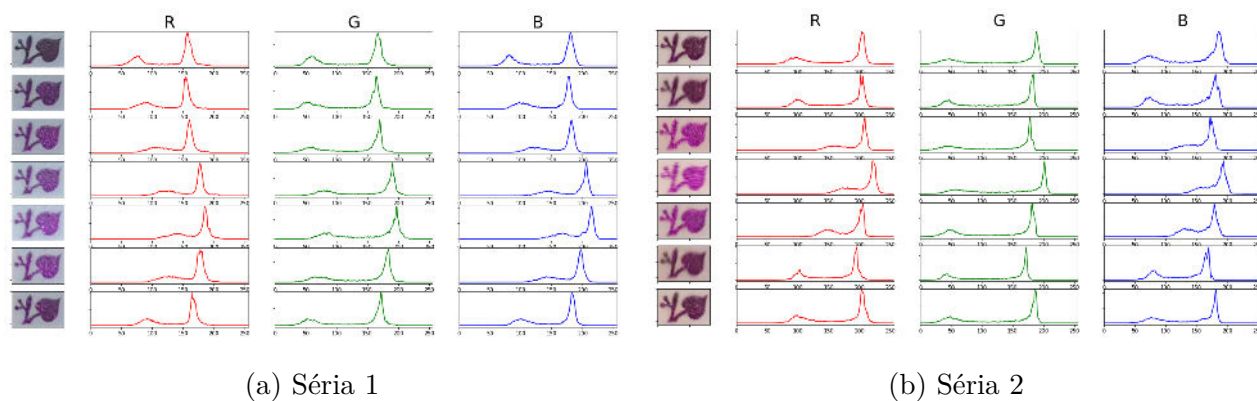
Obr. 3.31: Spôsoby overenia vizuálnych vlastností OVI ochranného prvku

3.6.1 Analýza farebnosti ochranného prvku

Farba a odlesk ochranného prvku sa mení v závislosti od pozície zdroja svetla a pozorovateľa voči pozícii ochranného prvku. Za predpokladu, že primárnym zdrojom svetla je blesk, sa analyzoval vzťah farby a pozície snímacieho zariadenia. Komplikáciou je vysoká variancia svetelných podmienok a snímacích zariadení, ktoré majú značný vplyv na farbu ochranného prvku na snímke.

V prvom kroku sa preskúmali histogramy sérií snímok. Použité snímky vznikli aplikovaním postupu na nájdenie ochranného prvku vo videách štvrtého datasetu, na ktorých bol občiansky preukaz horizontálne rotovaný z ľavej do pravej strany. Na obrázku 3.32 sú RGB histogramy dvoch sérií snímok staršieho ochranného prvku. Série boli snímané v mierne odlišných svetelných podmienkach a zariadeniami s rôznym bleskom, čo sa prejavilo aj na histogramoch, na všetkých troch farebných kanáloch. Hlavne červený kanál série 2 je výrazne posunutý ku vyšším hodnotám oproti sérii 1. Preto sa farby ochranných prvkov nedajú priamo porovnať, aj keď bol občiansky preukaz snímaný v rovnakej pozícii voči blesku. Riešením je vyváženie bielej farby na snímkach, alebo použitie takého farebného modelu, v ktorom nemá osvetlenie vplyv na niektoré jeho farebné kanály.

HSV farebný model oddeľuje farebnú informáciu od sýtosti a jasu. Histogramy sérií snímok staršieho ochranného prvku a jednej série novšieho prvku pre jednotlivé kanály HSV farebného modelu sú na obrázku 3.34. Pri skúmaní histogramov dvoch sérií snímok staršieho ochranného prvku, ktoré sú použité rovnaké ako pre obrázok 3.32, si je možné všimnúť, že hlavný posun

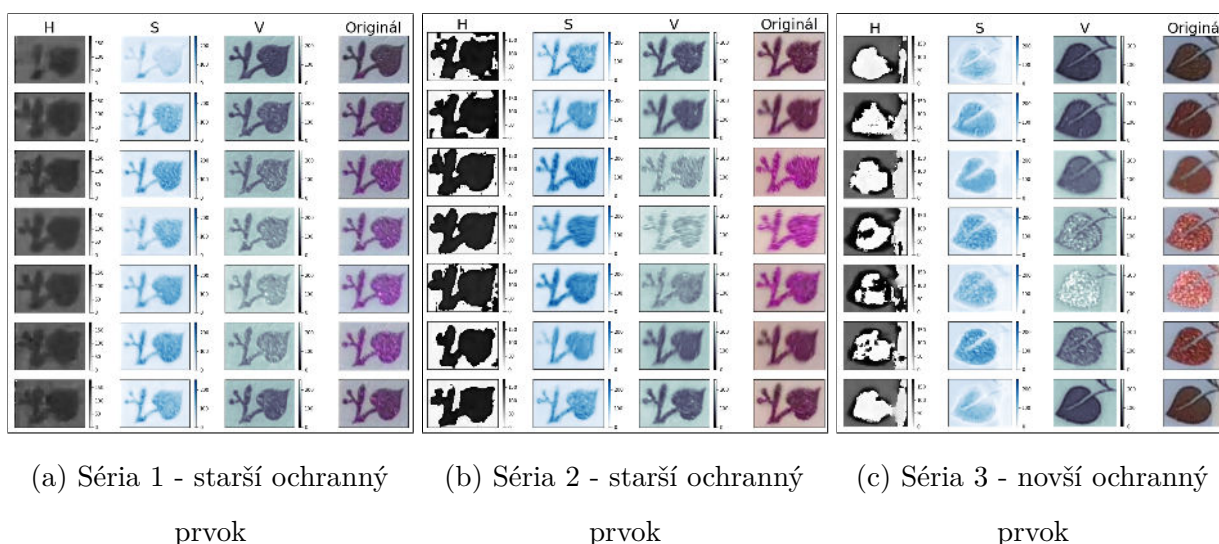


Obr. 3.32: RGB histogramy dvoch rôznych sérií obrázkov staršieho ochranného prvku

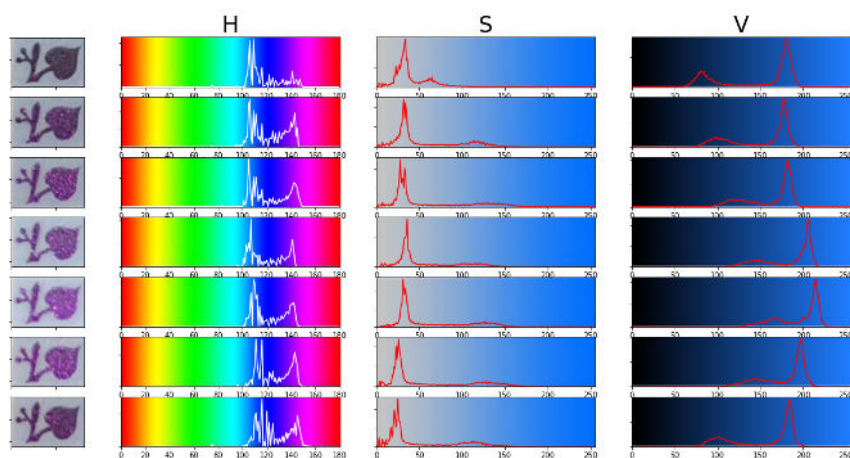
nastáva v zložke H, histogramy S a V sú podobné. To znamená, že zmena svetelných podmienok sa prejavuje hlavne na chromatickom H komponente, kde je farebné spektrum vychýlené voči vyváženiu bielej. Komponenty S a V je teda možné porovnávať medzi rôznymi sériami, aj bez normalizácie farby. Okrem HSV sa preskúmali histogramy HSL farebného modelu, ktoré sú veľmi podobné HSV histogramom, a teda sa v ďalšej analýze pokračuje s HSV modelom.

Na obrázku 3.33 sú heatmaps komponentov HSV, čiže zobrazenia jednotlivých farebných kanálov. Heatmapy sú skonštruované pre rovnaké snímky ochranných prvkov, ako sú histogramy na obrázku 3.34. Aj na základe heatmáp je možné usúdiť, že komponenty S a V sú porovnateľné. Odlesk a zmenu farby ochranného prvku zachytáva najlepšie komponent V, ktorý pre lesklejšie a jasnejšie farby nadobúda vyššie hodnoty.

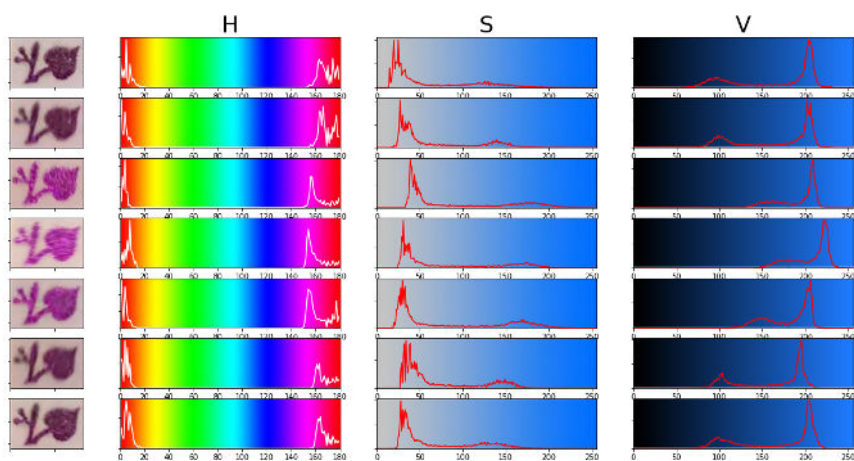
Nasledujúce navrhované metódy pracujú so snímkami ochranného prvku v HSV farebnej schéme, pričom sa zameriavajú na kontrolu komponentov S a V, ktoré sú menej citlivé na svetelné podmienky a vyváženie bielej farby na snímke. Kontrola farebného komponentu H je zložitejší problém, pri ktorého riešení je pravdepodobne nevyhnutné H zložku normalizovať. Ale pre kompletné overenie ho je v budúcnosti potrebné doplniť, pretože bez komponentu H sa vôbec nekontroluje odtieň farby. Jednou z možností je vytvoriť separátny model pre kontrolu farebnosti, čiže iba H komponentu. Druhou alternatívou je komplexnejší model, do ktorého vstupujú všetky tri HSV zložky.



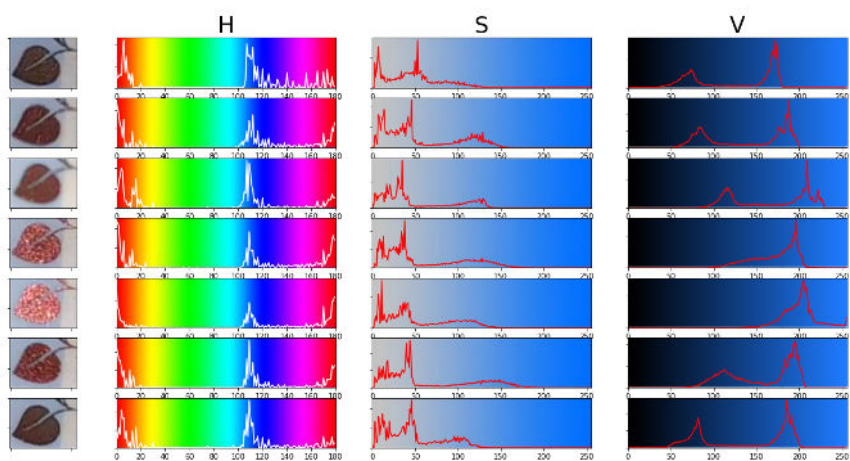
Obr. 3.33: HSV heatmaps sérií obrázkov ochranných prvkov



(a) Série 1 - starší ochranný prvok



(b) Série 2 - starší ochranný prvok



(c) Série 3 - novší ochranný prvok

Obr. 3.34: HSV histogramy sérií obrázků ochranných prvků

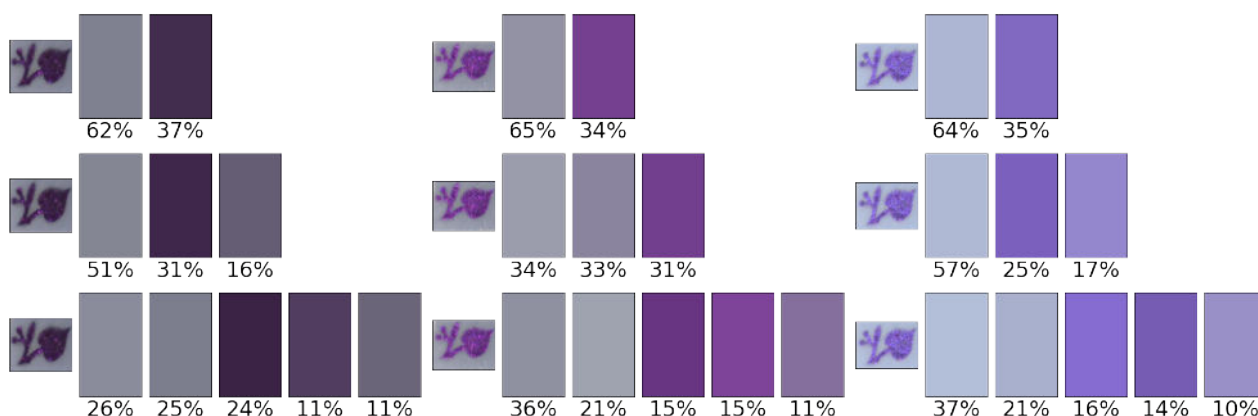
3.6.2 Reprezentácia farebnosti ochranného prvku na snímke

Farebnosť ochranného prvku na snímke je možné reprezentovať viacerými spôsobmi, na rôznej úrovni zjednodušenia vstupnej snímky. Najjednoduchším reprezentantom je jedna farba, ktorá ochrannému prvku dominuje. O niečo zložitejší je histogram farebných kanálov. V prípade týchto dvoch reprezentácií, čiže dominantnej farby a histogramu, sa zanedbáva priestorová informácia. Najviac informácií nesie 2D reprezentácia farebných komponentov pomocou heatmapy a reprezentácia samotnou snímkou ochranného prvku. V budúcnosti je možné zvážiť použitie sofistikovanejšej transformácie vstupných snímok aplikovaním signálneho spracovania obrazu.

Dominantná farba ochranného prvku

V práci sa preskúmala iba najjednoduchšia forma reprezentácie, čiže dominantná farba ochranného prvku. Na určenie dominantnej farby je použité zhľukovanie, konkrétne algoritmus K-means, implementovaný v knižnici Scikit-learn[36]. Vstupom do algoritmu je výrez s ochranným prvkom v RGB farebnom modeli. Reprezentanti zhľukov, ktorí sú vypočítaní ako priemerná farba pixlov zaradených do zhľuku, sú považovaní za dominantné farby snímky. V navrhovaných metódach overenia farebných charakteristík ochranného prvku sa pracuje s dominantnými farbami konvertovanými do HSV farebnej schémy.

Dominantné farby snímky sa radia do dvoch skupín, a to na farby ochranného prvku a na farby pozadia. Na obrázku 3.35 sú dominantné farby troch snímok s rôznym odtieňom staršieho ochranného prvku. Ku každej snímke sú vypočítané dominantné farby pre 2, 3 a 5 zhľukov. Pod dominantnou farbou je uvedené jej percentuálne zastúpenie na snímke. Na základe preskúmania dominantných farieb snímok z druhej verzie tretieho datasetu je možné usúdiť, ako vidieť aj na obrázku, že na oddelenie farby pozadia od farby ochranného prvku postačujú dva zhľuky. Farba ochranného prvku má na snímke väčšinou menšie zastúpenie a farba pozadia má vyššiu hodnotu modrého farebného kanálu B. Rovnaké závery platia aj pre novší typ ochranného prvku.

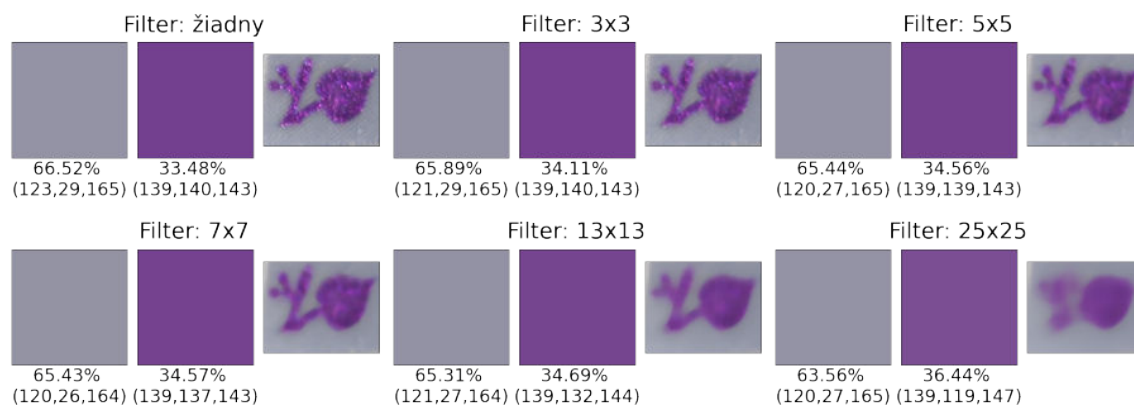


Obr. 3.35: Dominantné farby pre rôzny počet zhhlukov

Na obrázku 3.36 sú dominantné farby ochranných prvkov všetkých snímok tretieho datasetu. V každom riadku je jedna séria snímok, ktorá vznikla horizontálnou rotáciou občianskeho preukazu z ľavej do pravej strany. Na obrázku je možné pozorovať, že najjasnejšie sú ochranné prvky vždy na podobnej pozícii v rámci série, a teda existuje vzťah medzi farbou a pozíciou ochranného prvku. Fialové odtiene patria staršiemu typu ochranného prvku, ružové a hnedé novšiemu typu. V prípade priameho odrazu blesku vo výreze ochranného prvku je dominantná farba veľmi svetlá alebo až modrá, a teda nezachytáva skutočnú farbu ochranného prvku. Takýto typ snímky je nevyhnutné vylúčiť v predchádzajúcom kroku detekcie ochranného prvku, pretože na nej ochranný prvok nie je možné rozoznať.

V ďalšom experimente sa skúmal vplyv kvality snímky na výpočet dominantnej farby. Na snímku sa aplikoval mediánový filter rôznej veľkosti a pozorovala sa zmena dominantnej farby ochranného prvku. Výsledok pre jednu vybranú snímku je zachytený na obrázku 3.37. Pod dominantnou farbou je uvedené jej percentuálne zastúpenie a hodnota HSV. HSV zložky sa vplyvom filtra menia minimálne, a preto aj menej kvalitné alebo rozmazané snímky budú mať dominantnú farbu určenú správne.

Obr. 3.36:
Dominantné farby
séřií snímok

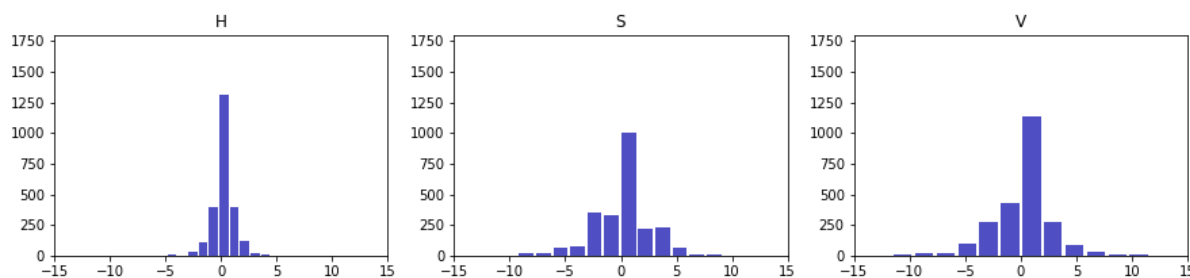


Obr. 3.37: Vplyv veľkosti filtra na dominantné farby

Spracovanie vstupného videa

Vstupom do metódy overenia pravosti ochranného prvku je video, čiže sekvencia snímok. Počet analyzovaných snímok závisí od dĺžky videa a nastavenia počtu snímok za sekundu, angl. frames per second (FPS). Pri veľmi veľkom počte snímok môže overenie trvať príliš dlho. Preto je vhodné zvážiť iba kontrolu každej n -tej snímky.

Na obrázku 3.38 sú histogramy rozdielov dominantných farieb po sebe nasledujúcich snímok vzorky videí štvrtého datasetu, pre každú HSV farebnú zložku. Rozdiely v hodnote H sú z rozsahu od -5 do 5, pričom H môže nadobudnúť hodnoty z intervalu $(0, 180)$. Komponenty S a V sa líšia o -10 až 10, a ich hodnoty sú z intervalu $(0, 255)$. Rozsahy hodnôt súvisia s použitím knižnice OpenCV[20], ktorá ich takto definuje, ale iné knižnice môžu pracovať s inými rozsahmi. Na základe histogramov je možné nájsť kompromis, koľko za sebou nasledujúcich snímok v sekvencii je možné vynechať, aby sa nestratili dôležité farebné zmeny, a súčasne bol proces overenia dostatočne rýchly. Pri testovaní metód sa brala do úvahy každá piata snímka.



Obr. 3.38: Histogram rozdielov za sebou nasledujúcich snímok videa

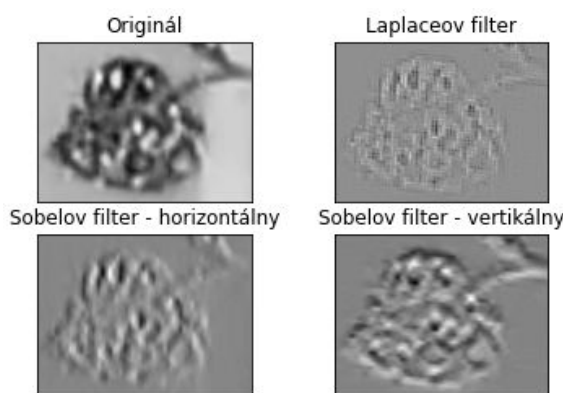
3.6.3 Overenie odlesku ochranného prvku

Dôležitou vlastnosťou OVI ochranného prvku je, že sa leskne. Dôvodom sú trblietavé mikroskopické pigmenty, z ktorých je OVI farba zložená. Na overenie odlesku je možné navrhnúť viacero metód a prístupov. Odlesk sa overuje jednotlivo na každom výreze ochranného prvku. Cieľom nie je odhaliť falošné výrezy ochranných prvkov, ale hlavne vylúčiť chybné výrezy, na ktorých sa ochranný prvok nenachádza.

Jednou z možností je sledovanie množstva rôznych farieb ochranného prvku. Na histogramoch obrázka 3.34 je možné pozorovať, že farebný komponent H nemá dva vrcholy, jeden pre farbu ochranného prvku a druhý pre farbu pozadia, ale väčší počet malých vrcholov. To znamená, že na relatívne malej ploche je zachytené veľké množstvo rôznych farieb. Je to spôsobené tým, že od farebných pigmentov OVI farby sa odráža rôzne spektrum svetla a rôznymi smermi. Požiadavka teda môže byť formulovaná tak, že na snímke musí byť zachytený dostatočný počet rôznych farieb, čiže dostatočný počet vrcholov histogramu. Táto metóda overenia nebola v tejto práci prakticky preskúmaná.

Overenie pomocou detekcie hrán

Detekcia hrán je ďalším možným prístupom k overeniu odlesku ochranného prvku. Na obrázku 3.39 sú porovnané výstupy troch hranových filtrov po aplikovaní na snímku ochranného prvku. Odlesky sú na čiernobielej snímke zachytené ako väčšie množstvo krátkych čiar, a teda by potenciálne mohli byť použité na detekciu a kvantifikovanie odlesku.



Obr. 3.39: Hranové filtre

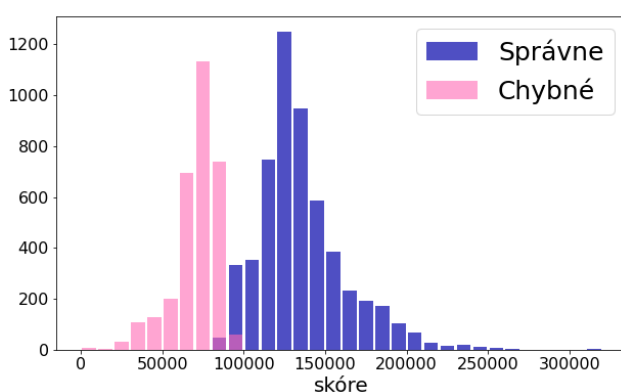
Pre ďalšiu analýzu sa vybral Laplaceov filter. Zdefinovalo sa hranové skóre, ktoré je vypočítané zo výstupného obrázka po použití filtra. Skóre vyjadruje mieru odlesku na základe množstva hrán. Je vypočítané ako súčet absolútnych rozdielov susedných pixelov obrázka a sumarizuje ho nasledovný vzorec:

$$\text{skóre}(X) = \sum_{i=1}^{M-1} \sum_{j=1}^{N-1} |X_{i,j} - X_{i+1,j+1}| \quad (3.2)$$

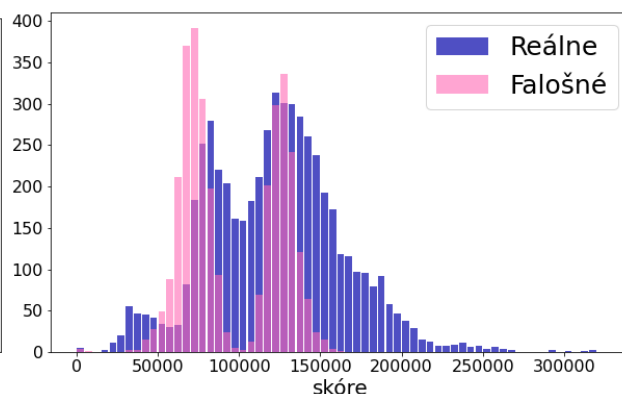
kde X je výstup z hranového filtra, ktorý bol aplikovaný na výrez snímky s ochranným prvkom o rozmere $M \times N$.

V experimente sa testovalo hranové skóre na výrezoch s ochranným prvkom, ktoré vznikli ako výstup metód detekcie ochranného prvku na videách štvrtého a piateho datasetu. Histogram na obrázku 3.40 úspešne oddeľuje správne a nesprávne detekované snímky ochranných prvkov, pričom hraničná hodnota hranového skóre je približne 100 000. Hranové skóre teda môže byť použité na vylúčenie chybných snímok, ktoré sú výstupom niektorej metódy detekcie ochranného prvku.

Porovnanie reálnych a falošných občianskych preukazov je na histograme obrázka 3.41. Obidva typy dokladu majú na histograme dva vrcholy s podobnou hodnotou skóre. To znamená, že hranové skóre nedokáže separovať reálne a falošné ochranné prvky. Napríklad, ak je ako predloha falošného občianskeho preukazu použitá kvalitná fotografia, na ktorej sa ochranný prvok leskne, odlesk je na snímke detekovaný a ohodnotený vysokým skóre.



Obr. 3.40: Porovnanie skóre správnych a chybných výrezov snímok



Obr. 3.41: Porovnanie skóre reálnych a falošných občianskych preukazov

Využitie detekcie odlesku pri hľadaní ochranného prvku

Navrhované metódy detekcie ochranného prvku pomocou keypointov alebo Template Matching majú svoje výhody aj nevýhody. Ich kombináciou je možné niektoré nedostatky minimalizovať alebo úplne odstrániť. Detekcia keypointov je použitá na určenie typu ochranného prvku. Z výstupov metódy Template Matching sú vybrané iba tie výrezy, na ktorých bol detekovaný daný typ ochranného prvku. Pre nasledujúci krok overenia vizuálnych vlastností ochranného prvku je veľmi dôležité, aby bola detekovaná pozícia prvku správna. Preto je vhodné zvážiť vylúčenie takých výrezov z analýzy, ktoré majú oproti ostatným oveľa horšie skóre. Okrem toho je možné doplniť ďalšie metódy na vyradenie zle detekovaných výrezov snímok, napríklad overenie odlesku pomocou popísanej detekcie hrán.

Ak do metódy postupne vstupujú výrezy pravého horného rohu normalizovaného občianskeho preukazu zo sekvencie snímok videa, tak navrhovaný postup je možné zhrnúť nasledovne. Metóda Template Matching označí na snímke pozíciu, ktorá je najpodobnejšia šablóne, a vznikne výrez s ochranným prvkom. Súčasne sa pomocou detekcie keypointov pokúsi určiť typ symbolu. Na záver, po prejdení všetkých vstupov, sa odstránia výrezy s nesprávnym typom prvku alebo výrezy s nízkym hranovým skóre.

Navrhovaná kombinácia metódy Template Matching, detekcie keypointov a detekcie hrán bola otestovaná na videách štvrtého a piateho datasetu, čiže reálnych a falošných občianskych preukazoch. Výsledky sú zhrnuté v tabuľke 3.5. Detekcia ochranných prvkov bola veľmi úspešná, pretože prioritou je do ďalšej analýzy posunúť iba tie snímky, ktoré sú s veľkou istotou správne. Z toho dôvodu boli mnohé snímky vylúčené, aj napriek správne detekovanému ochrannému prvku. Približne 75% všetkých vylúčených snímok bolo správnym výrezom ochranného prvku.

Pre 37 falošných testovacích videí z piateho datasetu nebol ani na jednej snímke detekovaný výrez ochranného prvku. To znamená, že už detektor odhalil falošné snímky tým, že na nich nedokázal nájsť občiansky preukaz alebo ochranný prvok. Videá sú preto správne označené ako falošné, ešte pred vstupom do analýzy vizuálnych vlastností ochranného prvku.

Tabuľka 3.5: Úspešnosť detekcie ochranného prvku

	reálne	falošné	spolu
správna detekcia	4128	1388	5516
chybná detekcia	2	5	7
úspešnosť	99,95%	99,64%	99,87%

Na obrázku 3.42 je príklad nesprávne určenej polohy ochranného prvku, ktorý úspešne prešiel všetkými krokmi detekcie. Chybnú detekciu ovplyvnilo viacero faktorov. Snímka je veľmi tmavá, ochranný prvok je mierne deformovaný a na snímke je posunutý viac doprava a nahor. Posun je spôsobený odchýlkou pri normalizácii občianskeho preukazu. Odchýlka a deformácia môžu nastať napríklad v prípade, ak je občiansky preukaz snímaný v príliš veľkom uhle oproti kamere alebo ak falošný občiansky preukaz nie je úplne rovný, ale mierne prehnutý.

Keďže pre analýzu farby je dôležité, aby do nej nevstupovali chybné výrezy snímok, detekcia hrán vylúčila aj mnohé snímky so správne nájdeným ochranným prvkom. Na obrázku 3.43 je chybný výrez ochranného prvku, ktorý má nízke hranové skóre, a preto je opodstatnene vylúčený z ďalšej analýzy. Obrázok 3.44 zachytáva opačnú situáciu, kedy je z viditeľne nekvalitnej snímky vybraný síce správny výrez, ale je ohodnotený nízkym skóre. Tento typ chyby nastáva väčšinou pri nekvalitných, rozmazaných alebo presvetlených snímkach, kedy vlastne ochranný prvok aj tak nemá zodpovedajúce vizuálne vlastnosti.



Obr. 3.42: Vysoké hranové skóre - chybný výrez



Obr. 3.43: Nízke hranové skóre - chybný výrez



Obr. 3.44: Nízke hranové skóre - správny výrez

3.6.4 Overenie farby vzhľadom na polohu občianskeho preukazu

Farba OVI ochranného prvku sa mení so zmenou polohy voči snímaciemu zariadeniu s bleskom. Ako bolo pozorované na obrázku 3.36, existuje vzťah medzi pozíciou občianskeho preukazu a dominantnou farbou ochranného prvku. Iné reprezentácie farby zatiaľ neboli prakticky preskúmané. Z dominantnej farby sa používajú iba hodnoty farebných kanálov S a V farebného modelu HSV. Dôvod vynechania H hodnoty je vysvetlený v oddieli 3.6.1.

Poloha občianskeho preukazu je reprezentovaná transformačnou maticou typu 3×3 , ktorá popisuje jeho perspektívnu transformáciu voči normalizovanej polohe. Transformačná matica je relatívne komplikovaná, a preto je do budúcnosti vhodné zvážiť použitie nejakej vhodnej modifikácie, napríklad extrahovať Eulerove uhly a pod.

Opticky variabilná farba OVI má pre dva typy ochranných prvkov odlišné farebné charakteristiky. Preto musia byť prvky skúmané samostatne a pre všetky navrhnuté modely by mali existovať dve verzie, jedna pre každý typ symbolu.

Overenie pomocou regresie

Cieľom aplikovania regresie je odhad obrazovej informácie, primárne farebnosti, na základe pozície občianskeho preukazu. S využitím regresie sa skúmala závislosť medzi polohou a dominantnou farbou ochranného prvku. Vyskúšali sa nasledujúce kombinácie vstupov a výstupov:

1. Vstup: Transformačná matica Výstup: V
2. Vstup: Transformačná matica, S Výstup: V
3. Vstup: Transformačná matica Výstup: S, V

Uvedené kombinácie vstupov a výstupov sa porovnali na menšej vzorke dát, pričom ich výsledky boli veľmi podobné. Aby boli do modelu zakomponované obidva farebné komponenty S a V, sa pre ďalšiu analýzu vybrala druhá možnosť, v ktorej je na vstupe transformačná matica spolu s komponentom S a výstupom je hodnota V. Čiže model odhaduje hodnotu komponentu V dominantnej farby na základe transformačnej matice a komponentu S.

Ako trérovacie dáta sú použité dlhšie videá natočené v rôznych svetelných podmienkach a s rôznou farbou pozadia. Pre každý typ symbolu sú zvolené tri reprezentatívne videá, na ktorých je pravý občiansky preukaz zachytený v rôznych pozíciách, vzdialenostiach a uhloch natočenia voči snímaču.

Modely sú testované na videách štvrtého a piateho datasetu, s reálnymi a falošnými občianskymi preukazmi. Na snímkach videa je najskôr nájdený občiansky preukaz, pre každú snímku je vypočítaná transformačná matica, pomocou ktorej je občiansky preukaz následne normalizovaný. Ďalej je z normalizovaného preukazu pomocou detekcie ochranného prvku urobený výrez s ochranným prvkom. Z výrezu je vypočítaná jeho dominantná farba, ktorá sa prevedie do HSV farebnej schémy. Do regresnej analýzy ďalej vstupuje iba transformačná matica a dominantná HSV farba ochranného prvku.

Komponent V nadobúda hodnoty z rozsahu $(0, 255)$. Vo výsledku sa pre video vypočítajú dva typy chyby odhadu hodnoty V . Maximálna chyba je maximálny rozdiel skutočnej a odhadovanej hodnoty V na analyzovaných snímkach videa. Priemerná chyba je aritmetický priemer z absolútnych rozdielov skutočnej a odhadovanej hodnoty V . Chyby sú vypočítané na základe nasledujúcich vzorcov 3.3 a 3.4, kde N je počet analyzovaných snímkov videa.

$$\max \text{ chyba} = \max_{i=1..N} (|V_{real_i} - V_{odhad_i}|) \quad (3.3)$$

$$\text{priemerná chyba} = \frac{1}{N} \sum_{i=1}^N (|V_{real_i} - V_{odhad_i}|) \quad (3.4)$$

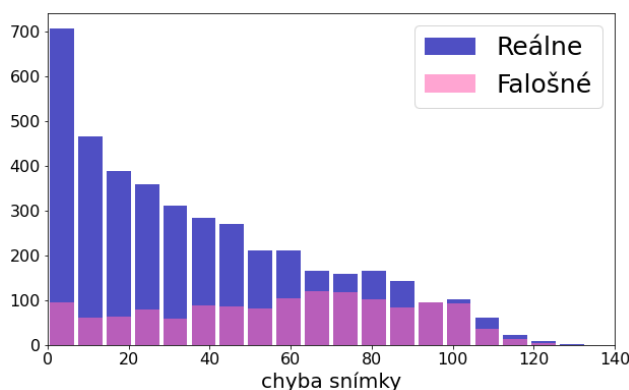
Na falošných občianskych preukazoch je farba ochranného prvku relatívne statická. Malé zmeny sú spôsobené vlastnosťami snímača, osvetlením alebo odrazom svetla od povrchu falošného občianskeho preukazu. Vo výsledku treba brať do úvahy, že existujú pozície, v ktorých sa farba falošného ochranného prvku zhoduje so skutočnou farbou prvku v tejto pozícii. A teda na istej časti snímkov videa s falošným občianskym preukazom je ochranný prvok považovaný za pravý.

Tabuľka 3.6: Porovnanie regresných modelov

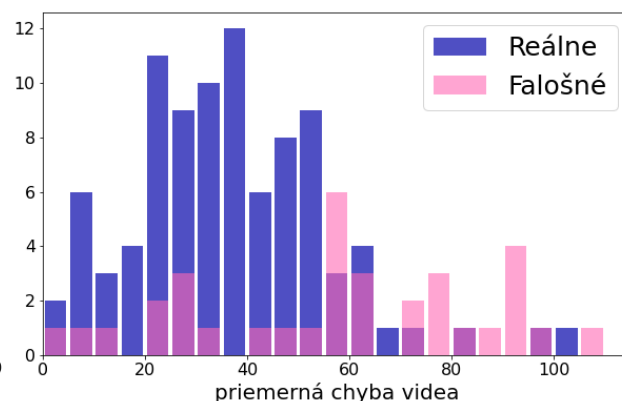
	reálny prvok		falošný prvok	
	priemerná chyba	max chyba	priemerná chyba	max chyba
Bayesian Ridge Regression	59,04	406,29	161,91	486,60
CatBoost Regressor	37,68	130,82	67,98	125,41
Elastic Net Regression	61,35	454,51	173,45	543,63
Gradient Boosting Regression	34,79	130,55	57,31	157,80
Kernel Ridge Regression	68,26	498,74	209,88	588,26
LGBM Regressor	35,43	131,31	59,34	163,08
Linear Regression	56,67	349,83	57,28	391,96
SVM	42,68	123,59	76,01	122,51
SGD Regression	56,96	338,77	64,11	394,43
XGBoost Regressor	37,77	136,78	68,93	171,83

V tabuľke 3.6 sú uvedené výsledky desiatich rôznych regresných modelov, ktoré podľa článku [2] patria medzi najpopulárnejšie. Modely sú použité z knižnice Scikit-learn[39, 38, 37, 41], LightGBM[14], XGBoost[51] a CatBoost[6]. Chyby modelov sú porovnané pre reálne a falošné občianske preukazy, pričom sa brali do úvahy snímky všetkých videí. Vzhľadom na priemernú a maximálnu chybu regresie pre reálne občianske preukazy, sú označené ako najlepšie regresné modely CatBoost Regressor, Gradient Boosting Regression, LGBM Regressor, SVM a XGBoost Regressor. Po zhodnotení výsledkov aj pre falošné občianske preukazy sa pre ďalšiu analýzu vybral CatBoost Regressor.

V ďalšom experimente sa testoval zvolený regresný model CatBoost Regressor a jeho schopnosť separovať reálne snímky a videá od falošných. Na histograme obrázka 3.45 je zachytená chyba odhadu hodnoty V pre všetky analyzované snímky videí štvrtého a piateho datasetu. Počet reálnych snímkov klesá so zvyšujúcou sa chybou. Lenže falošné snímky nemajú evidentne vyššiu chybu ako pravé. Z histogramu sa nedá určiť hranica veľkosti chyby, ktorá by dokázala oddeliť falošné a reálne snímky.



Obr. 3.45: Chyba regresie pre každú snímku



Obr. 3.46: Priemerná chyba regresie videí

Na obrázku 3.46 je histogram priemerných chýb videí štvrtého a piateho datasetu. Podobne ako na histograme 3.45, veľký počet pravých aj falošných videí má nízku hodnotu priemernej chyby. Z toho dôvodu je možné uzavrieť, že videá nie je možné separovať podľa priemernej chyby odhadu komponenta V, ktorá je vypočítaná v závislosti od transformačnej matice a komponenta S.

Na základe výsledkov sa usúdilo, že takto definovaný regresný model nedokáže samostatne odlíšiť reálne občianske preukazy od falošných, na samostatných snímkach ani na celých videách. Ale vzhľadom na to, že vo výsledkoch v tabuľke 3.6 je priemerná chyba reálnych občiansky preukazov nižšia ako falošných pre všetky regresné modely, možno inak formulovaný regresný problém by mohol byť úspešnejší. Zlepšiť výsledky by mohla vhodnejšia forma vstupných dát, iný spôsob ohodnotenia výsledkov, napr. iný výpočet chyby, doplnenie tréningových dát alebo kombinácia s ďalším typom modelu.

Detekcia anomálií

Detekcia anomálií, podobne ako regresia, skúma vzťah pozície a dominantnej HSV farby ochranného prvku. Ale je formulovaná ako klasifikačný problém, pričom klasifikuje ochranné prvky na pravé alebo falošné. Nesprávna kombinácia dominantnej farby a polohy občianskeho preukazu je považovaná za anomáliu. Preskúmali sa nasledovné typy vstupov:

1. Vstup: Transformačná matica, V
2. Vstup: Transformačná matica, S , V

Dva druhy vstupov boli porovnané na menšej vzorke dát, na ktorej mali podobné výsledky. Pre zapojenie obidvoch farebných komponentov S a V , sa pre ďalšie experimenty vybral druhý typ vstupu, čiže transformačná matica s komponentami S a V .

Ako trénovacie dáta sú použité rovnaké videá ako v regresných modeloch popísaných vyššie v tomto oddieli. Do tréningu sú zapojené iba pravé občianske preukazy. Na ohodnotenie výsledkov sa používajú tri metriky: celková správnosť (angl. accuracy), senzitivita (angl. recall) a presnosť (angl. precision). Metriky sú počítajú podľa nasledujúcich vzťahov:

$$\text{celková správnosť} = \frac{TP + TN}{TP + FP + TN + FN} \quad (3.5)$$

$$\text{senzitivita} = \frac{TP}{TP + FN} \quad (3.6)$$

$$\text{presnosť} = \frac{TP}{TP + FP} \quad (3.7)$$

kde TP je počet pravých prvkov určených ako pravé, FP počet falošných prvkov určených ako pravé, TN počet falošných prvkov určených ako falošné a FN je počet pravých prvkov určených ako falošné. Hodnoty TP , FP , TN a FN sa často zapisujú do tabuľky, ktorá sa nazýva matica zámen.

Porovnali sa tri modely detekcie anomálií: Isolation Forest, Local Outlier Factor a One Class SVM. Metódy sú použité z knižnice Scikit-learn[40]. Úspešnosť modelov, čiže celková

Tabuľka 3.7: Porovnanie detektorov anomálií

	novší reálny prvok	starší reálny prvok	novší falošný prvok	starší falošný prvok
Isolation Forest	12,63%	27,40%	97,44%	99,30%
Local Outlier Factor	24,85%	37,62%	92,00%	99,40%
One Class SVM	7,39%	13,00%	98,06%	99,90%

Tabuľka 3.8: Matica zámen detektora anomálií

Local Outlier Factor

	odhad reálny	odhad falošný
skutočne reálny	1210	2920
skutočne falošný	127	1266

Tabuľka 3.9: Výsledky detektora anomálií

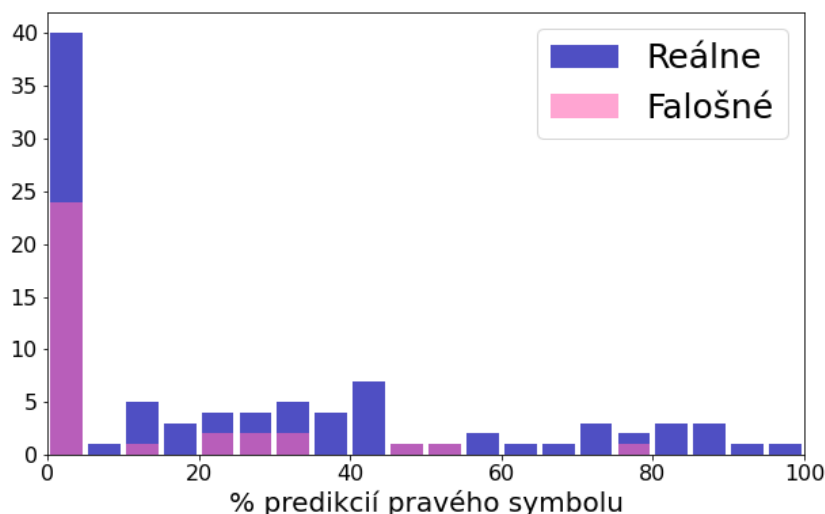
Local Outlier Factor

celková správnosť	44,83%
senzitivita	29,30%
presnosť	90,50%

správnosť, je uvedená v tabuľke 3.7, kde je porovnaná pre reálny a falošný ochranný prvok, a tiež starší a novší typ symbolu.

Modely majú veľmi nízku úspešnosť na reálnych občianskych preukazoch, pretože väčšinu vstupných snímok označujú za anomálie. Z toho dôvodu sú oveľa efektívnejšie na falošných občianskych preukazoch. Pre ďalšiu analýzu sa vybral Local Outlier Factor, ktorý má najvyššiu úspešnosť na reálnych ochranných prvkoch.

S detektorom anomálií Local Outlier Factor sa urobil podobný experiment ako s regresným modelom, v ktorom je klasifikátor otestovaný na videách štvrtého a piateho datasetu. V prvej časti experimentu detektor klasifikoval všetky analyzované snímky. Výsledná matica zámen je v tabuľke 3.8 a z nej vypočítané metriky sú zapísané vo vedľajšej tabuľke 3.9. Aj po podrobnejšom preskúmaní klasifikátora, z výsledkov vyplývajú rovnaké závery ako z tabuľky 3.7, a to že väčšinu snímok označuje za falošné. Klasifikátor je málo senzitívny, ale presný, a jeho celková úspešnosť je nižšia ako 50%.



Obr. 3.47: Pomer snímok vo videu označených ako reálne

Na obrázku 3.47 je histogram, ktorý vyjadruje, akú časť snímok vstupného videa klasifikátor určil za pravé. Pre väčšinu videí, reálnych aj falošných, označil skoro všetky snímky ako falošné, čiže podiel reálnych snímok vo videu je blízky 0%. Podľa klasifikátora iba malý počet videí obsahuje viac ako 50% snímok pravých ochranných prvkov. Detektor sa nedokázal naučiť vzťah polohy a farby, hlavne kvôli veľkej variancii dát na vstupe. Preto takto formulovaný model detekcie anomálií nie je použiteľný na odlíšenie falošných a pravých ochranných prvkov.

Doteraz sa skúmal iba vzťah pozície konkrétnej snímky a farby ochranného prvku. To znamená, že každá snímka sa overuje osobitne, a nie video ako celok. V rámci ďalšieho výskumu by sa ako vstup do modelu mohlo uvažovať celé video, ktoré je transformované do jedného bodu v latentnom priestore. Do komplexnejšieho modelu by sa pravdepodobne dal zakomponovať aj komponent H farebnej schémy HSV. Na takto definovanom priestore by mohol byť detektor anomálií oveľa úspešnejší.

3.6.5 Overenie dostatočnej zmeny farby ochranného prvku

V prípade, ak by používateľ na videu občianskym preukazom vôbec nepohyboval a jeho poloha by teda bola statická, predchádzajúce overenia by mohli aj falošný občiansky preukaz označiť za pravý. Napríklad, ak by bol na fotografii, ktorá sa prehlasuje za reálny občiansky preukaz, zachytený lesknúci sa ochranný prvok, a video je snímané v rovnakej pozícii, ako vznikla daná fotografia. V tomto prípade by falošné video úspešne prešlo kontrolou odlesku a aj vzťah pozície a farby by vyhovoval. Ale aj v prípade pohybujúceho sa falošného občianskeho preukazu, na videu môžu byť zaznamenané menšie zmeny dominantnej farby ochranného prvku spôsobené osvetlením, vlastnosťami snímača alebo odrazom svetla od povrchu falošného občianskeho preukazu. Preto je nevyhnutné overiť, či je na videu zachytená dostatočná zmena farby ochranného prvku.

Zmena jasů ochranného prvku

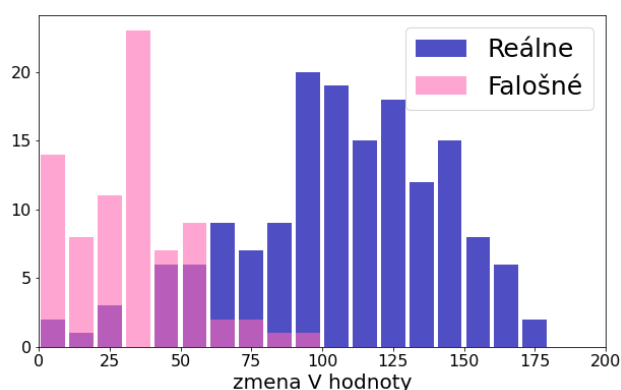
Jedným z možných prístupov overenia zmeny farby ochranného prvku je kontrola, či v jeho dominantnej farbe nastal dostatočný svetelný rozdiel. Z dôvodu vplyvu svetelných podmienok na farbu ochranného prvku, nie je možné porovnávať absolútne hodnoty farieb, ale len sledovať relatívnu zmenu v jednotlivých komponentoch. Ako je uvedené v oddieli 3.6.1, zmenu farby ochranného prvku najlepšie zachytáva komponent V farebného modelu HSV. Preto najjednoduchším spôsobom overenia dostatočnej zmeny farby ochranného prvku je overenie zmeny jasů, čiže hodnoty V , jeho dominantnej farby.

Vstupom do navrhovanej metódy sú dominantné farby ochranného prvku z analyzovaných snímok videa. Zo všetkých farieb sa vypočíta minimálna a maximálna nadobudnutá hodnota komponentu V . Rozdiel medzi minimálnou a maximálnou hodnotou V reprezentuje celkovú zmenu jasů ochranného prvku na videu. Ak je zmena jasů dostatočne veľká, farba, a teda aj poloha ochranného prvku sa na videu mení.

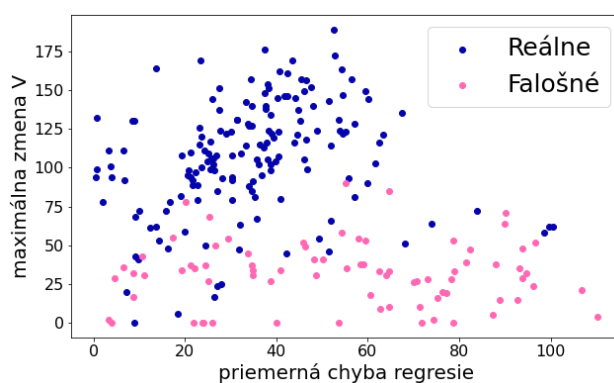
Na obrázku 3.49 je histogram zmeny jasů pre reálne a falošná videá. Zmena jasů falošných videí je viditeľne menšia ako reálnych. A po preskúmaní reálnych videí s nízkou zmenou jasů sa zistilo, že na danom videu skutočne nebola zachytená dostatočná zmena farby, a teda aj polohy občianskeho preukazu. Na základe histogramu je možné stanoviť hraničnú hodnotu zmeny jasů,

čiže minimálny akceptovaný rozdiel medzi najnižšou a najvyššou hodnotou komponentu V. To znamená, že na základe celkovej zmeny jasu videa je možné odlišiť pravé a falošné ochranné prvky.

Na grafe na obrázku 3.49 je vzťah priemernej chyby regresie CatBoost Regressora a zmeny jasu. Pre reálne občianske preukazy, väčšia zmena jasu znamená viac zachytených zložitejších polôh, ktoré je potrebné overiť, a preto aj vyššiu chybu regresie. Na falošných videách sa farba ochranného prvku mení minimálne, preto zmena jasu zostáva rovnaká aj pri vyššej hodnote chyby regresie.



Obr. 3.48: Zmena jasu videí
(hodnoty V)



Obr. 3.49: Vzťah priemernej chyby regresie a
maximálnej zmeny hodnoty V

Reprezentanti množiny snímok

Existujú dve možnosti, ako analyzovať vizuálne vlastnosti ochranného prvku na videu, a to buď na každej snímke alebo na podmnožine snímok. Doteraz popísané metódy zohľadňovali každú snímku videa samostatne. Alternatívou je podmnožina snímok vybraná tak, že reprezentuje celú množinu snímok, a súčasne sú jej reprezentanti dostatočne odlišní. Reprezentanti môžu byť teoreticky následne použitý na určenie diverzity množiny snímok, a tým overiť dostatočnú zmenu farby ochranného prvku na videu. V tejto časti práce preskúmame len spôsoby vytvorenia reprezentantov, a nie overenie farebnej zmeny.

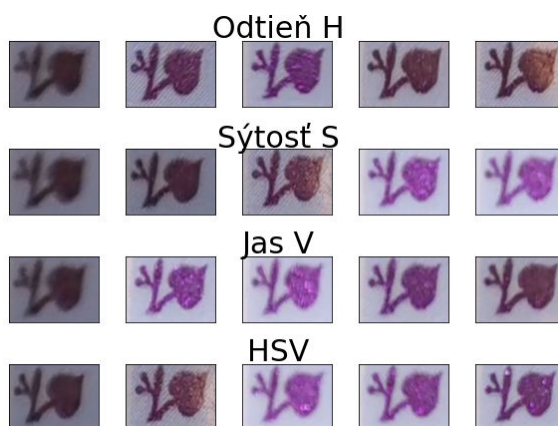
Reprezentantov je možné vybrať viacerými spôsobmi. Cieľom je, aby boli čo najviac rôznorodí, čiže aby mali čo najunikátnejšie dominantné farby. Najjednoduchší postup zvolí

za reprezentanta každú n -tú snímku videa. Iný spôsob výberu je pomocou hrubej sily. Ako prvý reprezentant sa zvolí náhodná snímka, a zvyšní sú vybraní tak, aby boli čo najodlišnejší od už vybraných reprezentantov. Tento postup nie je exaktný a pravdepodobne nezvolí najrôznorodejšie snímky. Sofistikovanejším riešením môže byť napríklad použitie niektorého zhlukovacieho algoritmu.

Prakticky sa preskúmal výber reprezentantov zhlukovaním, pričom sa porovnali zvolení reprezentanti podľa algoritmu K-means a podľa algoritmu DBSCAN. Metódy sú použité z knižnice Scikit-learn[36]. Ak sú snímky reprezentované dominantnou farbou ochranného prvku v HSV farebnom modeli, potom existuje niekoľko možností kombinácie vstupov do zhlukovacieho algoritmu. V práci boli preskúvané komponenty H, S, V jednotlivo, a celá HSV farba.

Pre algoritmus K-means ju nutné vopred definovať výsledný počet zhlukov. To môže byť výhodou aj nevýhodou, v závislosti od metódy použitej na ohodnotenie odlišnosti reprezentantov. Vstupom do algoritmu sú snímky reprezentované dominantnou farbou ochranného prvku. Výstupom je rozdelenie snímok do zhlukov, pričom ako reprezentant zhluku môže byť vybraná taká snímka, ktorá má najkratšiu vzdialenosť dominantnej farby k jeho centru. Centrum zhluku je klasicky vypočítané ako priemer snímok zhluku, čiže jeho priemerná dominantná farba.

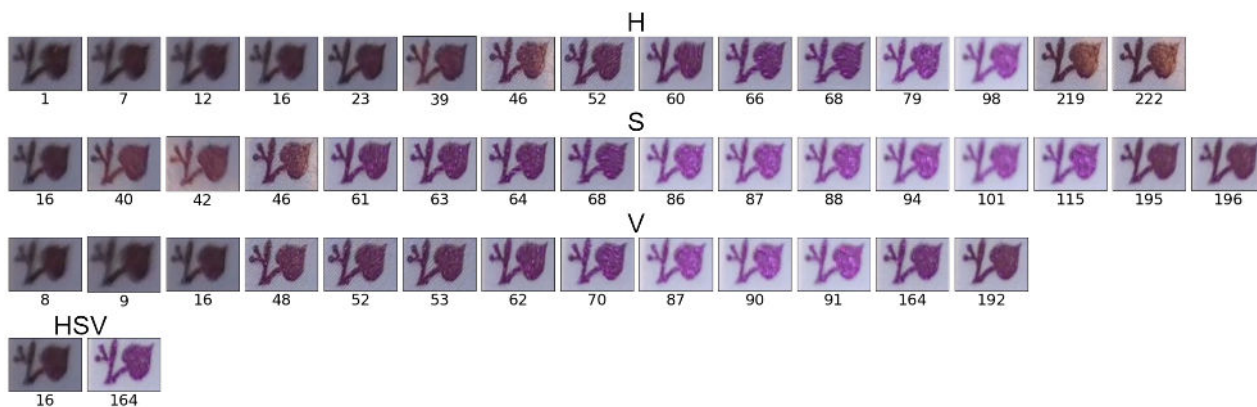
Na obrázku 3.50 sú reprezentanti zvolení zo sekvencie 200 snímok videa štvrtého datasetu podľa algoritmu K-means. V každom riadku je päť reprezentantov určených na základe jedného z komponentov alebo celej HSV farby. Reprezentanti sa medzi rôznymi vstupmi líšia, pretože každý komponent zachytáva inú vlastnosť farby ochranného prvku.



Obr. 3.50: Reprezentanti K-means podľa rôznych komponentov HSV ($k=5$)

Algoritmus DBSCAN sám odvodí počet zhlukov na základe vstupných dát, čiže sa ich počet medzi rôznymi vzorkami mení. Cieľom v tejto časti je nájsť reprezentantov, ktorí ale týmto algoritmom nie sú definovaní, preto sa za týmto účelom nedá použiť. Ale preskúmanie jeho výstupov, rozdelenia snímok a počtu zhlukov, môže priniesť nápady na návrh iných prístupov k overeniu zmeny farby ochranného prvku na videu.

V rámci analýzy výstupov algoritmu DBSCAN vznikol obrázok 3.51. V riadkoch sú zástupcovia zhlukov podľa jednotlivých komponentov H, S a V, a v poslednom riadku podľa celej dominantnej farby HSV. Keďže algoritmus nedefinuje reprezentantov, zástupcovia sú vybraní ako prvá snímka priradená do zhliku. Pre celú farbu DBSCAN určil iba dva zhluky, ale pre samostatné komponenty niekoľkonásobne vyšší počet zhlukov. Pod snímkami je uvedené ich poradové číslo, na základe čoho sa dá konštatovať, že zástupcovia sú medzi riadkami rôzni. Výstupy algoritmu pre rôzne vstupné komponenty sa teda líšia v počte zhlukov aj prerozdelení snímok. Podľa počtu zhlukov vo výsledku by sa mohlo napríklad vyhodnotiť, ktorý farebný komponent je najviac variabilný. V príklade na obrázku 3.51 by to bol komponent S, ktorý reprezentuje sýtosť farby.



Obr. 3.51: Reprezentanti DBSCAN podľa rôznych komponentov HSV

Prakticky sa preskúmali iba rôzne spôsoby vytvorenia reprezentantov na základe dominantnej farby výrezov ochranných prvkov. V prípade, ak reprezentanti budú použitý na overenie dostatočnej zmeny farby ochranného prvku, pravdepodobne nebude postačovať porovnávať len ich dominantné farby. S dominantnou farbou by mohla byť použitá aj transformačná matica alebo iná reprezentácia polohy, pričom všetky vstupné hodnoty budú mať priradené vhodné váhy.

Sofistikovanejšie riešenie by mohlo pracovať s celým výrezom ochranného prvku. Dôležitým parametrom takto navrhutej metódy je miera, ktorá meria odlišnosť snímok. Najpoužívanjšou mierou je euklidovská vzdialenosť, ktorá sa počíta nasledovne:

$$d(X, Y) = \sqrt{\sum_{i=1}^N \sum_{j=1}^M (X_{i,j} - Y_{i,j})^2} \quad (3.8)$$

kde X a Y sú posudzované obrázky o rozmere $N \times M$. Miery, ktoré porovnávajú snímky po jednotlivých pixeloch, nie sú veľmi vhodné, pretože na každej snímke môže byť ochranný prvok umiestnený na trochu inej pozícii. Takto meraná vzdialenosť je tiež výrazne ovplyvnená svetelnými podmienkami.

Ak je definovaná vhodná miera odlišnosti snímok, overenie dostatočnej zmeny farby ochranného prvku môže byť realizované napríklad tak, že sa vypočíta vzájomná odlišnosť pre všetky dvojice reprezentantov. Vo vyhodnotení sa potom môže použiť ich priemerná alebo maximálna odlišnosť.

3.7 Výsledný navrhovaný postup overenia pravosti ochranného prvku s opticky variabilnou farbou

V podkapitole je zhrnutý finálny navrhovaný postup overenia pravosti ochranného prvku s opticky variabilnou farbou OVI. Postup sa sústreďuje na prvý a druhý krok kompletného postupu overenia pravosti občianskeho preukazu, ktorý je znázornený na obrázku 3.8.

Vstupom do navrhovanej metódy je sekvencia snímok videa, na ktorých sa nachádza občiansky preukaz v rôznej pozícii a naklonení. Detekcia ochranného prvku sa vykonáva postupne pre každú snímku. Až po prejdení celej vstupnej sekvencie sa pristúpi k druhej časti, ktorá overí pravosť ochranného prvku analýzou jeho vizuálnych vlastností.

V prvom kroku sa detektor musí zorientovať v scéne aktuálnej snímky a nájsť na nej občiansky preukaz. Na detekciu dokladu sa používa algoritmus SIFT, ktorý je invariantný voči rotácii, posunu, škálovaniu, zmene osvetlenia a čiastočnému skresleniu objektu. Ako vzor sa využíva normalizovaný občiansky preukaz. Pomocou nájdených, spárovaných keypointov je vypočítaná transformačná matica, a s jej využitím je občiansky preukaz normalizovaný. Transformačná matica reprezentuje pôvodnú polohu občianskeho preukazu na snímke a je potrebné ju uložiť pre farebnú analýzu.

Vďaka normalizácii je možné bližšie určiť oblasť, kde sa nachádza ochranný prvok, čiže pravý horný roh občianskeho preukazu. Tým sa zaručí, že sa prvok nachádza na správnej pozícii v kontexte občianskeho preukazu. Táto oblasť sa vyreže a aplikuje sa na ňu metóda Template Matching, ktorá sa sústreďuje hlavne na farbu prvku. Výstupom je výrez s ochranným prvkom. K výrezu sa uloží informácia, ktorá šablóna, s ktorým typom symbolu, rozhodla o jeho pozícii. Postup detekcie ochranného prvku je znázornený na obrázku 3.52.

Pri extrémnom natočení občianskeho preukazu je problém ho na snímke nájsť alebo následne jeho ochranný prvok, ktorý môže byť po transformácii značne deformovaný. Nielen tvar, ale aj farba ochranného prvku alebo celého občianskeho preukazu môže byť výrazne vychýlená, čo je väčšinou spôsobené vonkajším vplyvom osvetlenia, napr. odrazeným bleskom. Preto je vhodné



Obr. 3.52: Postup detekcie ochranného prvku

použiť dodatočné overenia, či je výrez správny a ochranný prvok sa na ňom naozaj nachádza. Okrem toho, bez dôkladného overenia, že skúmaná farba naozaj patrí ochrannému prvku, by bolo model jednoduché pomýliť, napríklad prekrytím ochranného prvku iným objektom a pod.

V navrhovanom postupe je doplnená kontrola typu ochranného prvku pomocou detekcie keypointov algoritmom SIFT, ktorý sa sústreďuje na jeho tvar. Metóda vyžaduje, aby bol rovnaký typ ochranného prvku detekovaný aspoň na malom počte snímok videa. Podľa identifikovaného typu ochranného prvku sú z ďalšej analýzy vynechané všetky výrezy, ktoré Template Matching našiel v spojení so šablónou druhého typu symbolu. Krok vyradenie zle detekovaných snímok sa vykonáva až v závere, po prejdení všetkých snímok vstupnej sekvencie.

Ďalším účinným spôsobom, ako vyradiť zle detekované snímky, je využiť detekciu odlesku ochranného prvku. Overenie odlesku je už súčasťou kontroly vizuálnych vlastností ochranného prvku. Pre analyzovaný snímok sa vypočíta hranové skóre, ktoré ak je nižšie, ako stanovená hraničná hodnota, tak je snímka vyradená z ďalšieho spracovania a považovaná za chybné detekovanú.

Po nájdení výrezov s ochranným prvkom sa overujú ich ďalšie vizuálne vlastnosti, čo je najnáročnejšia časť postupu. V tomto kroku verifikácie sa robí farebná analýza prvku, pričom sa sústreďuje na farebnú zmenu. Pravý ochranný prvok na videu mení farbu, nepravý má farbu konštantnú a väčšinou sa nemení ani jeho reflexná charakteristika. Samotný odlesk pravosť nedokazuje, pretože je ho možné dosiahnuť rôznymi podvodnými technikami, napríklad prelepením prvku priesvitným lesklým materiálom a pod. Na konci detekcie sa z výrezov s ochranným prvkom, ktoré sú posúdené ako správne detekované, vypočíta ich dominantná farba. V navrhovanom postupe do analýzy vizuálnych vlastností vstupuje iba dominantná

farba ochranného prvku spolu s transformačnou maticou.

Overenie dostatočnej zmeny farby ochranného prvku na videu je realizované kontrolou zmeny jasů. Z dominantných farieb sa vypočíta minimálna a maximálna hodnota komponentu V. Ak je rozdiel medzi nimi dostatočne veľký, zmena farby sa považuje za overenú.

Posledný krok by mal analyzovať farbu ochranného prvku vzhľadom na polohu občianskeho preukazu. Keďže všetky preskúvané metódy overenia dominantnej farby vo vzťahu ku transformačnej matici sa ukázali byť nefunkčné, navrhovaný postup túto časť overenia zanedbáva. Ale pre úplnosť kontroly ju je v budúcnosti nutné doplniť.

Celý navrhovaný postup verifikácie OVI prvku je ilustrovaný na obrázku 3.53. Výsledky na videách štvrtého a piateho datasetu sú zhrnuté v nasledujúcich tabuľkách. Na ohodnotenie výsledkov sa používajú metriky uvedené v oddieli 3.6.4 v časti Detekcia anomálií. Výsledná matica zámen je v tabuľke 3.10 a vypočítané metriky sú v tabuľke 3.11. Postup je presný, ale menej senzitívny. Častejšie označí pravý občiansky preukaz za falošný ako falošný za pravý. Celková úspešnosť navrhovaného postupu je 82.82%.

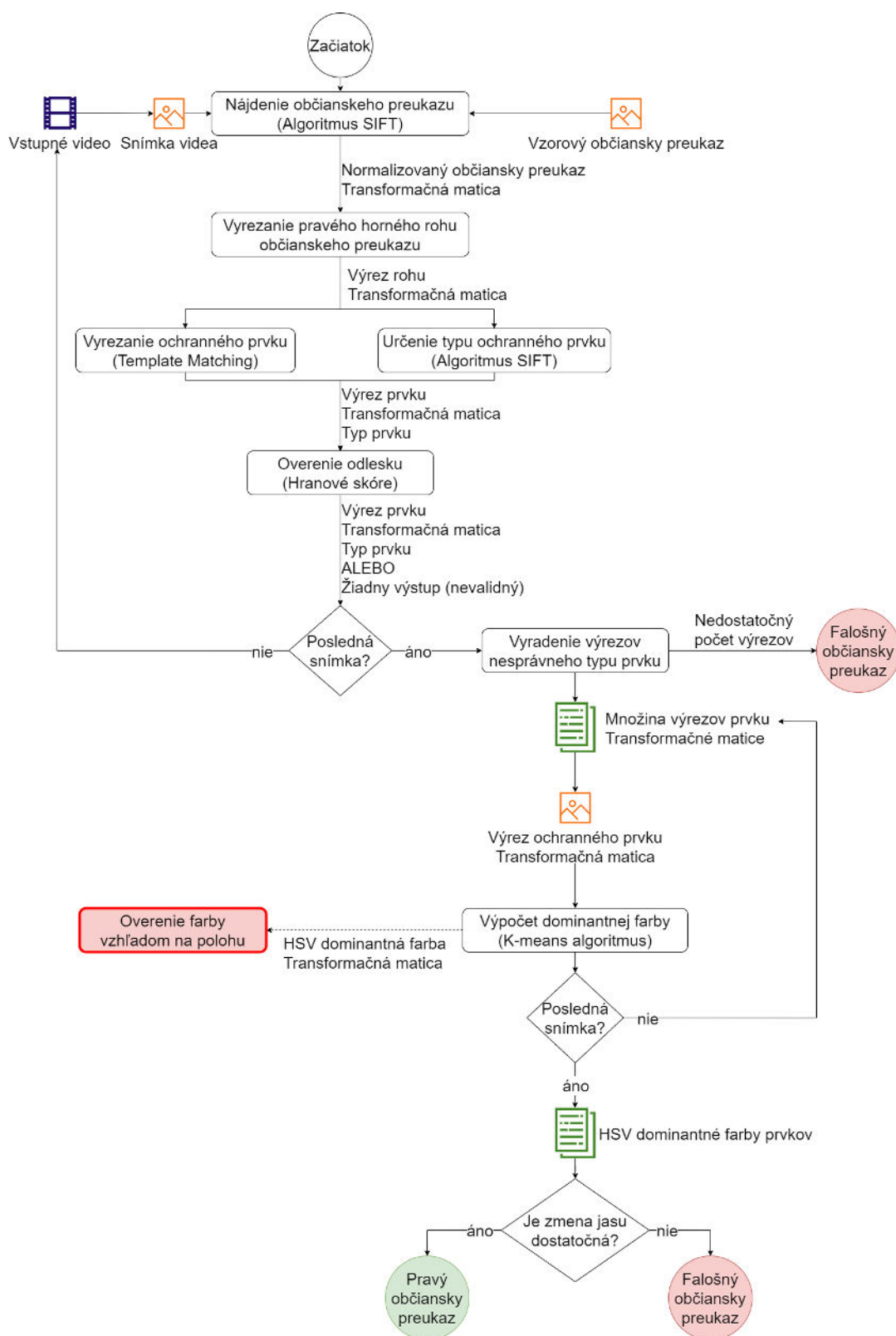
Tabuľka 3.10: Matica zámen navrhovaného postupu verifikácie

	odhad reálny	odhad falošný
skutočne reálny	66	26
skutočne falošný	2	69

Tabuľka 3.11: Výsledky navrhovaného postupu verifikácie

celková správnosť	82,82%
senzitivita	71,74%
presnosť	97,06%

Navrhovaný postup je len prvotné riešenie, ktoré vzniklo v rámci počiatočnej analýzy tohoto problému. Postup sa dá ďalej skúmať, vylepšovať a dopĺňať, aplikovať nové alebo inak formulované metódy, použiť zložitejšie reprezentácie farby ochranného prvku atď. Preskúvanie jedného ochranného prvku je len jeden krok v rámci množiny ďalších kontrol a overení. Podobný postup možno navrhnúť aj pre iné ochranné prvky občianskeho preukazu, ale s prihliadnutím na ich špecifické vizuálne vlastnosti.



Obr. 3.53: Výsledný navrhovaný postup overenia pravosti OVI ochranného prvku

Záver

Cieľom diplomovej práce bolo preskúmať možnosti detekcie falošného dokladu na základe analýzy jeho ochranných prvkov. Práca sa zamerala na detekciu a overenie vizuálnych vlastností ochranného prvku s opticky variabilnou farbou OVI. Diplomová práca je základným výskumom v danej problematike ochranných prvkov. Digitálnemu overeniu pravosti OVI ochranného prvku sa zatiaľ žiadne iné práce nevenovali.

Na začiatku práce sa preskúmalo, ako vznikajú farby, vplyv osvetlenia, prostredia a snímania na vizuálne vlastnosti objektu a špecifickejšie na vizuálne vlastnosti OVI ochranného prvku. Zmena farby OVI ochranného prvku sa skúmala teoreticky aj prakticky, pričom bol pozorovaný vzťah medzi farbou ochranného prvku a pozíciou občianskeho preukazu.

V práci bol navrhnutý celý postup snímania a overenia pravosti občianskeho preukazu, ktorý sa skladá z viacerých častí. Na vstupe očakáva video s primárnym zdrojom svetla bleskom, kde je zachytený občiansky preukaz, ktorý mení svoju polohu a natočenie voči snímaču. Tie kroky postupu, ktoré súvisia s overením pravosti OVI ochranného prvku, boli v práci podrobnejšie popísané a na ich riešenie boli navrhnuté rôzne metódy. Používali sa základné metódy spracovania obrazu a niektoré metódy strojového učenia. Za účelom testovania metód verifikácie vzniklo päť datasetov, z ktorých je každý použitý v inej časti postupu návrhu metód.

Na začiatku bolo potrebné nájsť občiansky preukaz na snímke. Vyskúšali sa dve možnosti detekcie občianskeho preukazu. Preukaz bola schopná správne nájsť metóda detekcie keypointov algoritmom SIFT. Ďalej sa preskúmali viaceré metódy nájdenia ochranného prvku na snímke. Najskôr sa skúmala detekcia prvku v celej scéne, ktorá nebola veľmi úspešná. Preto sa namiesto celej snímky použil výrez pravého horného rohu nájdeného občianskeho preukazu z predchádzajúceho kroku. Metóda Template Matching vie nájsť ochranný prvok vo výreze na základe jeho farby a detekcia keypointov na základe tvaru. V práci navrhnutý postup detekcie občianskeho preukazu a následne ochranného prvku dokáže veľmi presne nájsť ochranný prvok na snímke.

V práci boli navrhnuté metódy na overenie vizuálnych vlastností OVI ochranného prvku. Najskôr sa uvažovalo nad rôznymi reprezentáciami farby ochranného prvku. Doteraz sa skúmala iba najjednoduchšia z nich, a to dominantná farba. Zhrnuli sa tri vlastnosti ochranného prvku, ktoré je na videu potrebné overiť, a to odlesk prvku, farbu prvku vzhľadom na polohu občianskeho preukazu a zachytenie dostatočnej zmeny farby ochranného prvku. Na overenie odlesku sa navrhlo použiť detekciu hrán, na základe ktorej sa s pomocou hranového skóre podarilo odlesk kvantifikovať. Na modelovanie vzťahu polohy a farby sa neúspešne aplikovala regresia a detekcia anomálií. Overenie dostatočnej zmeny farby ochranného prvku sa zjednodušilo na overenie dostatočnej zmeny jasu, čo úspešne dokázalo oddeliť falošné videá od pravých.

Navrhovaný postup má svoje limitácie a na niektoré parciálne problémy sa zatiaľ nepodarilo nájsť vhodné riešenia. V práci boli uvedené viaceré odporúčania a návrhy ako vylepšiť a rozšíriť vizuálne overenie ochranného prvku. Výsledky analýzy sa môžu využiť na tvorbu komplexnejších modelov. Niektoré metódy tiež môžu byť použité na overenia iných ochranných prvkov s podobnými vlastnosťami. Modely sú teoreticky rozšíriteľné aj na iné doklady alebo úplne iné predmety, na ktorých sa nachádzajú obdobné ochranné prvky, napr. bankovky.

Existujúce riešenie je možné vylepšiť rôznymi spôsobmi. Jednou z možností je do tréningu použiť väčšie množstvo dát. Fotografie a videá občianskych preukazov obsahujú citlivé osobné údaje, s ktorými je nutné zaobchádzať opatrne. Získať väčšie množstvo kvalitných dát môže byť problematické, ale nevyhnutné pre tvorbu komplexnejšieho riešenia.

Sofistikovanejšie riešenie by mohlo vynechať požiadavku snímania, kedy je hlavným zdrojom svetla blesk fotoaparátu. Model bez podmienky použitia blesku by mohol pracovať so zmenou polohy zdroja svetla a zmenou polohy snímača, ktoré by boli v tomto prípade odlišné.

V navrhovaných metódach sa zanedbávala chromatická zložka HSV dominantnej farby, čiže komponent H, z dôvodu silného vplyvu svetelných podmienok. Komplexnejší model by mal v riešení zahrnúť aj tento farebný komponent. Jednou z možností je vytvoriť separátny model pre kontrolu farebnosti, čiže iba H komponentu. Druhou alternatívou je komplexnejší model, do ktorého vstupujú všetky tri HSV zložky. Iné riešenie môže používať zložitejšiu reprezentáciu farby, napríklad histogram alebo heatmapy farebných komponentov, alebo celú snímku ochranného prvku. Ďalšou možnosťou je preskúmať použitie iného farebného modelu.

Iná formulácia regresnej úlohy by mohla lepšie modelovať vzťah farby a polohy ochranného prvku. Napríklad by mohla pomôcť iná reprezentácia polohy. Do ďalšieho riešenia, nielen regresie, by sa tiež dali zakomponovať reprezentanti množiny snímok videa, ktorý by mohli zastupovať vstupné video.

V rámci ďalšieho výskumu by sa ako vstup do modelu mohlo uvažovať celé video, ktoré je transformované do jedného bodu v latentnom priestore. Do komplexnejšieho modelu by sa pravdepodobne dal zakomponovať aj komponent H farebnej schémy HSV. Na takto definovanom priestore by mohol byť detektor anomálií oveľa úspešnejší.

Komplexnejší model by mohol brať do úvahy aj čas snímky a poradie, v akom snímky prišli. Takýto model by chápal kontext snímky v rámci sekvencie, s ktorou by pracoval ako s časovým radom nad 2-rozmernými dátami. Aktuálne riešenie posudzuje uhol natočenia, nie poradie snímky.

Hlavným prínosom diplomovej práce je základná analýza vizuálnych vlastností OVI ochranného prvku a preskúmanie rôznych jednoduchších metód a prístupov k jeho overeniu pravosti. Navrhovaný postup dokáže odhaliť falošný občiansky preukaz na videu na základe OVI ochranného prvku, ale má svoje limitácie. Dosiahnuté výsledky sú dôkazom, že problém je prakticky riešiteľný. V diplomovej práci sa potvrdilo, že elektronické overenie ochranných prvkov má potenciál a oplatí sa mu venovať pozornosť.

Zoznam použitej literatúry

- [1] Javier Abellán Abenza. *HSV color model*. 2018. URL: <https://medium.com/neurosapiens/segmentation-and-classification-with-hsv-8f2406c62b39>.
- [2] Aman Anand. *Scikit-learn cheat sheet: methods for classification & regression*. 2020. URL: <https://www.educative.io/blog/scikit-learn-cheat-sheet-classification-regression-methods>.
- [3] Ravimal Bandara. *Bag-of-Features Descriptor on SIFT Features with OpenCV (BoF-SIFT)*. 2017. URL: <https://www.codeproject.com/Articles/619039/Bag-of-Features-Descriptor-on-SIFT-Features-with-0>.
- [4] Markus M Breunig et al. “LOF: identifying density-based local outliers”. In: *Proceedings of the 2000 ACM SIGMOD international conference on Management of data*. 2000, s. 93–104.
- [5] John Canny. “A computational approach to edge detection”. In: *IEEE Transactions on pattern analysis and machine intelligence* 6 (1986), s. 679–698.
- [6] CatBoost. *CatBoostRegressor*. URL: https://catboost.ai/en/docs/concepts/python-reference_catboostregressor.
- [7] Jimmy Chin. *What Is Lens Distortion in Photography?* 2021. URL: <https://www.masterclass.com/articles/what-is-lens-distortion-in-photography#what-is-optical-distortion>.
- [8] Anna Veronika Dorogush, Vasily Ershov a Andrey Gulin. “CatBoost: gradient boosting with categorical features support”. In: *arXiv preprint arXiv:1810.11363* (2018).
- [9] Harris Drucker et al. “Support vector regression machines”. In: *Advances in neural information processing systems* 9 (1996).
- [10] Martin Ester et al. “A density-based algorithm for discovering clusters in large spatial databases with noise.” In: *kdd. Zv. 96. 34*. 1996, s. 226–231.

- [11] Martin A Fischler a Robert C Bolles. “Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography”. In: *Communications of the ACM* 24.6 (1981), s. 381–395.
- [12] Theo Gevers et al. *Color in computer vision: fundamentals and applications*. Zv. 23. John Wiley & Sons, 2012.
- [13] IBM. *What is computer vision?* URL: <https://www.ibm.com/topics/computer-vision#:~:text=Computer%20vision%20is%20a%20field%20, recommendations%20based%20on%20that%20information..>
- [14] LightGBM. *LGBMRegressor*. URL: <https://lightgbm.readthedocs.io/en/latest/pythonapi/lightgbm.LGBMRegressor.html>.
- [15] Fei Tony Liu, Kai Ming Ting a Zhi-Hua Zhou. “Isolation forest”. In: *2008 eighth ieee international conference on data mining*. IEEE. 2008, s. 413–422.
- [16] R Beau Lotto a Dale Purves. “The empirical basis of color perception”. In: *Consciousness and Cognition* 11.4 (2002), s. 609–629.
- [17] David G Lowe. “Distinctive image features from scale-invariant keypoints”. In: *International journal of computer vision* 60.2 (2004), s. 91–110.
- [18] Douglas C Montgomery, Elizabeth A Peck a G Geoffrey Vining. *Introduction to linear regression analysis*. John Wiley & Sons, 2021.
- [19] OpenCV. *Canny Edge Detection*. 2022. URL: https://docs.opencv.org/4.x/da/d22/tutorial_py_canny.html.
- [20] OpenCV. *Changing Colorspaces*. 2022. URL: https://docs.opencv.org/4.x/df/d9d/tutorial_py_colorspaces.html.
- [21] OpenCV. *Feature Detection and Description*. 2022. URL: https://docs.opencv.org/4.x/db/d27/tutorial_py_table_of_contents_feature2d.html.
- [22] OpenCV. *Hough Line Transform*. 2021. URL: https://docs.opencv.org/4.5.5/d6/d10/tutorial_py_houghlines.html.
- [23] OpenCV. *Image Thresholding*. 2022. URL: https://docs.opencv.org/4.x/d7/d4d/tutorial_py_thresholding.html.

- [24] OpenCV. *Introduction to SIFT (Scale-Invariant Feature Transform)*. 2022. URL: https://docs.opencv.org/4.x/da/df5/tutorial_py_sift_intro.html.
- [25] OpenCV. *OpenCV metriky pre Template Matching*. 2021. URL: https://docs.opencv.org/4.5.5/df/dfb/group__imgproc__object.html.
- [26] OpenCV. *Template Matching*. 2022. URL: https://docs.opencv.org/4.x/d4/dc6/tutorial_py_template_matching.html.
- [27] Learning OpenCV. *3: Computer Vision in C++ with the OpenCV Library*. 2017.
- [28] Stephen M Pizer et al. “Adaptive histogram equalization and its variations”. In: *Computer vision, graphics, and image processing* 39.3 (1987), s. 355–368.
- [29] Rukshan Pramoditha. *5 Cute Features of CatBoost*. 2021. URL: <https://towardsdatascience.com/5-cute-features-of-catboost-61532c260f69>.
- [30] Liudmila Prokhorenkova et al. “CatBoost: unbiased boosting with categorical features”. In: *Advances in neural information processing systems* 31 (2018).
- [31] Generálny sekretariát Rady Európskej únie. *PRADO - VEREJNÝ REGISTER PRAVÝCH DOKLADOV TOTOŽNOSTI A CESTOVNÝCH DOKLADOV ONLINE*. 2007-2021. URL: <https://www.consilium.europa.eu/prado/sk/prado-glossary/prado-glossary.pdf>.
- [32] Muhammad Rifqi. *HSB/HSV color system*. 2021. URL: <https://bootcamp.uxdesign.cc/hsb-hsv-color-system-d14697d7c485>.
- [33] František Roček. *V občanském průkazu najdete i slova hymny*. 2016. URL: <https://ustecky.denik.cz/zlociny-a-soudy/v-obcanskem-prukazu-najdete-i-slova-hymny-20160117.html>.
- [34] Adrian Rosebrock. *Multi-template matching with OpenCV*. 2021. URL: <https://laptrinhx.com/multi-template-matching-with-opencv-1799855488/>.
- [35] Bernhard Schölkopf et al. “Estimating the support of a high-dimensional distribution”. In: *Neural computation* 13.7 (2001), s. 1443–1471.
- [36] Scikit-learn. *Clustering*. 2022. URL: <https://scikit-learn.org/stable/modules/clustering.html#k-means>.

- [37] Scikit-learn. *Ensemble methods*. 2022. URL: <https://scikit-learn.org/stable/modules/ensemble.html>.
- [38] Scikit-learn. *Kernel ridge regression*. 2022. URL: https://scikit-learn.org/stable/modules/kernel_ridge.html.
- [39] Scikit-learn. *Linear Models*. 2022. URL: https://scikit-learn.org/stable/modules/linear_model.html.
- [40] Scikit-learn. *Novelty and Outlier Detection*. 2022. URL: https://scikit-learn.org/stable/modules/outlier_detection.html.
- [41] Scikit-learn. *Support Vector Machines*. 2022. URL: <https://scikit-learn.org/stable/modules/svm.html>.
- [42] Tom Sharp. *An Introduction to Support Vector Regression (SVR)*. 2020. URL: <https://towardsdatascience.com/an-introduction-to-support-vector-regression-svr-a3ebc1672c2>.
- [43] E Šikudová et al. “Počítačové videnie. Detekcia a rozpoznávanie objektov”. In: *Praha: Wikina Praha* (2013).
- [44] Ministerstvo vnútra Slovenskej republiky. URL: <https://www.minv.sk/?vzory-dokladov>.
- [45] Ministerstvo vnútra Slovenskej republiky. *Ochranné prvky OP vydávaného od 1.3.2015*. 2015. URL: <https://www.minv.sk/?vzory-dokladov>.
- [46] Ministerstvo vnútra Slovenskej republiky. *Ochranné prvky OP vydávaného od 1.7.2008*. 2008. URL: <https://www.minv.sk/?vzory-dokladov>.
- [47] Ministerstvo vnútra Slovenskej republiky. *Ochranné prvky OP vydávaného od 30.11.2013*. 2013. URL: <https://www.minv.sk/?vzory-dokladov>.
- [48] Milan Sonka, Vaclav Hlavac a Roger Boyle. *Image processing, analysis, and machine vision*. Cengage Learning, 2014.
- [49] David Taylor. *The Advanced Photography Guide: Expert Techniques to Take Your Digital Photography to the Next Level*. DK, a Division of Penguin Random House LLC, 2018.

- [50] David Taylor et al. *Digital photography complete course*. DK Publishing, 2015.
- [51] XGBoost. *Python API Reference*. 2021. URL: https://xgboost.readthedocs.io/en/stable/python/python_api.html#module-xgboost.sklearn.
- [52] Yufeng. *Understanding DBSCAN and Implementation with Python*. 2022. URL: <https://towardsdatascience.com/understanding-dbscan-and-implementation-with-python-5de75a786f9f>.

Prílohy

Príloha A: Obsah CD disku

Práca obsahuje prílohu vo formáte CD disku. CD obsahuje:

- Text diplomovej práce vo formáte PDF.
- Zdrojové kódy testovacej aplikácie.
- Používateľskú príručku vo formáte PDF.
- Conda prostredie v YML súbore.
- Vzorový anonymizovaný občiansky preukaz a jeho keypointy vo formáte JPG a TXT.
- Šablóny s ochranným prvkom vo formáte JPG.
- Modely pre detekciu anomálií pre starší aj novší ochranný prvok.
- Regresné modely pre starší aj novší ochranný prvok.