VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

DETEKCE PREZENTAČNÍCH ÚTOKŮ POMOCÍ PODVRHŮ OBLIČEJE

DETECTING PRESENTATION ATTACKS USING FACE SPOOFING

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **TOMÁŠ HOMOLA**
AUTHOR

VEDOUCÍ PRÁCE **Ing. TOMÁŠ GOLDMANN**
SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Zadání bakalářské práce

156897

Ústav: Ústav inteligentních systémů (UITS)
Student: **Homola Tomáš**
Program: Informační technologie
Název: **Detekce prezentačních útoků pomocí podvrhů obličeje**
Kategorie: Umělá inteligence
Akademický rok: 2023/24

Zadání:

1. Seznamte se s problematikou detekce podvrhů snímku obličeje. Zjistěte, jaké falzifikáty se používají při prezentačních útocích na 2D senzory pro rozpoznávání osob podle obličeje.
2. Sumarizujte informace o dostupných algoritmech pro detekci podvrhů obličeje pomocí kamery. Seznamte se s algoritmy pro detekci živosti obličeje.
3. Navrhněte algoritmus, který bude v reálném čase detekovat, zdali je v záběru 2D kamery přítomen podvrh obličeje či nikoliv.
4. Navržený algoritmus implementujte v programovacím jazyce Python.
5. Proveďte experimenty s vaším řešení zaměřené na zhodnocení spolehlivosti detekce podvrhů a zhodnoťte jeho robustnost.

Literatura:

- DAMER, Naser, et al. Practical View on Face Presentation Attack Detection. In: *BMVC*. 2016.
- BENLAMOUDI, Azeddine, et al. Face spoofing detection from single images using active shape models with stasm and lbp. In: *Proceeding of the Troisime conference internationale sur la vision artificielle CVA*. 2015. p. 31.
- KIM, Sooyeon; BAN, Yuseok; LEE, Sangyoun. Face liveness detection using defocus. *Sensors*, 2015, 15.1: 1537-1563.
- RAMACHANDRA, Raghavendra; BUSCH, Christoph. Presentation attack detection methods for face recognition systems: A comprehensive survey. *ACM Computing Surveys (CSUR)*, 2017, 50.1: 1-37.

Při obhajobě semestrální části projektu je požadováno:
Body 1 a 2.

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Goldmann Tomáš, Ing.**
Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.
Datum zadání: 1.11.2023
Termín pro odevzdání: 9.5.2024
Datum schválení: 6.11.2023

Abstrakt

Detekcia tváre je jedna z najdôležitejších a najrozšírenejších spôsobov overenia identity osoby. Avšak tento spôsob vyvoláva taktiež obavy o súkromie a bezpečnosť. Je dôležité si uvedomiť nebezpečenstvá, ktoré to prináša a neustále vyvíjať prostriedky potrebné na ochranu proti nim. Táto práca sa zaoberá vysvetlením problematiky podvrhov tváre, hrozbou, ktorá vzniká pri úspešnom pokuse útočníka o podvrh a detekciou týchto podvrhov za pomoci algoritmov.

Abstract

Face detection is one of the most important and widespread methods of verifying a person's identity. However, this method also raises concerns about privacy and security. It is important to be aware of the dangers it brings and constantly develop the necessary means to protect against them. This thesis aims to explain the issue of face spoofing, the threat that arises from a successful attacker's attempt at spoofing, and the detection of these spoofs using algorithms.

Kľúčové slová

detekcia podvrhu, algoritmus, rozpoznávanie živosti, hlbkové učenie, fotografia

Keywords

spoof detection, algorithm, liveness recognition, deep learning, photography

Citácia

HOMOLA, Tomáš. *Detekce prezentačních útoků pomocí podvrhů obličeje*. Brno, 2024. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Tomáš Goldmann

Detekce prezentačních útoků pomocí podvrhů obličeje

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Ing. Tomáša Goldmanna. Uviedol som všetky literárne pramene, publikácie a ďalšie zdroje, z ktorých som čerpal.

.....
Tomáš Homola
6. mája 2024

Poďakovanie

Rád by som poďakoval Ing. Tomášovi Goldmannovi za pomoc a odborné rady pri riešení a naskytnutých problémoch pri vývoji tejto bakalárskej práce.

Obsah

Kapitola 1

Úvod

Vďaka rýchlemu rozvoju technológií za posledné desaťročia sa ľudom naskytli nové možnosti v podobe nových zariadení a služieb. Tento pokrok umožnil po prvýkrát široké nasadenie biometrických systémov, ktoré sú dnes prítomné takmer všade - od autentifikácie smartfónov, cez online služby, až po pohraničné kontroly. Medzi všetkými existujúcimi biometrickými znakmi je v súčasnosti rozpoznávanie tváre jedným z najrozšírenejších. Tvár bola skúmaná ako prostriedok rozpoznávania už od 60. rokov 20. storočia a je považovaná za jednu z biometrických čŕt s najvyšším ekonomickým a sociálnym vplyvom z viacerých dôvodov. Po odtlačkoch prstov je rozpoznávanie tváre druhou najrozšírenejšou biometriou na svete. Každý deň viac a viac výrobcov, napríklad spoločnosť Apple s technológiou FaceID, zaraďuje do svojich produktov rozpoznávanie tváre, čo začali využívať mnohé aplikácie ako spôsob autentizácie. Taktiež sa používa vo väčšine identifikačných dokumentov, ako sú biometrické pasy alebo národné preukazy totožnosti.

Avšak aj tieto systémy bojujú s útočníkmi, ktorých hlavným cieľom je zmeniť a ovplyvniť proces spracovania biometrických dát. V dôsledku toho je nevyhnutné vytvárať a neustále obnovovať opatrenia proti vírusom, ktoré sa snažia získavať a následne podvrhnúť tieto dáta. Pod pojmom opatrenia sa myslí neustály vývoj spoľahlivých algoritmov a metód zachytávajúcich pokusy o podvrh. Napríklad, vývoj rozšírených techník na detekciu živosti, ktoré dokážu rozlíšiť skutočnú ľudskú tvár od jej fotografie alebo videozáznamu, je kľúčový pre zvýšenie bezpečnosti.

Cieľom tejto práce je návrh a následná implementácia algoritmu, ktorý bude v reálnom čase detegovať, či je v 2D zábere kamery prítomný podvrh tváre alebo nie. Túto tému som si vybral kvôli rastúcej popularite využívania biometrického rozpoznávania tváre ako bezpečnostného zámku, ale aj kvôli potenciálnym rizikám, ktoré s tým súvisia. Rozpoznávanie tváre sa stáva neoddeliteľnou súčasťou mnohých bezpečnostných systémov, a preto je nevyhnutné zabezpečiť jeho spoľahlivosť a odolnosť voči možným útokom.

Kapitola 2 obsahuje základný prehľad biometrických systémov a následne konkrétny typ systému zameraný na rozpoznávanie tváre. V tejto kapitole je tiež zameranie na rôzne typy prezenčných útokov, ako napríklad foto útok či útok za pomoci 3D masky. Nasleduje kapitola 3, ktorá je zameraná už na konkrétne techniky a prístupy k rozpoznávaniu tváre a následne jej detekcie živosti. Kapitola 4 obsahuje detailný popis navrhnutého algoritmu a vysvetlenie spôsobu implementácie tohto návrhu. Na záver budú v kapitole 5 zhrnuté prevedené experimenty s mojím navrhnutým riešením, zhodnotenie spoľahlivosti tohto algoritmu a určenie jeho robustnosti v rôznych podmienkach.

Kapitola 2

Biometrické systémy a prezenčné útoky

Obsahom tejto kapitoly sú základné poznatky o biometrických systémoch a výzvach, ktorým čelia v dôsledku prezenčných útokov. Význam technológií v súčasných aplikáciach, ktoré zaisťujú rozpoznávanie tváre. Nasleduje analýza techník, ktoré používajú útočníci pri prezenčných útokoch a zraniteľné miesta prítomné v 2D snímačoch rozpoznávania tváre. V závere kapitoly sú zhrnuté dôvody ako tieto útoky ohrozujú naše bezpečie a súkromie.

2.1 Biometrický systém

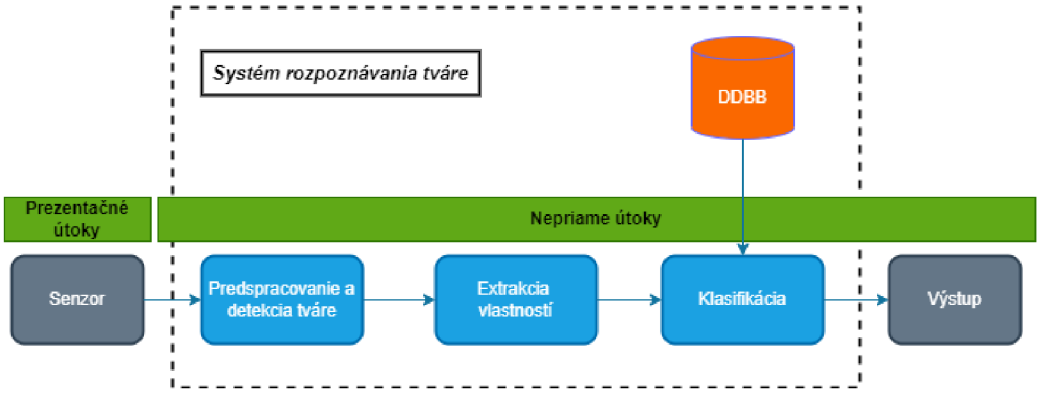
Biometria [23] je odvetvie, ktoré sa zaoberá identifikáciou jedincov na základe ich jedinečných charakteristík. Z etymologického hľadiska vychádza z gréckych slov *bios* (život) a *metron* (meranie).

Používanie biometrických systémov ovplyvnilo spôsob, akým sa identifikujeme a overujeme na celom svete. Využitím tejto technológie sa zmenila nielen identifikácia osôb, ale výrazne sa skrátil aj čas potrebný na zmienenú identifikáciu a overenie osôb. Zahŕňa širokú škálu systémov, ktoré môžu rozpoznávať osoby podľa ich odtlačkov prstov, geometrie tváre, dúhovky apod.

Biometrický systém [22], znázornený na obrázku 2.1, je technologický systém, ktorý využíva unikátne biologické a behaviorálne znaky ľudí na ich identifikáciu alebo overenie identity. Tieto systémy sú založené na princípe, že každý človek má jedinečné fyzické alebo správaním podmienené charakteristiky znázornené na obr. 2.2, ktoré je možné elektronicky zachytiť a analyzovať. Užívateľa identifikuje v 2 fázach:

- Fáza zápisu *enroll*: získavanie biometrických dát od jednotlivca a následné ukladanie do databázy spolu s identitou danej osoby. Typicky sú to informácie spracované ku extrakcií rozlišovacích rysov.
- Fáza rozpoznania *verify*: znovuzískavanie dát od jednotlivca a ich následné porovnanie s uloženými dátami z fáze zápisu k určeniu identity užívateľa.

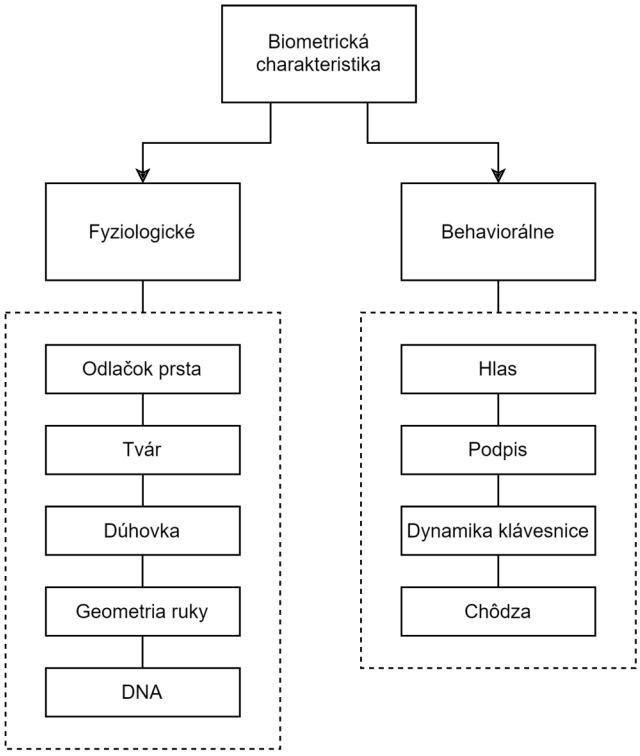
Tieto systémy sa skladajú z určitého počtu blokov [24] znázornených na obr. 2.1. Prvým dôležitým blokom je užívateľské rozhranie, ktoré integruje biometrický senzor či čítačku, aby dokázalo zmerať surové biometrické dáta užívateľa. Väčšina týchto dát je vo forme 2D obrazov (odtlačok prsta, dúhovka, atď.). Pre tieto dáta hrajú veľmi dôležitú rolu faktory ako rozlíšenie, snímkovacia frekvencia či citlivosť kamery.



Obr. 2.1: Schéma obecného biometrického systému, prevzaté z [34].

Ďalším stavebným blokom je extrakcia prvkov, ktoré budú neskôr použité na určovanie identity. Najprv sa posúdi kvalita surových dát, nasleduje segmentácia, pri ktorej odstráni systém nepotrebné časti ako pozadie a hluk. Na záver sa pomocou algoritmov zvýši kvalita a zníži šum segmentovaných dát. Najčastejšie sa to využíva pri obrazových dátach, kde sa používa najmä vyhladzovanie či vyrovnanie histogramu. Šablóna je digitálna reprezentácia extrahovaných dát. Tieto šablóny sa ukladajú do databázy [22].

Posledným blokom je biometrický porovnávač, ktorého úlohou je porovnať dáta - šablóny s dotazovacími rysmi a vygenerovať výsledok porovnania. Výsledkom tohto procesu je miera podobnosti medzi dotazom a šablónou. Práve pri získavaní dotazovacích rysov dochádza k útokom a pokusom o poslanie falošných dát rôznymi formami [15].



Obr. 2.2: Fyzické a behaviorálne charakteristiky používane biometrickými systémami.

2.2 Útok na biometrický systém

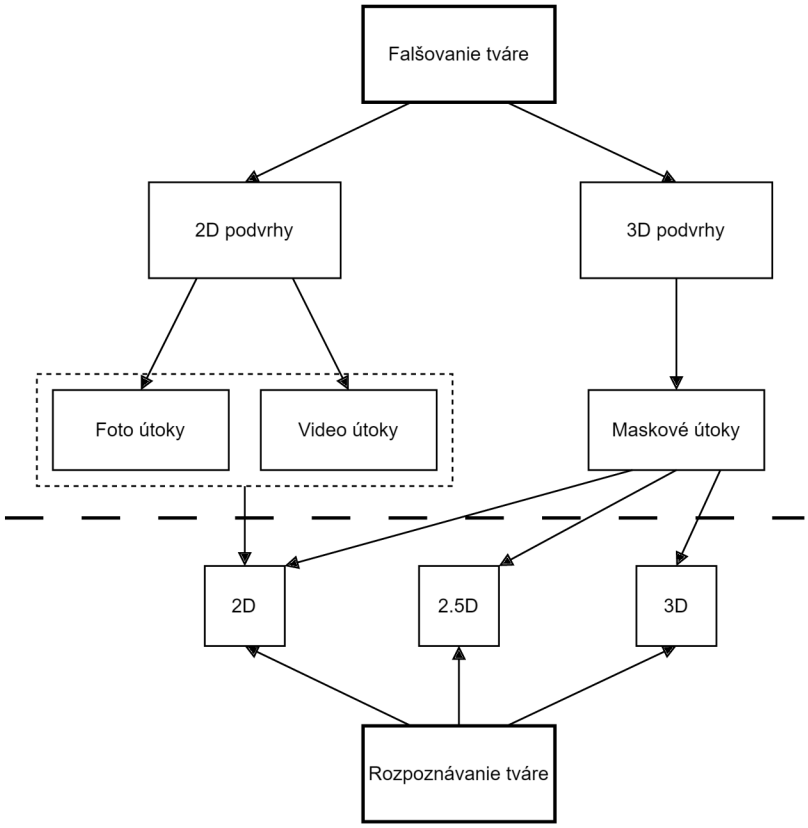
Na detekciu tváre biometrický systém využíva technológiu na identifikáciu jednotlivca na základe jedinečných charakteristík jeho tváre. Dá sa to dosiahnuť pomocou rôznych techník, ako je 2D či 3D rozpoznávanie tváre, teplotné zobrazovanie či mapovanie hĺbky [34]. Cieľom podvrhnutia biometrického systému je oklamať snímač pomocou nepravých biometrických údajov [24].

Na obrázku 2.1 je možné vidieť schému biometrického systému. Proces spracovania vstupov v biometrickom systéme prechádza cez niekoľko kľúčových fáz. Útoky môžu nastať v rôznych častiach tohto systému. Môžu byť priame i nepriame. Pri priamom útoku užívateľ pri vstupe do systému predloží podvrh a pri nepriamom sa jedná o zámenu dát či zmenu nastavenia samotného systému [34].

2.2.1 Priamy útok

Uskutočňuje sa imitáciou biometrických vlastností pri priamom, nazývanom i prezenčnom, útoku na senzore. Jedná sa konkrétne o útoky, ktoré nevyžadujú špecifické znalosti o fungovaní systému. Označuje sa taktiež aj ako *Sensor Attack*. Senzorový modul predstavený v schéme biometrického systému v 2.1 je náchylný na tento typ útoku [25].

Falšovanie tváre spočíva v predložení senzoru fotografie, video alebo 3D masky osoby, ktorej identitu sa útočník pokúša sfalšovať. Pomimo vymenovaných spôsobov sa dá systém na rozpoznanie tváre obísť aj použitím plastickej chirurgie či make-upu. Najpoužívanejší a najlacnejší spôsob je však použitie fotografie či videa.



Obr. 2.3: Klasifikácia falšovania tváre.

Na obrázku 2.3 je znázornená základná klasifikácia sfalšovania tváre. Tieto typy útokov sa spoločne nazývajú *Presentation Attack Instrumets* (PAI) [17].

Foto útoky
Najbežnejšou technikou na obídenie 2D senzoru na rozpoznávanie tváre je použitie fotografie. Táto fotografia obsahuje fotku tváre osoby, ktorej identitu sa snaží útočník sfalšovať. Je to najpoužívanejšia a najkritickejšia forma útoku. Jeden z dôvodov, prečo je táto forma najpoužívanejšia je to, že tlač farebného obrázku je v dnešnej dobe lacná a jednoduchá. V odbornej literatúre sa tento typ útoku nazýva tlačový útok z anglického *print attacks*.

Do tejto formy zaraďujeme i spôsob foto útoku, kedy je tvár obete zobrazená na obrazovke vysokého rozlíšenia (smartfón, tablet či laptop) [4]. Existujú i pokročilejšie metódy za použitia fotky. Napríklad pri snahe o oklamanie algoritmu, ktorý funguje na princípe pozorovania, či daná osoba žmurká alebo hýbe ústami je vytvorená maska z papiera, ktorá má otvory na oči a ústa. Aj keď sa tento spôsob zdá primitívny, niekoľko súkromných štúdií dokázalo, že množstvo firiem je voči tomuto typu útoku zraniteľný a je potrebné zabezpečiť spoľahlivé protiopatrenia, ktoré tomuto útoku zabránia [34].

Video útoky
Podobne ako pri útokoch za použitia fotografie, aj útoky formou videa taktiež nabrali na popularite z rovnakého dôvodu. Vďaka enormnému zvýšeniu používania sociálnych sietí, kde ľudia pridávajú svoje videá a fotografie, na ktorých sa nachádzajú, je pre útočníka jednoduché získať dostatočné množstvo záberov, ktoré neskôr môže zneužiť práve na pokus o sfalšovanie identity.

Útok formou videa sa dá považovať za výhodnejší a viac spoľahlivý než útok pomocou fotografie, pretože daný subjekt pri skúmaní pravosti preukazuje živosť. Tento typ útoku sa v literatúre nazýva opakovaný útok z anglického slovného spojenia *replay attacks*. Detekcia takejto formy podvrhu je náročnejšia, pretože sa nedeteguje len textúra a tvary tváre, ale aj akékoľvek pohyby tváre či žmurkanie očí. Vzhľadom na vyššiu prepracovanosť týchto falzifikátov sa dá predpokladať, že systémy náchylné na foto-útoky budú fungovať menej spoľahlivejšie pri video-útoku a preto je potrebné vyvinúť spoľahlivé protiopatrenia [4].

3D masky
Pokroky v 3D výrobných technológiách posúvajú spoofingové útoky o krok napred a zavádzajú nové výzvy pre štúdia protiopatrení. Pri tejto metóde sa používa 3D vytlačená alebo vymodelovaná maska tváre osoby, za cieľom obísť systém rozpoznávania tváre. Útok za pomoci 3D masky, obr. 2.4, vyžaduje viac zručnosti na správne vykonanie než predchádzajúce typy útokov. Taktiež je nutné získať viac informácií o tvári človeka, ktorú sa bude pokúšať útočník sfalšovať. Masky majú rôznorodé typy v závislosti od množstva získaných údajov a zložitosti procesu. Štúdie na detekcie tohto typu sa zameriavajú na rozlíšenie medzi pokožkou tváre a materiálmi masky využitím rozdielov v ich odrazových charakteristikách.

Tou najjednoduchšou formou výroby je vytlačenie 2D fotografie a nalepenie na deformovanú štruktúru (tričko alebo plastová taška). Tento útok vie napodobňovať niektoré deformovateľné vzorky človeka. Keďže je to primitívny a najjednoduchší spôsob vyhotovenia 3D masky, používa sa to len na niektoré nízkoúrovňové 3D systémy rozpoznávania tváre. Sofistikovanejší spôsob spočíva v priamom 3D zachytení originálu tváre užívateľa. Je to možné vykonať iba pomocou špeciálneho zariadenia a je veľmi náročné to získať bez spolupráce koncového užívateľa, obete útoku. Avšak novou generáciou technológií sa táto metóda postupne stáva jednoduchšou a dostupnejšou použitím akvizičných senzorov [12].

Tento typ má vysokú úspešnosť, pretože je napodobňovaná úplná štruktúra tváre. Napríklad algoritmy, ktoré využívajú hĺbkové informácie, sa stávajú neúčinnými. I napriek veľkej náročnosti sa začali tieto útoky skúmať vďaka špecifickým databázam, ktoré zahŕňajú rôzne masky rôznych veľkostí a materiálov [33].

Obr. 2.4: Ukážka 17 rôznych tvárových masiek, prevzaté z [12].

Make-up alebo protéza
Zahŕňa použitie make-upu či špeciálnej tvárovej protézy na zmenu vzhľadu s cieľom obísť systém rozpoznávania. Za využitia make-upu sa môže zoštíhliť kontúra tváre, zmeniť veľkosti nosa a podobne. Tento spôsob predstavuje veľké riziko, pretože detekcia make-upu je náročná. Pleťová kozmetika sa stala každodennou nevyhnutnosťou mnoho žien na zlepšenie estetiky tváre jednoduchým a nákladovo efektívnym spôsobom [44].

Tvárová protéza
Taktiež je možné využitie tvárovej protézy na oklamanie senzoru. Je to umelá náhrada rôznych častí tváre, ako napríklad ucha, nosa, očí či inej časti tváre. Obnovuje normálny vzhľad. Je vytvorená z lekárskeho silikónového kaučuku a je vyrobená na mieru, aby vyhovovala prispôsobeniu a vzhľadu pacienta. Táto forma útoku je využívaná len výnimočne, pretože sú potrebné veľmi detailné informácie o tvári osoby [26].

Dátové sady
Spočiatku mal výskum na protiopatrenia tohto typu útoku ťažkosti udržať krok [25]. Bol problém vytvoriť spoľahlivú techniku, ktorá by zabránila týmto pokusom o sfalšovanie identity.

Na skvalitnenie vývoja sa začali vytvárať štandardné databázy. Tie slúžili na testovanie protiopatrení. Obsahovali súbory protokolov na vyhodnotenie výkonu a umožnenie objektívneho porovnávania. S nedávnym rozšírením biometrie aplikácií, hrozba prezentačných útokov vzrástla a biometrická komunita začala získavať veľké a kompletné databázy na vytváranie rozpoznávacích systémov, ktoré budú odolnejšie voči týmto útokom.

Napriek rastúcemu záujmu komunity o štúdium zraniteľnosti je dostupnosť databáz stále obmedzená.
Získavanie nových dát je ťažké z 2 hlavných dôvodov [26]:

- **Technické aspekty:** získavanie údajov o prezentačných útokoch ponúka ďalšie výzvy k bežným problémom, s ktorými sa stretávame pri získavaní štandardných biometrických databáz, aby sa správne zachytili falošné údaje, ako sú pri súčasných reálnych útokoch [26].

- **Právne aspekty:** v oblasti rozpoznávania tváre vo všeobecnosti legislatíva na ochranu osobných údajov obmedzuje zdieľanie biometrických databáz medzi výskumnými skupinami. Tieto právne obmedzenia prinútili väčšinu laboratórií alebo spoločností pracujúcich v oblasti prezentačných útokov získať vlastné dátové súbory, ktoré boli avšak zväčša malé a obmedzené [26].

Prvou verejne dostupnou databázou PAD *Presentation attack detection* bola databáza NUAA [48]. Súbor údajov je tvorený zábermi 15 osôb, na ktorých základe ktorých bolo vytvorených 5105 platných prístupových záberov a 7509 falošných záberov určených k prezentačným útokom. Zábery boli zachytávané webovou kamerou pri 20 FPS s rozlíšením 640×480 pixlov. Subjekty boli zachytené v 3 rôznych priestoroch a rôznych svetelných podmienkach.

Medzi najnovšie a zároveň najrobustnejšie datasety patrí CelebA-Spoof. Tento súbor je tvorený celkom 625 537 obrázkami 10 177 subjektov, pomer živého a falošného obsahu je 1:3. Je rozdelený na trénovaciu, validačnú a testovaciu sadu v pomere 8:1:1. Sfalšované obrázky sú zachytené z 8 scén (2 prostredia $\times$ 4 svetelné podmienky) s viac ako 10 senzormi [54]. V priebehu rokov sa vyvinulo množstvo verejne dostupných databáz na danú problematiku [1]. Ich zoznam je zhrnutý v tabuľke 2.1.

Tabuľka 2.1: Zoznam verejne dostupných datasetov [1].

Názov datasetu	**Počet LIVE/SPOOF**	**Typ súboru**	**Typ podvrhu**
NUAA	5105/7509	Image	Warped photo
PRINT-ATTACK Database	200/200	Video	Print Photos
Yale-Recaptured	640/1920	Image	Flat printed phot
IIIT-D Sketch Database	4603	Image	Flat sketched images
REPLAY-ATTACK DB	200/1000	Video	Print and replay
CASIA-FAS DB	150/450	Video	Warpod, cut: Replay video
3DMAD	30600/45900	Video	Video & 3D mask attacks
Kose and Dugelay	200/198	Video	3D Mask
MSU MFSD	110/330	Video	Print and Replay
UVAD	808/16268	Video	Video Replay
MSSPOOF	4704	Image	Print
REPLAY-MOBILE	390/640	Video	Photo and Video Attack
MSU-USSA	1140/9120	Image	print, Replay
SMAD	1008	Video	3D silicon mask
OULU-NPU	1980/3960	Video	Print and video/replay
SiW	1320/3300	Video	Print and Replay
MFAD	1000/1100	Video	Print, Replay
CASIA-SURF CeFA	23538	Video	Print, Replay, 3D print & Silica mask
CASIA-SURF	3000/18000	Video	Print, Cut
CelebA-Spoof	625,537	Video	Print, Replay, 3D mask
ROSE-Youtu	3350	Video	Printed, replay, and 3D mask attacks

Obr. 2.5: Príklady útokov z datasetu CelebA-Spoof, prevzaté z [5].

2.2.2 Nepriamy útok

- Keď senzor získa surové biometrické údaje, posiela tieto surové dáta modulu na extrakciu príznakov na predspracovanie prostredníctvom komunikačného kanála. Tento kanál je medzi senzorom a modulom na extrakciu príznakov. Je prestrihnutý s cieľom ukradnúť biometrický znak a uložiť ho niekde inde. Následne sa predtým uložený biometrický znak znovu prehrá modulu na extrakciu príznakov, aby sa obišiel senzor [30].

- Senzor získa surové biometrické údaje, posiela tieto dáta do modulu extraktora príznakov. Podvodník vyvíja tlak na modul extraktora príznakov, aby produkoval hodnoty príznakov vybrané útočníkom namiesto generovania hodnôt príznakov vytvorených z pôvodných údajov získaných zo senzora [25].

- Tento útok je podobný útoku *replay attack*, ale rozdiel spočíva v tom, že podvodník prestrihne komunikačný kanál medzi modulom na extrakciu príznakov a modulom na porovnávanie a ukradne hodnoty príznakov pravého používateľa . Tieto hodnoty môžu byť neskôr prehrané modulu na porovnávanie [30].

- Tento typ útočí s cieľom vygenerovať vysoké skóre zhody, aké si vybral podvodník, aby sa obišiel biometrický autentifikačný systém bez ohľadu na hodnoty získané zo vstupnej sady príznakov [35].

- K útoku dochádza, keď podvodník naruší bezpečnosť databázy pridaním nových šablón, úpravou existujúcich šablón a odstránením existujúcich šablón. Útok na systémovú databázu nie je ľahký, pretože šablóny sú chránené digitálnymi mechanizmami, ako sú steganografia, watermarking atď. Na úspešný útok na systémovú databázu musí byť potrebné určité poznanie vnútorného fungovania systému [35].

- Útok je možný len vtedy, keď sa šablóna prenáša cez komunikačný kanál medzi systémovou databázou a modulom na porovnávanie. K tomu dochádza, keď podvodník

modifikuje alebo upravuje obsah prenášanej šablóny. Podvodník prestrihuje kanál, aby ukradol, nahradil alebo zmenil biometrickú šablónu [30].

- Podvodník môže prepísať výsledok vyhlásený modulom na porovnávanie. V tomto útoku môže podvodník narušiť skóre zhody, ktoré je prenášané cez komunikačný kanál medzi modulom na porovnávanie a aplikáčnym zariadením. Prepína skóre zhody, aby zmenil pôvodné rozhodnutie (akceptovať alebo zamietnuť) modulu na porovnávanie [30].

2.3 Testovanie odolnosti proti prezenčnému útoku

Normy a certifikácie sú základ pre zabezpečenie, že biometrické systémy sú spoľahlivé a ochránia užívateľov pred neoprávneným prístupom. Vďaka nim sú technológie na detekciu overované a certifikované medzinárodnými autoritatívnymi organizáciami [51].

ISO/IEC 30107-3
ISO/IEC 30107-3 [21] je súčasťou série medzinárodných noriem zameraných na detekciu útokov na biometrickú prezentáciu (PAD), ktoré založila Medzinárodná organizácia pre normalizáciu (ISO) a Medzinárodná elektrotechnická komisia (IEC). Tieto štandardy stanovujú princípy pre metódy zisťovania prezentačných útokov v systémoch, ktoré sa spoliehajú na biometrické rozpoznávanie. Jeho cieľom je poskytnúť štandardizovaný a metodický prístup na hodnotenie výkonu biometrických systémov z hľadiska ich schopnosti odhaliť a zabrániť spoofingovým útokom. Norma ISO/IEC 30107-3 je rozhodujúca pre vývojárov a integrátorov biometrických systémov, ako aj pre koncových používateľov, ktorí sa spoliehajú na integritu týchto systémov pre bezpečnú autentifikáciu. Súlad s týmto štandardom zaisťuje, že systémy sú podrobené prísnym a jednotným testovacím postupom, čo poskytuje istotu, že dokážu spoľahlivo identifikovať a zabrániť prezentačným útokom.

Národný ústav pre normy a technológie (NIST)
Národný inštitút pre štandardy a technológie, bežne označovaný ako NIST [36], je neregulačná federálna agentúra v rámci Ministerstva obchodu USA. Poslanie NIST zahŕňa širokú škálu fyzikálnych vied, inžinierstva a informačných technológií. V oblasti biometrie hrá NIST kľúčovú úlohu pri vývoji referenčných hodnôt, vykonávaní výskumu a vytváraní noriem pre detekciu živosti a iných biometrických technológií prostredníctvom svojho laboratória informačných technológií (ITL). ITL podporuje vývoj a zavádzanie pokročilých informačných technológií na zlepšenie obchodu a posilnenie národnej bezpečnosti. Konkrétne v prípade biometrie testuje NIST výkon systémov detekcie živosti, aby sa zistila ich účinnosť pri rozlišovaní medzi živou osobou a syntetickým alebo neživým falošným artefaktom.

Aliancia FIDO
Aliancia Fast Identity Online (FIDO) [27] je združenie s cieleným poslaním: znížiť celosvetovú závislosť na heslách pre digitálnu bezpečnosť. Aliancia vyvíja a podporuje štandardy autentifikácie, ktoré pomáhajú webovým stránkam a organizáciám posunúť sa od zabezpečenia iba heslom. Pokiaľ ide o detekciu živosti, Aliancia FIDO stanovuje usmernenia a certifikačné procesy, ktoré zaisťujú, že biometrické systémy sú bezpečné a odolné voči podvodom. Štandardy FIDO sa považujú za jedny z najrobustnejších, ktorých cieľom je zjednodušiť a zabezpečiť autentifikáciu pre používateľov aj poskytovateľov služieb. Špecifi-

kácie podporujú širokú škálu autentifikačných technológií vrátane biometrie, kde je detekcia živosti kľúčovým komponentom na zabezpečenie toho, aby prezentovaná biometria nebola falošná.

iBeta Quality Assurance
iBeta Quality Assurance [19] je nezávislé testovacie laboratórium, ktoré sa špecializuje na zabezpečenie kvality a certifikáciu pre rôzne softvérové produkty, vrátane produktov z oblasti biometrie. Sú akreditované na testovanie zhody s normou ISO/IEC 30107-3 [21] pre detekciu útokov prezentácií (PAD), ktorá sa priamo týka detekcie živosti v biometrických systémoch. Ako laboratórium akreditované národným dobrovoľným laboratórnym akreditačným programom (NVLAP), iBeta vykonáva prísne testovanie biometrických riešení, aby sa zaistilo, že dokážu spoľahlivo odhaliť a zabrániť podvodným pokusom o prístup pomocou syntetických alebo pozmenených biometrických údajov.

Európska asociácia pre biometriu (EAB)
EAB [8] je organizácia, ktorá sa snaží presadzovať správne a prospešné používanie biometrie v Európe, pričom zdôrazňuje potrebu výskumu a vývoja v tejto oblasti. EAB funguje ako sieťová platforma, ktorá poskytuje fórum pre biometrické zainteresované strany na výmenu informácií a odborných znalostí. Jednou z kľúčových funkcií EAB je informovať a ovplyvňovať predpisy v európskom biometrickom priestore a zabezpečiť, aby odrážali najnovší vedecký a technologický pokrok. Podporuje etické používanie biometrie a podporuje rozvoj biometrických noriem na posilnenie dôvery v tieto technológie. EAB tiež organizuje konferencie, workshopy a školenia s cieľom vzdelávať a šíriť najlepšie postupy v biometrickom overovaní a identifikácii vrátane kritického aspektu zisťovania živosti.

2.4 Zhrnutie

Kapitola poskytuje podrobný pohľad na súčasný stav biometrických systémov, ich dôležitosť v rôznych aplikáciách a neustále sa meniace výzvy, ktoré predstavujú prezenčné útoky. Biometrické systémy, definované unikátnymi fyzickými a správaním podmienenými charakteristikami, sa čoraz viac integrujú do bezpečnostných protokolov na celom svete, či už ide o jednoduché systémy založené na odtlačkoch prstov alebo sofistikované rozpoznávanie tváre.

Diskutuje sa o viacerých typoch prezenčných útokov vrátane falšovania tváre, foto a video útokov, a tiež použitia 3D masiek a make-upu alebo protéz, ktoré môžu kompromitovať integritu biometrických systémov. Čo sa týka najčastejšieho typu útoku na biometrické systémy, útoky pomocou falšovaných fotografií sú považované za najbežnejšiu a najkritickejšiu formu útoku, pretože tlač farebného obrázku je dnes lacná a jednoduchá.

Kľúčové normy a certifikácie, ako je ISO/IEC 30107-3 [21], spolu s autoritatívnymi organizáciami ako NIST [36], FIDO Alliance [27], iBeta Quality Assurance [19] a Európska asociácia pre biometriu (EAB) [8], hrajú zásadnú úlohu v stanovení bezpečnostných štandardov a protokolov. Tieto normy zabezpečujú, že systémy sú spoľahlivé a sú schopné identifikovať a odolať sofistikovaným útokom.

Vzhľadom na neustály vývoj útokových techník musí byť vývoj bezpečnostných riešení dynamický a neustále sa vyvíjajúci proces. Dostupné verejné databázy a štandardizované testovacie súpravy, ako sú CelebA-Spoof [54] a mnohé iné, poskytujú cenné zdroje pre porovnávanie a hodnotenie aktuálnych biometrických systémov a ich odolnosti voči útokom.

Záverom je, že hoci sú biometrické systémy v súčasnosti vysoko odolné voči mnohým formám prezenčných útokov, nepretržitý výskum a vývoj sú nevyhnutné pre udržanie kroku s neustále sa meniacimi stratégiami útočníkov. Jedným z najväčších únikov dát z biometrického systému bol incident s databázou BioStar 2 spoločnosti Suprema[1], ktorý odhalil údaje o 28 miliónoch záznamov. Tieto záznamy obsahovali údaje o odtlačkoch prstov a rozpoznávaní tváre, a to všetko bolo uložené nezašifrovane. V databáze boli aj používateľské mená a heslá zobrazené ako obyčajný text, čo viedlo k vážnym bezpečnostným rizikám. Tento únik sa týkal organizácií po celom svete vrátane vládnych a policajných služieb v 83 krajinách. Po jeho objavení bola databáza zabezpečená, ale incident poukazuje na kritickejšie dôsledky úniku biometrických dát v porovnaní s inými typmi údajov, pretože biometrické informácie nemožno ľahko zmeniť alebo resetovať ako heslá.

[1] https://www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/

Kapitola 3

Rozpoznávanie tváre a detekcia živosti

Účelom tejto kapitoly je zameranie sa na jeden z kľúčových aspektov biometrických systémov, a tým je detekcia živosti tváre. Rozvádza rôzne prístupy k detekcií, vrátane analýzy pohybu tváre, termálnu analýzu, techniky hlbokého učenia a podobne. Za úspešnou detekciou živosti tváre spočíva prvotne jej samotné rozpoznanie na skúmanom zábere. Taktiež je zahrnutý prehľad niektorých spôsobov vektorizácie tváre, ako sú ArcFace [11] alebo CosFace [55], ktoré prispievajú k rozvoju a širšiemu uplatneniu biometrických technológií.

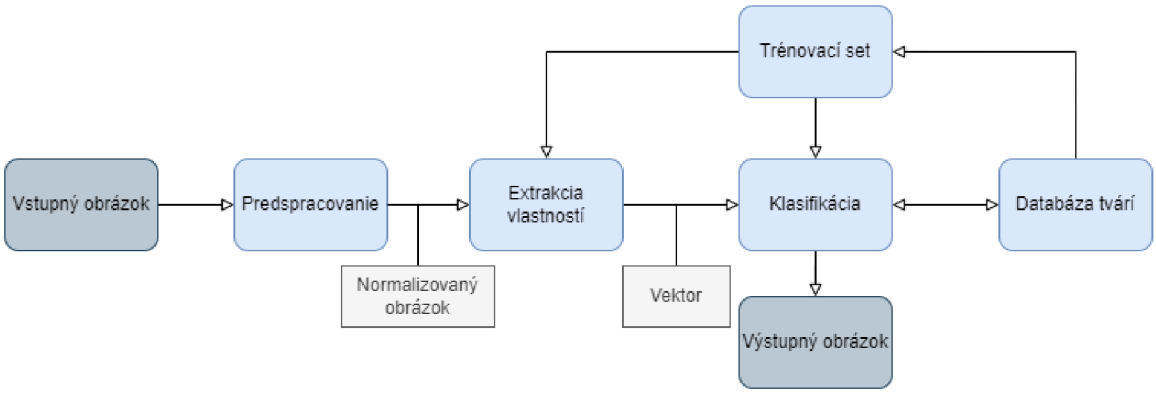
3.1 Rozpoznávanie tváre

Proces, ktorý je potrebný na rozpoznávanie tváre na obrázku, využíva pokročilé metódy počítačového videnia a strojového učenia, aby nie len identifikoval prítomnosť ľudských tvárí v digitálnych obrazoch alebo video sekvenciách, ale aj určil ich identitu.

Tento proces je kľúčový v rôznych aplikáciách, od zabezpečovacích systémov cez interaktívne reklamy až po pokročilé užívateľské rozhrania. Úspešnosť rozpoznávania tváre závisí od schopnosti algoritmu spracovať a interpretovať obrovské množstvo vizuálnych dát a rozpoznať špecifické vzory, ktoré definujú ľudskú tvár. Rozpoznávanie tváre zahŕňa viaceré kroky [46]:

- Predspracovanie obrazu - kritickým krokom, ktorý zahŕňa úpravy obrazu, ako sú normalizácie intenzity, odstránenie šumu a vylepšenie kontrastu, čo umožňuje algoritmom efektívnejšie rozpoznávanie tvárí.
- Extrakcia vlastností - sústreďuje sa na získavanie podstatných informácií z identifikovaných čŕt, ako sú vzdialenosť medzi očami, tvar nosa, proporcie tváre a podobne, ktoré sú prevedené do numerického vektora.
- Klasifikácia - využíva vytvorený vektor na porovnanie s vektormi v databáze tvárí. Algoritmy strojového učenia tu analyzujú vektory na zhodu, aby určili, či tvár na obrázku zodpovedá nejakej osobe v databáze.
- Databáza tvárí - obsahuje predom definované a trénované vektory tvárí, ktoré slúžia ako referenčný materiál pre rozpoznávanie.

Tento proces je ilustrovaný na obrázku 3.1, ktorý začína vstupným obrázkom a je ukončený zobrazením výsledného obrázku s identifikovanou osobou.



Obr. 3.1: Blokový diagram systému rozpoznávania tváre.

3.2 Analýza pokročilých prístupov rozpoznávania

Prístupy k rozpoznávaniu tváre sa časom vyvíjali a adaptovali. Spočiatku sa jednalo o nízku presnosť a efektívnosť. S príchodom hlbokého učenia a konvolučných neurónových sietí (CNN) sa kapacita pre presné rozpoznávanie dramaticky zvýšila. Tieto techniky, vďaka ich schopnosti učiť sa z veľkých objemov dát a identifikovať zložité vzory, otvorili dvere k omnoho presnejším a adaptívnejším systémom. Moderné algoritmy dokážu s nevídanou presnosťou identifikovať jednotlivé rysy, dokonca i v rôznych podmienkach, ako sú rôzne úrovne osvetlenia alebo čiastočné prekrytie. Nižšie sú uvedené 2 vybrané moderné algoritmy.

3.2.1 ArcFace

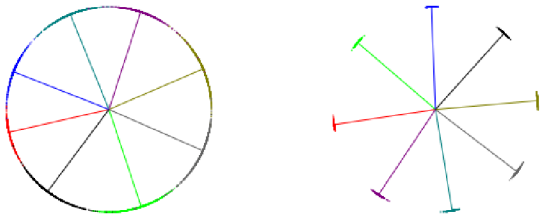
Stratová funkcia ArcFace (ang. *Additive Angular Margin Loss*) [11] je používaná pri úlohách rozpoznávania tváre. Tradične pri ich riešení využíva softmax (normalizovaná exponenciálna funkcia, ktorá konvertuje vektor K reálnych čísel na rozloženie pravdepodobnosti K možných výsledkov). Avšak softmax neoptimalizuje explicitne vloženie vlastností na to, aby nútila k vyššej podobnosti vzorkov v rámci triedy a rozmanitosť vzorkov medzitriedy. Toto vedie k výkonnostnej medzere pre hlboké rozpoznávanie tváre pri veľkých variáciách vzhľadu v rámci triedy.

Stratová funkcia ArcFace transformuje logity $W_j^T x_i = \|W_j\| \, \|x_i\| \cos\theta_j$, kde θ_j je uhol medzi váhou W_j a vlastnosťou x_i. Individuálna váha $\|W_j\| = 1$ je fixovaná normalizáciou L_2[1]. Vložená vlastnosť $\|x_i\|$ je fixovaná L_2 normalizáciou a znova škálovaná na s. Krok normalizácie vlastností a váh zabezpečuje, že predikcie závisia iba na uhle medzi vlastnosťou a váhou. Naučené vlastnosti sú tak distribuované na hypergule s polomerom s. Nakoniec sa pridáva aditívna uhlová miera penalty m medzi x_i a W_{y_i} na súčasné zvýšenie kompaktnosti in-triedy a rozdielu medzitriedy. Kedže navrhnutá aditívna uhlová miera penalty je rovnaká ako miera penalty v geodetickom rozostupe na normalizovanej hypergule, metóda sa nazýva ArcFace [11]:

$$L_3 = -\frac{1}{N}\sum_{i=1}^{N}\log\frac{e^{s\left(\cos\left(\theta_{y_i}+m\right)\right)}}{e^{s\left(\cos\left(\theta_{y_i}+m\right)\right)}+\sum_{j=1,j\neq y_i}^{n}e^{s\cos\theta_j}}$$

[1] https://www.kaggle.com/code/paulrohan2020/euclidean-distance-and-normalizing-a-vector

Ako ukazuje obr. 3.2, softmax poskytuje hrubo oddeliteľné vloženie vlastností, ale spôsobuje zreteľnú nejednoznačnosť v rozhodovacích hraniciach, zatiaľ čo ArFace evidentne vynucuje viac zreteľnú medzeru medzi najbližšími triedami.



(a) Softmax (b) ArcFace

Obr. 3.2: Bodky značia vzorky a čiary smerujú k centrálnemu smeru každej identity. Na základe normalizácie vlastností sú všetky vlastnosti tváre posunuté do oblúkového priestoru s fixným polomerom. Geodetický rozdiel vzdialenosti medzi najbližšími triedami sa stáva zrejmým, keď je pridaná aditívna uhlová penalizácia [11].

3.2.2 CosFace

LMCL (ang. *Large Margine Cosine Loss*) [55] známy aj ako CosFace je metóda, ktorá sa snaží skvalitniť výsledky tým, že zmení spôsob, akým model učí rozlišovať medzi tvárami. Oproti iným prístupom pracuje priamo v priestore kosínusov, namiesto priestoru uhlov. Matematicky možno vyjadriť CosFace ako [55]:

$$L_{lmcl} = \frac{1}{N}\sum_{i} -\log \frac{e^{s\left(\cos\left(\theta_{y_i,i}\right)-m\right)}}{e^{s\left(\cos\left(\theta_{y_i,i}\right)-m\right)} + \sum_{j\neq y_i} e^{s\cos\left(\theta_{j,i}\right)}},$$

ktorý je podmienený

$$\begin{aligned} W &= \frac{W^*}{\|W^*\|}, \\ x &= \frac{x^*}{\|x^*\|}, \\ \cos\left(\theta_j, i\right) &= W_j^T x_i, \end{aligned}$$

kde:

- N je celkový počet vzoriek, ktoré sa berú do úvahy,
- s je škálovací faktor, ktorý upravuje veľkosť,
- m je Uhlová penalizácia, pridaná k uhlu θ na zlepšenie presnosti,
- $\cos(\theta_j, i)$ vyjadruje mieru podobnosti alebo rozlíšenia medzi rôznymi identitami,
- y_i predstavuje skutočnú triedu pre vzorku i,
- x_i je normalizovaná vlastnosť,
- W Normalizovaná váha po normalizácii L_2.

Techniky rozličných prístupov v porovnaní s LMCL [55]:

- **Softmax Loss:**

$$\|W_1\| \cos(\theta_1) = \|W_2\| \cos(\theta_2).$$

  Hranica rozhodovania závisí od magnitúdy vektorov váh a kosínusy uhlov, čo vedie k prekrývajúcej sa oblasti rozhodovania (margin < 0) v priestore kosínusov. Počas testovania sa používa iba podobnosť kosínusov medzi testovanými vektormi príznakov tvárí.

- **Normalizovaný Softmax Loss:** K riešeniu pridáva normalizáciu, ktorá normalizuje vektory váh W_1 a W_2 na konštantnú magnitúdu 1, čo vedie k rozhodovacej hrane:

$$\cos(\theta_1) = \cos(\theta_2)$$

  Rozhodovacia hrana odstraňuje radikálne variácie, čím dosahuje dokonalú klasifikáciu testovacích vzoriek v priestore kosínusov. Je však citlivá na šum, pretože neexistuje rozhodovací margin.

- **A-Softmax:** Zvyšuje presnosť rozoznávania tváre pridaním dodatočného marginu, pričom jeho rozhodovacia hrana je daná ako:

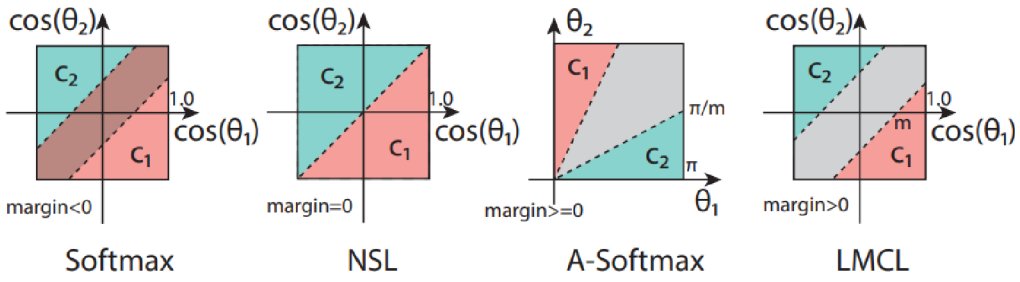
$$C_1 : \cos(m\theta_1) \geq \cos(\theta_2),$$
$$C_2 : \cos(m\theta_2) \geq \cos(\theta_1).$$

  Avšak nie je konzistentný pre všetky hodnoty uhlov, margin sa zmenšuje s klesajúcim uhlom a úplne zmizne pri $\theta = 0$. To môže spôsobiť problémy pre triedy C_1 a C_2, ktoré su vizuálne podobné a majú menší uhol medzi W_1 a W_2.

- **LMCL:** definuje rozhodovací margin v priestore kosínusov namiesto uhlov:

$$\cos(\theta_1) \geq \cos(\theta_2) + m$$
$$\cos(\theta_2) \geq \cos(\theta_1) + m$$

  Vďaka tomu je LMCL robustnejší než NSL, pretože malá perturbácia okolo rozhodovacej hrany nevedie k nesprávnemu rozhodnutiu. Kosínusový margin sa aplikuje konzistnentne na všetky vzorky, bez ohľadu uhly ich vektorových váh.



Obr. 3.3: Porovnanie rôznych rozhodovacích margín pre rôzne stratové funkcie v prípade 2 tried. Čiarkovaná čiara predstavuje rozhodovaciu hranicu, a šedé oblasti sú rozhodovacie marginy [55].

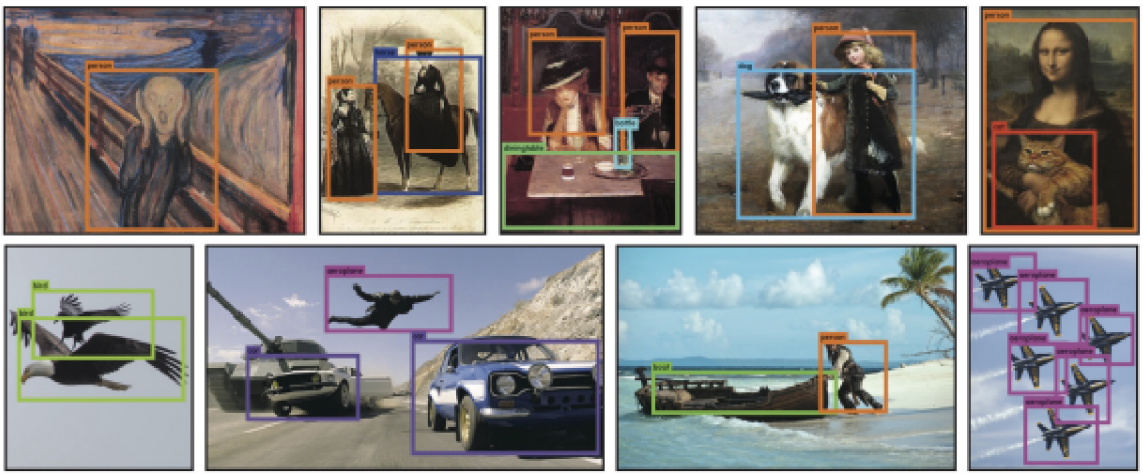
3.3 Detekčné modely

3.3.1 YOLO

YOLO (You Only Look Once) [45] je veľmi populárny model detekcie objektov a segmentácie obrazu. Vyvinuli ho Joseph Redmon a Ali Farhadi na univerzite vo Washingtone. Na trh bol uvedený v roku 2015. Je známy pre svoju rýchlosť a presnosť.

Princíp detekcie spočíva v tom, že sa vstupný obrázok rozdelí do mriežky o veľkosti $S \times S$, obvykle s veľkosťou 13×13 alebo 26×26, v závislosti od konkrétneho typu. Každá bunka mriežky je zodpovedná za predikciu objektov vo svojom priestore. Následne sieť extrahuje vysokoúrovňové črty zo vstupného obrázka pomocou konvolučnej neurónovej siete, cez ktorú prechádza len raz. Potom predikuje ohraničený priestor (obdĺžnik) regresiou súradníc ľavého horného rohu, šírky a výšky boxu. Navyše vypočíta aj skóre istoty, ktoré zodpovedá pravdepodobnosti, že je v danom ohraničenom priestore objekt. Okrem tejto predikcie predikuje aj pravdepodobnosť tried pre každú mriežku bunky. To znamená, že vie nielen detegovať objekty, ale i identifikovať ich príslušné kategórie [53].

Po vykonaní tohto procesu sa na ne aplikuje prah istoty na filtrovanie detekcie s nízkou istotou. Následne sa použije nerekurzívne potlačenie maximálnej hodnoty, aby sa odstránili duplikované alebo prekrývajúce sa priestory, zabezpečujúc, že pokračuje iba najpresnejšie vyhľadávanie. Na toto je využitý algoritmus NMS (*Non-maximum suppression*) [18].



Obr. 3.4: Príkladné využitie YOLO detekcie na rôznych objektoch. I keď je to väčšinou presné, ale i tak sa nájdu výnimky ako napríklad detekcia osoby ako lietadlo, prevzaté z [45].

Aktuálne najnovším modelom je YOLOv8 vydaným v roku 2023. Architektúra YOLOv8 sa stala štandardom v oblasti objektovej detekcie, a to vďaka rôznym inováciám a vylepšeniam, ktoré priniesla oproti svojim predchodcom. Jedným z kľúčových prínosov je odstránenie potreby definovať fixné *anchor boxes* pre jednotlivé triedy objektov. Namiesto toho sa model sám naučí predikovať obdĺžniky okolo objektov, čím sa zvyšuje jeho schopnosť správne lokalizovať objekty rôznych tvarov a veľkostí.

Model YOLOv8 podporuje používanie predtrénovaných modelov, ktoré sú špeciálne navrhnuté na detekciu bežných objektov. Tým sa užívateľom umožňuje jednoducho využívať existujúce vedomosti a zároveň model prispôsobovať špecifickým potrebám pomocou vlast-

ných trénovacích dát. V rámci detekčných metód YOLOv8 podporuje klasifikáciu, objektovú detekciu a segmentáciu obrazu. Klasifikácia je zameraná na priradenie celého obrázka k jednej triede, zatiaľ čo objektová detekcia ide o identifikáciu a lokalizáciu viacerých objektov v obraze. Segmentácia obrazu ide ešte ďalej a určuje presné tvary a hranice objektov na pixlovej úrovni, čo umožňuje detailnejšiu analýzu obsahu obrazu [53].

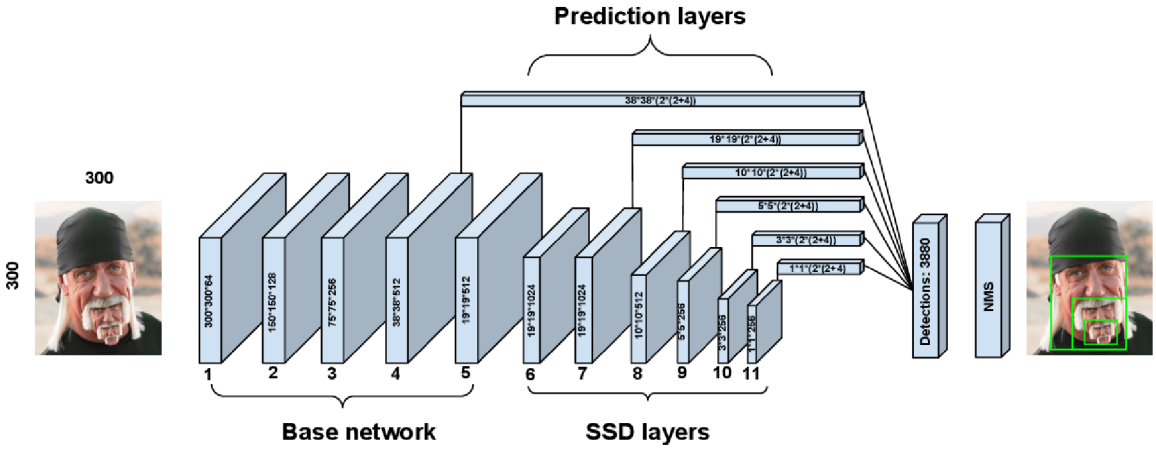
3.3.2 RetinaFace

Jednofázový detektor tváre RetinaFace [10] je špecializovaný nástroj, ktorý dokáže s vysokou presnosťou lokalizovať tváre a ich orientačné body. Využíva *backbone* architektúru, ktorá je obvykle založená na predtrénovaných konvolučných neurónových sieťach. Tieto *backbone* siete začleňujú i koncept *Feature Pyramid Network* (FPN) [32], čo je kľúčová architektonická zložka umožňujúca efektívne zachytávať vizuálne informácie na rôznych úrovniach rozlíšenia. FPN pomáha tým, že integruje vysoko-rozlišovacie detaily z nižších vrstiev s kontextovými informáciami z vyšších vrstiev.

RetinaFace taktiež využíva viaczložkovú stratovú funkciu, ktorá obsahuje viacero typov chýb pre rôzne aspekty detekcie - od rozpoznania samotnej tváre, cez určenie jej hraníc, až po presnú lokalizáciu kľúčových bodov, ako sú oči alebo ústa. Tento integrovaný prístup umožňuje efektívne identifikovať tváre naprieč rôznymi mierkami a za rôznych podmienok.

3.3.3 SSD

SSD (*Single Shot Detection*) je metóda detekcie objektov v obraze, ktorá dokáže identifikovať a lokalizovať rôzne objekty v jednom kroku, bez potreby predbežného navrhovania kandidátnych regiónov [50]. Tento model je navrhnutý tak, aby predikoval množstvo ohraničovacích boxov s rôznymi pomermi strán a rozmermi priamo na viacerých úrovniach funkcie mapy. SSD kombinuje tieto predikcie s dôveryhodnostým skóre, aby určil pravdepodobnosť prítomnosti objektu v každom boxem, čím poskytuje rýchlu a spoľahlivú detekciu objektov v reálnom čase.



Obr. 3.5: Architektúra modelu SSD, prevzaté z [50].

Obrázok 3.5 ilustruje architektúru modelu SSD pre detekciu objektov. Základná sieť predstavuje konvolučnú neurónovú sieť, ktorá spracováva vstupný obraz a extrahuje z neho črty. SSD vrstvy zahŕňajú dodatočné konvolučné vrstvy, ktoré poskytujú predikcie na viacerých úrovniach. Sú to predikčné vrstvy, ktoré predpovedajú polohu a klasifikáciu poten-

ciálnych objektov. Rôzne veľkosti predikčných vrstiev umožňujú detekciu objektov v rôznych mierkach. Nakoniec, NMS (*Non-Maximum Suppression*) je postprocesný krok, ktorý zlepšuje detekcie odstránením prekrývajúcich sa boxov, pričom ponecháva len najpravdepodobnejšie detekcie pre každý objekt [18].

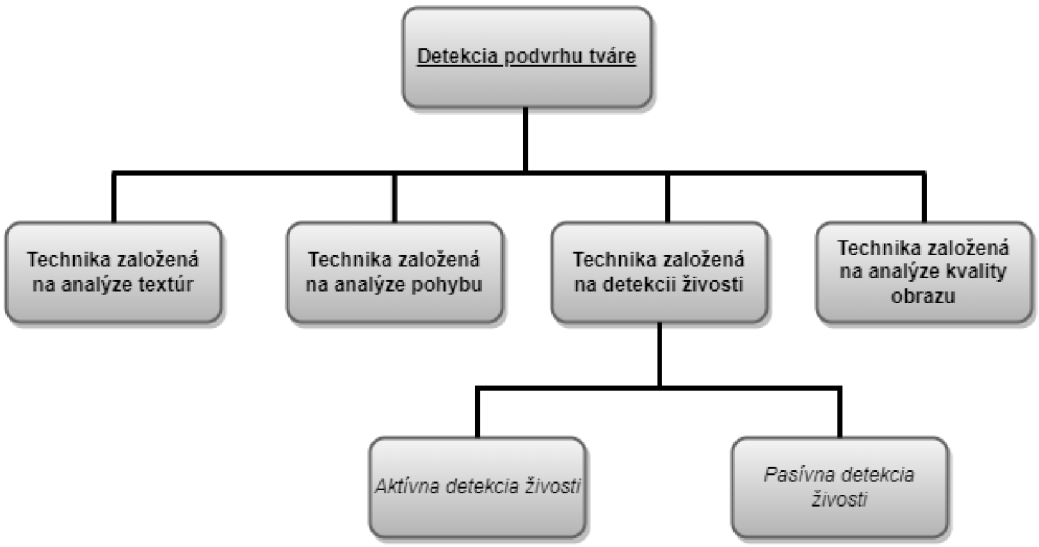
3.4 Detekcia živosti

Ku rozpoznávaniu tváre je nesmierne dôležitá i detekcia jej živosti. Táto technika je veľmi dôležitým krokom ku zaisteniu bezpečnosti systémov rozpoznávania tváre. Pomáha predchádzať pokusom o obídenie systému pomocou falošných alebo sfalšovaných obrázkov alebo videí tváre osoby. Bez tejto detekcie by útočník mohol potencionálne obísť systém predložením fotografie alebo videa tváre osoby, a nie samotnej reálnej osoby. Okrem toho môže použitie detekcie živosti pomôcť zlepšiť celkovú presnosť systému rozpoznávania tváre odstránením falošných nezhôd s fotografiami či videami. Pomáha tiež chrániť súkromie jednotlivcov tým, že zabraňuje neoprávnenému prístupu k ich osobným údajom. rôznym podvodom a krádežiam identity.

Najpoužívanejšími metódami na zvládnutie útokov sú analýzy pohybu a textúr, ako aj umelá inteligencia. Pre autentifikáciu delíme metódy detekcie živosti na aktívnu a pasívnu [20].

Aktívna metóda vyžaduje priamu interakciu užívateľa so systémom, napríklad pohybom hlavy, žmurknutím či rozprávaním. Tento prístup môže byť niekedy problematický. Útočníci dokážu ľahko tento systém oklamať pomocou rôznych pomôcok medzi ktoré patrí napríklad i 3D papierová maska.

Pasívna metóda narozdiel od tej aktívnej využíva senzory na detekciu signálov, ako je srdcový tep a pohyb, ktorými určí, že skúmajúci objekt je živá osoba. Vo všeobecnosti je táto metóda presnejšia, avšak i drahšia. Pre užívateľa je tento spôsob pohodlnejší, pretože nemusí vykonávať žiadne pohyby vyžadované systémom overovania živosti.



Obr. 3.6: Klasifikácia techník detekcie falošnej tváre.

3.5 Algoritmy detekcie živosti tváre

Existuje niekoľko algoritmov pre detekciu podvrhu tváre pomocou kamery. Útoky sa každým rokom stávajú viac sofistikovanými, a preto je nutné neustále testovať a vytvárať spoľahlivé metódy a algoritmy. Možno ich klasifikovať do rôznych kategórií na základe ich prístupov a metód použitých pri detekcií:

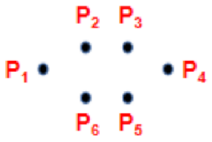
- **Pohybová analýza:** je sústredená na sledovanie mikro-pohybov a blikania. Môže to zahrňovať sledovanie drobných pohybov očí, pohybov pier a tvárových svalov. Živá tvár vykazuje prirodzené pohyby, ktoré sa ťažko napodobňujú statickými obrazmi alebo videami [42].
- **Analýza termálnych vlastností:** využíva rozdiely v teple vyžarovanom živou pokožkou oproti statickým objektom a fotografiám. Tepelná infračervená kamera môže zachytiť teplotné rozdiely, čo umožňuje identifikovať tváre i pri nízkych svetelných podmienkach [29].
- **Analýza textúry pokožky:** spočíva v drobnom skúmaní štruktúry a detailov textúry pokožky. Využíva sa pri tom pokročilá technika analýzy obrazu [31].
- **Analýza 3D tvaru:** využívaním 3D kamier umožňuje získať informácie o trojrozmernom obraze. 3D informácie umožňujú lepšiu diferenciáciu medzi skutočnými a falošnými tvárami [56].
- **Detekcia odleskov:** Štruktúry na tvári, ako sú noc, oči a pery môžu vytvárať odlesk pri osvetlení. Tieto odlesky môžu slúžiť ako jedinečné prvky, ktoré sa dajú analyzovať [49].
- **Kombinácia metód:** Kombinácia rôznych vyššie spomenutých metód pre zvýšenie účinnosti a spoľahlivosti detekcie.

Každá metóda ma svoje výhody a obmedzenia a výber vhodnej závisí od konkrétnych požiadaviek a kontexte nasadenia.

3.5.1 Algoritmus detekcie žmurknutia

Metóda je mnohokrát využívaná v kombinácií s iným prístupom. Je zameraná na odhalenie žmurknutia ako spôsob identifikácie podvrhu. V odbornom článku [42] zameranom na detekciu žmurkania je to v kombinácií s lokálnymi binárnymi vzormi (LBP). Prvotne sa extrahujú textúrne črty obrazu za pomoci LBP [40], čím sa do istej miery eliminuje problém so zmenami osvetlenia. Následne sú extrahované črty vstupované do siete ResNet [28] s pridaním mechanizmu detekcie žmurknutia.

Mechanizmus funguje tak, že analyzuje vzorec žmurkania očí človeka, aby určil, či tvár patrí živej osobe alebo nie. Prvým krokom algoritmu je detekcia očí na obrázku a potom extrahuje nájdenú oblasť. Následne analyzuje vzory žmurkania hľadaním zmien intenzity v oblasti oka v priebehu času. Pokiaľ oči žmurkajú prirodzenou frekvenciou a zmeny intenzity odpovedajú skutočnému žmurkaniu, potom algoritmus určí, či je tvár živá alebo nie. Pokiaľ zmeny intenzity neodpovedajú skutočnému žmurkaniu alebo sa oči nemrkajú vôbec, potom algoritmus určí, že tvár je falošná. Tento spôsob je pomerne jednoduchý na implementáciu, je rýchly a výpočetne efektívny. Každé oko je reprezentované 6 bodmi, ako je znázornené na obrázku 3.7. Na základe týchto bodov sa následne vypočíta EAR (*Eye*



Obr. 3.7: Body anotácie funkcie oka [42].

Aspect Ratio), čo je metrika používaná na kvantifikáciu otvorenosti alebo zatvorenosti očí v obraze alebo videu. Jeho princíp je založený na pomere dĺžky a šírky očného priestoru. Vypočíta sa pre každý pár očí a ak tento pomer klesne pod istý prah, môže to naznačovať žmurknutie alebo zatvorenie očí. Výpočet je definovaný nasledovne [42]:

$$EA\ R = \frac{\|P_2 - P_6\| + \|P_3 - P_5\|}{2\,\|P_1 - P_4\|}$$

kde body P1 až P6 prezentujú koordináty kútikov oka. Môže byť použitý samostatne alebo ako súčasť zložitejšieho systému detekcie živosti.

Výsledky experimentov ukazujú, že navrhovaný algoritmus dosahuje výbornej presnosti na datasetoch NUAA, CASIA-SURF a CASIA-FASD, čo sú štandardné benchmarky v oblasti rozpoznávania tváre, s dosiahnutou presnosťou až 99,48 %, 98,65 % a 99,17 % na jednotlivých datasetoch. Tento výsledok je dôkazom účinnosti metódy, ktorá zohľadňuje nie len statické črty obrazu, ale aj dynamické aspekty ako žmurknutie, na zvýšenie odolnosti proti podvrhom.

3.5.2 Tepelné infračervené zobrazovanie

Špecifická založená na využití tepelného infračerveného zobrazovania ponúka unikátne fyzikálne vlastnosti, ktoré môžu zvýšiť schopnosť detekcie útokov [29]. Termálny obraz ľudskej tváre je využitý ako jedinečný tepelný podpis, ktorý možno použiť ako vzor na rozpoznanie. Metóda spočíva v analýze relatívneho rozloženia teploty na povrchu tváre a susedných

(a) 3D-maska (b) Latexová maska

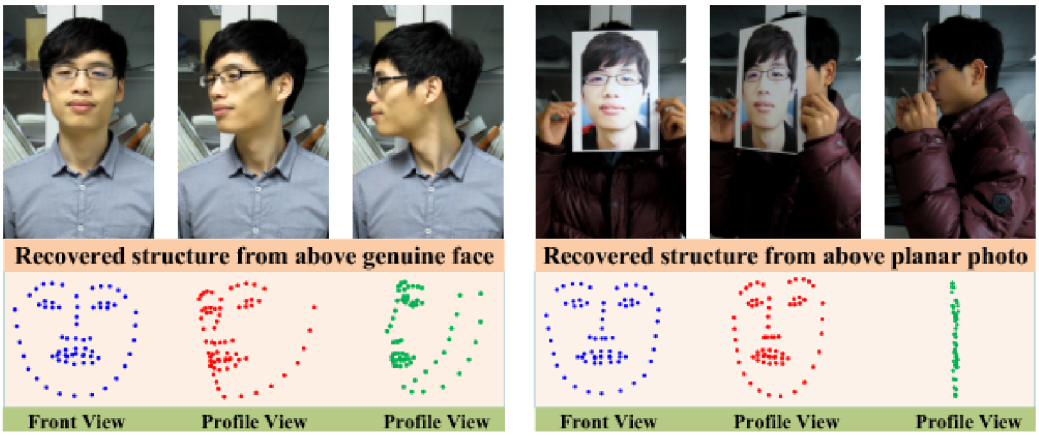
Obr. 3.8: Termo-snímky zobrazujúce osoby s maskami, prevzaté z [29].

oblastiach. Zobrazenie sa spolieha na pasívne emisie a nepotrebuje osvetlenie. Registrované žiarenie je priamo úmerné relatívnemu rozloženiu zdanlivej teploty objektov umiestených v zornom poli kamery. Schopnosť zachytiť tepelnú energiu závisí aj od parametrov kamery. Detekcia pri použití tohto algoritmu sa spolieha na analýzu rozdielov medzi obrazovými pixlami alebo ich skupinami. Tento spôsob je vhodný pri použití podvrhov 3D-maskami či latexovými maskami.

Validácia metódy odhalila vysokú účinnosť pri detekcii rôznych typov útokov, vrátane tých, ktoré využívali sofistikované PAI (*Presentation Attack Instruments*). Výsledky naznačujú, že prístup založený na termálnom infračervenom zobrazovaní môže byť účinným riešením pre detekciu sofistikovanejších foriem útokov na systémy rozpoznávania tváre, čím sa zvyšuje bezpečnosť a spoľahlivosť týchto systémov.

3.5.3 Analýza získanej trojrozmernej štruktúry

Návrh metódy spočíva v získaní 3D štruktúry tváre z videa alebo niekoľkých snímok zachytených z viac ako dvoch uhlov pohľadu [56]. Na rozlíšenie medzi pravým a falošným objektom sa tentokrát využíva SVM (*Support Vector Machine*), viz. sekcia 4.1.3. Algoritmus lokalizuje významné body na tvári a vyberá kľúčové snímky pre rekonštrukciu 3D štruktúry. Tie sa vyberajú na základe grafickej podobnosti, pričom sa uprednostňujú snímky s rôznymi uhľovými pohľadmi, čo zvyšuje diverzitu pre rekonštrukciu.



Obr. 3.9: Porovnanie 3D štruktúr tváre medzi falošnou a pravou tvárou, prevzaté z [56].

Táto metóda bola v štúdii porovnávaná s modernými metódami, ktoré zahŕňajú prístupy založené na vlastnostiach textúry, ako je napríklad metóda lokálnych binárnych vzorov (LBP) a s ich porovnaniami vyšla veľmi obstojne. Výskum bol založený na 3 databázach, pričom každá z nich bola vytvorená pomocou iného zariadenia. Tieto databázy obsahovali autentické tváre i falošné fotografie, vrátane planárnych fotografií a fotografií deformovaných vertikálne alebo horizontálne.

3.5.4 Algoritmus analýzy úrovne chyby (ELA)

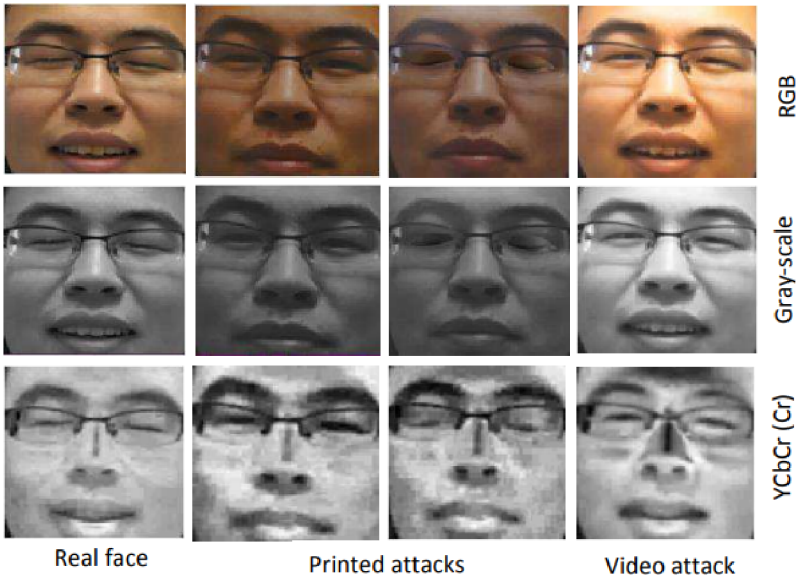
Analyzuje úroveň chyby obrazu, aby odhalil nezrovnalosti či anomálie [43], ktoré môžu naznačovať podvrh. Funguje tak, že sa najprv prevedie obrázok na snímok v odtieňoch sivej a potom ho skomprimuje na nižšiu úroveň kvality. Komprimovaný obrázok je potom porovnávaný s tým pôvodným a sú vypočítané rozdiely medzi nimi. Tieto rozdiely sú potom

mapované na rozličné úrovne chýb, pričom vyššie úrovne chýb indikujú vyššiu pravdepodobnosť podvrhu. Potom algoritmus analyzuje úrovne chýb v rôznych oblastiach obrazu, ako je pozadie, popredie a rysy tváre, aby odhalil akékoľvek nezrovnalosti. Pokiaľ je úroveň chýb omnoho vyššia než úroveň chýb prvkov tváre, môže to znamenať, že s pozadím bolo manipulované. Na záver porovná algoritmus úrovne chýb s predom definovanou prahovou hodnotou. Pokiaľ sú úrovne chýb nad prahovou hodnotou, algoritmus určí, že obrázok je podvrh. Je nenáročný na implementáciu, a podobne rýchly a výpočetne efektívny. Problém pri použití tohto algoritmu môže nastať ak sa použije sofistikovanejší podvrh, ktorý vznikol použitím pokročilého softwaru na úpravu obrázkov.

Navrhovaná metóda dosiahla najvyššiu presnosť 89,5 % využitím kombinácie Residual Network (ResNet) a K-Nearest Neighbor (KNN). Boli uskutočnené rozsiahle experimenty na optimalizáciu hyperparametrov, pričom sa zistilo, že kombinácia ResNet a KNN s konfiguráciou zahŕňajúcou 881 susedov a metriku vzdialenosti založenú na korelácii poskytuje najlepšie výsledky. SVM dosiahol presnosť 88,6 %. Ďalšie architektúry konvolučných neurónových sietí (CNN), GoogLeNet a SqueezeNet, boli tiež testované, kde GoogLeNet dosiahol presnosť 81 % s KNN, ktorý mal 154 susedov a používal metriku vzdialenosti Chebyshev. SVM s GoogLeNet dosiahol presnosť 80,9 % s gaussovským jadrom so škálou 0,41. SqueezeNet dosiahol presnosť 69,4 % s SVM a 68,8 % s KNN, čím sa ukázalo, že ResNet kombinovaný s KNN je najefektívnejší v detekcii *deepfake* obrázkov. Navrhovaný prístup ponúka solídny základ pre ďalší vývoj a výskum v kritickej oblasti.

3.5.5 Analýza farebnej textúry

Využitie farebných textúr spočíva v zakomponovaní rôznych farebných priestoroch [7]. Prvým krokom v procese je transformácia vstupného farebného obrázka do troch farebných priestorov: RGB, HSV a YCbCr. Tieto priestory umožňujú lepšiu separáciu luminancie a chrominancie, čo je kritické pre analýzu farebnej textúry. Na obr. 3.10 možno pozorovať rozdiely a spôsob zobrazenia tváre a jej podvrhov v rôznych farebných priestoroch. Následne



Obr. 3.10: Príklad skutočnej tváre a zodpovedajúcich útokov vo farebnom priestore RGB, odtieňoch sivej a YCbCr, prevzaté z [7].

sa na základe obrázkov identifikujú oblasti tváre pomocou špecializovaného algoritmu pre detekciu tvárí. Tie sú potom orezané a normalizované do rovnakých rozmerov pre ďalšie spracovanie. Potom sa pre každý spomenutý farebný priestor extrahuje niekoľko deskriptorov textúry [7]:

- **Local Binary Patterns (LBP):** Pre každý farebný kanál sa vypočíta binárny kód každého pixlu porovnaním hodnôt susedných pixlov v kruhovo symetrickej oblasti.
- **Co-occurrence of Adjacent Local Binary Patterns (CoALBP):** zachytáva koreláciu medzi susednými LBP vzormi v rôznych smeroch.
- **Local Phase Quantization (LPQ):** využíva lokálne informácie o fáze extrahované pomocou Fourierovej transformácie z okolia každého pixlu.
- **Binarized Statistical Image Features (BSIF):** binárne kódy pre každý pixel sú získané filtrovaním odpovedí obrázka a následnou binarizáciou.
- **Scale-Invariant Descriptor (SID):** využíva vlastnosti posunu Fourierovej transformácie pre dosiahnutie invariancie voči škále a rotácií.

Získané výsledné deskriptory textúry z týchto rôznych farebných priestorov sa konkatenujú do jedného vylepšeného vektoru, ktorý komplexne reprezentuje farebnú textúru tváre. Vektor je následne podrobený binárnej klasifikácií, kde výstupná hodnota indikuje, či pred kamerou stojí živá osoba alebo falošný podvrh.

3.5.6 Analýza pohybovej nerovnosti

Zameraním sa na analýzu pohybovej nerovnosti možno úspešne detegovať opakované video útoky [31]. Jadrom tohto princípu sú 2 charakteristické analytické komponenty: jednorozmerná konvolučná neurónová sieť (1D CNN) na hodnotenie variácií intenzity rozmazania pohybu a technika extrakcie funkcie LSP (*Local Similar Pattern*) na vyhodnotenie šírky rozmazania pohybu. Komponent 1D CNN je navrhnutý tak, aby zachytával časové zmeny intenzity rozmazania pohybu, ktoré odlišujú skutočné pohyby tváre od pohybov zobrazených na LCD obrazovke počas prehrávaného video útoku. Tento aspekt algoritmu využíva jedinečné charakteristiky odozvy LCD obrazoviek, ktoré sa výrazne líšia od prirodzeného pohybu skutočných tvárí. Spracovanie video snímkov cez sériu konvolučných a združovacích filtrov 1D CNN účinne izoluje vzory zmien intenzity rozmazania, ktoré naznačujú opakované útoky.

Ako doplnok využíva táto metóda extrakciu LSP fukncií, vďaka ktorej možno vyšetrovať šírku rozmazania pohybu. Toto kódovanie je založené na porovnávaní hodnôt intenzity pixlov v rámci lokalizovaných oblastí, zachytávajúc priestorové rozloženie a rozsah rozmazania pohybu.

Testovanie prebiehalo za využitia databáz Replay-Attack a OULU-NPU. Pri validácií na rovnakých databázach, ako na tých, čo boli trénované, výsledky ukázali 100 % detekčnú mieru, za použitia krížovej validácie boli dosiahnuté výsledky s presnosťou 79.5 % a 71.2 %. Tieto výsledky poukazujú na to, že predstavená metóda má významný potenciál v aplikáciach, kde je nutné overovanie živosti [31].

3.6 Komerčné riešenia detekcie živosti tváre

V súčasnom digitálnom veku sa bezpečnosť a ochrana osobných údajov stali prioritami pre organizácie aj jednotlivcov po celom svete. Táto sekcia kapitoly sa venuje prehľadu komerčných riešení detekcie živosti tváre, ktoré sú na trhu dostupné, s cieľom hlbšieho porozumenia o tom, ako tieto technológie fungujú, aké majú výhody a obmedzenia, a ako môžu byť implementované do existujúcich systémov.

3.6.1 Regula Forensics - Face SDK

Spoločnosť Regula Forensics[2] sa špecializuje na softvérové riešenia pre overovanie dokladov a biometrickú autentifikáciu. Ich Face SDK ponúka pokročilé riešenia na detekciu živosti tváre, ktoré sú navrhnuté tak, aby minimalizovali riziko falšovania identity pomocou fotografií, videí, alebo masiek. Využíva algoritmy strojového učenia a umelú inteligenciu na analýzu mikro-výrazov, blikania, a ďalších pohybov tváre, čím dokáže rozlíšiť skutočnú tvár od jej napodobeniny. Jednou z hlavných predností je schopnosť integrácie do rôznych aplikácií a systémov bez nutnosti drahého hardvéru.

3.6.2 Innovatrics - Liveness Detection

Ďalším lídrom v oblasti biometrických riešení je Innovatrics[3]. Zameriava sa na vysokú presnosť a rýchlosť svojich systémov. Innovatrics využíva sofistikované algoritmy na detekciu drobných pohybov tváre a zmeny výrazov, ako aj na analýzu textúry kože a ďalších detailov, ktoré napodobeniny neobsahujú. Systém je kompatibilný s rôznymi biometrickými zariadeniami a aplikáciami, čo ho robí flexibilným riešením pre mnohé sektory.

3.6.3 ID R&D - IDLive Face

Špecializáciou ID R&D[4] je vývoj riešení pre biometrickú autentifikáciu s využitím hlasu, tváre a behaviorálnych znakov. Ich produkt IDLive Face je zameraný na prevenciu podvodov prostredníctvom detekcie živosti tváre bez potreby užívateľskej interakcie. Tento systém používa pokročilé AI a analýzu behaviorálnych biometrických údajov k detekcii prírodných pohybov a reakcií tváre, čím sa líši od statických obrazov. Je to riešenie, ktoré umožňuje rýchlu a bezproblémovú autentifikáciu bez kompromisu v bezpečnosti.

3.7 Zhrnutie

Sme svedkami, ako sa kombinácia rôznych prístupov a technológií stáva kľúčom k vytváraniu spoľahlivých a odolných systémov rozpoznávania tváre. Napriek výzvam spojeným so zmenami osvetlenia, rôznymi pózami a potenciálnymi podvodnými útokmi, ako sú napríklad útoky maskami, fotografiami alebo videami, technologický pokrok, ako bol prezentovaný, poukazuje na schopnosť adaptácie a inovácie v oblasti zabezpečenia biometrických systémov.

Dôležité je zdôrazniť, že úspech v detekcii živosti a rozpoznávaní tváre závisí nielen od presnosti algoritmov, ale aj od ich schopnosti fungovať v rôznych reálnych scenároch.

[2] https://regulaforensics.com/
[3] https://www.innovatrics.com/
[4] https://www.idrnd.ai/

Dobrou správou je, že väčšina moderných metód je vysoko odolná voči najčastejšie používaným podvrhom, teda fotografiám či videám zobrazených na smartfóne alebo vytlačených na papieri. Na opačnú stranu sú ale stále veľké nedostatky v detekcií omnoho sofistikovanejším útokom. Jedným z hlavných výziev v biometrických systémoch je obrana proti používaniu vysokokvalitných 3D masiek alebo pokročilých techník syntézy obrazu, ako sú *deepfakes*. Zatiaľ čo metódy ako detekcia podľa hĺbky a analýza textúry kože prinášajú zlepšenie v obrane proti týmto útokom, stále je potrebný vývoj ďalších inovatívnych prístupov na posilnenie bezpečnosti.

Budúcnosť biometrického rozpoznávania tváre sľubuje ešte väčšie inovácie a zdokonalenie. S rastúcou potrebou zabezpečenia a autentifikácie v digitálnej dobe sa výskum a vývoj v tejto oblasti nezastaví a bude naďalej hľadať nové spôsoby, ako zlepšiť presnosť, rýchlosť a odolnosť proti podvodom. Zároveň je nevyhnutné zdôrazniť potrebu vyššej odolnosti proti útokom na prezentačné útoky spojené s využívaním syntetických mediálnych obsahov, ktoré sú čoraz ľahšie dostupné a presvedčivejšie.

Kapitola 4

Návrh a implementácia riešenia

Táto kapitola sa venuje predstaveniu návrhu systému pre detekciu podvrhov snímkov tváre a jeho následná implementácia. Navrhnuté riešenie kombinuje metódy strojového učenia a počítačového videnia.

Na základe dostupných štúdií a experimentov boli identifikované potenciálne prístupy, ktoré by mohli byť efektívne. Prvý prístup zahŕňal použitie metódy lokálnych binárnych vzorov (LBP) [40] bez modifikácií, ktorý sa ukázal ako nedostatočný vzhľadom na jeho obmedzenia v rôznych scenároch použitia. Zo vstupného obrázku sa po normalizácií vypočítali hodnoty jednotlivých pixlov na základe LBP. Po krátkom experimentovaní preukázal daný algoritmus viaceré nedostatky pri použití akéhokoľvek typu útoku.

Následne bol skúmaný algoritmus detekcie mrknutia [42], ktorý poskytoval uspokojivé výsledky pri analýze fotografií, no jeho efektívnosť bola znížená pri aplikácii na videá, čo si vyžiadalo ďalšie testovanie alternatív.

Testovanie detekcie hrán ukázalo, že tento prístup je perspektívny v určitých situáciách. Pre zlepšenie celkových výsledkov bolo rozhodnuté kombinovať tento prístup s pokročilejšími technikami detekcie živosti.

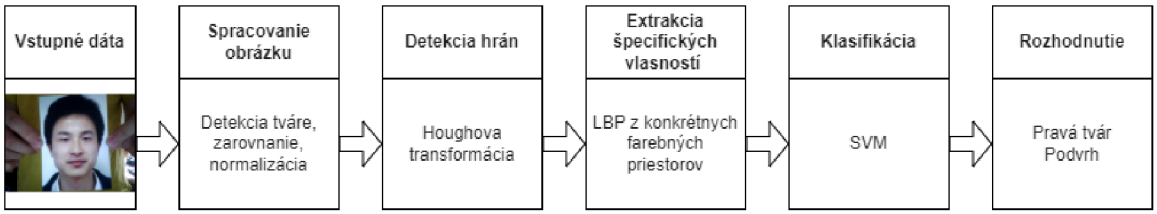
Postup finálneho návrhu aplikácie bude pozostávať z niekoľkých dôležitých častí zobrazených na obr. 4.1. Vstupnými dátami budú obrázky. Tie následne podliehajú spracovaniu (viz sekcia 4.1.5), ktorý zahŕňa niekoľko procesov. Prvým a najdôležitejším krokom tohto spracovania je detekcia tváre. Po nej nasleduje procedúra zarovnania tváre na základe polohy očí a normalizácia.

Po spracovaní obrázka do potrebnej formy nasleduje detekcia hrán v oblasti tváre. Na to je využitá Houghova transformácia spolu s využitím Cannyho detektoru hrán. V tejto časti je skúmané, či sú v okolí tváre detegované paralelné línie, ktoré môžu poukazovať na prítomnosť podvrhu v podobe vytlačenej fotografie či fotky zo smartfónu. V prípade, že sa v tejto časti nezistí podozrenie, obrázok prechádza do druhej časti.

Návrh druhej časti vychádza čiastočne z kľúčových zistení a metód opísaných v článku Turhala, Yılmaza a Nabiyeva (2023) [52], ktorý poskytol základné smerovanie pre toto inovatívne riešenie. V nej sa za pomoci LBP (viz sekcia 4.1.2) pre analýzu textúry spolu s využitím viacerých farebných priestorov(viz sekcia 4.1.1), konkrétne HSV a Lab, získajú jedinečné vektory.

Tieto vektory sa využijú ako vstup do metódy podporných vektorov (viz. sekcia 4.1.3), za pomoci ktorej bude získaný natrénovaný model určený na klasifikáciu. Ako vstupné dáta na trénovanie modelu boli využité obrázky z datasetu NUAA.

Bola zavedená i metóda využívajúca kombináciu spomenutých farebných priestorov s LBP, ktoré umožnili generovať unikátne vektory. Tie poskytli presvedčivejšie výsledky a zvýšili robustnosť systému detekcie živosti tváre.



Obr. 4.1: Proces spracovania vstupných dát na finálnu klasifikáciu.

4.1 Návrh riešenia

4.1.1 Výber farebných priestorov

Farebné priestory, ako sú RGB (červená, zelená, modrá), HSV [37](odtieň, sýtosť, hodnota) a Lab [16], poskytujú rôzne perspektívy obrazových dát a majú rôzne využitia pri analýze obrazu. Každý priestor má unikátne vlastnosti, ktoré umožňujú odhalenie špecifických aspektov obrazu relevantných pre konkrétne aplikácie.

Pri návrhu sa uprednostnia farebné priestory HSV a L*a*b* pred tradičným RGB farebným priestorom. Toto rozhodnutie bolo motivované získanými faktami a dôležitými zisteniami reprezentovanými v odbornom článku [52], ktorý zdôrazňoval unikátne výhody týchto farebných priestorov. Integráciou týchto 2 priestorov sa získal robustnejší a presnejší systém, ktorý je schopný efektívne čeliť výzvam spojeným s rôznymi typmi a technikami falšovania.

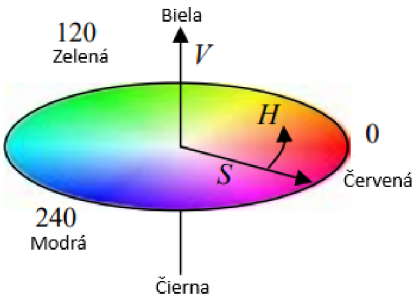
HSV

Tento model oddeľuje farebný odtieň od svetlosti a sýtosti, čo umožňuje lepšie analyzovať farebné variácie nezávisle od osvetlenia. V kontexte detekcie je obzvlášť užitočný pri rozlišovaní medzi skutočnými a falšovanými tvárami v rôznych svetelných podmienkach [37]. Skladá sa z 3 zložiek ako je znázornené na obrázku 4.2a. Odtieň reprezentuje prevládajúcu farbu odrazenú alebo prechádzajúcu objektom. Obecne je označený názvom farby. Sýtosť predstavuje množstvo sivej farby v pomere k odtieňu a meria sa v percentách. Hodnota jasu vyjadruje množstvo bieleho svetla, respektíve koľko svetla farba odráža [6].

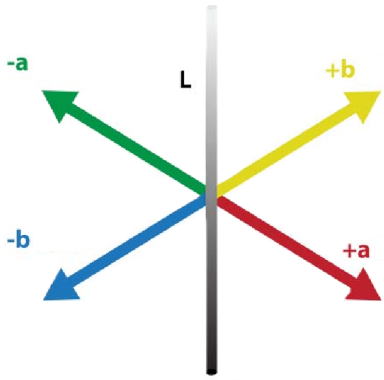
L*a*b*

L*a*b*, známy ako CIELAB alebo jednoducho Lab, ako farebne nezávislý priestor, poskytuje konzistentné farebné merania, ktoré sú invariantné voči zdroju svetla, čo z neho robí ideálny nástroj pre aplikácie vyžadujúce presné farebné porovnania. Ďalším kľúčovým aspektom je, že umožňuje odhaľovať jemné farebné rozdiely, ktoré sú často prehliadnuté v bežnejších farebných priestoroch, ako je RGB či CMYK [16].

Štruktúra tohto farebného priestoru je založená na 3 osách: L*, a* a b*, kde L* reprezentuje svetlosť od najtmavšej (0) po najsvetlejšiu (100), zatiaľčo a* a b* osi mapujú chromatickosť, teda farebné rozmery - a* osa sa pohybuje od zelenej k červenej a b* od modrej k žltej. Toto rozdelenie umožňuje popísať celú škálu farieb vnímaných ľudským okom s vysokou mierou presnosti [6].



(a) HSV farebný priestor, prevzaté z [37].



(b) L*a*b* farebný priestor, prevzaté z [6].

Obr. 4.2: Vybrané farebné priestory.

4.1.2 Textúrna reprezentácia

Schopnosť presne identifikovať a charakterizovať textúrne vzory v digitálnych obrazoch umožňuje systémom odlíšiť pravé ľudské tváre od sofistikovaných falzifikátov. S použitím pokročilých metód ako sú LBP a ich viacfarebného rozšírenia, je možné hlboko preskúmať a interpretovať textúrnu bohatosť obrazových dát.

Lokálne binárne vzory

Efektívny deskriptor textúr LBP [38] je jednoduchá metóda použiteľná na rôzne úlohy analýzy obrazu a rozpoznávania vzorov. Charakteristický LBP vektor je vytvorený porovnávaním každého pixlu v obraze s jeho susedmi v okolí. Pre každý jeden pixel sa generuje binárna hodnota porovnávaním intenzity pixlov jeho susedov. Ak je hodnota susedného pixlu vyššia, priradí sa danej bunke binárna hodnota 1, v opačnom prípade 0. Finálnym výsledkom tohto procesu je binárne číslo pre každý pixel, ktoré sa potom prevedie na desatinné číslo predstavujúce lokálny vzor textúry.

Pôvodný návrh tejto metódy uvažoval len o susedstve 3×3, ale neskôr to bolo rozšírené na kruhové susedstvá s rôznymi polomermi a počtom pixlov v susedstve. Táto metóda je odolná voči zmenám osvetlenia, vďaka čomu je užitočná v rôznych aplikáciach. LBP vzorec pre vybraný pixel (x, y) odvodený z $S^{(i)}$možno vyjadriť ako [38]:

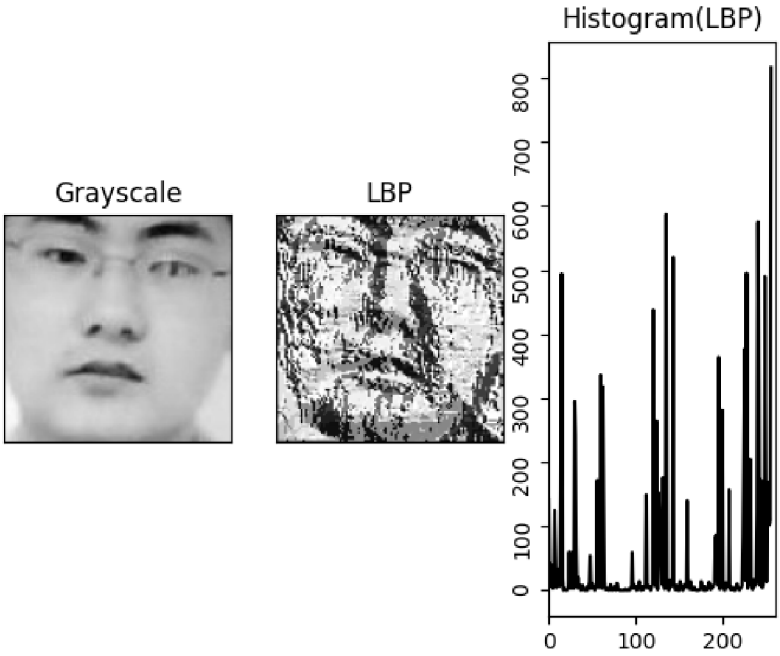
$$LBP^{(i)}_{P,R}(x,y) = \begin{cases} \sum_{p=0}^{P-1} s\left(g_p^{(i)} - g_c^{(i)}\right) * 2^n & \text{ak } U^{(i)} \leq 2 \\ P(P-1)+2 & \text{inak,} \end{cases}$$

kde:

$$U^{(i)} = \left|s\left(g_{P-1}^{(i)} - g_c^{(i)}\right) - s\left(g_0^{(i)} - g_c^{(i)}\right)\right| + \sum_{p=1}^{P-1} \left|s\left(g_p^{(i)} - g_c^{(i)}\right) - s\left(g_{p-1}^{(i)} - g_c^{(i)}\right)\right|$$

g_c a $g_p (p = 0, 1, ..., P-1)$ zodpovedajú hodnote stredového pixelu (x, y) a hodnoty P rovnomerne rozmiestnených pixelov na kružnici s polomerom $R (R > 0), U^{(i)}$ je pre jednotné LBP a s je prahová funkcia, ktorá je definovaná nasledovne:

$$s(x) = \begin{cases} 1, & \text{ak } x \geq 0 \\ 0, & \text{ak } x < 0 : \text{ inak.} \end{cases}$$



Obr. 4.3: Príkladný výstup spracovania obrázka z datasetu pomocou LBP.

Rozdiely v textúre medzi skutočnými a falošnými fotografiami primárne pramenia z prirodzených vlastností a reprodukčných metód materiálov používaných pri spoofingu. Skutočné tváre vykazujú jemné odchýlky vo farbe a štruktúre v dôsledku prietoku krvi, prirodzeného sfarbenia pokožky a tieňov vrhaných kontúrami tváre. Falošné fotografie nemusia presne kopírovať tieto jemné variácie, najmä v rôznych svetelných podmienkach. LBP dokáže zachytiť tieto nezrovnalosti, keď analyzuje textúru v rôznych farebných kanáloch.

Pri spoofingových útokoch pomocou masiek alebo výrezov môžu okraje týchto materiálov vytvárať neprirodzené prechody a okraje, ktoré nie sú prítomné v skutočných tvárach. LBP je citlivý na tieto okrajové artefakty a deteguje abnormálne prechody, ktoré naznačujú prítomnosť masky alebo prekrytia.

Po extrahovaní všetkých požadovaných funkcií je nutné použiť klasifikátor strojového učenia na kategorizáciu vstupu. Nemennosť LBP voči zmenám svetelných podmienok a jej robustnosť voči malým zmenám je obzvlášť výhodný faktor pre daný problém detekcie podvrhov.

4.1.3 Princíp SVM klasifikátoru a jeho aplikácia

Klasifikačný algoritmus SVM je metóda podporných vektorov používaná v riadenom strojovom učení na riešenie problémov súvisiacich s klasifikáciou a regresiou [13]. Funguje tak, že identifikuje optimálnu nadrovinu, ktorá zreteľne kategorizuje dátové body patriace do rôznych tried v rámci priestoru prvkov. V kontexte úloh binárnej klasifikácie, ako je rozlišovanie medzi autentickými a falošnými obrázkami, je zvolená rovina navrhnutá tak, aby maximalizovala priestor, známy ako okraj, medzi skutočnými a falošnými kategóriami. Okraj je vzdialenosť medzi nadrovinou a najbližšími bodmi každej kategórie, ktoré sa nazývajú podporné vektory. Pre dáta, ktoré nie sú lineárne separovateľné v pôvodnom priestore, SVM

používa tzv. kernelové funkcie k transformácií dát do vyššieho dimenzionálneho priestoru, kde môžu byť lineárne separovateľné. Základná matematická formulácia SVM pre lineárne deliteľné dáta je [13]:

$$f(\mathbf{w}, b) = \frac{1}{2}\|\mathbf{w}\|^2$$

$$g(\mathbf{w}, b) = y_i \left(\mathbf{x}_i \cdot \mathbf{w} + b\right) - 1 = 0$$

$$L_{\min}(\mathbf{w}, b) = \frac{1}{2}\|\mathbf{w}\|^2 - \sum_i \alpha_i \left[y_i \left(\mathbf{x}_i \cdot \mathbf{w} + b\right) - 1\right]$$

kde:

- $f(\mathbf{w}, b)$ je objektívna funkcia SVM, ktorá sa snaží minimalizovať, čím sa dosiahne maximálna marža medzi klasifikovanými triedami.
- $\mathbf{w}$ predstavuje vektor váh hyperroviny a b je bias.
- Kvadratická norma $\|\mathbf{w}\|^2$ sa používa na nájdenie hyperroviny s najväčšou možnou maržou.
- $g(\mathbf{w}, b)$ sú obmedzenia modelu SVM, ktoré zabezpečujú, že každý dátový bod $\mathbf{x}_i$ je správne klasifikovaný s maržou aspoň 1.
- y_i je skutočná trieda i-tého dátového bodu a $\mathbf{x}_i$ sú príznaky i-tého dátového bodu. Tieto obmedzenia sú aplikované pre všetky dátové body.
- $L_{\min}(\mathbf{w}, b)$ je Lagrangeova funkcia pre minimalizáciu, ktorá je používaná na nájdenie optimálnych hodnôt pre w a b pri zohľadnení obmedzení SVM.
- α_i sú Lagrangeove multiplikátory pre každé obmedzenie. Táto funkcia umožňuje transformovať problém minimalizácie s obmedzeniami na bez-obmedzený problém optimalizácie.

LBP vektory, získané extrakciou vzorov textúry, možno využiť ako vstupné znaky pre SVM klasifikátor. Ten sa na ich základe trénuje a učí rozlišovať medzi triedami. Keď je model natrénovaný, je možné ho použiť na klasifikáciu nových obrázkov. Keď sa zobrazí nový obrázok, najskôr sa spracuje pomocou techniky LBP, ten získaný vektor sa vloží do klasifikátora SVM, ktorý používa nadrovinu, ktorú sa naučil, na určenie, či je obrázok živý alebo falošný.

4.1.4 Dátová sada

Pre tréning algoritmu SVM bol použitý dataset NUAA [48], ktorý je voľne dostupný a nevyžaduje žiadne špeciálne licenčné dohody. Pôvodne sa zvažovalo využitie viacerých datasetov, avšak prístup k iným relevantným zdrojom dát bol obmedzený kvôli licenčným požiadavkám. Medzi ne patrila dátova sada CASIA Face Anti-Spoofing[1], Replay-Attack[2] či Replay-Mobile[3], ktoré sú súčasťou tab. 2.1. Zmienené datasety sú súčasťou tabuľky 2.1, ktorá poskytne informácie o počte obrázkov a typu útokov. Tieto datasety vyžadovali uzatvorenie licenčnej zmluvy, ktorú musel podpísať zástupca školy. Vzhľadom na dané okolnosti

[1] http://www.cbsr.ia.ac.cn/english/FaceAntiSpoofDatabases.asp
[2] https://www.idiap.ch/en/scientific-research/data/replayattack
[3] https://paperswithcode.com/dataset/replay-mobile-1

sa rozhodlo pre výhradné využitie datasetu NUAA. Tento krok zabezpečil dodržanie všetkých právnych a etických normál pri využívaní digitálnych zdrojov pre vedecké účely.

NUAA (*Near-Ultraviolet Angle-Attack*)
Súbor dát bol vytvorený na účely testovania a vývoja systémov rozpoznávania tváre proti útokom typu *photo attack*, kde útočník používa fotografiu osoby, aby oklamal systém rozpoznávania tváre. Tento dataset obsahuje fotografie tvárí v rôznych podmienkach a s rôznymi úrovňami osvetlenia, aby simuloval reálne scenáre, s ktorými by mohli systémy rozpoznávania tváre čeliť. Cieľom je pomôcť vývojárom a výskumníkom vytvoriť robustnejšie systémy, ktoré dokážu rozpoznať a odmietnuť pokusy o falšovanie identity pomocou fotografií. Dataset NUAA pred spracovaním nie je rozdelený do skupín (trénovanie, rozvoj, hodnotenie).

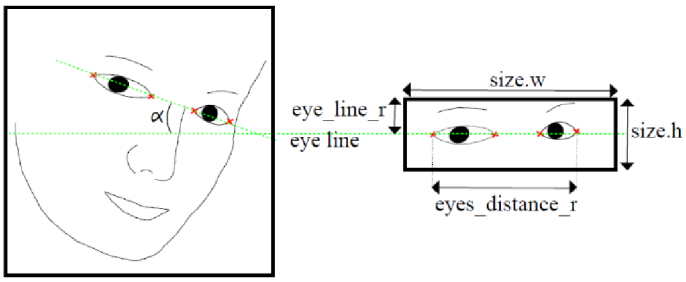
Identity	Pravé obrázky	Podvrhy
15	5105	7509

Tabuľka 4.1: Štatistika datasetu NUAA

4.1.5 Predspracovanie snímkov pre extrakciu

Kľúčový krok v procese spracovania vstupných dát riešenia sa skladá z niekoľkých častí. Každá jedna časť má svoj osobitný význam pre zaistenie konzistentného tvaru vstupných obrázkov pre ďalšie procesy.

Zarovnanie a úprava veľkosti
Vzhľadom k variabilite veľkosti tvárí a rozlíšenia vstupných snímkov je dôležité previesť všetky snímky na štandardizovanú veľkosť a rozlíšenie. Tento proces zaisťuje, že vstupné dáta budú homogénne, čo uľahčuje identifikáciu a extrakciu rysov tváre. Keďže cieľom je zachovať i rovnorodý tvar všetkých fotografií, nasleduje proces zarovnania tváre podľa roviny očí. Predtrénovaný model deteguje oblasť očí a následne je fotografia zarovnaná podľa ich roviny ako je znázornené na obr. 4.4.



Obr. 4.4: Ilustrácia znázorňujúca princíp rotácie obrázka, prevzaté z [14].

Detekcia tváre
Pre účinnú detekciu podvrhov je nutné presne identifikovať a segmentovať oblasti, na ktorých je tvár na snímke použitím pokročilého algoritmu YOLOv8, viz. sekcia 3.3.1, ktorý efektívne umožňuje lokalizovať rysy v rôznorodých podmienkach osvetlenia a pozadia. Sú-

časťou tohto kroku je i vytvorenie ohraničujúceho rámca okolo tváre s pridaným offsetom, čo slúži ako základ pre ďalšie spracovanie.

4.1.6 Detekcia hrán

V rámci návrhu predstavuje detekcia hrán počiatočnú, rozhodujúcu fázu, ktorej úlohou je identifikovať významné prechody v intenzite alebo farbe obrazu, ktoré označujú okraje. Vytvára pôdu pre sofistikovanú sekvenčnú analýzu, v ktorej sú snímky obsahujúce špecifické geometrické charakteristiky - paralelné čiary - určené na ďalšie preskúmanie.

Detekcia takýchto línií je nápomocná pri identifikácii potencionálnych pokusov o podvrh, kedy by podvodníci mohli použiť fotografie alebo digitálne zobrazenia na napodobnenie skutočnej tváre. Po prípadnom nájdení čiar, ktoré obsahujú tieto geometrické podnety, systém vyhodnotí daný vstup ako falošný, tzn. nejedná sa o živú tvár. V prípade, že neboli detegované žiadne hrany, ktoré by mali rovnakú smernicu, vstupné dáta prechádzajú do druhej klasifikačnej fázy. Tento následný krok zahŕňa pripravený model, vyvinutý na metóde lokálnych binárnych vzorov popísaný v 4.1.2. Prostredníctvom zapojenia detekcie hrán sa snažíme zvýšiť nie len presnosť, ale aj celkovú efektivitu systému.

Existuje niekoľko techník, z ktorých každá má svoje výhody a aplikácie. Toto riešenie sa zameriava na 2 hlavné metódy, ktorými je Canny Edge Detection [9] a Houghova transformácia [39].

Canny Edge Detection

Sofistikovaný algoritmus navrhnutý na detekciu hrán v obrázkoch vyvinul John F. Canny v roku 1986 [9]. Proces začína redukciou šumu, aby sa eliminovalo potencionálne rušenie, ktoré sa zvyčajne dosahuje pomocou Gaussovho rozmazania, čím sa obraz pripraví na presnejšiu detekciu hrán.

Po redukcií šumu algoritmus vypočíta veľkosť a smer gradientu v každom pixle, čo zvýrazní zmenu intenzity na obrázku a navrhne potencionálne hrany. Tento krok je rozhodujúci pre identifikáciu sily a orientácie hrán.

Ďalšia fáza, nemaximálne potlačenie, tieto hrany zjemňuje. Zriedením oblastí, ktoré nie sú súčasťou lokálnych maxím, zaisťuje, že výsledné hrany sú ostré a presné, čím sa eliminuje akýkoľvek pixel, ktorý netvorí hlavný smer hrany.

Potom sa použije dvojité prahovanie na rozlíšenie medzi skutočnými hranami a potencionálnym šumom. To zahŕňa kategorizáciu magnitúd gradientu do troch skupín: silné, slabé a irelevantné. Silné okraje sú okamžite zahrnuté ako súčasť konečného obrazu okrajov, zatiaľ čo slabé okraje sú podmienečne zahrnuté, ak sa spájajú so silnými okrajmi, čo pomáha znížiť počet falošných poplachov.

Nakoniec algoritmus využíva sledovanie hrán pomocou hysterézie na spevnenie mapy hrán. Tento krok účinne odfiltruje slabé hrany, ktoré nie sú spojené so silnými hranami, čím sa zabezpečí, že zistené hrany budú významné a zníži sa pravdepodobnosť detekcie falošných hrán.

Houghova transformácia

Medzi známe extrakcie funkcií používaných pri analýze obrazu patrí Houghova transformácia [39]. Jej účelom je nájsť nedokonalé inštancie objektov v rámci určitej triedy tvarov pomocou postupu hlasovania. Tento hlasovací postup sa uskutočňuje v parametrickom priestore, z ktorého sa získajú kandidáti na objekt ako lokálne maximá v akumulačnom priestore, ktorý je explicitne skonštruovaný algoritmom na detekciu určitého typu tvaru.

V prípade detekcie čiar, každý bod v priestore obrazu zodpovedá čiare v priestore Houghových parametrov a naopak. Priestor parametrov pre čiary môže byť definovaný 2 parametrami [39]:

- uhlom θ čiary od horizontálnej osi,
- vzdialenosťou ρ od začiatku k najbližšiemu bodu na priamke.

Houghova transformácia akumuluje hlasy v priestore parametrov pre prítomnosť čiary na každej pozícií(ρ, θ). Vrcholy v tomto priestore akumulátora zodpovedajú potencionálnym čiaram v priestore obrazu.

4.1.7 Viacfarebná LBP (MC-LBP)

Vstupné obrázky sú oddelené do farebných kanálov. Zreťazením vlastností extrahovaných z každého tohto kanála vzniká nový znakový vektor, pre každý farebný priestor jeden. Výsledný MC-LBP vektor sa získa kombináciou znakových vektorov získaných z rozličných farebných v priestorov, v tomto prípade z farebných priestorov HSV a Lab .

4.2 Implementácia návrhu

4.2.1 Použité technológie

V rámci implementácie projektu bol zvolený programovací jazyk Python vďaka jeho bohatému ekosystému knižníc a aplikačných rámcov vhodných pre úlohy strojového učenia a spracovania obrazu. Používané kľúčové knižnice zahŕňajú:

- **OpenCV**[4]**:** Pre úlohy spracovania obrazu a detekcie tváre.
- **Ultralytics YOLO**[5]**:** Najmodernejší model detekcie objektov používaný na efektívnu a presnú detekciu tváre v reálnom čase.
- **scikit-image**[6]**:** Na aplikovanie transformácií LBP na obrázky, čo pomáha pri extrakcií funkcie.
- **scikit-learn**[7]**:** Používa sa na implementáciu PCA (*Principal Component Analysis*) [2] a modely strojového učenia, najmä podporný vektorový klasifikátor používaný na klasifikáciu tvárí.
- **NumPy**[8]**:** pre vysokovýkonné numerické výpočty a manipuláciu s údajmi.
- **Matplotlib**[9]**:** Na vizualizáciu obrázkov a výsledkov, ako je zobrazovanie LBP obrázkov či grafov z priebehu trénovania modelu.
- **joblib**[10]**:** Na ukladanie a načítanie natrénovaných modelov a škálovačov, čo uľahčuje opätovné použitie.

[4] https://opencv.org/
[5] https://docs.ultralytics.com/
[6] https://scikit-image.org/
[7] https://scikit-learn.org/
[8] https://numpy.org/
[9] https://matplotlib.org/
[10] https://joblib.readthedocs.io/

4.2.2 Technický postup a popisy skriptov

Augumentácia dát

Augumentácia dát `data_augmentation.py` je určená na automatickú augumentáciu obrazových dát uložených v adresári. Jeho hlavným účelom je rozšíriť dataset tým, že pridáva rôzne transformácie k existujúcim obrázkom, čo pomáha zlepšiť schopnosť modelu generalizovať na nové dáta. Skript využíva knižnicu imgaug, ktorá poskytuje rozsiahle možnosti pre augmentáciu obrázkov.

Začína importovaním potrebných knižníc a modulov, vrátane os pre prácu so súborovým systémom, imageio pre načítanie a ukladanie obrázkov a imgaug.augmenters pre rôzne augmentačné techniky. Nasleduje definícia sekvenčného augmentátora, ktorý kombinuje dve špecifické transformácie: rotáciu a zmenu osvetlenia. Rotácia obrázkov je nastavená na náhodný uhol medzi -45 a 45 stupňami a zmena osvetlenia sa pohybuje od stmavenia po zjasnenie obrázkov v rozmedzí 50 % až 150 % pôvodnej intenzity.

Výstupné obrázky sa ukladajú do toho istého adresára, čo znamená, že pôvodný adresár obsahuje ako originálne, tak augmentované obrázky.

Skript prechádza cez všetky súbory v adresári, pričom spracováva len obrázkové súbory s príponami .png, .jpg a .jpeg. Augmentácia sa neaplikuje na každý obrázok, ale len na každý desiaty, čo znižuje množstvo generovaných dát a zameriava sa na zvýšenie diverzity bez prehnaného nárastu veľkosti datasetu. Pre každý vybraný obrázok sa vykoná augmentácia a výsledný obrázok je uložený s pôvodným menom s príponou _aug, čo umožňuje ľahké rozlíšenie medzi pôvodnými a transformovanými obrázkami.

Na záver skript vypíše cestu, kde boli obrázky uložené, a informuje o dokončení procesu augmentácie.

Detekcia tváre v reálnom čase

Skript `face_detection`, ktorý bol navrhnutý pre detekciu a spracovanie tvárí v reálnom čase, používa kombináciu technológií na detekciu tvárí, predspracovanie obrazu, extrakciu príznakov, a klasifikáciu pomocou modelu SVM. Začína načítaním predtrénovaného SVM modelu, PCA transformátora a scaleru z ukladacích súborov, čo umožňuje neskôr aplikovať rovnaké transformácie na nové dáta. Tieto komponenty sú základom pre predikciu a klasifikáciu v reálnom čase.

Funkcia `align_face` slúži na zarovnanie tváre tak, aby oči boli na horizontálnej línii. Toto zarovnanie je dôležité pre konzistentné extrahovanie príznakov tváre, nezávisle od polohy hlavy na obrázku. Vypočíta sa uhol rotácie medzi očami a následne sa aplikuje geometrická transformácia na obrázok. Funkcia `preprocess_face` transformuje tvár do potrebných farebných priestorov, extrahuje príznaky a aplikuje PCA a škálovanie, tak ako bolo toto predspracovanie definované počas trénovania modelu. Táto konzistentnosť v predspracovaní je kľúčová pre úspešnú klasifikáciu.

Hlavná funkcia `detect_and_save_faces` využíva model YOLOv8 pre detekciu tvárí v obraze. Pre každú detegovanú tvár sa vykoná viacero krokov, vrátane extrakcie príznakov, zarovnania, predspracovania a nakoniec klasifikácie pomocou SVM. Výsledky sú zobrazené v reálnom čase a prípadne uložené pre ďalšiu analýzu.

Skript zobrazuje výsledky v reálnom čase, vrátane označenia detegovaných tvárí a klasifikácie (reálna alebo falošná).

Extrakcia funkcií

Tento skript `feature_extraction` je určený na extrakciu príznakov z obrazových dát pre

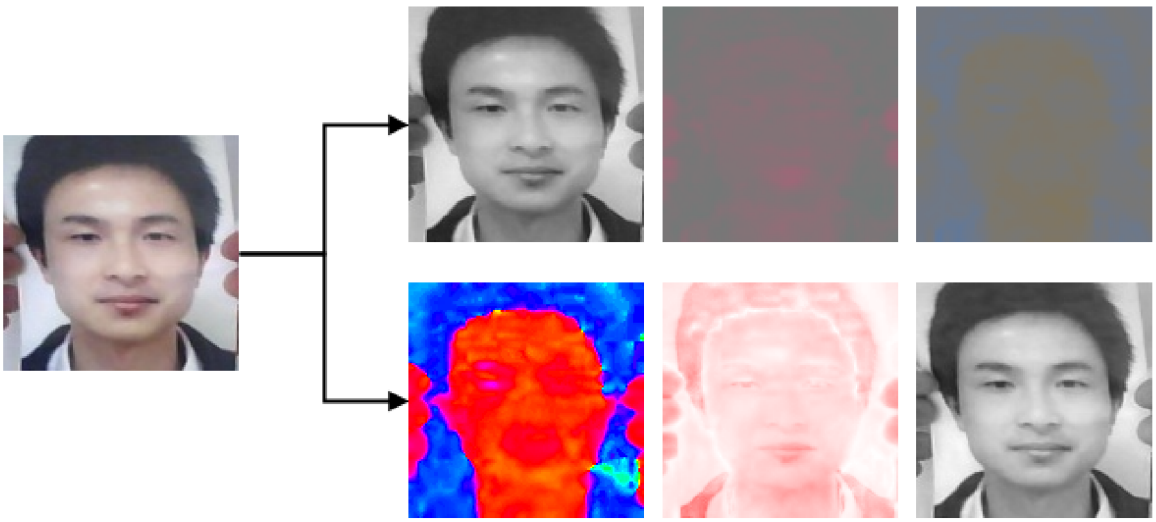
účely strojového učenia, špecificky zamerané na rozlišovanie medzi reálnymi a falšovanými tvárami. Skript využíva kombináciu farebných priestorov HSV a Lab na získanie komplexného súboru príznakov, ktoré sú následne upravené pomocou PCA a škálované.

Na začiatku skript načíta predtrénovaný SVM model, scaler a PCA transformátor z už existujúcich súborov, ktoré sú uložené v adresári. Tieto nástroje sú následne použité na transformáciu nových dát získaných z obrazov. Funkcie pre prácu s obrazom:

- `get_uniform_lbp_image`: Táto funkcia využíva metódu lokálneho binárneho vzoru (LBP) na transformáciu obrazu do formy, ktorá uľahčuje extrakciu textúrnych príznakov.
- `calculate_histogram`: Po získaní LBP obrazu, funkcia vypočíta histogram, ktorý sumarizuje rozloženie príznakov v obraze.
- `visualize_lbp_image`: Voliteľná funkcia na vizualizáciu LBP obrazu, ktorá môže byť užitočná pre debugovanie alebo analýzu.

Proces extrakcie príznakov:

- `extract_features_from_channel`: Táto funkcia rozdelí obraz do blokov a z každého bloku extrahuje LBP príznaky.
- `process_image_and_extract_features`: Hlavná funkcia, ktorá načíta obraz, prevedie ho do HSV a Lab farebných priestorov, a potom extrahuje a kombinuje príznaky z každého kanálu (viz obr. 4.5).

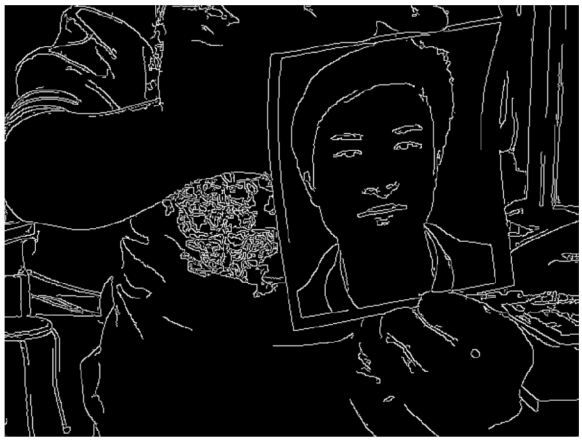


Obr. 4.5: Extrakcia farebných kanálov do priestorov HSV a Lab.

Po extrakcii príznakov sa aplikuje PCA a škálovanie na zníženie dimenzionality dát pri zachovaní 95 % variability. Výsledný súbor príznakov je potom uložený spolu so škálermi a PCA modelmi pre neskoršie použitie.

Skript iteruje cez všetky obrázky v zadaných adresároch, vykonáva extrakciu príznakov a ukladá výsledky. Záverečná časť skriptu kombinuje príznaky z reálnych a falšovaných tvárí, čím vytvára komplexný dataset pre tréning alebo testovanie modelov.

Detekcia hrán
Cieľom skriptu `edge_detector.py` je predbežné spracovanie a analýza obrázku, aby rozpoznal prítomnosť štrukturálnych charakteristík, ktoré sú indikatívne pre fotografické alebo digitálne zobrazenia.



Obr. 4.6: Výstup po spracovaní obrázku metódou Canny Edge.

Skladá sa z viacerých dôležitých funkcií:

- **`calculate_slope`**: Táto funkcia vypočíta sklon línie definovanej dvoma bodmi (x1, y1) a (x2, y2). Sklon sa vypočíta ako zmena y (vertikálne zmeny) delená zmenou x (horizontálne zmeny). V prípade, že x1 je rovnaké ako x2, čo by viedlo k deleniu nulou, funkcia vráti float('inf'), čo indikuje nekonečný sklon (vertikálnu líniu).

- **`calculate_angle_between_lines`**: Vypočíta uhol medzi dvoma líniami založenými na ich sklone. Využíva predchádzajúcu funkciu `calculate_slope` na získanie sklonov pre obe línie. Ak má aspoň jedna línia nekonečný sklon, funkcia vráti 90 stupňov, čo znamená, že línie sú perpendikulárne (pravý uhol). Inak, funkcia vypočíta absolútnu hodnotu tangens uhla a následne prevedie tento tangens na stupne pomocou arkus tangens funkcie atan.

- **`draw_lines`**: Funkcia je určená na vykreslenie línií na obrázku. Pre každú líniu zadanú v argumente lines, funkcia použije OpenCV funkciu cv2.line na nakreslenie tejto línie na obrázku.

- **`line_length`**: Vypočíta dĺžku danej línie. Dĺžka sa vypočíta pomocou Pytagorovej vety z rozdielov súradníc koncových bodov línie.

- **`detect_lines_in_roi`**: Hlavná funkcia skriptu, ktorá deteguje línie v zadanom regióne záujmu obrázka. Používa Canny detektor hrán na vytvorenie mapy hrán, a následne Houghovu transformáciu na identifikáciu línií v týchto hranách. Funkcia klasifikuje zistené línie ako perpendikulárne alebo paralelné založené na ich uhle vzájomnej orientácie. Taktiež vizualizuje detegované línie na obrázku (viz obr. 4.6).

Klasifikácia

Tento kód `NUAA_svm_classifier.py` ukazuje postup načítania predspracovaných príznakov z uložených súborov, ich škálovanie, aplikáciu PCA a následné použitie klasifikátora SVM na klasifikáciu dát.

Skript načíta PCA transformované príznaky (pre farebné priestory HSV, Lab a kombinované) a príslušné štítky z diskov. Tieto dáta sú uložené v špecifikovanom adresári. Na analýzu a trénovanie modelu sú vybrané kombinované PCA príznaky. Tieto príznaky sú najprv škálované pomocou načítaného scaleru a potom transformované pomocou načítaného PCA modelu.

Na validáciu modelu sa používa stratifikovaná krosová validácia s 5 foldmi, pričom dáta sú pred trénovaním zamiešané. `cross_val_predict` funkcia sa používa na predpovedanie štítkov pre každý fold, čo umožňuje vypočítať klasifikačné metriky ako presnosť, maticu zámeny a úplný klasifikačný report.

Na základe predpovedí sa vypočítavajú rôzne metriky a zobrazuje sa klasifikačný report, presnosť a matica zámeny. Následne sa SVM klasifikátor natrénuje na celom datasete a uloží sa na disk pre budúce použitie.

Výsledný model je uložený v špecifikovanom adresári, a skript vypíše cesty, kde boli model a jeho komponenty uložené.

Kapitola 5

Experimenty

Kapitola je zameraná na porovnanie a vyhodnotenie 3 modelov pre detekciu živosti tváre, kde každý model bol špecificky trénovaný s využitím rozličných farebných priestorov a trénovaný na NUAA datasete. Cieľom experimentov je identifikovať model, ktorý dosahuje najvyššiu účinnosť a presnosť, aby mohol byť následne využitý v reálnom čase pre overenie živosti. S vybraným modelom bude testovaná jeho robustnosť v rozličných prostrediach a s rôznymi typmi útokov.

5.1 Metriky pre hodnotenie

Hodnotenie výkonu modelov si vyžaduje komplexný prístup s použitím súboru štatistických metrík. Tieto metriky sú založené na dobre zavedených matematických vzorcoch, ktoré dôsledne hodnotia predikčnú presnosť modelu. Pri hodnotení sa bude uvažovať o 2 triedach. Trieda 0, ktorá predstavuje obrázky bez podvrhu so živou tvárou a trieda 1, ktorá bude predstavovať obrázky s prítomnosťou podvrhu v rôznej forme.

Cross-validation
Krížová validácia (*Cross-validation*) je statická metóda používaná pri vývoji predikatívnych modelov, ktorá slúži na overenie schopnosti modelu generalizovať na nezávislej dátovej sade [3]. Tento postup je zvlášť užitočný v prípadoch, kde je celkový počet dostupných dát obmedzený a je nevyhnutné čo najefektívnejšie využiť dáta k odhadu výkonnosti modelu.

Pri krížovej validácií sa dataset rozdelí na niekoľko menších častí, obvykle nazývaných *folds*. Model sa potom opakovane trénuje na kombináciu týchto segmentov a testuje sa na zvyšnom segmente, ktorý nebol použitý pri tréningu. Tento proces sa opakuje tak, že každý segment je použitý práve jedenkrát ako testovacia sada.

Na overenie nášho modelu používame k-násobnú krížovú validáciu, metódu, kde je súbor údajov rozdelený na k podmnožiny. Model je trénovaný na $k-1$ podmnožinách a validovaný na zostávajúcej podmnožine, pričom tento proces sa opakuje k krát. Celkový výkon je potom priemerom všetkých k pokusov, vypočítaný ako [3]:

$$\text{CV Accuracy} = \frac{1}{k}\sum_{i=1}^{k}\text{Accuracy}_i$$

Precision-Recall

Precision-Recall poskytujú pohľad na presnosť a úplnosť modelu. Sú definované ako [41]:

$$\text{precision} = \frac{TP}{TP + FP} \qquad \text{recall} = \frac{TP}{TP + FN}$$

kde TP, FP a FN znamenajú skutočne pozitívne, falošne pozitívne a falošne negatívne hodnoty.

Precision, známa aj ako presnosť pozitívnej predikcie, je metrika, ktorá určuje, aký podiel identifikovaných pozitívnych výsledkov je skutočne pozitívnych. Je dôležitá najmä v aplikáciách, kde sú náklady na falošne pozitívne výsledky vysoké, napríklad v medicínskej diagnostike alebo v súdnych prípadoch [41].

Recall, známy aj ako úplnosť alebo citlivosť, je metrika, ktorá určuje, aký podiel skutočných pozitívnych prípadov bol správne identifikovaný modelom. Tento ukazovateľ je kritický v situáciách, kde je dôležité identifikovať všetky možné pozitívne prípady, ako napríklad v detekcii rakovinových buniek, kde prehliadnutie pozitívneho prípadu môže mať vážne následky. Model s vysokým recall teda efektívne identifikuje pozitívne prípady, ale môže to byť na úkor vyššieho počtu falošných pozitívov [41].

F1 skóre

F1 skóre je harmonický priemer precision a recall a je užitočný v prípadoch, kde je potrebné nájsť rovnováhu medzi týmito dvoma metrikami [47]. F1 skóre poskytuje jedno číslo, ktoré zhrnutie oba aspekty výkonnosti modelu, čo je užitočné, keď sú precision a recall rovnako dôležité. F1 skóre dosahuje svoje maximum na 1 (perfektná presnosť a úplnosť) a minimum na 0.

F1 skóre je obzvlášť dôležité v situáciách, kde majú falošne pozitívne a falošne negatívne výsledky výrazne rozdielny dopad a kde je distribúcia tried nevyrovnaná. Napríklad, v práci s textami, kde môže byť mnoho negatívnych príkladov (neškodné dokumenty) a len niekoľko pozitívnych príkladov (dokumenty obsahujúce určitú informáciu), F1 skóre pomáha zabezpečiť, že model efektívne rozpoznáva pozitívne príklady bez nadmerného označovania negatívnych príkladov ako pozitívnych. Vzorec je definovaný nasledovne [47]:

$$F1 = 2 \times \frac{\text{precision} \times \text{recall}}{\text{precision} + \text{recall}}$$

Accuracy

Presnosť (*Accuracy*) je jednou z najzákladnejších metrík v hodnotení klasifikačných modelov a meria podiel správne klasifikovaných prípadov (tj. suma skutočne pozitívnych a skutočne negatívnych) ku celkovému počtu prípadov v datasete. Tento ukazovateľ je intuitívne jednoduchý a poskytuje rýchly prehľad o tom, ako dobre model funguje na daných dátach. Vypočíta sa podľa vzorca [41]:

$$\text{accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Presnosť môže byť však zavádzajúca v prípadoch, kde je distribúcia medzi triedami nevyrovnaná. Napríklad, ak 95 % dát sú negatívne a len 5 % pozitívne, model, ktorý všetky prípady klasifikuje ako negatívne, môže mať vysokú presnosť, ale je zjavne nevhodný pre potreby reálneho sveta [41]. V takýchto prípadoch je dôležité zvážiť aj iné metriky, ako sú precision, recall a F1 skóre.

5.2 Experimenty s modelmi

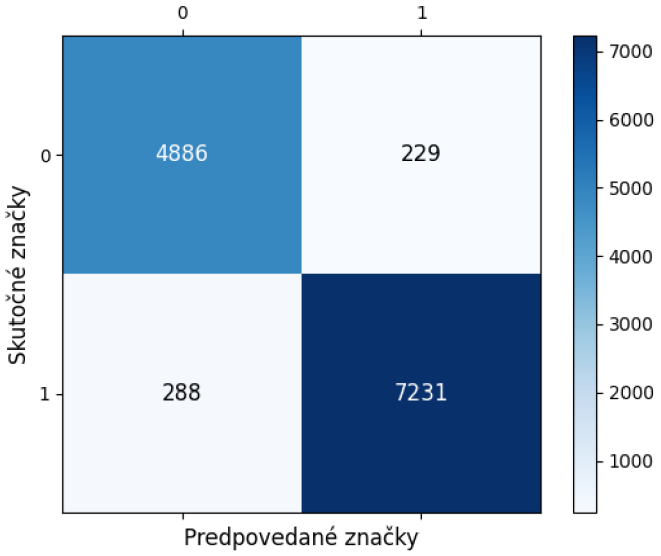
5.2.1 Experiment 1 - HSV farebný priestor

Experiment začal prevodom obrázkov z datasetu NUAA, ktorý obsahuje rôzne obrázky tvárí, do HSV farebného priestoru (*Hue*, *Saturation*, *Value*). Po konverzii do tohto farebného priestoru bol na každom vstupnom obrázku použitý algoritmus LBP, viz sekcia 4.1.2. Výsledné LBP histogramy, poskytli číselné reprezentácie textúrnych vlastností obrázkov. Tieto histogramy následne boli použité na trénovanie klasifikačných modelu.

Štatistika

Výsledky overovacej fázy dosiahli pôsobivú presnosť. Konkrétne sa dosiahla presnosť 95,91 % na validačnej sade, ktorá je súčasťou datasetu použitého na tréning. Model ukázal presnosť 0,94 a recall 0,96 pre správne identifikované prípady, čo znamená výnimočnú schopnosť identifikovať skutočné identity s minimálnym počtom falošných poplachov.

Graficky vykreslená matica zámeny na obr. 5.1 značí, že z 5155 skutočných prípadov model správne identifikoval 4886, pričom len okrajových 229 prípadov prešlo jeho kontrolou. Naopak, z 7519 prípadov skreslenia údajov presne rozpoznal 7231, pričom iba 288 prípadov bolo nesprávne klasifikovaných. To ďalej posilňuje robustnosť modelu a ukazuje chvályhodnú rovnováhu medzi citlivosťou a špecifickosťou.



Obr. 5.1: Matica zámeny experimentu 1 (0 pre snímky so živou tvárou a 1 pre podvrhy).

Tabuľka 5.1: Správa o klasifikácií experimentu 1.

	Precision	**Recall**	**F1-score**	**Support**
Real	0,94	0,96	0,95	5115
Spoof	0,97	0,96	0,97	7519
Accuracy			0,96	12634

5.2.2 Experiment 2 - CIELAB farebný priestor

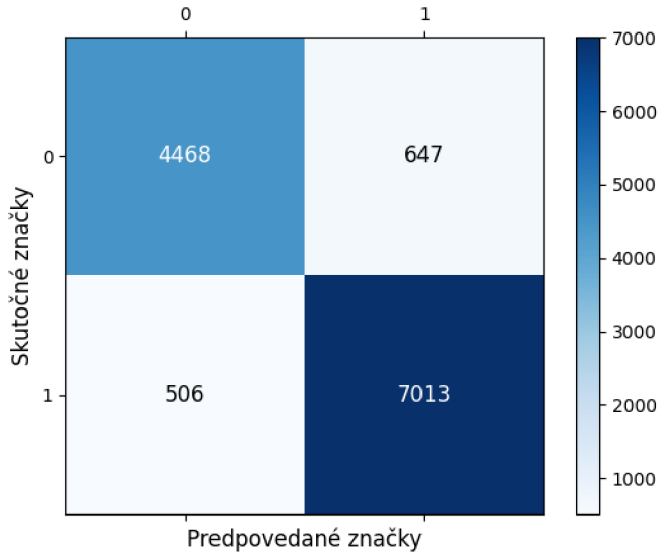
V tomto experimente sme použili farebný priestor CIELAB, uznávaný pre svoju účinnosť zvládaní zmien osvetlenia a intenzity farieb. Využitie datasetu NUAA umožnilo robustné posúdenie výkonnosti modelu. Súbor údajov bol zodpovedajúcim spôsobom rozdelený tak, aby poskytoval trénovaciu a validačnú množinu, ktorá je nápomocná pri hodnotení výkonu modelu v kontrolovanom, ale realistickom prostredí.

Štatistika

Po vyhodnotení model HSV dosiahol celkovú presnosť 90,87 %. Pri skúmaní správy o klasifikácii presnosť 0,90 a vyvolanie 0,87 pre triedu „0“ označuje konzervatívny model a naznačuje dostatočnú presnosť pri identifikácii autentických zobrazení. Naopak, model vykazoval vynikajúcu presnosť a vyvolanie pre triedu 1 na úrovni 0,92 a 0,93, čiže má tendenciu minimalizovať falošné pozitívne výsledky na úkor vynechania niektorých podvodných prípadov..

Skóre F1, ktoré vyvažuje presnosť a zapamätanie, bolo 0,89 pre triedu 0 a pôsobivých 0,92 pre triedu 1, čo odráža silný výkon pri potvrdzovaní skutočnej identity a zároveň ponúka priestor na zlepšenie v odhaľovaní napodobňovania identity.

Matica zámeny (obr. 5.2) poskytla ďalšie poznatky, z ktorých vyplýva, že z 7519 prípadov skreslenia informácií bolo 7013 presne zistených, pričom 506 prípadov bolo nesprávne klasifikovaných ako pravé. Na rozdiel od toho model správne identifikoval 4468 z 5115 skutočných prípadov, pričom 647 prípadov bolo omylom označených ako nepravdivé.



Obr. 5.2: Matica zámeny experimentu 2 (0 pre snímky so živou tvárou a 1 pre podvrhy).

Celkovo teda na základe získaných hodnôt vidieť, že model, ktorý využíval farebný priestor HSV obstál lepšie, keďže jeho presnosť dosahovala o 0,5 % väčšiu presnosť na rovnakej dátovej sade, aká bola použitá pri trénovaní modelu z experimentu 2.

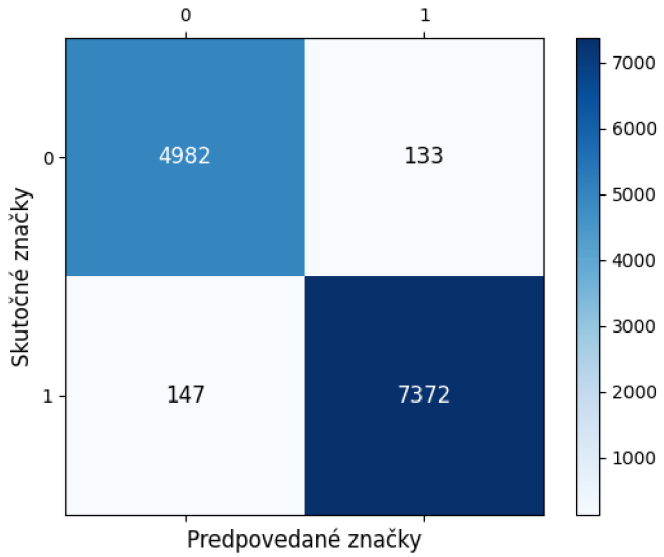
Tabuľka 5.2: Správa o klasifikácií experimentu 2.

	Precision	Recall	F1-score	Support
Real	0,90	0,87	0,89	5115
Spoof	0,92	0,93	0,92	7519
Accuracy			0,91	12634

5.2.3 Experiment 3 - Kombinácia farebných priestorov

Zámerom tretieho experimentu je konkatenácia 2 vektorov, konkrétne vektoru z farebného priestoru HSV a vektoru z priestoru Lab. Použijú sa vektory získané v experimente 1 a vektory získané z rovnakého obrázka z experimentu 2, čím sa vytvorí cieľový vektor. Myšlienkou tohto hybridného prístupu je zlepšiť schopnosť modelu rozlišovať medzi autentickými a skreslenými identitami s ešte väčšou presnosťou. S využitím rovnakého súboru údajov NUAA sa pokračuje s podobným rozdelením údajov, čim sa zabezpečí konzistentnosť vo všetkých experimentoch.

Štatistika
Kombinácia farebných priestorov sa ukázala ako účinná, čo dokazuje výrazná presnosť 97,78 %. Model vykazoval vysokú úroveň presnosti, najmä pri klasifikácii pravých identít (trieda 0) s presnosťou 0,97. Odvolanie pre triedu 1 bolo tiež vynikajúce na úrovni 0,98, čo naznačuje výnimočnú schopnosť modelu identifikovať falošné pokusy. Trieda 1, ktorá predstavuje skreslené informácie, tiež zaznamenala zlepšené výsledky s presnosťou 0,98 a vyvolanie 0,98. Tieto čísla naznačujú dobrý výkon pri správnej identifikácii nepravdivých rozhodnutí. Skóre F1 bolo 0,97 pre triedu 0 a 0,98 pre triedu 1, čo odzrkadľovalo rovnováhu



Obr. 5.3: Matica zámeny experimentu 3 (0 pre snímky so živou tvárou a 1 pre podvrhy).

presnosti a spätného získavania dosiahnutú týmto kombinovaným modelom. Porovnaním

spomenutých hodnôt s predchádzajúcimi 2 modelmi je jasne vidieť rozdiel, a to, že kombinácia vektorov skutočne zvyšuje presnosť detegovať živosť tváre. Matica zámeny (obr. 5.3)posilňuje úspešnosť modelu a vykazuje malý počet nesprávnych klasifikácií. Z 7519 prípadov skresľovania informácií bolo 7372 zistených správne, pričom 147 prípadov nebolo vynechaných. Pokiaľ ide o autentické identity, 4982 z 5115 bolo správne rozpoznaných, iba s 133 chybami.

Tabuľka 5.3: Správa o klasifikácií experimentu 3.

	Precision	**Recall**	**F1-score**	**Support**
Real	0,97	0,97	0,97	5115
Spoof	0,98	0,98	0,98	7519
Accuracy			0,98	12634

5.2.4 Experiment 4 - Algoritmus detekcie hrán

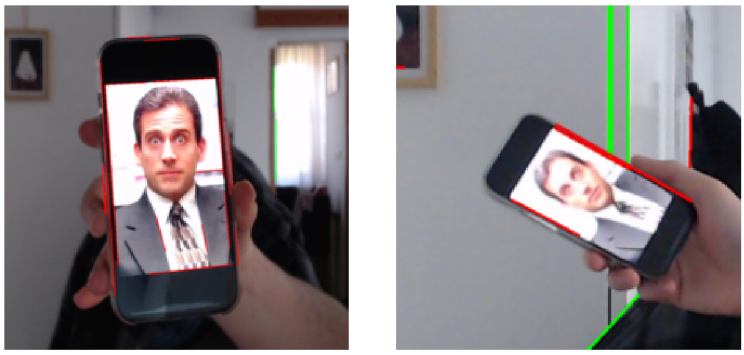
Algoritmus detekcie hrán slúži ako podporný rozhodovací algoritmus, ktorý ma zvýšiť presnosť detekcie v kombinácií s vybraným natrénovaným modelom. Cieľom tohto experimentu je určiť jeho presnosť a robustnosť a tým rozhodnúť, či je vhodný na použitie v spolupráci s modelom. Proces samotnej detekcie hrán predchádza celému procesu algoritmu využitom na predchádzajúcich experimentoch. Rovnako tak bol využitý rovnaký dátový set NUAA s pridaním menšej dátovej sady vytvorenej pre tento experiment. Hlavnou myšlienkou je detekcia hrán smartfónov, ako jednu z ďalších alternatív útoku, keďže spomenutý dátový set pozostáva len z podvrhov vo forme vytlačených fotografií.

Štatistika

Detekciou hrán hľadá algoritmus na zachytenom zábere hrany s rovnakou smernicou, čo môže predpokladať za podozrivé a vyhodnotí to ako podvrh. V prípade nenájdenia takýchto hrán prechádza snímok do ďalšieho spracovania. V súbore so živými tvárami bez prítomnosti podvrhu detegoval iba minimálne množstvo takýchto hrán, čím preukázal, že neovplyvní v tomto smere celkové spracovanie. V prípade súboru s podvrhmi dokázal z celkového počtu 8263 fotografií detegovať 32 % obrázkov s prítomnosťou hrán. Príkladný výstup programu, na ktorom je znázornená detekcia hrán je vyobrazená na obr. 5.4.

Cieľom experimentu pomimo využitia dátovej sady bolo i zistenie, či je algoritmus schopný detekcie hrán pri použití smartfónu s fotkou. K tomu bola vytvorená menšia dátová sada, ktorá pozostáva zo 108 záberov, na ktorých je prítomný podvrh v podobe fotky v smartfóne. Smartfón sa nachádza v rôznych pozíciach a uhloch. Takisto je zahrnutá i zmena jasu displeja.

V danom prípade sa ukázal byť ako presvedčivejší nástroj v porovnaní s modelom získaným v experimente číslo 3, pretože tento model dokázal na datasete vytvorenom pre účely tohto testu klasifikovať len 34 záberov ako pravé. Tieto zábery boli predovšetkým charakteristické nízkym jasom displeja. V kontraste s tým, detekcia hrán identifikovala prítomnosť falšovania v 82 prípadoch, čo demonštruje, že jej aplikácia je oprávnená a efektívna.



Obr. 5.4: Príklady záberov s detegovanými hranami. Červené čiary znázorňujú hrany, ktoré majú rovnakú smernicu.

5.3 Praktické testovanie v reálnom čase

Najzásadnejší experiment sa zameriava na účinnosť najlepšieho natrénovaného modelu. Ten bol vybraný na základe predchádzajúcich testov, kde preukázal najvyššiu presnosť a spoľahlivosť. Ako podporný algoritmus k tomuto vybranému modelu využívame detekciu hrán, ktorý pri testovaní ukázal dostatočnú spoľahlivosť na filtrovanie niektorých typov podvrhov, ktoré samostatný model nedokázal zachytiť. Testy boli vykonané v rôznych prostrediach - od izby, cez kancelárske priestory až po vonkajšie podmienky, aby sa mohla ohodnotiť robustnosť a adaptabilita systému v rôznych scenároch. Cieľom je nie len overenie schopnosti, ale i identifikácia potencionálnych slabín systému v praxi.

Pri analýze výsledkov sa využila metrika presnosti, vypočítaná ako pomer počtu správne identifikovaných snímkov k celkovému počtu zachytených snímkov zachytených za určitý časový úsek.

5.3.1 Použité technológie

Popis testovacieho prostredia
Výskum robustnosti a adaptabilite prebiehal v rôznych prostrediach a podmienkach:

- **Izba** - Farebné steny, rôzne predmety na pozadí rôznych tvarov, zmena osvetlenia za použitia blesku na mobile a stolnej lampy.
- **Kancelársky priestor** - LED kancelárske osvetlenie, bez rušivých elementov na pozadí, jednofarebné pozadie.
- **Vonkajšie priestory** - Rôzne podmienky osvetlenia, počas tmy za využitia blesku na telefóne a zmenou jasu na smartfóne. V tomto type prostredia bolo testované použitie podvrhu za použitia smartfónu.

Hardvérové nástroje
Počas testovania v reálnom čase boli využité 3 typy web-kamier:

- **Logitech C920 HD Pro**[1] - Full HD rozlíšenie pri 30 fps, snímač CMOS,
- **Integrovaná web-kamera**[2] - 1280 × 720 (HD) pri 30 fps, snímač,

[1] https://www.logitech.com/cs-cz/products/webcams/c920-pro-hd-webcam.960-001055.html
[2] https://www.dell.com/support/home/en-us/product-support/product/precision-15-5570-laptop/docs

- **TrueDepth kamera (iPhone 14 Pro)**[3] - 1080p HD video pri 60 fps, snímač CMOS.

5.3.2 Typy testovaných podvrhov

V sekcií 2.2.1 sú spomenuté všetky typy prezenčných útokov na systém. V rámci testovania boli použité 4 rôzne typy:

- **Vytlačené fotografie na fotopapier** - Osoby a ich tváre vytlačené na fotopapier. Charakteristickým znakom je odlesk, ktorý fotopapier poskytuje.
- **Časopis/noviny** - Obrázky tvárí z časopisov a novín. Papier použitý na tlač novín má inú textúru a menej výrazný odlesk.
- **3D masky** - Modely tvárí vytlačené na 3D tlačiarni poskytujú trojrozmerný pohľad namiesto predchádzajúcich útokov z dôvodu priestorovej presnosti a textúry pokožky.
- **Smartfón** - Použitím telefónu získame ďalšie typy odleskov a rozlíšení zobrazenia. Konkrétny model využitý pri testovaní je iPhone 14 Pro.

5.3.3 Analýza výsledkov pre jednotlivé typy podvrhov

Tabuľka 5.4: Tabuľka zobrazujúca prehľad efektívnosti.

Typ podvrhu	Presnosť detekcie (%)	Poznámky
Živá tvár	90	
3D maska	28,8	Problémy s realistickými detailmi
Fotografia	79,1	Odlesky pomáhajú v detekcii
Časopis	80,8	Podobné výsledky ako pri fotografiách
Mobilný telefón	60 (s hranami)	Zlepšenie s detektorom hrán, bez 11 %

Živá tvár bez podvrhu
Systém konzistentne a spoľahlivo rozpoznal pravú tvár, čo indikuje, že základné detekčné schopnosti systému sú vynikajúce v kontrolovanom prostredí. Avšak, s poklesom intenzity osvetlenia bola evidovaná značná degradácia kvality obrazu, čo malo za následok zhoršenie schopnosti modelu správne identifikovať pravé tváre.

3D maska
Detekcia podvrhu v podobe 3D masky mala presnosť iba 28,8 %, čo naznačuje výrazné problémy pri rozlišovaní medzi vysoko realistickými falzifikátmi a skutočnými tvárami.

Fotografia na fotopapiery
Detekcia fotografických podvrhov s presnosťou 79,1 % je relatívne vysoká, čo ukazuje, že systém je dobre vybavený na rozpoznávanie statických obrázkov a ich odleskov.

Časopis
S presnosťou 80,8 % sa výkon len málo líši od výkonu pri fotografiách, čo ukazuje podobné schopnosti systému pri rozpoznávaní papierových médií.

[3] https://support.apple.com/cs-cz/111849

Smartfón
Pri použití detektora hrán dosahovala presnosť detekcie 60 % oproti 11 % bez použitia tejto techniky. Tento výrazný rozdiel poukazuje na významnú úlohu detektora hrán pri identifikácií digitálnych zobrazení.

5.3.4 Komparatívna analýza prostredí testovania

Izba
Izba obsahuje viac rušivých okolitých elementov ako kancelária, cieľom teda bolo zistiť ako sa model vysporiada s týmito prekážkami. Testovali sa tu všetky spomenuté formy útokov. Reálnu tvár detegoval takmer v každom prípade, falošné vyhodnotenia nastávali len v momentoch, kedy sa tvár veľmi prudko hýbala a za zhoršených svetelných podmienok. 3D maska spôsobovala detekcií najväčšie problémy zo všetkých typov útokov, pretože správne bolo detegovaných iba 40 snímkov z celkovo 129 obsahujúcich masku. Útoky vo forme fotografií na fotopapiery a vytlačenej fotky v časopise či na obyčajnom papieri zdieľali presnosť. Z 151 snímkov s prítomnosťou fotopapieru bolo správne určených 123 ako podvrh, čo predstavuje presnosť 81 %, zatiaľ čo pri použití časopisu bolo z 172 zistených správne 139. To predstavuje presnosť 80 %. Pri použití smartfónu bola dosiahnutá presnosť 49 % v kombinácií modelu s detektorom hrán. Bez jeho použitia bol samotný model schopný dosiahnuť presnosť iba 11 %.

Kancelária
Prostredie kancelárie je využité najmä vďaka typu osvetlenia, ktorý sa v podobných priestoroch nachádza. Nasnímaných bolo dokopy 178 záberov, z toho 133 s použitím rôznych typov útokov. Živé tváre boli rozpoznané s presnosťou 85 %, teda 39 zo 45 bolo správne určených. Celková úspešnosť v detekcií útokov bola 69 %. Najhoršiu úspešnosť mala detekcia 3D tváre, kde sa podarilo úspešne detegovať iba 3 z 20 záberov. V prípade fotografií model detegoval správne 63 % a smartfón s vysokou presnosťou 94 %. Túto presnosť možno pripísať odrazom kancelárskych LED svetiel na obrazovke smartfónu, ktoré model dokáže efektívne detegovať.

Vonkajšie prostredie
Zameraním tohto experimentu bola najmä detekcia hrán smartfónu. Za nízkych svetelných podmienok je vidieť výrazne prechod medzi mobilným zariadením a okolitým pozadím. Z natočeného video-záznamu, v ktorom boli prítomné podvrhy bol zachytených 270 snímkov programom. Z toho na 207 bola identifikovaná prítomnosť podvrhu, čím vznikla presnosť 77 %. Preukázalo sa, že detektor hrán vie na dobrej úrovni detegovať zmenu a zachytiť okraje mobilu. Pri pokuse o testovanie vytlačených obrázkov vznikal v tomto prostredí príliš veľký šum, detektor tváre YOLO (viz sekcia 3.3.1) nedokázal lokalizovať tvár na videu.

5.4 Perspektívy rozvoja a implementačné bariéry

Hlavnou príležitosťou pre rozšírenie je vývoj a integrácia rozmanitejších dátových sád, ktoré pokrývajú širšie spektrum útokov, ako sú video útoky alebo pokročilé maskovacie techniky. Aktuálne používaný dataset NUAA je obmedzený na útoky pomocou fotografie, čo neodráža všetky možné scenáre, s ktorými sa systém môže stretnúť v praxi. Rozšírenie datasetu by

umožnilo modelu naučiť sa rozpoznávať sofistikovanejšie podvody a zlepšiť jeho schopnosť generalizácie.

Ďalšou možnosťou rozšírenia je vývoj hybridných modelov, ktoré kombinujú viacero typov príznakov a techník strojového učenia, čo by mohlo priniesť výrazné zlepšenie v presnosti a robustnosti modelu.

Významnou oblasťou, ktorá si vyžaduje ďalší výskum, je vplyv šumu na správanie a presnosť detekčných modelov tváre pri nízkych svetelných podmienkach. Vývoj špecializovaných techník na redukciu šumu a zlepšenie vizuálnej kvality obrazu môže výrazne prispieť k robustnosti modelu. Zavedenie metód ako je napríklad adaptívne filtrovanie, využitie pokročilých techník strojového učenia pre rozpoznávanie vzorov aj v šumovom prostredí, a implementácia konvolučných neurónových sietí špecificky navrhnutých pre prácu v nízkosvetelných podmienkach by mohlo značne vylepšiť schopnosť modelu správne identifikovať autentické tváre aj v suboptimálnych podmienkach.

5.4.1 Problémy pri implementácii

Počas implementácie systému sme narazili na niekoľko problémov, ktoré môžu ovplyvniť výkon a spoľahlivosť modelu. Medzi hlavné problémy patrí:

- Nedostatok diverzity v trénovanom datasete - Ako bolo spomenuté, dataset NUAA sa zameriava primárne na útoky za pomoci fotografií. Toto môže viesť k modelu, ktorý je síce vysoko efektívny v konkrétnych podmienkach, ale má obmedzenú aplikáciu v reálnom svete, kde útočníci môžu používať rozmanitejšie metódy.
- Pretrénovanie modelov na špecifické údaje - Existuje riziko, že modely sú pretrénované na konkrétne charakteristiky datasetu, čo znižuje ich schopnosť generalizovať na nevidené dáta.
- Znateľný vplyv šumu pri detekcii tváre v nízkosvetelných podmienkach - Šum v obraze, ktorý je často prítomný v podmienkach nedostatočného osvetlenia, môže výrazne ovplyvniť presnosť detekcie tváre, čo vedie k nesprávnym alebo neúplným rozpoznávaniam.

5.4.2 Návrhy na zlepšenie

Rozšírenie a diverzifikácia trénovacích dát, vrátane zahrnutia rozmanitejších foriem útokov ako sú 3D masky, video záznamy a syntetické obrazy, by mohlo výrazne pomôcť zlepšiť odolnosť modelu proti sofistikovanejším útokom.

Ďalej, implementácia pokročilejších metód validácie, napríklad použitie nezávislých testovacích datasetov alebo testovanie v dynamických prostrediach, by mohla poskytnúť realistické hodnotenie výkonu modelu, čo umožní lepšie pochopenie jeho efektivity v rôznych situáciách.

Kapitola 6

Záver

Táto práca je zameraná na návrh, implementáciu a testovanie efektívnych systémov detekcie podvrhov tvárí, ktoré sú kritickým komponentom v bezpečnostných biometrických systémoch. Prvá kapitola poskytla prehľad existujúcich techník a technológií v oblasti biometrického rozpoznávania, zatiaľ čo druhá kapitola sa sústredila na detailný popis rôznych typov útokov, s ktorými sa biometrické systémy môžu stretnúť, vrátane podvrhov tvárí a útokov pomocou maskovania. Tieto úvodné kapitoly nastavili teoretický a praktický rámec pre hĺbkové pochopenie problematiky, ktorá bola ďalej rozpracovaná prostredníctvom vlastného výskumu a experimentov.

Hlavným cieľom bolo posilniť obranyschopnosť proti prezenčným útokom, ktoré predstavujú vážnu hrozbu pre autentifikačné procesy. Výsledkom je integrovaný prístup, ktorý spája pokročilé algoritmy strojového učenia, hlboké učenie a techniky spracovania obrazu, vďaka čomu sa dosiahlo robustné a spoľahlivé riešenie schopné identifikovať a odolať rôznym typom útokov. Experimentálna časť práce predstavuje kľúčovú súčasť, kde je demonštrovaná vysoká účinnosť navrhovaných metód. Testy uskutočnené na dátových sadách ukázali, že navrhnuté algoritmy dosahujú vysokú presnosť detekcie. Detekcia živosti a falšovaných tvárí bola analyzovaná v rôznych scenároch, vrátane použitia rôznych typov útočných nástrojov, ako sú fotografie, videá a 3D masky.

Osobitne zaujímavým výsledkom bolo zistenie, že detekcia hrán výrazne zlepšila schopnosť systému identifikovať podvrhy, ktoré používajú digitálne zobrazenia v smartfónoch, čo demonštruje značnú efektívnosť tejto techniky v praktických aplikáciách. Rovnako tak zaujímavým výsledkom je konzistentne vysoká úspešnosť detekcie živých tvárí bez podvrhov, ktorá bola dosiahnutá v rôznych testovaných prostrediach. Tento výsledok je významný, pretože potvrdzuje základnú spoľahlivosť a efektívnosť systému v rozpoznávaní autentických tvárí, čo je kľúčové pre každý biometrický bezpečnostný systém.

Okrem technických aspektov sa práca venuje aj metodologickým a teoretickým otázkam. Diskutuje sa o limitách a možných slabých miestach súčasných biometrických systémov, ako aj o dôležitosti kontinuálneho vývoja a adaptácie na nové útoky. Pri analýze výsledkov je nevyhnutné zdôrazniť rozdiely medzi testovaním na kontrolovanej testovacej dátovej sade a výzvami, ktoré prinášajú reálne prostredia ako kancelárie, izby alebo vonkajšie priestory. Použitý testovací dataset obsahuje obmedzené typy snímok a scenárov, ktoré boli vybrané alebo vytvorené za špecifických podmienok. Tieto dáta môžu byť systematicky iné od dát, s ktorými sa algoritmus stretne v reálnych prostrediach. Tie prinášajú neustále meniace sa podmienky, ktoré môžu významne ovplyvniť detekciu, a preto si vyžadujú prispôsobené riešenia a špecifické testovanie, aby sa zabezpečila skutočná odolnosť a spoľahlivosť systémov.

Pre budúci výskum sa ukazuje ako dôležité pokračovať v experimentovaní s novými technológiami a prístupmi. Zvlášť perspektívne by mohlo byť zapojenie nových typov neurónových sietí, experimentovanie s rôzne komplexnými útočnými vektormi a adaptácia systémov na nové typy biometrických údajov. Záverom možno povedať, že táto práca predstavuje významný príspevok k pochopeniu a zlepšeniu bezpečnostných opatrení biometrických systémov. Prezentované techniky a metódy detekcie otvárajú cestu k budúcim inováciám, ktoré by mohli ešte viac zvýšiť odolnosť proti sofistikovaným útokom a zároveň poskytujú pevný základ pre bezpečnostné aplikácie v praxi. Napokon, dôraz na etické a právne aspekty pri implementácii a používaní biometrických technológií zdôrazňuje potrebu vyváženého prístupu, ktorý zabezpečí, že nové technológie budú využívané zodpovedne a v súlade s ochranou osobných údajov a súkromia jednotlivcov.

Literatúra

[1] Albakri, G. a Alghowinem, S. The Effectiveness of Depth Data in Liveness Face Authentication Using 3D Sensor Cameras. Switzerland: MDPI AG. 2019, zv. 19, č. 8, s. 1928. ISSN 1424-8220.

[2] Alkandari, A. a Aljaber, S. J. Principle Component Analysis algorithm (PCA) for image recognition. In: *2015 Second International Conference on Computing Technology and Information Management (ICCTIM)*. April 2015, s. 76–80. DOI: 10.1109/ICCTIM.2015.7224596.

[3] Anguita, D., Ghio, A., Ridella, S. a Sterpi, D. K-Fold Cross Validation for Error Rate Estimate in Support Vector Machines. Január 2009, s. 291–297.

[4] Anjos, A. a Marcel, S. Counter-measures to photo attacks in face recognition: A public database and a baseline. In: *2011 International Joint Conference on Biometrics (IJCB)*. IEEE, 2011, s. 1–7. ISBN 1457713586.

[5] Aravena, C., Pasmino, D., Tapia, J. E. a Busch, C. *Impact of Face Image Quality Estimation on Presentation Attack Detection*. 2022. DOI: 10.48550/arXiv.2209.15489.

[6] Bora, D. J., Gupta, A. K. a Khan, F. A. *Comparing the Performance of L*A*B* and HSV Color Spaces with Respect to Color Image Segmentation*. 2015.

[7] Boulkenafet, Z., Komulainen, J. a Hadid, A. Face Spoofing Detection Using Colour Texture Analysis. *IEEE Transactions on Information Forensics and Security*. 1. vyd. 2016, zv. 11, č. 8, s. 1818–1830. DOI: 10.1109/TIFS.2016.2555286.

[8] Busch, C., Czajka, A., Deravi, F., Drozdowski, P., Gomez-Barrero, M. et al. A response to the European Data Protection Supervisor 'Misunderstandings in Biometrics' by the European Association for Biometrics. *IET biometrics*. Hindawi-IET. 2022, zv. 11, č. 1, s. 79–86. ISSN 2047-4938.

[9] Canny, J. A Computational Approach to Edge Detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1. vyd. IEEE. 1986, PAMI-8, č. 6, s. 679–698.

[10] Deng, J., Guo, J., Ververas, E., Kotsia, I. a Zafeiriou, S. RetinaFace: Single-Shot Multi-Level Face Localisation in the Wild. In: *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*. June 2020, s. 5202–5211. DOI: 10.1109/CVPR42600.2020.00525. ISSN 2575-7075.

[11] Deng, J., Guo, J., Xue, N. a Zafeiriou, S. ArcFace: Additive Angular Margin Loss for Deep Face Recognition. In: *2019 IEEE/CVF Conference on Computer*

Vision and Pattern Recognition (CVPR). 2019, s. 4685–4694. DOI: 10.1109/CVPR.2019.00482. ISSN 2575-7075.

[12] Erdogmus, N. a Marcel, S. Spoofing Face Recognition With 3D Masks. *IEEE Transactions on Information Forensics and Security*. 2014, zv. 9, č. 7, s. 1084–1097. DOI: 10.1109/TIFS.2014.2322255.

[13] Evgeniou, T. a Pontil, M. Support Vector Machines: Theory and Applications. In: Paliouras, G., Karkaletsis, V. a Spyropoulos, C. D., ed. *Machine Learning and Its Applications: Advanced Lectures*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, s. 249–257. DOI: 10.1007/3-540-44673-7_12. ISBN 978-3-540-44673-6. Dostupné z: https://doi.org/10.1007/3-540-44673-7_12.

[14] Fernández, A., García, R., Usamentiaga, R. a Casado, R. Glasses detection on real images based on robust alignment. *Machine Vision and Applications*. Máj 2015, zv. 26, č. 4, s. 519–531. DOI: 10.1007/s00138-015-0674-1. ISSN 1432-1769.

[15] GeeksforGeeks. *Biometric System Architecture*. 2022. Citované: 22.4.2024. Dostupné z: https://www.geeksforgeeks.org/biometric-system-architecture/.

[16] Hastings, G. D. a Rubin, A. Colour Spaces - A Review of Historic and Modern Colour Models. *African Vision and Eye Health*. 2012, zv. 71, č. 3, s. 133–143. DOI: 10.4102/aveh.v71i3.76. Dostupné z: https://avehjournal.org/index.php/aveh/article/view/76.

[17] Hernandez-Ortega, J., Fiérrez, J., Morales, A. a Galbally, J. Introduction to Presentation Attack Detection in Face Biometrics and Recent Advances. *CoRR*. 2021, abs/2111.11794. Dostupné z: https://arxiv.org/abs/2111.11794.

[18] Hosang, J., Benenson, R. a Schiele, B. Learning non-maximum suppression. *ArXiv preprint arXiv:1705.02950*. 2017.

[19] iBeta. *IBeta* [Dostupné online]. 2018. Citované: 22.4.2024. Dostupné z: https://www.ibeta.com/about-ibeta/.

[20] IEEE. IEEE Standard for Biometric Liveness Detection. *IEEE Std 2790-2020*. 2020, s. 1–24. DOI: 10.1109/IEEESTD.2020.9080669.

[21] ISO/IEC. *ISO/IEC JTC 1/SC 37: International Standard* [International Standard published]. 2. vyd. február 2024. Number of pages: 14. Dostupné z: https://www.iso.org/standard/82584.html.

[22] Jain, A., Wayman, J., Maltoni, D. a Maio, D. *Biometric Systems*. 1. vyd. Springer London, 2010. ISBN 978-1-84628-064-1.

[23] Jain, A. K., Ross, A. A. a Nandakumar, K. *Introduction to Biometrics*. 2011. vyd. New York, NY: Springer, 2011. ISBN 978-0387773254.

[24] Jain, A. K., Ross, A. A. a Nandakumar, K. *Introduction to Biometrics*. New York, NY: Springer Nature, 2011. ISBN 0387773266.

[25] Jain, R. a Kant, C. Attacks on Biometric Systems: An Overview. *International Journal of Advances in Scientific Research*. September 2015, zv. 1, s. 283. DOI: 10.7439/ijasr.v1i7.1975.

[26] Khairnar, S., Gite, S., Kotecha, K. a Thepade, S. D. Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions. *Big Data and Cognitive Computing*. 2023, zv. 7, č. 1. DOI: 10.3390/bdcc7010037. ISSN 2504-2289. Dostupné z: https://www.mdpi.com/2504-2289/7/1/37.

[27] Kolarov, P. *Centralized vs. Decentralized Biometric Authentication* [Dostupné online]. 2021. Citované: 22.4.2024. Dostupné z: https://www.linkedin.com/pulse/centralized-vs-decentralized-biometric-authentication-peter-kolarov/.

[28] Koonce, B. a Koonce, B. ResNet 50. *Convolutional neural networks with swift for tensorflow: image recognition and dataset categorization*. Springer. 2021, s. 63–72.

[29] Kowalski, M. A Study on Presentation Attack Detection in Thermal Infrared. *Sensors*. 2020, zv. 20, č. 14. DOI: 10.3390/s20143988. ISSN 1424-8220. Dostupné z: https://www.mdpi.com/1424-8220/20/14/3988.

[30] Kumar, D. K. R. a Latha, U. A Study on Attacks and Security Against Fingerprint Template Database. *International Journal of Emerging Trends & Technology in Computer Science*. Október 2013, zv. 2, s. 13.

[31] Li, L., Xia, Z., Hadid, A., Jiang, X., Zhang, H. et al. Replayed Video Attack Detection Based on Motion Blur Analysis. *IEEE Transactions on Information Forensics and Security*. 2019, zv. 14, č. 9, s. 2246–2261. DOI: 10.1109/TIFS.2019.2895212.

[32] Lin, T.-Y., Dollár, P., Girshick, R., He, K., Hariharan, B. et al. *Feature Pyramid Networks for Object Detection*. 2017.

[33] Liu, S., Yang, B., Yuen, P. C. a Zhao, G. A 3D Mask Face Anti-Spoofing Database with Real World Variations. In: *2016 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*. 2016, s. 1551–1557. DOI: 10.1109/CVPRW.2016.193. ISBN 978-1-5090-1437-8. Dostupné z: https://researchr.org/publication/LiuYYZ16.

[34] Marcel, S., Nixon, M. S., Fierrez, J. a Evans, N. *Handbook of Biometric Anti-Spoofing*. 2. vyd. Springer Cham, 2019. ISBN 978-3-319-92627-8.

[35] Mwema, J., Kimwele, M. a Kimani, S. A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates. *International Journal of Computer Trends and Technology*. Február 2015, zv. 20, s. 12–18. DOI: 10.14445/22312803/IJCTT-V20P103.

[36] NIST. *National Institute of Standards and Technology* [Dostupné online]. 2009. Citované: 22.4.2024. Dostupné z: https://www.nist.gov/.

[37] Ohashi, T., Al Aghbari, Z. a Makinouchi, a. Hill-climbing Algorithm for Efficient Color-based Image Segmentation. *Signal Processing, Pattern Recognition, and Applications*. Január 2003.

[38] Ojala, T., Pietikainen, M. a Maenpaa, T. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE*

Transactions on Pattern Analysis and Machine Intelligence. July 2002, zv. 24, č. 7, s. 971–987. DOI: 10.1109/TPAMI.2002.1017623. ISSN 1939-3539.

[39] OpenCV. *Hough Line Transform*. 2022. Citované: 2023-04-30. Dostupné z: https://docs.opencv.org/3.4/d9/db0/tutorial_hough_lines.html.

[40] Pietikäinen, M., Hadid, A., Zhao, G. a Ahonen, T. *Computer Vision Using Local Binary Patterns*. Springer Science + Business Media, 2011. ISBN 978-0-85729-747-1. Dostupné z: https://link.springer.com/book/10.1007/978-0-85729-748-8.

[41] Powers, D. Evaluation: From Precision, Recall and F-Factor to ROC, Informedness, Markedness & Correlation. *Mach. Learn. Technol.* Január 2008, zv. 2.

[42] Qi, H., Wu, C., Shi, Y., Qi, X., Duan, K. et al. A Real-Time Face Detection Method Based on Blink Detection. *IEEE Access*. 2023, zv. 11, s. 28180–28189. DOI: 10.1109/ACCESS.2023.3257986.

[43] Rafique, R., Gantassi, R., Amin, R., Frnda, J., Mustapha, A. et al. Deep fake detection and classification using error-level analysis and deep learning. *Scientific Reports*. 2023, zv. 13, č. 1, s. 7422. DOI: 10.1038/s41598-023-34629-3. Dostupné z: https://doi.org/10.1038/s41598-023-34629-3.

[44] Rathgeb, C., Drozdowski, P. a Busch, C. Vulnerability Assessment and Detection of Makeup Presentation Attacks. *IEEE Transactions on Information Forensics and Security*. 2021, zv. 16, s. 3607–3621. DOI: 10.1109/TIFS.2021.3075307. Dostupné z: https://ieeexplore.ieee.org/document/9442243.

[45] Redmon, J., Divvala, S., Girshick, R. a Farhadi, A. *You Only Look Once: Unified, Real-Time Object Detection*. 2016.

[46] Schroff, F., Kalenichenko, D. a Philbin, J. FaceNet: A unified embedding for face recognition and clustering. In: *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. IEEE, June 2015, s. 815–823. DOI: 10.1109/CVPR.2015.7298682. ISSN 1063-6919.

[47] SOKOLOVA, M., JAPKOWICZ, N. a SZPAKOWICZ, S. Beyond accuracy, F-score and ROC : A family of discriminant measures for performance evaluation. In: *Lecture notes in computer science*. Heidelberg: Springer, 2006, s. 1015–1021. ISBN 3540497870.

[48] Tan, X., Li, Y., Liu, J. a Jiang, L. Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model. In: Daniilidis, K., Maragos, P. a Paragios, N., ed. *Computer Vision – ECCV 2010*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, s. 504–517. ISBN 978-3-642-15567-3.

[49] Tang, D., Zhou, Z., Zhang, Y. a Zhang, K. Face flashing: a secure liveness detection protocol based on light reflections. *ArXiv preprint arXiv:1801.01949*. 2018.

[50] Thuis, C. *SSD-Sface : Single shot multibox detector for small faces*. 2018. Dostupné z: https://api.semanticscholar.org/CorpusID:52830663.

[51] Tot, I. A., Bajetić, J. B., Jovanović, B. B., Trikoš, M. B., Bogišević, D. L. et al. Biometric standards and methods. *Vojnotehnicki glasnik/Military Technical Courier*. University of Defence, Serbia. 2021, zv. 69, č. 4. DOI: 10.5937/vojtehg69-32296. Dostupné z: https://www.redalyc.org/articulo.oa?id=661770260009.

[52] Turhal, U., Günay Yilmaz, A. a Nabiyev, V. A new face presentation attack detection method based on face-weighted multi-color multi-level texture features. *The Visual Computer*. Mar 2024, zv. 40, č. 3, s. 1537–1552. DOI: 10.1007/s00371-023-02866-2. ISSN 1432-2315. Dostupné z: https://doi.org/10.1007/s00371-023-02866-2.

[53] Ultralytics. *YOLOv8 Documentation*. 2023. Citované: 22.4.2024. Dostupné z: https://docs.ultralytics.com/.

[54] Vedaldi, A., Bischof, H., Brox, T. a Frahm, J.-M. CelebA-Spoof: Large-Scale Face Anti-spoofing Dataset with Rich Annotations. In: *Computer Vision - ECCV 2020*. Switzerland: Springer International Publishing AG, 2020, sv. 12357, s. 70–85. Lecture Notes in Computer Science. ISBN 9783030586096.

[55] Wang, H., Wang, Y., Zhou, Z., Ji, X., Gong, D. et al. CosFace: Large Margin Cosine Loss for Deep Face Recognition. In: *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*. June 2018, s. 5265–5274. DOI: 10.1109/CVPR.2018.00552. ISSN 2575-7075.

[56] Wang, T., Yang, J., Lei, Z., Liao, S. a Li, S. Z. Face liveness detection using 3D structure recovered from a single camera. In: *2013 International Conference on Biometrics (ICB)*. June 2013, s. 1–6. DOI: 10.1109/ICB.2013.6612957. ISSN 2376-4201.

Príloha A

Obsah priloženého pamäťového média

- src/ Priečinok so zdrojovými súbormi.
- models/ Priečinok s modelmi.
- features/ Priečinok s vektormi získanými zo spracovania dátovej sady.
- requirements.txt Závislosti knižníc Pythonu.
- thesis.pdf Súbor záverečnej práce.
- README.md README súbor pre projekt.
- latex/ Priečinok so zdrojovými súbormi LaTeX.