VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

DETEKCE PREZENTAČNÍHO ÚTOKU NA OTISKY PRSTŮ POMOCÍ ŽIL

PRESENTATION ATTACK DETECTION ON FINGERPRINT IMAGES USING VEINS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **TOMÁŠ ONDRUŠEK**
AUTHOR

VEDOUCÍ PRÁCE **Ing. ONDŘEJ KANICH, Ph.D.**
SUPERVISOR

BRNO 2023

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Zadání bakalářské práce

147449

Ústav: Ústav inteligentních systémů (UITS)
Student: **Ondrušek Tomáš**
Program: Informační technologie
Specializace: Informační technologie

Název: **Detekce prezentačního útoku na otisky prstů pomocí žil**
Kategorie: Bezpečnost
Akademický rok: 2022/23

Zadání:

1. Prostudujte literaturu týkající se rozpoznávání podle otisků prstů a detekci prezentačního útoku. Seznamte se se zařízeními na snímání a rozpoznání žilního řečiště.
2. Navrhněte metodu detekce prezentačního útoku, na systém rozpoznávající podle otisků prstů, využívající žilního řečiště.
3. Spolupracujte na nasnímání datasetu minimálně 100 obrázků z experimentálního zařízení snímající otisky i žíly prstu. Součástí tohoto datasetu budou i snímky využívající nástroj prezentačního útoku (falzifikát otisku prstu).
4. Implementujte navrženou metodu z bodu dva.
5. Analyzujte přesnost metody implementované v předchozím bodě na nasnímaném datasetu.
6. Dosažené výsledky shrňte a diskutujte. Uveďte možná vylepšení a rozšíření vašeho řešení.

Literatura:

- Drahanský, M., Kanich, O., Dvořák, M.: *Spoofing methods in hand-based biometrics*, Hand-based Biometrics: Methods and Technologies, IET, 2018, p. 32, ISBN 978-1-78561-224-4.
- Marcel, S., Nixon, M.S., Fierrez, J., Evans, N.: *Handbook of Biometrics Anti-Spoofing*, Springer, 2014, ISBN 978-1-4471-6523-1.
- Uhl, A., Busch, C., Marcel, S., Veldhuis, R.: *Handbook of vascular biometrics*. Springer Open, 2020. Advances in computer vision and pattern recognition. ISBN 978-3-030-27730-7.

Při obhajobě semestrální části projektu je požadováno:

- Body 1, 2 a částečně bod 3.

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

Vedoucí práce: **Kanich Ondřej, Ing., Ph.D.**
Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.
Datum zadání: 1.11.2022
Termín pro odevzdání: 10.5.2023
Datum schválení: 3.11.2022

Abstrakt

Táto práca sa zaoberá detekciou prezentačného útoku na biometrický snímač odtlačkov prstov zachytávajúci snímku žilového riečiska. Obsahuje návrh metódy detekcie prezentačného útoku na snímač, ktorý používa NIR osvetlenie na zvýraznenie žilového riečiska v prste. Metóda je testovaná a trénovaná na dátovej sade obsahujúcej 294 snímkov prstov extrahovaných zo 143 snímkov rúk. Metóda je založená na extrahovaní texturálnych informácií zo snímku a následnej klasifikácií pomocou SVM klasifikátora. Extrakcia používa paralelné spracovanie a prvky z 294 snímkov prstov spracuje v priemere za 25 minút. Následná klasifikácia dosahuje priemernú úspešnosť detekcie 97 %. V práci sú takisto opísané kroky potrebné na prevedenie rôznych typov útokov na biometrický systém používajúci práve žilové riečisko.

Abstract

This work deals with the detection of a presentation attack on a biometric fingerprint sensor capturing an image of a vein. It contains a proposal for a method of detecting a presentation attack on a sensor that uses NIR illumination to highlight a vein in a finger. The method is tested and trained on a dataset containing 294 finger images extracted from 143 pictures of hands. The method is based on extracting textural information from the image and subsequent classification using the SVM classifier. The extraction uses parallel processing and processes features from 294 fingerprint images in 25 minutes on average. Subsequent classification achieves an average detection success rate of 97 %. The work also describes the steps necessary to carry out various types of attacks on a biometric system using the vein system.

Kľúčové slová

odtlačok prsta, krvné riečisko, detekcia prezentačného útoku, falzifikát odtlačku prsta, falzifikát krvného riečiska, blízke infračervené svetlo, Python

Keywords

fingerprint, blood stream, detection of presentation attack, fingerprint spoof, finger vein spoof, near infrared light, Python

Citácia

ONDRUŠEK, Tomáš. *Detekce prezentačního útoku na otisky prstů pomocí žil.* Brno, 2023. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Ondřej Kanich, Ph.D.

Detekce prezentačního útoku na otisky prstů pomocí žil

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Ing. Ondřeja Kanicha Ph.D. Ďalšie informácie mi poskytol pán Ing. Štěpán Rydlo. Uviedol som všetky literárne pramene, publikácie a ďalšie zdroje, z ktorých som čerpal.

.....
Tomáš Ondrušek
7. mája 2023

Poďakovanie

Ďakujem vedúcemu práce pánovi Ing. Ondřejovi Kanichovi Ph.D za odborné rady a konzultácie poskytnuté pri vypracovaní práce. Tiež ďakujem za pomoc pri práci s experimentálnym zariadením pánovi Ing. Štěpánovi Rydlovi.

Obsah

Kapitola 1

Úvod

Identifikácia človeka za pomoci biometrie sa rok po roku stáva sympatickejšou alternatívou oproti používaniu teraz už bežných spôsobov ako napríklad prikladanie ID kariet, zadávanie hesiel či odomykanie pomocou kľúčov. Za veľkú obľúbenosť biometrie značí práve fakt, že na overenie identity nie je potreba mať pri sebe žiadne predmety potrebné na overenie, alebo potreba si pamätať heslo či viacmiestny kód. Pri overení identity za použití biometrie je jediným predmetom ktorý daná osoba potrebuje časť tela, ktorou sa identita overuje.

Biometrické overovanie sa dá rozdeliť na bez-kontaktné (použitie tváre alebo dúhovky) alebo kontaktné, pri ktorom sa na overenie používa odtlačok danej časti tela (odtlačok dlane alebo prsta). Vďaka faktu, že každý človek má jedinečné črty je možné ľudí identifikovať s veľkou presnosťou a v dnešnej dobe aj rýchlosťou. Najrozšírenejšia metóda overovania za pomoci biometrie je použitie odtlačkov prsta. Jedným z najrozšírenejších zariadení, ktoré využíva odtlačok prsta na overenie identity je mobilný telefón. No vďaka rýchlo rastúcemu trendu používania biometrickej autentifikácie priamo úmerne rastie aj záujem o oklamanie týchto zariadení a to či už výrobou falzifikátov (vonkajší útok) alebo preniknutím do systému a vložením falošných dát za účelom získania prístupu (vnútorný útok). Falšovateľ môže takýmto spôsobom získať prístup napríklad do internetového bankovníctva, rôznym účtom alebo osobným údajom.

Ako ďalší krok v overovaní zabezpečenia pri použití odtlačku prsta boli navrhnuté metódy a hardvér na overenie živosti prsta alebo na sledovanie ďalších snímateľných charakteristík, ktoré ľudský prsta nadobúda, ako je napríklad snímok žilového riečiska. Detekcia živosti slúži na lepšiu detekciu falzifikátov prsta (napríklad gumený odliatok prsta) a to sledovaním rôznych charakteristík, ktoré nadobúda živý prst priložený na snímač odtlačkov zatiaľ čo snímok žilového riečiska slúži ako doplňujúci údaj ku odtlačku prsta na zaistenie lepšej a presnejšej detekcie útokov na biometrický systém.

Cieľom tejto bakalárskej práce je nasnímanie databázy odtlačkov skutočného prsta a rôznych falzifikátov použitých pri prezentačnom útoku, pričom daný snímok obsahuje informácie o žilovom riečisku. Následne návrh metódy detekcie prezentačného útoku na systém rozpoznávajúci podľa odtlačkov prstov, využívajúci žilové riečisko. Metóda bude založená na extrahovaní informácií získaných zo zachytených snímkov, ktoré následne slúžia na trénovanie SVM klasifikátora použitom na binárnu klasifikáciu snímku. Výsledky úspešnosti klasifikácie budú prezentované a diskutované v kapitole 6.

Kapitola 2

Biometrické vlastnosti prsta

Táto kapitola predstavuje terminológiu súvisiacu s biometriou potrebnú na pochopenie nasledujúcich kapitol. Konkrétne sa bude zaoberať biometriou odtlačku prsta a biometriou žilového riečiska v prste. Zavedú sa tu základné pojmy a metriky použité v následných kapitolách.

2.1 Biometria

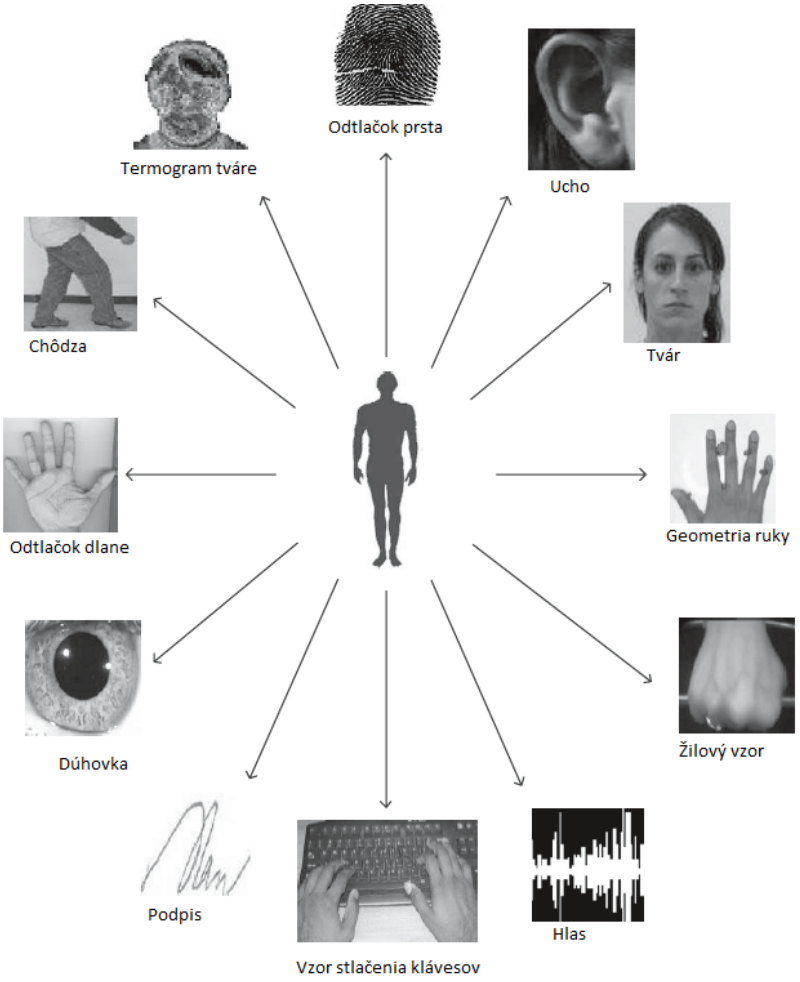
Slovo biometria je odvodené z gréckych slov bios (čo znamená život) a metron (čo znamená meranie), teda meranie charakteristík z ľudského tela alebo doslovnejší preklad "*meranie života*"[12].

Biometrické rozpoznávanie (alebo jednoduchšie biometria) sa týka použitia anatomických (napr. odtlačky prstov, tváre, dúhovky) a behaviorálnych (napr. reč) charakteristík, ktoré sa nazývajú biometrické identifikátory alebo črty na automatické rozpoznávanie jednotlivcov, ako je ukázané na obrázku 2.1. Biometria sa stáva nevyhnutnou súčasťou efektívnych riešení identifikácie osôb, pretože biometrické identifikátory nemožno zdieľať ani stratiť a vo svojej podstate predstavujú telesnú identitu jednotlivca. Rozpoznanie osoby podľa tela a následné prepojenie tohto tela s externe stanovenou „identitou“ tvorí veľmi silný nástroj riadenia identity s obrovskými potenciálnymi dôsledkami, pozitívnymi aj negatívnymi. V dôsledku toho nie je biometria len fascinujúcim výskumným problémom rozpoznávania vzorov, ale ak sa používa opatrne, je to podporná technológia s potenciálom urobiť našu spoločnosť bezpečnejšou, znížiť podvody a poskytnúť užívateľské pohodlie (používateľsky prívetivé rozhranie človek-stroj) [12].

2.1.1 Biometrický systém

Ako biometrický identifikátor možno použiť akúkoľvek ľudskú fyziologickú a/alebo behaviorálnu charakteristiku rozpoznať osobu, pokiaľ spĺňa tieto požiadavky:

- **univerzálnosť**, čo znamená, že každý človek by mal mať požadované biometrické údaje [11].
- **rozlišovacia spôsobilosť**, ktorá naznačuje, že akékoľvek dve osoby by mali byť dostatočne odlišné z hľadiska ich biometrických identifikátorov [11].
- **trvalosť**, čo znamená, že biometria daného identifikátora by mala byť dostatočne nemenná (vzhľadom na kritérium zhody) počas určitého časového obdobia [11].



Obr. 2.1: Príklady biometrických identifikátorov, ktoré možno použiť na overenie jednotlivca. Medzi fyzické vlastnosti môže patriť napríklad odtlačok prsta, dúhovka, tvár alebo geometria ruky a medzi behaviorálne črty môže patriť podpis, dynamika stlačenia klávesov alebo chôdza. (Obrázok prevzatý z [18].)

- **zberateľnosť**, čo znamená, že biometriu možno merať kvantitatívne [11].

V praktickom biometrickom systéme však existuje množstvo ďalších problémov, ktoré by mali byť zvážené pri jeho návrhu. Medzi tieto problémy patrí napríklad **výkon**, ktorý sa vzťahuje na dosiahnuteľnú presnosť rozpoznávania, rýchlosť, robustnosť, požiadavky na zdroje na dosiahnutie požadovanej presnosti a rýchlosti rozpoznávania, ako aj prevádzkové alebo environmentálne faktory, ktoré ovplyvňujú presnosť rozpoznávania a rýchlosť. Ďalej medzi tieto problémy patrí **prijateľnosť**, ktorá vyjadruje mieru, do akej sú ľudia ochotní akceptovať konkrétny biometrický systém vo svojom každodennom živote a nakoniec **obchádzanie alebo robustnosť**, ktoré odráža, aké ľahké je oklamať systém podvodnými metódami [11].

2.1.2 Registrácia, Verifikácia a Identifikácia

Biometrický systém plní tri základné procesy, a to:

- **Registráciu**: Registrácia používateľa je proces, ktorý je zodpovedný za registráciu jednotlivcov v úložisku biometrického systému. Počas procesu zápisu sa biometrické charakteristiky subjektu najprv zachytia biometrickým skenerom, aby sa vytvorila vzorka. Často sa vykonáva kontrola kvality, aby sa zabezpečilo, že získaná vzorka môže byť spoľahlivo spracovaná v nasledujúcich fázach. Modul extrakcie prvkov sa potom použije na vytvorenie sady prvkov. Modul na vytváranie šablón používa sadu prvkov na vytvorenie šablóny registrácie. Niektoré systémy zhromažďujú viacero vzoriek používateľa a potom buď vyberú najlepší obrázok (alebo sadu prvkov), alebo zlúčia viacero obrázkov (alebo sád prvkov), aby vytvorili zloženú šablónu. Proces registrácie potom vezme šablónu registrácie a uloží ju do systémového úložiska spolu s demografickými informáciami o používateľovi (ako je identifikátor, meno, pohlavie, výška, atď...) [12].

- **Verifikáciu**: Verifikačný proces je zodpovedný za potvrdenie alebo vyvrátenie tvrdenia o totožnosti subjektu. Počas fázy rozpoznávania je poskytnutý *identifikátor subjektu* (ako je používateľské meno alebo PIN ("Personal Identification Number") (napr. prostredníctvom klávesnice alebo klávesnice alebo bez-dotykovej karty) na uplatnenie identity. Biometrický skener zachytí danú charakteristiku subjektu a prevedie ju na vzorku, ktorá je ďalej spracovaná modulom extrakcie prvkov, aby sa vytvorila sada prvkov. Výsledná sada prvkov sa odošle do `porovnávača`, kde sa porovná so šablónou (šablónami) registrácie daného subjektu (získané zo systémového úložiska na základe identifikátora subjektu). Proces overovania vytvára **rozhodnutie o zhode/nezhode** na základe vopred daného prahu [12].

- **Identifikáciu**: V procese identifikácie si subjekt výslovne nenárokuje identitu a systém porovnáva sadu prvkov (extrahovaný zo zachytenej biometrickej vzorky) so šablónami všetkých (alebo podmnožiny) subjektov v systémovom úložisku. Výstupom je *zoznam kandidátov*, ktorý môže byť prázdny (ak sa nenájde žiadna zhoda) alebo môže obsahovať jeden (alebo viac) identifikátorov zodpovedajúcich šablón prihlášok. Pretože identifikácia vo veľkých databázach je výpočtovo nákladná, často sa na filtrovanie počtu registračných šablón, ktoré je potrebné porovnať so súborom vstupných funkcií, používa fáza predbežného výberu (filtrácie) [12].

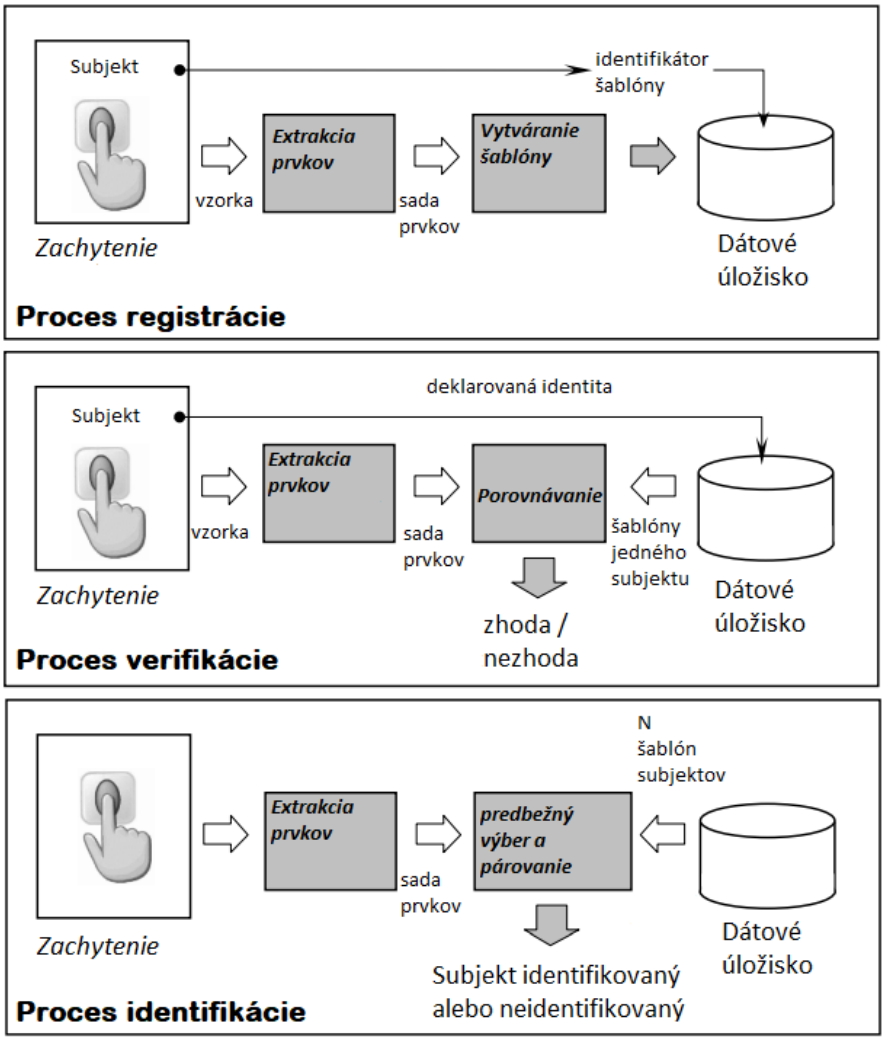
Plnohodnotný systém na biometrické overovanie je taký systém, ktorý dokáže nasnímať biometrický identifikátor, spracovať ho a uložiť do databázy v systéme. Následne ho použiť pri jednom z procesov verifikácie alebo identifikácie na porovnanie vzorky získanej z databázy a vzorky, ktorá je prezentovaná pri vstupe do systému.

Rozlišujeme dva základné typy biometrických systémov a to **verifikačný systém**, ktorý využíva procesy registrácie a overovania, zatiaľ čo druhý typ, **identifikačný systém** používa procesy registrácie a identifikácie. Tieto procesy sú bližšie znázornené na obrázku 2.2.

2.1.3 Prvky biometrického systému

Procesy registrácie, verifikácie a identifikácie, ktoré sú zapojené do rozpoznávania užívateľov využívajú nasledujúce systémové moduly:

- **Zachytávací modul**: digitálna reprezentácia biometrických charakteristík musí byť snímaná a zachytená. Biometrický snímač, ako je napríklad snímač odtlačkov prs-



Obr. 2.2: Príklady procesov registrácie, verifikácie a identifikácie v biometrickom systéme a moduly potrebné na ich realizáciu. (Obrázok prevzatý z [12].)

tov, je jednou z centrálnych častí modulu biometrického snímania. Zachytená digitálna reprezentácia biometrickej charakteristiky je často známa ako *vzorka*. Napríklad v prípade systému odtlačkov prstov je vzorkou nespracovaný digitálny obraz odtlačku prsta zachytený snímačom odtlačkov prstov. Modul na zachytávanie údajov môže obsahovať aj ďalšie komponenty (napr. klávesnicu a obrazovku) na zachytávanie iných (nebiometrických) údajov [12].

- **Modul pre extrakcia prvkov**: na uľahčenie prirovnávania alebo porovnávania sa surová digitálna reprezentácia (vzorka) zvyčajne ďalej spracováva pomocou extraktora prvkov ("*feature extraction*"), aby sa vytvorila kompaktná, ale expresívna reprezentácia, ktorá sa nazýva sada prvkov ("*feature set*") [12].

- **Modul na vytváranie šablón**: modul spracováva jednu alebo viacero sád prvkov do *šablóny*, ktorá bude uložená v nejakom trvalom úložisku. Šablóna prihlášky sa niekedy

označuje aj ako *referencia* a slúži pri identifikácií alebo autorizácií ako referenčný člen pri porovnávaní [12].

- **Predvýber a priraďovanie**: fáza predbežného výberu (alebo filtrovania) sa primárne používa v identifikačnom systéme, keď je počet zaregistrovaných šablón (osôb) veľký. Jeho úlohou je **zmenšiť efektívnu veľkosť databázy šablón** tak, aby sa vstupy museli zhodovať na relatívne malý počet šablón. Fáza priraďovania (alebo porovnávania) (známa aj ako priraďovač) berie ako vstupy sadu prvkov a prihlasovaciu šablónu a vypočítava podobnosť medzi nimi, známu aj ako *skóre podobnosti*. Skóre podobnosti sa porovnáva so systémovým prahom, aby sa urobilo konečné rozhodnutie. Ak je skóre zhody vyššie ako prah, osoba je uznaná, inak nie [12].

- **Modul dátového úložiska / Databázový modul**: slúži na ukladanie šablón a iných demografických informácií o užívateľovi. V závislosti od aplikácie môže byť šablóna uložená v interných alebo externých pamäťových zariadeniach alebo môže byť zaznamenaná na čipovej karte vydanej danej osobe [12].

Pri spojení týchto modulov vzniká **plnohodnotný systém na biometrické overovanie**, ktorý dokáže nasnímať biometrický identifikátor, spracovať ho do podoby, v ktorej môže byť uložený do systémovej databázy a následne ho použiť pri jednom z procesov na porovnanie vzorky získanej z databázy a vzorky, ktorá je prezentovaná pri vstupe do systému.

Pomocou týchto piatich modulov možno vykonať tri hlavné procesy, ukázané v sekcii 2.1.2 vyššie.

2.1.4 Slabiny biometrického systému

Ako každý systém iný systém aj biometrický systém je terčom útokov, ktorých cieľom je získanie neoprávneného prístupu do systému za účelom páchania škôd. Na biometrický systém sa dá útočiť fyzicky (útok na snímač alebo senzor) alebo elektronicky (vloženie falošných alebo upravených dát pri komunikácií medzi modulmi). Tieto útoky sa dajú rozdeliť na:

Útok na snímač, pri ktorom sa útočník môže snažiť upraviť alebo zachytiť *výstup* údajov zo senzora. Predtým zachytená vzorka sa môže prehrať alebo môže byť nahradená biometrickými údajmi iného jednotlivca (útočníka) pri registrácii [20]. Takisto môže byť zachytená vzorka získaná zo *vstupu* snímača za účelom zahalenia identity alebo predstierania identity iného jednotlivca.

Útok na databázu alebo šablónu registrácie: Útočník sa v tomto type útoku môže zamerať na údaje počas prenosu alebo v ukladaní biometrickým systémom. Môže upraviť biometrickú šablónu o jedincovi v databáze tak, aby obsahovala biometrické znaky útočníka [20]. Alebo pri registrácií útočník pozmení informácie v šablóne za informácie o biometrických znakoch útočníka. (Obidva typy útokov sú podobné v tom že sa zameriavajú na **nahradenie originálnych biometrických informácií** v šablóne za falošné informácie. Jediný rozdiel je v mieste, kde sa tieto informácie pozmenia).

Útok na porovnávací modul: Cieľom tohto útoku je pozmenenie prahu v porovnávacom module [20] tak, aby sa predstavená vzorka v každom prípade zhodovala so šablónou získanou z databázy a tak neoprávneným vstupom do systému (*predstieranie identity*).

Na útok pri komunikácií medzi modulmi je potreba mať prístup do vnútornej štruktúry systému a cieľom takéhoto útoku je vo väčšine prípadov vloženie falošných šablón s informáciami útočníka do systému. S falošnými informáciami v systéme sa pri predstavení

útočníkovej vzorky do porovnávacieho modulu systému vzorka vyhodnotí a útočníkovi bude pridelený vstup do systému.

Viac častý typ útoku je `fyzický útok na snímač` (prezentačný útok), ktorý predstaví pred snímač falzifikát za účelom vniknutia do systému.

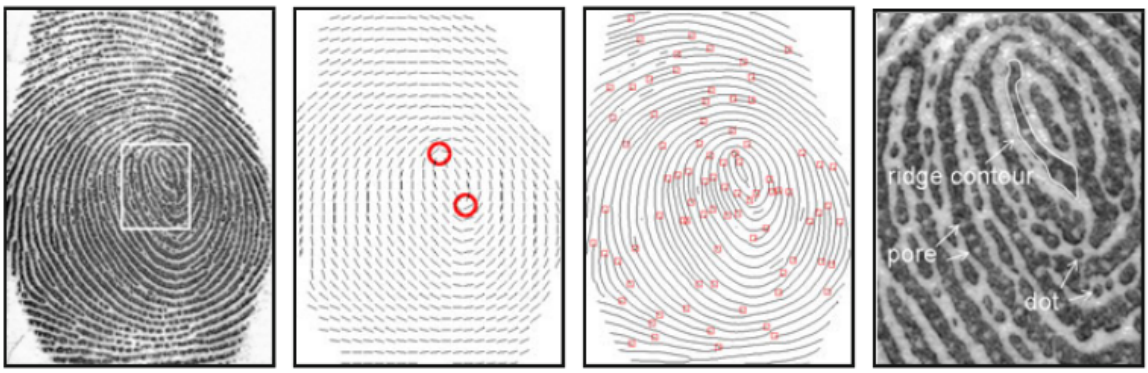
2.2 Odtlačok prsta

Používanie odtlačkov prstov ako biometrických údajov je najstarším spôsobom počítačom podporovanej osobnej identifikácie a zároveň najrozšírenejším spôsobom, ktorý sa dnes používa. Odtlačky prstov používajú policajné orgány od konca 18. storočia a spracovanie odtlačkov prstov počítačom je bežné od roku 1960 [33].

Používanie odtlačkov prstov vo forenznej vede je založené na niekoľkých základných princípoch. Po prvé, pravdepodobnosť, že sa nájdu dvaja ľudia s identickými odtlačkami. Bolo vypočítané, že pravdepodobnosť nájdenia identických výtlačkov je **1 ku 64 miliónom**. Druhým princípom je, že odtlačky prstov jednotlivca sa časom nemenia. Vzor ryhovania na končekoch prstov, dlaniach a chodidlách človeka pri narodení zostáva nezmenený až do smrti. Nakoniec existuje dostatok podobností vo vzoroch hrebeňov na ľudských prstoch, ktoré možno klasifikovať [23].

2.2.1 Analógia odtlačku prsta

Informácie, ktoré vieme získať z odtlačku prsta možno charakterizovať na troch rôznych úrovniach, od takzvaných *hrubých* po takzvané *jemné*. Za ideálnych podmienok je možné odvodiť hrubé rysy z jemnejších úrovní znázornenia odtlačkov prstov.



Obr. 2.3: Typy reprezentácie odtlačku prsta. (a) Šedo-tónový snímok, (b) Vlastnosti prvej úrovne (mapa orientácie hrebeňa), (c) Vlastnosti druhej úrovne (markanty), (d) Vlastnosti tretej úrovne (póry). (Obrázok prevzatý z [19].)

Rôzne typy detailov sa dajú zachytiť na rôznych úrovniach. Vlastnosti, ktoré je možné získať z detailov danej úrovne sa rozdeľujú ako vlastnosti prvej úrovne, vlastnosti druhej úrovne a vlastnosti tretej úrovne.

Pri **vlastnostiach prvej úrovne** alebo najhrubšej úrovne je odtlačok prsta reprezentovaný ako mapa orientácie hrebeňa ("ridge orientation map") (obrázok 2.3b), ktorá

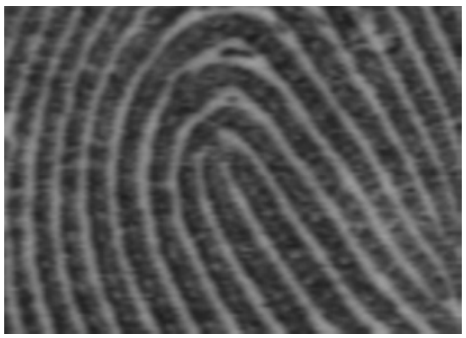
zaznamenáva *lokálnu orientáciu* hrebeňa na každom mieste odtlačku prsta, a *mapu frekvencie* hrebeňa ("ridge frequency map"), ktorá zaznamenáva frekvenciu lokálneho hrebeňa v každom mieste odtlačku prsta.

Odtlačok prsta sa často označuje ako `orientovaný vzor textúry` ("oriented texture pattern"), pretože jeho globálny tvar a štruktúru možno definovať orientáciou a frekvenciou jeho hrebeňov. V detaile prvej úrovne sa pozoruje iba hrebeňový tok a frekvencia hrebeňa, teda presné umiestnenie a rozmerové detaily hrebeňov sa ignorujú [19].

Lokálna orientácia hrebeňa v pixeli (x, y) predstavuje *tangenciálny smer* hrebeňových línií prechádzajúcich cez pixel (x, y). Orientácia hrebeňa je definovaná v rozsahu $< 0, \pi)$. Na mapu orientácie hrebeňa sa teda možno pozerať ako na vektorové pole jednotkovej dĺžky, ktorého smer je definovaný medzi 0 a π. Orientácia hrebeňa v pixeli je znázornená na obrázku 2.3b. Frekvencia lokálnych hrebeňov v (x, y) je priemerný počet hrebeňov na jednotku dĺžky pozdĺž úsečky so stredom v (x, y) kolmej na miestnu orientáciu hrebeňa. Vo všeobecnosti sa informácie o orientácii hrebeňa považujú za dôležitejšie ako informácie o frekvencii hrebeňa na účely porovnávania odtlačkov prstov a klasifikácie [19].

Mapa orientácie hrebeňa zvyčajne obsahuje miesta, kde sa orientácie hrebeňov náhle menia. Takéto miesta sa nazývajú **singulárne body**.

Existujú dva základné typy singulárnych bodov – *slučka (jadro)* a *delta*, ktoré sú vizuálne charakteristické. Singularita typu *slučky*, nazývaná aj **jadro**, sa vzťahuje na oblasť, kde súbor hrebeňov vstupuje z jedného smeru a vystupuje v rovnakom smere (obrázok 2.4). Slučku v odtlačku prsta možno použiť ako orientačný bod na zarovnanie odtlačku prsta. Vo všeobecnosti bod jadra zodpovedá najsevernejšiemu singulárnemu bodu typu slučky v odtlačku prsta. Singularita typu **delta** označuje miestnu oblasť, kde sa zdá, že sa stretávajú tri hrebeňové systémy (obrázok 2.5) [31].

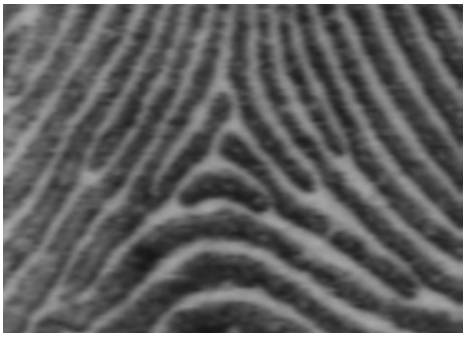


Obr. 2.4: Singularita typu **jadro**. (Obrázok prevzatý z [19].)

Vlastnosti druhej úrovne alebo strednej úrovne predstavujú odtlačok prsta znázornený ako *obrázok kostry hrebeňa* ("ridge skeleton image"), na ktorom je každý hrebeň široký iba jeden pixel (po prevedení skeletonizácie) (obrázok 2.3c). Na tejto úrovni sa zaznamenávajú presné polohy hrebeňov. Miesta, kde sa hrebeň objavuje, končí, rozdeľuje alebo spája s iným hrebeňom, sa nazývajú charakteristiky alebo *markanty* hrebeňa ("minutiae") [19, 12].

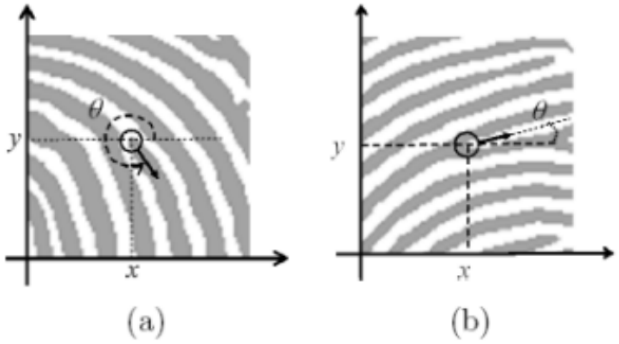
Každý markant možno charakterizovať troma vlastnosťami ktorými je **umiestnenie na obrázku, smer a typ**.

Umiestnením markantu na snímke odtlačku prstu rozumieme pozíciu, kde sa daný markant vyskytuje. Táto pozícia sa dá zaznamenať ako pozícia pixela (x, y) relatívna ku snímku (obrázok 2.6). Okrem umiestnenia má markant vo všeobecnosti dve ďalšie vlastnosti: *smer* a *typ*.



Obr. 2.5: Singularita typu **delta**. (Obrázok prevzatý z [19].)

Smer markantov je definovaný ako smer hrebeňa v mieste markantu (obrázok 2.6)



Obr. 2.6: (a) Markant na konci hrebeňa. (b) Markant rozvetvenia hrebeňa. (x, y) sú súradnice markantov, θ je orientácia markantu. (Obrázok prevzatý z [5].)

Typ markantu označuje, aká vlastnosť v hrebeni prestavuje markant.
Existujú dva základné typy markantov:

1. `Zakončenie` (alebo ukončenie)
2. `Rozdvojenie`

Ďalšie menej používané typy sú napríklad:

1. `Zlúčenie/rozdelenie (bifurkáciá)`
2. `Výbežok`
3. `Ostrovček`

Tieto typy markantov sú znázornené na obrázku 2.7.

Podrobnosti druhej úrovne odtlačku prsta možno ľahko pozorovať na snímkach získaných v rozlíšení 500 ppi. Počty markantov nájdených v odtlačku prsta sa veľmi líšia v závislosti od spôsobu získavania a iných faktorov [19].

Súbor markantov ("minutiae set"), ktorý pozostáva zo všetkých markantov v odtlačku prsta, je abstraktným znázornením kostry markantov v tom zmysle, že súbor markantov zachytáva väčšinu rozlišujúcich informácií na druhej úrovni a kostry markantov možno približne odvodiť len zo samotných informácií o markantoch [19]. Reprezentácie založené na

Obr. 2.7: Typy markantov (zakončenie, zlúčenie/rozdelenie (bifurkáciá),výbežok a ostrovček, prechod). (Obrázok prevzatý z [4].)

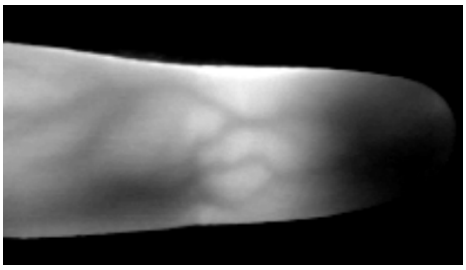
markantoch sú sa vo veľkej miere používané v biometrických systémoch na rozpoznávanie odtlačkov prstov, a to najmä z týchto dôvodov:

1. markanty zachytávajú veľkú časť diskriminačných alebo individuálnych informácií v odtlačkoch prstov [19].
2. reprezentácie založené na markantoch sa dajú efektívne ukladať [19].
3. extrakcia markantov je primerane robustná k rôznym zdrojom degradácie [19].

Vlastnosti tretej úrovne alebo veľmi jemnej úrovne ukazujú detaily vo vnútri hrebeňa. Medzi tieto detaily patria šírka, tvar, zakrivenie, okrajové obrysy hrebeňov, ako aj ďalšie trvalé detaily, ako sú bodky a začínajúce hrebene. Jedným z najdôležitejších detailov na tretej úrovni sú póry na potenie prstov ("sweat pores") (obrázok 2.3d), ktorých polohy a tvary sa považujú za veľmi výrazné a diskriminačné. Extrahovanie veľmi jemných detailov vrátane pórov je však možné len na obrázkoch odtlačkov prstov s vysokým rozlíšením (napr. 1 000 dpi) a preto tento druh zobrazenia nie je praktický pre neforenzné aplikácie [11].

2.3 Krvné riečisko

Kardiovaskulárny systém (obrázok 2.8) možno nájsť u ľudí a zvierat a jeho základnou funkciou je udržiavať homeostázu – konštantný súbor podmienok v bunkách [15]. V kardiovaskulárnom systéme existujú dva kruhy: *pľúcny a systémový*. Prvý spomínaný kruh je zo srdca do pľúc, kde sa znova okysličuje krv ochudobnená o kyslík. V druhom prípade je nasýtená krv prenášaná zo srdca sieťou krvných ciev do všetkých častí tela a späť do srdca [15]. Existujú tri hlavné typy krvných ciev: **tepny**, **kapiláry** a **žily**. Tepny vedú kyslíkom

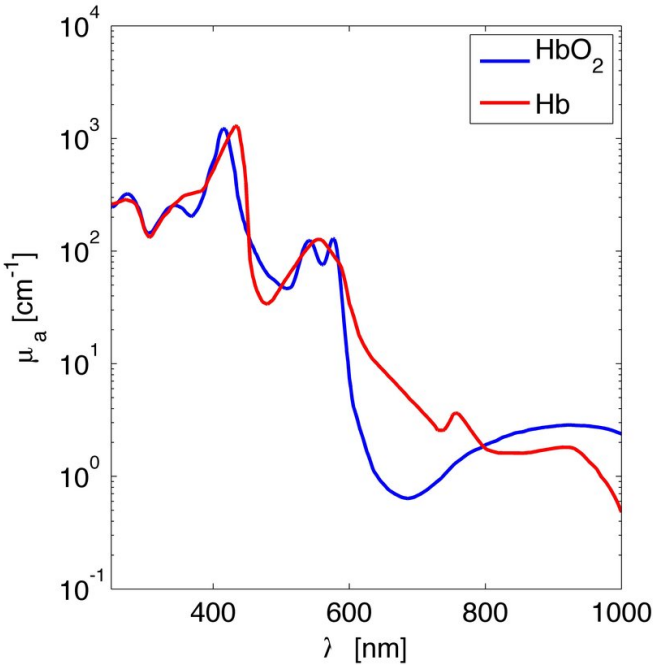


Obr. 2.8: Snímka žilového riečiska prsta získaná s pomocou NIR. (Obrázok prevzatý z [28].)

nasýtenú krv zo srdca. Kapiláry umožňujú výmenu látok a tekutín medzi krvou a tkanivom a nakoniec žily vedú krv z kapilár späť do srdca. Charakter týchto ciev sa líši. Kým steny

tepien sú veľmi hrubé a pevné (aby zvládli vysoký tlak krvi), steny žíl sú tenšie, pružnejšie a priemer žíl je väčší. Kapiláry sú najmenšie z ciev s vnútorným priemerom okolo 8 µm [15]. Priemer žíl aj tepien sa úmerne zmenšuje so vzdialenosťou od srdca. Najvzdialenejšie krvné cievy sa nachádzajú priamo pod epidermou (pokožkou) pričom hlavné kmene sú umiestnené hlbšie v podkoží. Vo všeobecnosti sú žily umiestnené bližšie ku koži v porovnaní s tepnami.

Krv pozostáva z tekutej plazmy, v ktorej sú suspendované tri druhy krviniek [15] – *erytrocyty* (99 %), *leukocyty* (menej ako 1 %) a *trombocyty* (menej ako 1 %). Erytrocyty pozostávajú z proteínu hemoglobínu obsahujúceho železo, ktorý dokáže viazať kyslík. V dôsledku prítomnosti okysličeného hemoglobínu (HbO2) v krvi nasýtenej kyslíkom, prenášanej tepnami, má krv jasne červenú farbu a krv ochudobnená o kyslík v žilách má tmavočervenú alebo fialovú farbu v dôsledku prítomnosti odkysličeného hemoglobínu (Hb).



Obr. 2.9: Absorpčné koeficienty pre okysličený hemoglobín (HbO_2) a neokyslyčený hemoglobín (Hb) ako funkcia vlnovej dĺžky. (Obrázok prevzatý z [37].)

2.3.1 Snímanie krvného riečiska

Existuje niekoľko spôsobov, ako získať *obraz ľudských ciev*, napríklad pomocou röntgenu, magnetickej rezonancie, ultrazvuku, ďalekého infračerveného svetla (FIR), blízkeho infračerveného svetla (NIR) alebo termálneho prístupu [15]. Prístup blízkeho infračerveného svetla sa v biometrii používa najčastejšie kvôli jeho kompromisu medzi cenou, požiadavkami na napájanie, veľkosťou snímača a kvalitou výsledného obrazu. Dva typy hemoglobínov (Hb, HbO2) majú rôzne absorpčné spektrá, ako je možné vidieť na obrázku 2.9. Experimenty dokázali, že priepustnosť ľudského tkaniva je vysoká pre elektromagnetické žiarenie v rozsahu od 600 nm do 1 300 nm [16], tento rozsah sa často nazýva optické okno. Najmä v rozsahu medzi 750-950 nm [41] môže žiarenie preniknúť dostatočne hlboko do kože, aby sa dostalo až k povrchovým tepnám a žilám, a následne sa absorbuje v cievach v dôsledku vyššieho

absorpčného koeficientu krvi. Tento efekt dokáže zachytiť kamera – škvrny na snímke, kde sa nachádzajú cievy, sú tmavšie.

Existujú dva hlavné spôsoby získania obrazu krvných ciev prsta pomocou blízkeho infračerveného (NIR) prístupu – **odraz** a **prienik**.

2.3.2 NIR

Štandardnou praxou pri získavaní snímkov žíl prstov je snímanie pomocou blízkej infračervenej spektroskopie. Keď je prst priložený na blízke infračervené svetelné lúče s vlnovou dĺžkou 760 nm, zachytia sa vzory žíl prsta v podkožnom tkanive prsta, pretože odkysličený hemoglobín v žile absorbuje svetelné lúče [41]. Keďže sa väčšina hemoglobínu v ľudskom tele nachádza v červených krvinkách, ktoré prúdia v krvných cievach, obrazce siete krvných ciev možno pomocou infračervených zobrazovacích systémov vidieť ako tmavú oblasť. `Vzorce cievnej siete` ("Vascular network patterns") sú vo vnútri prsta jednotlivca vizualizované využitím tejto optickej charakteristiky hemoglobínu. Práve kvôli tomuto môžu byť sieťové vzory použité ako biometrická modalita vhodnými zobrazovacími technológiami. Keďže priemery artérií sú také malé ako približne 1/3 priemerov cielených žíl na prste, je rozumné predpokladať, že väčšina zobrazených krvných ciev sú žily. To je dôvod, prečo je veľa vaskulárnych biometrických technológií známych ako „žilová" biometria, hoci artérie a žily na prste sú rovnako vizualizované infračerveným svetlom a v praxi sa k ním dá správať rovnakým spôsobom [16].

2.3.3 Prienik a odraz svetla

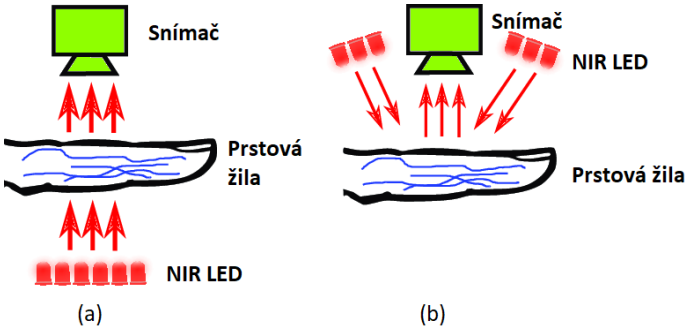
Ako bolo naznačené v časti 2.3.1, dva hlavné prístupy k vizualizácii cievnych vzorcov za pomoci NIR na biometrické použitie. Konkrétne metóda `prieniku svetla` a metóda `odrazu svetla`, ako je možné vidieť na obrázku 2.10.

Metóda prieniku svetla

Metóda prieniku svetla využíva infračervené svetlo prenášané cez cieľový objekt, zatiaľ čo metóda odrazu svetla využíva svetlo odrazené cieľom. Pri metóde prieniku svetla je potrebné použiť intenzívnejšie NIR svetlo, aby bola snímaná časť dostatočne. To ale znamená použitie či už viacerých NIR LED diód, alebo použitie výkonnejších NIR diód. Každopádne je výsledkom mohutnejší snímač a vyššia spotreba na napájanie oproti metóde odrazu. Tieto komplikácia majú avšak jednu veľkú výhodu a to zobrazenie viacerých detailov (žíl), ktoré sa môžu nachádzať vo vnútri prsta a nielen na povrchu a ktoré môžu dosahovať menších priemerov.

Metóda odrazu svetla

Metóda odrazu svetla nie je zvyčajne prvou voľbou, pokiaľ to nie je nevyhnutné, pretože je ťažké spracovať takéto obrázky, ktoré môžu obsahovať nasýtené (preexponované) oblasti alebo textúru na povrchu kože. Kontrast snímok zachytených prenikavým svetlom je vo všeobecnosti vyšší ako kontrast zachytených odrazením. Obrazy s vysokým kontrastom vedú k vysokej presnosti autentifikácie, pretože z obrazu s vysokým odstupom signálu od šumu možno extrahovať viac informácií na rozlíšenie vzorov [16]. Prsty patria medzi časti ľudského tela, ktoré možno ľahko prezentovať autentifikačnému zariadeniu a z ktorých možno pomocou „metódy odrazu svetla" zachytiť jasné obrazy vzorov. Preto sa biometria žily na prste považuje za jednu z najspoľahlivejších a najstabilnejších biometrických metód. Hoci biometria žily na prste je jednou z najnovších biometrických technológií, jej vysoká



Obr. 2.10: Príklad prieniku (a) a odrazu (b) NIR svetla použitom pri snímaní prstových žíl. (Obrázok prevzatý z [22].)

využiteľnosť ako základ pre osobnú autentifikáciu bola uznaná z medicínskeho hľadiska a už preukázala technickú aj štatistickú realizovateľnosť [16].

2.4 Zariadenie na snímanie prsta

Na účely detekcie prezentačného útoku ako aj k použitiu na overenie identity musí kamera dokázať urobiť snímku žilovej štruktúry ruky, poprípade prstov. V závislosti od požiadaviek musí byť kamera schopná sprostredkovať obraz v reálnom čase. Na tieto účely sa využívajú CCD ("Charged Coupled Device") alebo CMOS ("Complementary Metal Oxide Semiconductor") kamery [21].

Prerekvizitou kamery musí byť vysoká citlivosť infračerveného svetla. Aby bolo nasvietenie infračerveného svetla možné a použiteľné (snímaný objekt nemôže byť preexponovaný), je potreba zamedziť vniku nechceného svetla na snímač kamery. Na toto opatrenie je možnosť dovybaviť kameru patričným filtrom, poprípade zaobstarať kameru so vstavaným filtrom. Pridaním filtra, ktorý prepúšťa iba infračervené svetlo na určitej vlnovej dĺžke, sa eliminuje viditeľné svetlo a tým sa zvyšuje kvalita získanej snímky alebo prenášaného obrazu. Cena hardvérového zariadenia sa tým zároveň razantne nezvyšuje [21].

V závislosti od typu aplikácie je možné meniť rozsah prepúšťaného infračerveného svetla pomocou príslušných filtrov alebo zmenou intenzity podsvietenia NIR LED diódami. Zodpovedajúce filtre umožňujú používať svetlo s vyššou alebo nižšou vlnovou dĺžkou, čím sa zvyšuje flexibilita systému a rozširuje sa možné využitia tohto systému na rôzne aplikácie [22].

Snímka z kamery avšak ani po použití filtra nie je dostatočne kvalitná na okamžitú extrakciu. Je za potrebu ďalej zvýrazniť vzory, ktoré budú ďalej použité pri extrakcii, ako je popísané v časti 3.2.

Obrazové snímače CCD aj CMOS sa vyrábajú z rovnakých základných materiálov (kremík, oxid kremičitý, polysilikón, ...). Procesy CCD a zobrazovacie zariadenia tohto typu sú však už viac ako 3 desaťročia optimalizované špeciálne pre zobrazovacie aplikácie. Dnes prezentujú vynikajúci výkon a kvalitu obrazu vďaka extrémne nízkemu šumu, nízkemu tmavému prúdu, vysokej kvantovej účinnosti a faktoru plnenia. Hlavný rozdiel spočíva v architektúre a flexibilite dizajnu snímačov CMOS, najmä pre aplikácie vyžadujúce špeciálne spracovanie signálu alebo obrazu, ktoré možno integrovať do čipu, čo vedie k novej rodine inteligentných a kompaktných snímačov [7].

CCD

CCD obsahuje fotomiesta (buď fotodiódy alebo fotobrány) typicky usporiadané v 2D matici riadkov a stĺpcov. Po expozícii je každý nábojový paket v matrici fyzicky transportovaný do spoločnej výstupnej štruktúry, ktorá premieňa náboj na napätie. Architektúra CCD snímačov tak vedie k sekvenčnému čítaniu obrazových dát s vysokou rovnomernosťou. Často sú možné ďalšie funkcie, ako napríklad združovanie pixelov, ktoré ponúkajú nižšie priestorové rozlíšenie pri vyššej snímkovej frekvencii alebo s vyššou citlivosťou. Napriek tomu väčšina CCD stále potrebuje hodinové signály s relatívne veľkými amplitúdami (5 – 10 voltov) a dobre definovanými tvarmi, ktoré sú rozhodujúce pre ich úspešnú prevádzku a vyžadujú si špecializované hodinové ovládače. Často sú potrebné viaceré napájacie hladiny a rôzne predpätia pri neštandardných hodnotách, čo zvyšuje zložitosť systému a zvyšuje spotrebu energie, keďže tieto zmeny sú stratové. Nedávne CCD snímače dosahujú lepšiu spotrebu s nižším taktovacím napätím (2,5 V) a spotrebou energie (146 mW pre 1,3 megapixelový snímač @ 15 snímok/s) [13].

CMOS

`Tradičné „pasívne" obrazové snímače CMOS` obsahujú v každom jednotlivom pixeli iba prvok na snímanie fotografií (zvyčajne fotodiódu) a prepínací MOSFET, pričom signál je detegovaný a spracovaný výstupným zosilňovačom umiestnenom v každom stĺpci alebo jediným prvkom umiestneným pred výstupom pre kompletné zobrazenie zariadenia. Tieto MOS-pole senzory ponúkajú výhodu náhodného prístupu k jednotlivým pixelom, čo umožňuje definovanie podokien alebo "Regions Of Interest" (ROI), ktoré sú veľmi užitočné napríklad pre strojové videnie. Šumový výkon a citlivosť sú však nižšie ako u CCD snímačov, hlavne kvôli veľkým kapacitám na vstupe výstupného zosilňovača [7].

V `aktívnych senzoroch` ("Active Pixel Sensors" (APS)) je prvý zosilňovací stupeň implementovaný v každom pixeli, čím sa zlepšuje (znižuje) šum a tým aj dosiahnuteľný dynamický rozsah [39]. Aj z hľadiska priestorového rozlíšenia a citlivosti (okrem najnižších úrovní osvetlenia alebo vyšších teplôt) CMOS APS dnes predstavujú výkon blízky alebo lepší ako ich ekvivalentný CCD.

Kapitola 3

Prezentačný útok na biometrické zariadenie

Prezentačné útoky sú definované v rámci normy ISO/IEC 30107 o detekcii prezentačných útokov na biometrické zariadenie [1] ako „*prezentácia do subsystému zachytávania biometrických údajov s cieľom zasahovať do prevádzky biometrického systému*“. Útočník môže mať za cieľ vydávať sa za niekoho iného (teda užívateľa, ktorý je v systéme registrovaný a útočník sa snaží o prístup do systému vydávajúc sa za daného užívateľa) alebo sa vyhnúť tomu, aby bol rozpoznaný kvôli zapísaniu útočníka na čiernu listinu (za motívom skrytia jeho vlastnej identity).

V nasledujúcom texte sú uvedené hlavné definície prezentované v rámci normy ISO/IEC 30107 — časť 3: testovanie a hlásenie, ktoré sa budú v rámci práce ďalej používať:

- **Prezentácia v dobrej viere (Bona fide presentation)**: „interakcia subjektu biometrického snímania a subsystému zachytávania biometrických údajov spôsobom, ktorý zamýšľa politika biometrického systému“. Teda normálna alebo pravá prezentácia [2].
- **Prezentačný útok**: „prezentácia do subsystému zachytávania biometrických údajov s cieľom zasahovať do prevádzky biometrického systému“. To znamená, že ide o útok vykonaný na zachytávacie zariadenie s cieľom zakryť identitu alebo sa vydávať za niekoho iného [2].
- **Nástroj na prezentačný útok (Presentation Attack Instrument) – PAI**: „biometrická charakteristika alebo objekt použitý pri prezentačnom útoku“. Napríklad silikónová 3D maska alebo maska na prekrytie odtlačkov prstov [2].
- **Druhy PAI**: „trieda prezentačných útočných nástrojov vytvorených pomocou bežnej výrobnej metódy a založených na rôznych biometrických charakteristikách“ [2].

Na vyhodnotenie zraniteľnosti biometrického systému voči prezentačnému útoku budú v práci použité nasledovné metriky:

- **Miera zhody prezentácie útokov podvodníkov (Impostor Attack Presentation Match Rate) – IAPMR**: „podiel prezentačných útokov podvodníkov s použitím rovnakého druhu PAI, v ktorom sa zhoduje cieľová referencia“ [2].

- **Miera chybovosti klasifikácie prezentácií útokov (Attack Presentation Classification Error Rate) – APCER**: „podiel prezentačných útokov s použitím rovnakého druhu PAI nesprávne klasifikovaných ako prezentácie v dobrej viere (bona fide) v konkrétnom scenári“ [2].
- **Miera chybovosti klasifikácie prezentácie v Bona Fide (Bona Fide Presentation Classification Error Rate) – BPCER**: „podiel prezentácií v dobrej viere nesprávne klasifikovaných ako prezentačné útoky v špecifickom scenári“ [2].
- **Priemerná miera chybovosti klasifikácie (Average Classification Error Rate) – ACER**: sa vypočíta pomocou rovnice 3.1 a slúži na meranie priemernej chyby biometrického systému voči prezentačným útokom [32].

$$ACER = \frac{APCER + BPCER}{2} \tag{3.1}$$

3.1 Materiály pri prezentačných útokoch

Pri predložení objektu pred snímač je potreba zistiť, či sa jedná o prezentáciu v dobrej viere alebo o prezentačný útok. Pri pokuse o predloženie falošného vzorku na snímač sa môže jednať o viacero rôznych materiálov v rôznych prevedeniach. Na overenie metódy detekcie prezentačného útoku boli použité rôzne materiály v rôznych kombináciách.

PAI (Presentation Attack Instrument) možno rozdeliť do troch kategórií, a to: **(2D výtlačky**, **celé prsty** a **prekrytia**, pričom 2D výtlačky možno použiť aj ako prekrytie počas prezentácie [25].

Na vytvorenie datasetu boli použité vyššie spomínané druhy PAI v rôznych kombináciách. Ako je možné vidieť na obrázku 3.1, na vytvorenie datasetu bolo použitých dokopy šesť druhov umelých rúk, ktoré boli vytvorené z materiálov ako je guma, sádra, plastelína,...

Na dané ruky ako aj na živé ruky boli pri snímaní prikladané rôzne materiály, ktoré napodobňovali prstovú žilu alebo prekrytie na špičku prsta. Tieto materiály sú ukázané na obrázku 3.2.

Obr. 3.1: Príklad falzifikátov použitých na snímanie prstov použitých pri prezentačnom útoku.

3.2 Metódy na detekciu prezentačného útoku na snímku krvného riečiska

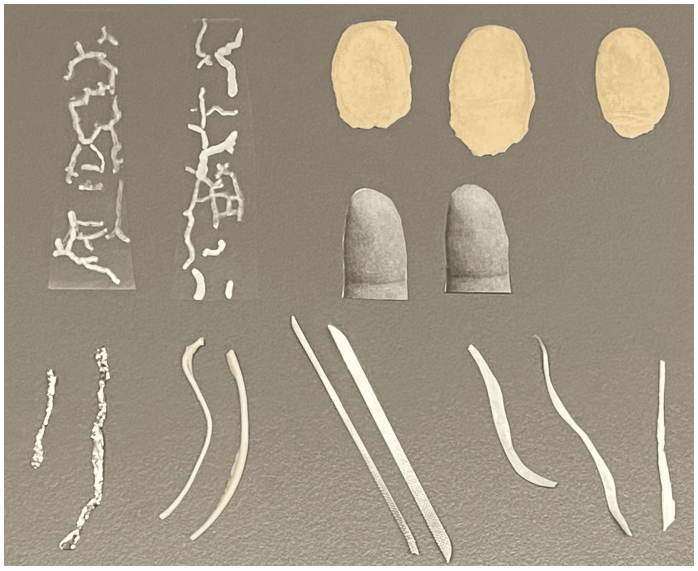
V tejto časti sú informácie prevzaté z [40, 25, 32]. Detekcia prezentačného útoku sa v rámci implementácie delí na tri základné moduly a to `predspracovanie, extrakcia prvkov a rozhodovanie`.

Ako bolo naznačené v kapitole 2.4, získaný snímok priamo z kamery sa nedá okamžite použiť na extrakciu, keďže takéto snímky obsahujú veľa informácií, ktoré sú nepresné. Takéto snímky majú nežiadúce následky na extrakciu prvkov a celkový proces vyhodnocovania prezentačného útoku. Preto pred extrakciou je za potrebu previesť úpravy, ktoré by mali zaistiť kvalitnejší snímok a tým pádom aj kvalitnejšie a presnejšie spracovanie spoločne s vyhodnocovaním.

Tieto jednotlivé kroky budú presnejšie popísané v nasledujúcich sekciách.

Predspracovanie: Obraz žily na snímku je spracovaný na vylepšenie vzorcov žíl a odstránenie akéhokoľvek šumu alebo artefaktov. To zabraňuje skresleniu vzorov žíl alebo zamenenie si rôzneho artefaktu za žilu. Predspracovanie je možné vykonať pomocou techník, ako sú napríklad:

`Vylepšenie obrazu`, kde sa zvýšením kontrastu a jasu obrazu zviditeľnia žilové vzory. To sa dá urobiť pomocou techník, ako je vyrovnávanie histogramu, Adaptívna ekvalizácia histogramu alebo roztahovanie kontrastu.



Obr. 3.2: Príklad materiálov použitých ako falzifikát žíl, ktoré boli použité pri snímaní dátovej sady predstavujúcej prezentačný útok. V poradí zľava doprava – strieborná fixka, silikónové prekrytie, výtlačok prekrytia špičky prsta, strieborná fólia (alobal), nitrilový ústrižok, strieborná fólia, biely papier.

`Odšumovanie obrazu` slúži na elimináciu akéhokoľvek šumu alebo artefaktov z obrazu, za účelom zlepšenia kvality vzorcov žíl. To sa dá zaistiť pomocou techník, ako je napríklad mediánové filtrovanie, Gaussovo filtrovanie alebo filtrovanie nemiestnými prostriedkami.

`Segmentácia snímky` znamená izoláciu oblasti záujmu (ROI ("Region Of Interest")), ktorá obsahuje vzory žíl na prstoch. Implementovať sa to dá pomocou techník prahovania, ako je Otsu prahovanie, adaptívne prahovanie alebo viacúrovňové prahovanie. Výsledkom týchto metód je takzvaná "maska", ktorá rozdeľuje okolie obrázku od vzoru prstu, ktorý je spracovávaný. Následne existujú metódy na ohraničenie obrázku prsta za použitia masky získanej z prahovania. Výsledkom týchto metód sú obdĺžniky, ktoré sa nazývajú **ohraničujúci box ("bounding box")**. Delia sa na *vonkajší* a *vnútorný*. Slúžia na získanie len použiteľnej časti z ROI, keďže maska môže nadobúdať nekonvenčných tvarov. Po aplikovaní ohraničujúceho boxu je výstupné ROI časť snímku v tvare štvorca alebo obdĺžnika a tým sa zjednodušuje spracovanie a možnosť opakovaného použitia pri rôznych snímkoch.

`Normalizácia obrazu`: Normalizácia obrazu na štandardnú veľkosť a orientáciu. Dá sa dosiahnuť zmenou veľkosti obrázka a/alebo jeho otočením tak, aby boli či už jednotlivé prsty alebo vzory žíl na prstoch zarovnané konzistentným spôsobom.

Extrakcia prvkov: Vylepšený obraz po predspracovaní prechádza algoritmom extrakcie prvkov, aby sa extrahovali relevantné informácie o vzorcoch žíl. To môže zahŕňať:

- `Detekciu hrán`: Na extrakciu hrán vzorcov žíl použitím techniky detekcie hrán, ako je detekcia hrán Canny alebo detekcia hrán Sobel. To môže pomôcť identifikovať umiestnenie a tvar žíl.
- `Extrakciu vzorcov`: Na extrakciu vzorcov žíl sa používajú rôzne metódy použitím techniky extrakcie markantov, ako je detekcia konca hrebeňa alebo bifurkácie. Medzi markantné body patria body, kde žila končí, body, kde sa žila rozdeľuje a body, kde sa mení smer žily.

- `Skeletonizáciu`: Použitie techniky skeletonizácie, ako je stenčenie alebo transformácia mediálnej osi, aby sme extrahovali stredovú líniu vzorcov žíl. To môže pomôcť identifikovať jedinečné vlastnosti žíl, ako je ich šírka, zakrivenie a vzory vetvenia.

Rozhodovanie: Na základe rozdielu extrahovaných prvkov vstupného obrázku od pravých obrázkov v databáze sa rozhodne, či ide o skutočný obrázok žily na prste alebo o prezentačný útok. Toto rozhodnutie je možné urobiť pomocou prahovej hodnoty alebo trénovaním klasifikátora, ako sú napríklad podporný vektorový stroj alebo neurónová sieť, ktoré urobia rozhodnutie.

3.3 Detekcia oblasti záujmu

Ako bolo spomínané vyššie, detekcia oblasti záujmu (ďalej ROI) slúži na rozdelenie okolia snímku od vzoru prstu, ktorý bude spracovávaný. Výstupom tejto detekcie je binárna maska. Na snímky rúk, ktoré budú ďalej spracovávané budú použité rôzne techniky prahovania, no techniky, ktorá sa na túto aplikáciu osvedčili najviac boli binárne a OTSU prahovanie ("OTSU tresholding").

Klasické prahovanie spočíva vo veľmi jednoduchom porovnávaní. Ak je hodnota pixelu menšia ako prahová hodnota, hodnota daného pixelu sa nastaví na 0, v opačnom prípade sa nastaví na maximálnu hodnotu. Prahová hodnota je získaná ako parameter funkcie, ktorá je použitá na prevedenie prahovania.

3.3.1 OTSU prahovanie

Otsuova metóda prahovania zodpovedá lineárnym diskriminačným kritériám, ktoré predpokladajú, že obrázok pozostáva iba z objektu (popredia) a pozadia, pričom heterogenita a rôznorodosť pozadia sa ignoruje [34]. Otsu nastavil prah tak, aby sa pokúsil minimalizovať prekrývanie tried distribúcií [34]. Vzhľadom na túto definíciu Otsuova metóda segmentuje obraz na dve oblasti, svetlú a tmavú oblasť, respektívne T0 a T1, kde oblasť T0 je množina úrovne intenzity od 0 do t alebo v množine označenia $T0 = 0, 1, \ldots, t$ a oblasť $T1 = t, t+1, \ldots, l-1, l$ kde t je prahová hodnota, l je maximálna úroveň šedej snímky (napríklad 255). T0 a T1 môžu byť priradené k popredíu a pozadiu alebo naopak, keďže nie vždy je objekt v svetlejšej časti obrázku.

Otsuova metóda prahovania skenuje všetky možné prahové hodnoty a vypočíta minimálnu hodnotu pre úrovne pixelov na každej strane prahu. Cieľom je nájsť prahovú hodnotu s minimálnou entropiou pre súčet popredia a pozadia. Otsuova metóda určuje prahovú hodnotu na základe štatistických informácií o obrázku, kde pre zvolenú prahovú hodnotu t možno vypočítať rozptyl zhlukov $T0$ a $T1$. Optimálna prahová hodnota sa vypočíta tak, že sa minimalizuje súčet vážených skupinových rozptylov, kde váhy sú pravdepodobnosťou príslušných skupín [42].

Dané: $P(i)$ ako pravdepodobnosti histogramu pozorovanej hodnoty šedej, kde i patrí do intervalu $< 1, l >$.

$$P(i) \quad = \quad \frac{number\{(r,c)|image(r,c) = i\}}{(R,C)} \tag{3.2}$$

Kde r, c je index pre riadok a stĺpec obrázka, R a C je počet riadkov a stĺpcov obrázka.

$\omega_b(t)$, $\mu_b(t)$ *a* $\sigma_b^2(t)$ ako hmotnosť, priemer a rozptyl triedy $T0$ s hodnotou intenzity od 0 do t.

$\omega_f(t)$, $\mu_f(t)$ a $\sigma_f^2(t)$ ako hmotnosť, priemer a rozptyl triedy $T1$ s hodnotou intenzity od $t+1$ do l.

σ_ω^2 ako vážená suma variácie tried.

Pomocou týchto hodnôt je získaná prahová hodnota $t*$ predstavujúca `hodnotu s minimálnym rozptylom v rámci triedy`. Tá sa definuje ako:

$$\sigma_\omega^2 = \omega_b(t) * \sigma_b^2(t) + \omega_f(t) * \sigma_f^2(t) \tag{3.3}$$

kde

$$\omega_b(t) = \sum_{i=1}^{t} P(i)$$

$$\omega_f(t) = \sum_{i=t+1}^{l} P(i)$$

$$\mu_b(t) = \frac{\sum_{i=1}^{t} P(i)}{\omega_b(t)}$$

$$\mu_f(t) = \frac{\sum_{i=t+1}^{l} P(i)}{\omega_f(t)}$$

$$\sigma_b^2(t) = \frac{\sum_{i=1}^{t} (i - \mu_b(t))^2 * P(i)}{\omega_b(t)}$$

$$\sigma_f^2(t) = \frac{\sum_{i=t+1}^{f} (i - \mu_f(t))^2 * P(i)}{\omega_f(t)}$$

ktoré opisujú hodnoty potrebné na výpočet σ_ω^2 (vzorce prevzaté z [42]).

Existujú ďalšie metódy na prahovanie, ktoré sú použité na extrahovanie prstov zo snímkov (napríklad metódy od **Lee**, **TomesLee** a **Kono**). Tieto metódy ale nedosahovali potrebných výsledkov a preto nebudú v rámci práce podrobnejšie rozpísané.

3.4 Predspracovanie

Predspracovanie alebo *preprocessing* má za účel vylepšiť kvalitu obrázku pred aplikovaním extrakcie prvkov. Na vylepšenie kvality sa využívajú rôzne metódy, ktoré `upravujú kontrast snímky` a tým zvýrazňujú vzorce žíl, ktoré sú potrebné v ďalších krokoch. Konkrétne metódy, ktoré boli brané do úvahy budú opísané nižšie.

3.4.1 Ekvalizácia histogramu

Ekvalizácia histogramu (HE) je technika zvýraznenia kontrastu v priestorovej doméne pri spracovaní obrazu pomocou histogramu obrazu. Vyrovnanie histogramu zvyčajne zvyšuje celkový kontrast spracovávaného obrazu. Táto metóda je užitočná pre obrázky, ktoré sú príliš svetlé alebo tmavé [35].

Ekvalizácia histogramu je schéma, ktorá **mapuje vstupný obraz do celého dynamického rozsahu** $[X_0, X_{L-1}]$, kde:

- L predstavuje počet odtieňov šedej v obrázku
- $X = x(i,j)$, kde $x(i,j)$ predstavuje intenzitu odtieňa šedej v priestorovej doméne

pomocou funkcie kumulatívneho rozdelenia ako transformačnej funkcie. Transformačnú funkciu $f(x)$ teda definujeme pomocou funkcie kumulatívneho rozdelenia $cdf(X_i)$ [35].

3.4.2 Adaptívna ekvalizácia histogramu s obmedzeným kontrastom

Adaptívna ekvalizácia histogramu s obmedzeným kontrastom (CLAHE), bola pôvodne vyvinutá na zlepšenie nízko-kontrastných lekárskych obrazov [36]. Od bežného AHE (Adaptívna ekvalizácia kontrastu) sa líši `obmedzením kontrastu`. Na rozdiel od HE (Ekvalizácie histogramu), CLAHE pracuje na malých oblastiach v snímku a vypočítava niektoré histogramy, ktoré zodpovedajú inej oblasti obrazu, a používa ich na prerozdelenie hodnoty jasu snímku [6]. CLAHE obmedzuje zosilnenie orezaním histogramu na užívateľom definovanú hodnotu nazývanú limit klipu ("Clip Limit"). Vo všeobecnosti je matematický výraz pre CLAHE znázornený v rovnici 3.4.

$$g = [g_{max} - g_{min}] * P(f) + g_{min} \tag{3.4}$$

kde hodnota g predstavuje vypočítanú hodnotu jednotlivých pixelov, zatiaľ čo g_{min} a g_{max} prestavujú maximálnu a minimálnu hodnotu snímku. $P(f)$ znamená kumulatívne rozdelenie pravdepodobnosti (CPD) Rayleighovho rozdelenia, ktoré je uvedené ako rovnica 3.5 [27].

$$P(f(\frac{x}{b})) = \int_0^x \frac{x}{b^2} e^{(\frac{-x^2}{2b^2})} \tag{3.5}$$

Ďalším algoritmom na predspracovanie je **STRESS ("Stress Spatio Temporal Retinex-inspired Envelope with Stochastic Sampling")**. Princíp fungovania algoritmu je prepočítavanie každého pixelu pre lokálnu hornú a dolnú hranicu v obraze pomocou obálok. Získané obálky možno interpretovať ako lokálne referenčné maximum a minimum použité na vzorkovanie susedných pixelov [24].

Hoci algoritmus STRESS je zvyčajne vnímaný ako najlepší na vylepšenie obrazu, veľkou nevýhodou tohto algoritmu pri spracovaní žíl v prste je fakt, že **algoritmus STRESS zanáša do snímku veľké množstvo šumu**, ktorý má negatívny vplyv na klasifikáciu prezentačných útokov.

3.5 Extrakcia informácií zo snímku

Extrakcia informácií (prvkov) zo snímku je finálna časť spracovania snímku. V tejto sekcií budú popísané dva prístupy, ktoré boli študované na vytvorenie sady prvkov, ktorá bude použitá pri klasifikácií.

Prístupy sa odlišujú od informácií, ktoré dane metódy dokážu extrahovať zo snímku. Prvý prístup je **extrakcia žilného vzoru** zo snímku, ktorý prešiel predspracovaním a ROI detekciou s následným orezaním. Druhý prístup spracováva informácie o textúre snímku, ktorý je orezaný podla vnútorného ROI, no nieje na ňom prevedené žiadne predspracovanie.

3.5.1 Extrakcia žilového vzoru prsta

Pri extrakcii žíl z prsta boli zvážené rôzne metódy, medzi vybrané metódy patrí metóda **Maximálneho zakrivenia ("Maximum Curvature" (MC))**, metóda **Opakovaného sledovania čiary ("Repeated Line Tracking" (RLT))** a metóda **Hlavného zakrivenia ("Principal Curvature" (PC))**.

Výstupom týchto metód je binárny obraz (maska), ktorý znázorňuje štruktúru žíl nachádzajúcu sa v prste.

Maximálne zakrivenie

Maximálne zakrivenie je metóda na extrakciu žíl na prstoch zo snímky. Metóda je odolná voči rôznym šírkam žíl a rôznym úrovniam jasu.

Extrakciu možno rozdeliť do troch oddeliteľných krokov [29]. V prvom kroku sa pomocou prierezových profilov extrahujú centrá žíl. Metóda predstavuje obrázok ako funkciu $f(x, y)$, ktorá udáva hodnotu šedej v pixeloch (x, y) obrázka. Profil $P_f(z)$ je profil prierezu získaný z $f(x, y)$ v akomkoľvek smere a polohe, kde z je poloha v profile. Zakrivenie κ takéhoto profilu možno vypočítať pomocou rovnice 3.6 [29].

$$\kappa(z) \ = \ \frac{P_f(z)^{``}}{[1 + (P_f(z)^{`})^2]^{\frac{3}{2}}} \tag{3.6}$$

Vypočítajú sa všetky kladné lokálne maximá všetkých konkávnych oblastí zakrivenia profilu a tieto body sú stredovými polohami žíl. Kompletný súbor týchto bodov je označený ako I a pre každý záznam je vypočítané skóre S_{cr} určujúce pravdepodobnosť, že bod je centrom žily. Tento výpočet je definovaný v rovnici 3.7 [29].

$$\forall z_i \in I \ : S_{cr}(z_i) = \kappa(z_i) * W_r(z_i) \tag{3.7}$$

kde W_r je šírka konkávnej kladnej oblasti $\kappa(z)$ okolo polohy z_i.

Aby sa získal žilový vzor šíriaci sa v celom obraze, analyzujú sa všetky profily v jednom smere. Na získanie žilového vzoru šíriaceho sa vo všetkých smeroch sú analyzované profily v štyroch smeroch. Použité smery sú horizontálne, vertikálne a dva šikmé smery pretínajúce horizontálu a vertikálu pri 45°. Všetky stredové polohy žíl sa teda detegujú výpočtom lokálnych maximálnych zakrivení [29].

Na prepojenie centier žíl a elimináciu šumu sa vykonáva nasledujúca operácia filtrovania. Najprv sa skontrolujú dva susediace pixely na pravej strane a dva susedné pixely na ľavej strane pixelu (x, y). Ak (x, y) a pixely na oboch stranách majú veľké hodnoty, je nakreslená vodorovná čiara. Keď (x, y) má malú hodnotu a pixely na oboch stranách majú veľké hodnoty, nakreslí sa čiara s medzerou (x, y). Preto by sa hodnota (x, y) mala zvýšiť, aby sa linka spojila. Keď (x, y) má veľkú hodnotu a pixely na oboch stranách (x, y) majú malé hodnoty je zistené, že bodka šumu je na (x, y). Preto by sa hodnota na (x, y) mala znížiť, aby sa eliminoval šum [29]. Táto operácia je znázornená na rovnici 3.8.

$$C_{d1}(x, y) \ = \ min[max(V(x + 1, y), V(x + 2, y)) + max(V(x - 1, y), V(x - 2, y))] \tag{3.8}$$

Operácia sa aplikuje na všetky pixely. Pri ďalšom kroku sa tento výpočet urobí pre každý zo štyroch smerov rovnakým spôsobom a získa sa C_{d2}, C_{d3}, C_{d4}. Nakoniec sa výberom získa konečný obrázok $G(x, y)$. Vyber spočíva v získaní maxima $C_{d1}, C_{d2}, C_{d3}, C_{d4}$ pre každý pixel [29]. Teda G sa dá definovať ako $G \ = \ max(C_{d1}, C_{d2}, C_{d3}, C_{d4})$.

Opakované sledovanie čiary

Ďalší spôsob extrakcie prvkov je založený na **Opakovanom Sledovaní Čiary**. $F(x, y)$ definuje intenzitu pixelu (x, y), (x_c, y_c) je poloha aktuálneho bodu sledovania čiary v obraze, R_f je množina pixelov v rámci obrysu prsta a T_r je lokusový priestor ("locus space"). Predpokladá sa, že pixel vľavo dole na obrázku leží na súradniciach $(0, 0)$, kladný smer osi

x má byť doprava na obrázku, kladný smer osi y nahor v rámci obrázka a $T_r(x, y)$, ktorý sa má inicializovať na 0 [28].

Fungovanie metódy sa dá opísať v nasledujúcich krokoch:

1. Určenie počiatočného bodu pre sledovanie čiary a atribútu pre smer pohybu
2. Detekcia smeru tmavej čiary a pohybu bodu sledovania
3. Aktualizácia počtu detekcie bodov v lokusovom priestore, ktoré boli sledované
4. Opakované vykonanie kroku 1 až kroku 3 (N-krát)
5. Získanie vzoru prstových žíl z lokusového priestoru

Nevýhodou tejto metódy je v porovnaní s ostatnými **veľká výpočtová doba**, keďže na správne fungovanie je potreba veľký počet N (opakovaní krokov).

Hlavné zakrivenie

Poslednou metódou je **Hlavné zakrivenie**, ktoré používa prístup založený na zakrivení (teda na princípe podobnom ako MC). Je založené na gradientovom poli obrazu.

Prvým krokom je výpočet gradientového poľa. Tvrdé prahovanie na odfiltrovanie malých gradientov nastavením ich hodnôt na nulu je vykonané, aby sa zabránilo zosilneniu malých bodov predstavujúcich šum. Potom sa získa normalizované pole gradientu normalizáciou intenzity (jasu) na 1 pri každom pixeli, ktorá sa potom vyhladí použitím Gaussovho filtra. Skutočný výpočet hlavného zakrivenia sa potom vykoná na základe tohto vyhladeného normalizovaného gradientového poľa výpočtom vlastných hodnôt Hessovej matice ("Eigenvalues of the Hessian matrix") pre každý pixel. Dve vlastné hodnoty sú hlavné zakrivenia a zodpovedajúce vlastné vektory Hessovej matice predstavujúce smery maximálneho a minimálneho zakrivenia. Väčšia vlastná hodnota zodpovedá maximálnemu zakriveniu medzi všetkými smermi. Táto hodnota je zaznamenaná a ďalej používaná.

Posledným krokom je opäť prahová binarizácia základných hodnôt zakrivenia, aby sa získal vektor výstupného znaku, ktorý predstavuje binárny obraz žily [36].

3.5.2 Extrakcia informácií o textúre snímku

Ako ďalšie informácie, ktoré bude potrebné extrahovať zo snímku prsta budú informácie opisujúce textúru. Tie budú slúžiť na `detekciu rôznych anomálií` v snímkoch, ktoré sa nedajú zistiť z mapy žilových vzorov. Medzi vybrané metódy opísané nižšie patria **Matica spoločného výskytu na úrovni šedej ("Gray level co-occurrence matrix" (GLCM))** a **Histogram orientovaných gradientov ("Histogram of Oriented Gradients" (HOG))**.

GLCM

Matica spoločného výskytu na úrovni šedej (ďalej GLCM)) je populárna metóda extrakcie prvkov založená na textúre. GLCM určuje textúrny vzťah medzi pixelmi vykonaním operácie podľa štatistík derivácie druhého rádu v obrázkoch. Na túto operáciu sa

zvyčajne používajú dva pixely [3]. GLCM určuje frekvenciu kombinácií týchto určených hodnôt jasu pixelov. To znamená, že predstavuje frekvenčnú tvorbu párov pixelov [38].

Vlastnosti GLCM obrázka sú vyjadrené ako **matica s rovnakým počtom riadkov a stĺpcov ako hodnoty šedej na obrázku**. Prvky tejto matice závisia od frekvencie dvoch špecifikovaných pixelov. Oba páry pixelov sa môžu líšiť v závislosti od ich susedstva. Ak sú hodnoty intenzity široké (napríklad v rozsahu $< 0, 1024 >$, prechodová matica je dosť veľká. To vytvára časovo náročné podmienky na vypočítanie matice [30]. GLCM je pre obrázok zaznačený ako P(i,j,d,θ), kde i a j sú prvky v GLCM definované vzdialenosťou d v smere θ.

Haralickove texturálne vlastnosti

Haralickove texturálne vlastnosti ("Haralick texture features") sú bežné deskriptory textúr v analýze obrazu. Na výpočet Haralickových prvkov sa najskôr znížia úrovne šedej na obrázku, čo je proces nazývaný **kvantizácia**. Výsledné vlastnosti silne závisia od kroku kvantovania (zmenšenia kroku úrovne šedej / zmena rozlíšenia), takže Haralickove vlastnosti nie sú reprodukovateľné, pokiaľ sa nevykoná rovnaká kvantizácia [26].

Haralickove vlastnosti, ktoré sú invariantné k počtu kvantizačných úrovní šedej sa dajú dosiahnuť za pomoci GLCM matice predstavenej v časti 3.5.2. Haralick zadefinoval 28 vlastností [14] opisujúcich texturálne vlastnosti, no medzi často používané Haralickove texturálne vlastnosti patria vlastnosti definované v rovniciach 3.9-3.14,

$$contrast = \sum_{i,j=0}^{levels-1} P_{i,j}(i-j)^2 \tag{3.9}$$

$$dissimilarity = \sum_{i,j=0}^{levels-1} P_{i,j}|i-j| \tag{3.10}$$

$$homogeneity = \sum_{i,j=0}^{levels-1} \frac{P_{i,j}}{1+(i-j)^2} \tag{3.11}$$

$$ASM = \sum_{i,j=0}^{levels-1} P_{i,j}^2 \tag{3.12}$$

$$energy = \sqrt{ASM} \tag{3.13}$$

$$correlation = \sum_{i,j=0}^{levels-1} P_{i,j} \left[\frac{(i-\mu_i)(j-\mu_j)}{\sqrt{(\sigma_i^2)(\sigma_j^2)}} \right] \tag{3.14}$$

kde μ_i, μ_j a σ_i, σ_j sú priemerná a štandardná odchýlka z p_i a p_j. $P_{i,j}$ je hodnota v GLCM matici na indexe i, j. *Levels* je počet odlišných hodnôt v GLCM matici [14].

HOG

Histogram orientovaných gradientov ("Histogram of Oriented Gradients" (HOG)) využíva orientáciu gradientu obrazu a normalizovaný histogram. Kroky extrakcie vlastností sú zhrnuté nasledovne.

Najprv sa veľkosť vstupného obrázka zmení na 64 × 128 pixelov. Potom sa na obrázku vykoná `gama normalizácia`, po ktorej nasleduje výpočet veľkosti a uhla gradientu pre každý pixel. Výsledný obrázok sa potom rozdelí na mriežku buniek s veľkosťou 8 × 8 pixelov. Ďalej sa na vrch mriežky umiestni posuvné okno s rozmermi 16 × 16 pixelov a posúva sa cez bunky. V každom kroku posuvné okno prekrýva štyri bunky tvoriace blok. Následne sa pre každý blok použije `trilineárna interpolácia` na vyjadrenie veľkosti gradientu do histogramu na základe orientácie gradientu. Histogramy sú potom normalizované a zostavené tak, aby vytvorili jednorozmerný vektor prvkov [9].

3.6 Klasifikácia

Na klasifikáciu prezentačného útoku je za potrebu použitie klasifikátora, ktorý dokáže rozlíšiť medzi dvoma prípadmi (prezentácia v dobrej viere a prezentačný útok). Na túto úlohu bol spomedzi rôznych klasifikátorov zvolený **SVM klasifikátor**. Ďalšou možnosťou bol **Random Forest klasifikátor**, ktorý avšak nie je ideálnou voľbou pre binárnu klasifikáciu snímkov kvôli jeho princípu fungovania, ktorý je založený na rozhodovacích stromoch. Tie majú tendenciu sa presilovať pri veľkom množstve prvkov, takisto trpia neschopnosťou generalizovania na nové snímky. Tieto nedostatky vedú ku chybám pri klasifikácií.

3.6.1 SVM

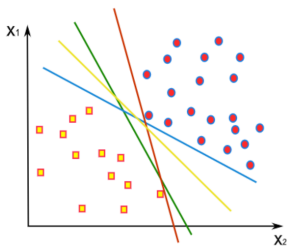
Hlavnou funkciou **podporného vektorového stroja ("Support Vector Machine" (SVM))** je oddeliť niekoľko tried v tréningovej sade povrchom, ktorý maximalizuje rozpätie medzi nimi. Inými slovami, *SVM umožňuje maximalizovať schopnosť zovšeobecnenia modelu.*

Trénovanie SVM vyžaduje súbor n príkladov. Každý príklad pozostáva z páru, vstupného vektora x_i a súvisiaceho označenia y_i [8] za predpokladu, že trénovacia množina X je daná ako:

$$(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n) \tag{3.15}$$

teda $X = \{x_i, y_i\}_{i=1}^{n}$, kde $x_i \in \mathbb{R}^n$ a $y_i \in \{0, 1\}$.

Dáta môžu byť lineárne oddeliteľné a môže existovať veľa nadrovín, ktoré môžu vykonávať oddelenie. Obrázok 3.3 ukazuje niekoľko rozhodovacích nadrovín, ktoré dokonale oddeľujú súbor vstupných údajov. Z obrázka je jasne vidieť, že existuje nekonečne veľa nadrovín, ktoré by mohli vykonávať túto prácu. Schopnosť zovšeobecnenia však závisí od umiestnenia separačnej nadroviny a nadroviny s maximálnym okrajom. Táto nadrovina sa nazýva `optimálna separačná nadrovina` [10].



Obr. 3.3: Lineárne rozhodovacie nadroviny, ktoré používa SVM na klasifikáciu. (Obrázok prevzatý z [8].)

Najjednoduchším prípadom SVM je `lineárne oddeliteľný prípad` v priestore prvkov (ukázaný na obrázku 3.3). Niekedy nie je množina trénovacích údajov dokonale lineárne oddeliteľná a potom je nadrovina umiestnená tak, aby čo najviac rozlíšila medzi oboma triedami. V SVM sú trénovacie vektory mapované do priestoru vyššej dimenzie pomocou funkcie jadra. Medzi bežne používané funkcie jadra sú považované lineárna, polynomická, sigmoidná a radiálna bázová funkcia (RBF) [17].

Kapitola 4

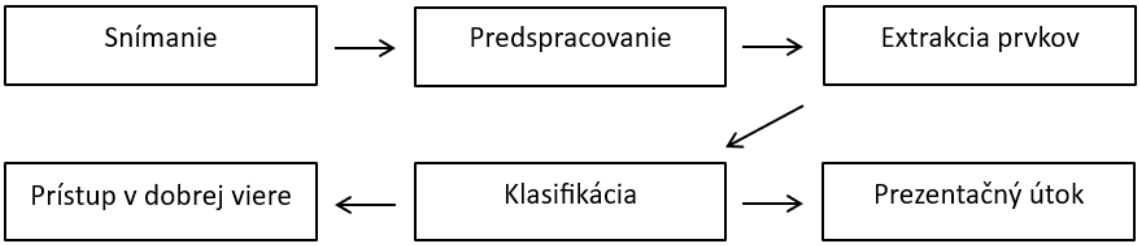
Návrh a realizácia metódy detekcie prezentačného útoku

V tejto kapitole je popísaný navrhovaný systém na detekciu prezentačných útokov. Detekciu prezentačného útoku možno vnímať buď ako samostatný systém alebo ako rozšírenie pre existujúci biometrický systém. Hlavnou úlohou v oboch prípadoch je rozlíšiť prezentované biometrické vzorky medzi živou a neživou triedou.

Požiadavky na navrhovaný systém sú dané nasledovne:

- Systém je rozdelený na dva samostatné podsystémy – získavanie snímkov a spracovanie snímkov.
- Prvý podsystém je vytvorený pomocou `existujúceho snímača na báze CMOS senzoru`.
- Druhý podsystém je navrhnutý na nezávislosť na zariadení ako `plne automatizovaný program`, ktorý spracuje vstupný obraz a `automaticky ho klasifikuje ako živý alebo neživý` bez akéhokoľvek zásahu používateľa.

Návrh architektúry navrhovaného systému je znázornený na obrázku 4.1. Po prvé, snímok je získaný pomocou samostatného subsystému na získavanie obrazu žilového riečiska v prste. Podrobný popis použitého snímača prstov a jeho použitie bude popísané nižšie.



Obr. 4.1: Návrh architektúry systému.

Následne sa vo všetkých zosnímaných snímkach prevedie predspracovanie. Ďalej sa prevedie získanie mapy žíl z prsta a následne modul extrakcie prvkov extrahuje vektor prvkov z oblasti záujmu (ROI). Nakoniec sa v závislosti od nastavenia klasifikátora prevedie rozhodnutie o triede, do ktorej snímok patrí.

4.1 Získanie snímkov

Snímky použité na detekciu boli snímané za pomoci kamery obsahujúcej filter, ktorý prepúšťa špecifickú vlnovú dĺžku a NIR LED diód, ako je ukázané na snímku 4.2. Konštrukcia obklopujúca snímač obsahuje 8 NIR LED diód, ktoré boli napájané na laboratórnom zdroji. Diódy boli napájané na napätí 11,8V a prúdovom odbere 0,44A. Na napájanie diód bolo teda celkovo potreba $P = U * I$, teda $11,8V * 0,44A \approx 5,2W$ ($Wattu$). Keďže diódy sú zapojené sériovo, úbytok napätia na jednotlivých diódach sa dá vypočítať za pomoci **kirchhoffových zákonov** ako $U_i = U/8$, teda $11,4V/8 = 1,425V$. Z úbytku napätia na dióde a prúde v obvode sa dá vyjadriť potrebný výkon na napájanie jednej diódy podobne ako vyššie, teda $P_i = U_i * I$, teda $1,425V * 0,44A \approx 0,6W$.

Pri týchto nastaveniach diód boli snímané dáta, ktoré budú následne spracované navrhnutou metódou na detekciu prezentačného útoku. Snímanie bude prebiehať v tmavej miestnosti, aby sa zamedzilo prístupu vonkajších podnetov pri snímaní, čo by mohlo zapríčiniť nerovnomerné nasvietenie a prezenciu artefaktov pri snímaní.

Obr. 4.2: Kamera použitá na snímanie falzifikátov použitých pri implementácií a testovaní metódy detekcie prezentačného útoku.

4.2 Spracovanie snímkov

V nasledujúcich častiach bude opísaný postup spracovania snímkov a ich klasifikácia. Konkrétne v časti 4.2.1 bude opísaný postup maskovania ruky, v časti 4.2.2 a 4.2.3 bude opísaný postup rozdelenia snímku ruky na jednotlivé prsty a v časti 4.2.4 opísaný postup predspracovania.

4.2.1 Maskovanie ruky

Prvým krokom po získaní snímku ruky je oddelenie samotnej ruky od pozadia. Ako bolo spomínané v časti 3.3, na prevedenie tohto oddelenia budú použité metódy *prahovania*. Na nájdenie prahu, ktorý by vyhovoval snímkom bol prevedený histogram šedej úrovne ("grey level histogram"), na ktorom boli sledované výskyty (početnosť) rôznych hodnôt šedej (pri rozsahu hodnôt obrázku

$image(x, y) \in < 0, 255 >$). Z grafu týchto snímok bola získaná hranica, ktorá bola následne použitá ako prahová hodnota.

Prahová hodnota z grafu bola určená na podľa miesta, ktoré predstavuje lokálne minimum medzi vrchmi, ktoré najlepšie charakterizuje prechod medzi pozadím a získavaným objektom. Výstup z tohto prahovania predstavuje binárny obraz (masku), ktorý oddeľuje pozadie od vzoru ruky, ako je ukázané na obrázku 4.3.

Obr. 4.3: Maska zo snímku ruky (získaná po binárnom prahovaní), kde sú spojené 3 prsty mostíkom, ktorý sa nachádza v dolej časti.

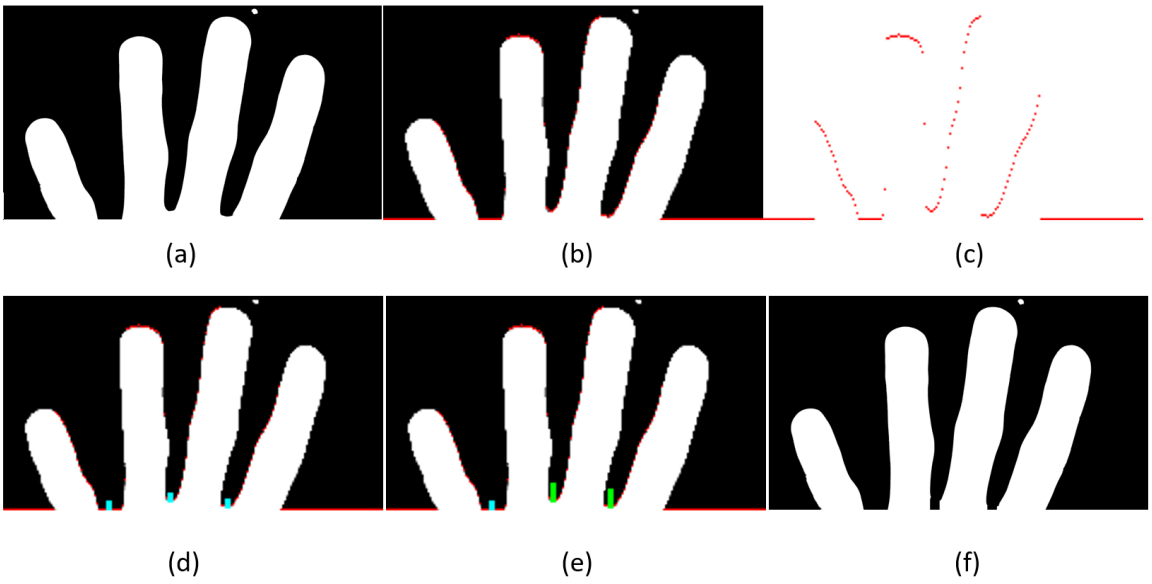
4.2.2 Segmentácia prstov z masky ruky

Po získaní masky snímku ruky je za potrebu `rozdeliť danú ruku na jednotlivé prsty`, keďže na snímku niesu prsty oddelené ale spojené, ako je možné vidieť na obrázku 4.3.

Jedným z riešení na elimináciu tohto problému by bolo orezanie obrázku zo spodnej časti dovtedy, kým by boli jednotlivé prsty oddelené a bolo by možné ich následne jednotlivo spracovávať. Iným riešením by bolo prsty ručne orezať no to by pri väčšej vzorke prstov zabralo veľa času.

Ďalším riešením je pokúsiť sa oddeliť tieto prsty a to zafarbením časti masky hodnotou predstavujúcou pozadie tak, aby medzi prstami nebolo žiadne spojenie a pri ďalšom spracovaní ich bolo možné spracovávať jednotlivo.

Na elimináciu problému spojených prstov bola vybraná druhá možnosť, a to **oddelením prstov za pomoci upravenia masky**. Táto metóda spočíva v nájdení údolí na maske ruky. Po nájdení údolí je ich pravdivosť overená kontrolou, či sa údolie nenachádza na hrane obrázku. Na získanie informácií, kde sa môže údolie nachádzať sa do jednorozmerného poľa zapisujú výšky prvého výskytu prechodu z bielej farby (1) na čiernu farbu (0), a to po celej šírke obrázku. Tento krok je ale pri originálnej veľkosti obrázka (približne 8 000 000 pixelov) výpočtovo náročný, preto pred prevedením tohto kroku je obrázok zmenšený na $\frac{1}{20}$ originálnej veľkosti, čo je v prepočte z 8 000 000 bodov len 20 000, teda **400-násobné zmenšenie** celkového počtu bodov, s ktorými treba pracovať. Po získaní údolí z masky ruky je nad získanými bodmi nakreslená čiara, ktorá smeruje od súradníc špičky údolia až po kraj obrázka smerom dole, ktorá má hodnotu 0 a rozdeľuje jednotlivé prsty od seba. Celý tento postup je znázornený na algoritme 1 a obrázkoch 4.4a-f.



Obr. 4.4: Postup spracovania masky ruky. (a) Načítanie a zmena veľkosti obrázku, (b) Prechody medzi farbami, (c) Výška jednotlivých bodov znázornená mimo masky ruky, (d) Údolia získané z bodov v predchádzajúcom kroku, (e) Kontrola pravdivosti údolí, (f) Segmentácia prstov.

4.2.3 Extrakcia prstov zo snímku ruky

Na extrakciu prstov zo snímku ruky bude potrebná maska získaná v časti 4.2.2. Metóda bola vymyslená a inšpirovaná na základe `ohraničujúceho boxu`. Čím sa líši od základnej implementácie je možnosť získať viacero objektov v rámci jedného obrázku. V rámci každého boxu bude získavaný sekundárny box. Tento box bude získavaný pod uhlom, ako je znázornené na obrázku 4.5. Box získaný pod uhlom prsta predstavuje ROI, ktorý bude použitý na získavanie sád prvkov.

Tento krok predstavuje orezanie jednotlivých prstov z ohraničujúcich boxov ako je znázornené na obrázku 4.6 červenou farbou. Pre zjednodušenie bude postup opísaný pre jeden ohraničujúci box na celom snímku. Na získanie prsta je potreba poznať súradnice naklonenéhо boxu, ktorý obklopuje daný prst. Z tohto boxu je následne použitá jedna strana pozdĺž prsta. Z tejto strany je za pomoci funkcie *arkus tangens* vypočítaný uhol, ktorý táto strana zviera ku hrane celej snímky.

Zo získaného uhlu je následne vypočítaná **rotačná matica**, ktorá bude aplikovaná na otočenie celého snímku tak aby bol cieľový prst natočený vertikálne a ohraničujúci box bol v 90° uhle. Touto operáciou ale vzniká *deformácia* jednej strany obrázka v dolnej časti (trojuholníkový tvar ktorý spôsobila rotácia obrázku, ktorý je následkom natočenia časti snímku mimo jej okraje), ktorá je pred vystrihnutím odpočítaná z danej časti obrázku. Táto strana je získaná za pomoci goniometrickej funkcie *sínus*, ktorá vypočíta dĺžku protiľahlej strany k vyššie získanému uhlu. Táto dĺžka je odčítaná a výsledný tvar je zo snímku vystrihnutý a uložený na ďalšie spracovanie.

Algoritmus 1: MASK HAND

Input: *path*
Output: *mask*

```
1:  mask = load_file(path)
2:  mask = resize_image(mask, 0.05)
3:  ridges = find_first_dark(mask)
4:  peaks = find_peaks(ridges)
5:  for every peak in peaks do
6:      if peak.height = 0 then
7:          peak.delete()
8:      end if
9:  end for
10: for every peak in peaks do
11:     mask.draw_line(peak.height, 0)
12: end for
13: return mask
```

4.2.4 Predspracovanie

Vstupom do časti predspracovania sú snímky prstov získané v časti 4.2.3. V tejto časti je cieľom pripraviť snímok na extrakciu žilovej mapy zo snímku. Výsledkom tejto časti bude snímok pripravený na extrakciu sád prvkov, ktoré budú použité pri klasifikácií.

Normalizácia

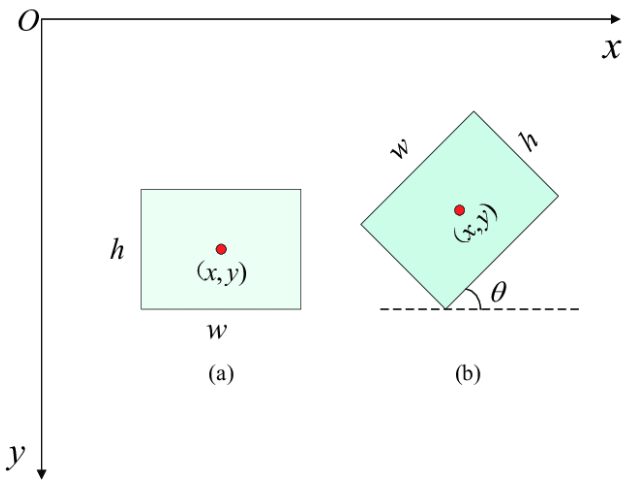
Ku ďalšiemu spracovaniu je žiadúce, aby sa pracovalo so snímkami s konštantnou veľkosťou. Na zabezpečenie tohto kroku bude slúžiť normalizácia snímku. Snímky budú normalizované na šírku **250 pixelov**. Dĺžka snímky bude upravená na hodnotu tak, aby sa `zachoval pôvodný tvar` (pomer strán) originálnej snímky.

Konvertovanie do jedného kanálu

Vo všetkých predchádzajúcich krokoch sa pracovalo s troj-kanálovým obrázkom (RGB). Ku ďalšej práci so snímkom bude potreba jeho prevedenie do jedného kanála (intenzity) – odtieňa šedej. Prevedenie snímku do jedného kanálu zaisťuje zmenšenie nákladov na výpočet ale aj na potrebnú veľkosť na uloženie. Takisto niektoré z ďalej používaných metód dokážu pracovať len so snímkami v odtieni šedej.

Maskovanie prsta

Ako posledný krok predspracovania bude získanie masky ktorá bude ohraničovať tvar, ktorý bude použitý na ďalšie spracovanie ako bolo prevedené v časti 4.2.1. Na maskovanie prsta ale nebude použitá základná metóda prahovania. Namiesto nej bude použitá metóda **OTSU prahovania**, ktorá bola priblížená v časti 3.3.1. Výsledkom tejto metódy je tak ako aj pri klasickom prahovaní `binárna maska`, ktorá oddeľuje prst od pozadia.



Obr. 4.5: (a) Ohraničujúci box (Bounding box), ktorý je bez natočenia. (b) Ohraničujúci box, ktorý je v uhle θ. (Obrázok prevzatý z [43].)

4.3 Extrakcia informácií zo snímkov

Táto časť sa bude venovať extrakcií informácií zo snímkov za použitia dvoch rôznych prístupov.

Prvý z prístupov bude z predspracovaného snímku `extrahovať žilový vzor`, z ktorého dát budú následne vybrané metriky, ktoré budú pridané do výslednej sady prvkov.

Druhý prístup bude používať `metriky opisujúce textúru`. Tieto metriky sú často používané na klasifikáciu pri podobných použitiach. Tento prístup bude opisovať rôzne farebné a texturálne štatistiky snímku.

4.3.1 Zvýraznenie kontrastu

Naznačené v častiach 3.4.1 a 3.4.2, metódy ekvalizácie histogramu sa používajú na zvýraznenie kontrastu v snímku. Ako je ukázané na obrázku 4.7, postup a metódy, ktoré boli zvolené na zvýraznenie žilových vzorov boli najskôr CLAHE a následne HE. Ako je z obrázka 4.7c vidno, na snímku po prevedení ekvalizácií je `značne jednoduchšie nájsť vzory žíl`. Tie majú po úpravách väčší kontrast oproti originálnemu snímku, čo zjednodušuje prácu pre metódu extrakcie žilového vzoru.

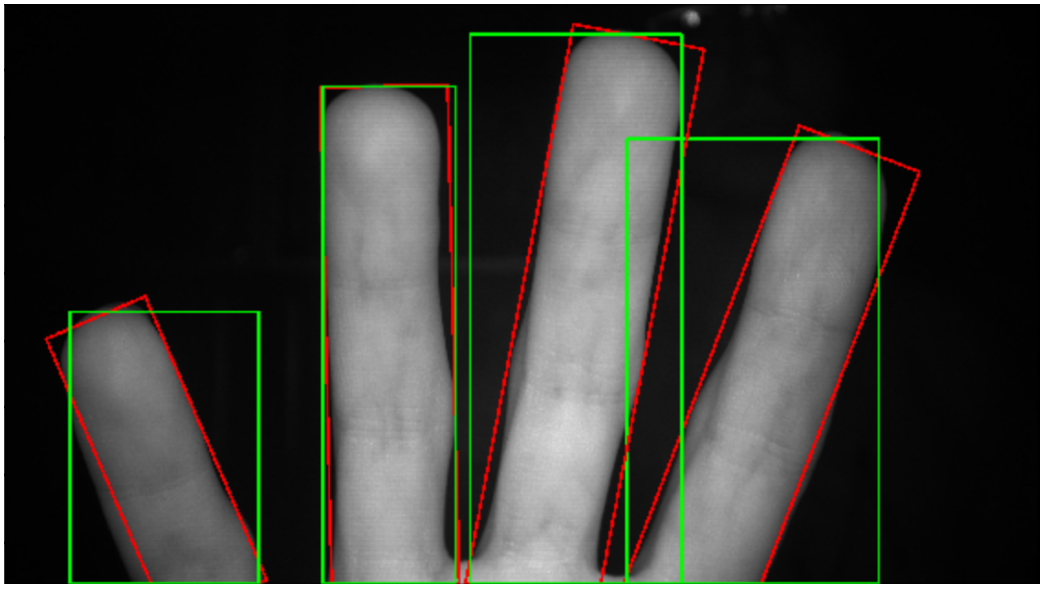
4.3.2 Extrakcia žilového vzoru

Na extrakciu žilového vzoru bude použitá **metóda maximálneho zakrivenia**, ktorá je opísaná v časti 3.5.1.

Pred začiatkom aplikovania metódy maximálneho zakrivenia na snímok je za potrebu dodatočné filtrovanie pomocou gausiánskeho filtra o rôznej veľkosti. Jadro pre zostavenie tohto filtra je zobrazené na rovnici 4.1

$$\mathcal{N}(x,y) = \frac{1}{2\pi\sigma^2} e^{\frac{-(x^2+y^2)}{2\sigma^2}} \tag{4.1}$$

kde σ predstavuje veľkosť filtra. Tento filter zamedzí zobrazeniu šumu ako žily zo snímku. V prípade tejto práce bola veľkosť filtra nastavená na 8.



Obr. 4.6: Ohraničujúci box (”Bounding box”) aplikovaný na snímku ruky za pomoci masky získanej v časti 4.2.2. Zelenou farbou je označený prvotný ohraničujúci box, červenou je označený ohraničujúci box, ktorý bol natočený aby obklopoval čo najlepšie tvar získavaného prsta.

Metóda maximálneho zakrivenia je použitá v štyroch rôznych smeroch a to **horizontálnom**, **vertikálnom** a na **diagonálach** 45° a −45°. Tieto smery sú vložené do rovnice zadefinovanej v 3.6. Výsledkom sú ako bolo spomínané vyššie kladné lokálne maximá, ktoré predstavujú stredové body žíl.

Ďalšia časť pri metóde je ohodnotiť tieto maximá. Jedná sa o hodnotu, ktorá značí pravdepodobnosť, že tento bod predstavuje žilu. Metóda priradí bodu hodnotu, ktorá závisí od šírky daného útvaru a jeho maximálnej hĺbky (minimálnej hodnoty útvaru). Tieto hodnoty sú vypočítané pre každý zo štyroch smerov definovaných v prvom kroku.

Nasleduje filtrovanie hodnôt z prvého kroku podľa hodnôt z druhého kroku. Výsledkom je vzor žíl, ktorý má rôznu šírku, preto je posledným krokom binarizácia, ktorá stenčuje jednotlivé žily.

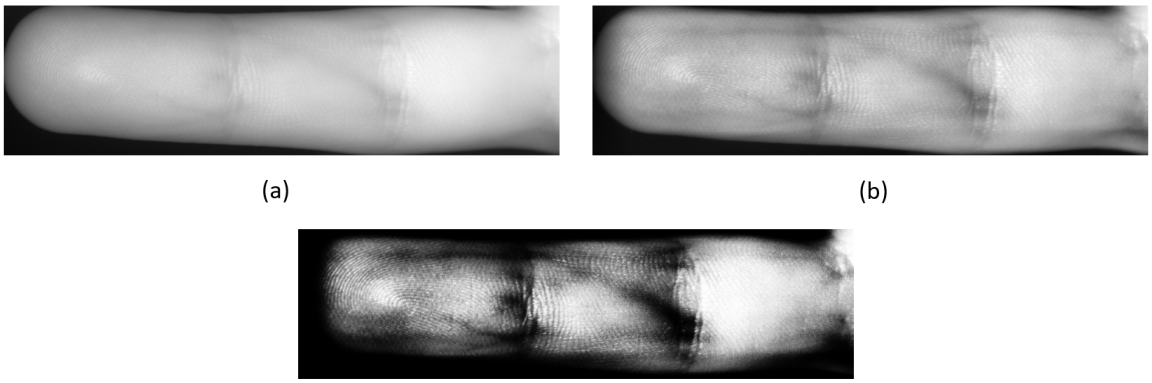
4.3.3 Vytvorenie sady prvkov zo žilového vzoru

Z vyššie opísaných metrík budú v tejto časti metriky rozdelené na dva rôzne prístupy, opisujúce rôzne typy vlastností získaných zo snímku, ako bolo opísané na začiatku v časti 4.3.

Prvý prístup – Charakteristiky získané zo žilového vzoru

Pri použití žilového vzoru získaného vyššie priamo do sady prvkov by sa veľkosť tejto sady pohybovala v rozmeroch $W * H$ (šírka $*$ výška snímku), keďže sada prvkov je jednorozmerné pole. Sada prvkov o takejto veľkosti je ale **extrémne náročná na výpočet a takisto nemá veľkú výpovednú hodnotu**, keďže informácie ktoré poskytuje sú binárne hodnoty.

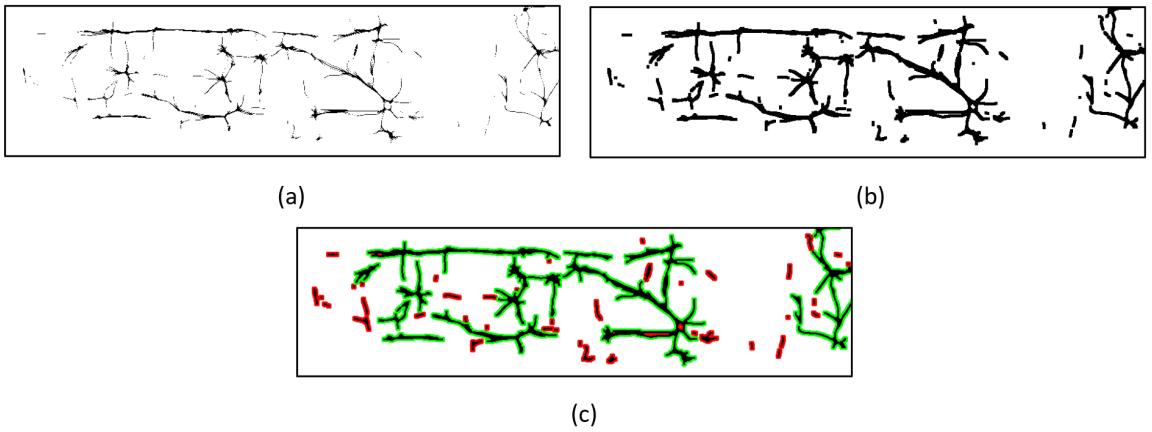
Na elimináciu tohto problému boli **zavedené tri metriky**, ktoré sú získané z tejto mapy. Konkrétne sa jedná o **početnosť krátkych a dlhých žíl**. Posledná metrika je



Obr. 4.7: Postup zvýšenia kontrastu na snímku prsta za účelom zvýraznenia vzorov žíl. (a) Originálny snímok (b) Snímok po CLAHE (c) Snímok po CLAHE a HE.

priemerná dĺžka dlhých žíl. Priemerná dĺžka krátkych žíl nebola ako metrika zvolená z dôvodu *malej výpovednej hodnoty*, keďže sa napriek krokom na zamedzenie vo výsledkoch objavuje šum. Na rôznych snímkoch sa táto hodnota pohybovala vo veľmi úzkom intervale a preto nebola do výslednej sady prvkov zaradená.

Na získanie týchto metrík je najskôr potrebné rozšíriť žily, aby nedošlo k situácií, že je jedna žila v istom mieste prerušená a tak rátaná ako dve samostatné žily. Žily sú **erodované** (nafúknuté) o jeden pixel z každej strany tak, že pôvodná žila o veľkosti 1 pixel má po nafúknutí rozmery 3x3. Následne sú jednotlivé tvary rozdelené na krátke a dlhé. Prahová hodnota na toto rozdelenie bola nastavená na 150 pixelov ($\frac{3}{5}$ hrúbky snímku). Snímok 4.8c ukazuje rozdelenie žíl medzi krátkymi a dlhými.



Obr. 4.8: Rozdelenie žíl podľa dĺžky na vytvorenie výslednej sady prvkov zo žilového vzoru. (a) Originálna mapa žíl (b) Mapa žíl po eródovaní (c) Žily po rozdelení. Červenou sú obkreslené krátke žily. Zelenou sú obkreslené dlhé žily.

Druhý prístup – Texturálne charakteristiky

Zo žilového vzoru sa pri detekcii bude používať aj iná metrika, a to **prezencia žíl v rôznych častiach prsta**. Výsledkom tejto metódy sú pomery svetlých a tmavých pixe-

lov vo vnútri masky získanej v časti 4.2.4. Tieto hodnoty sú `získavané z celého prsta ako aj z rôznych oddelených častí`. Týmto prístupom je možné zistiť rôzne pomery prítomnosti žíl v prste.

Metóda pracuje na princípe rozdelenia snímku na takzvané dlaždice ("tiles"). Tieto dlaždice delia obrázok na **jeden riadok** a **štyri stĺpce**, keď je prst vo vodorovnej orientácií. Jednotlivé dlaždice sú v tvare štvorca o rozmeroch $250 * 250$ pixelov (šírka snímku). Niekedy sa zo snímku dajú vytvoriť viac ako štyri dlaždice. V tom prípade sú zvyšné dlaždice zahodené. V tejto implementácií sa dlaždice neprekrývajú, čo sa v niektorých aplikáciách používa na zjemnenie rozdielu medzi extrahovanými dátami a presnejšou predstavou o zmenách medzi dlaždicami. Vytvorenie prekrývajúcich sa dlaždíc nebolo zvolené kvôli `skresleniu a vyššie spomínanému zjemneniu`, čo sú nechcené vlastnosti pri tejto aplikácií.

Z jednotlivých dlaždíc ako aj z celkového snímku sú vypočítané `percentuálne pomery` rôznych hodnôt na žilovej mape (0 a 1). Príklad na výpočet metrík pre dlaždicu je znázornený na rovniciach 4.2 a 4.3. Tieto metriky sú následne vložené do sady prvkov.

$$white = \frac{\sum_{x=0}^{width} \sum_{y=0}^{height} tile(x, y)}{width * height} \tag{4.2}$$

$$black = 1 - white \tag{4.3}$$

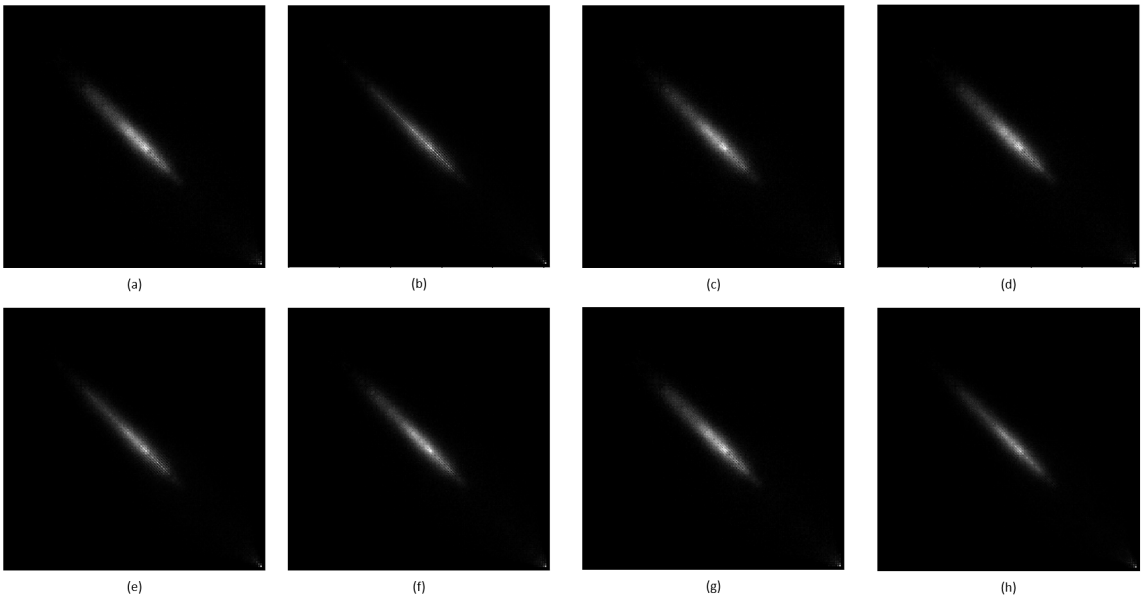
kde je predpokladané $height = width$ a $width = 250$ pixelov.

Ďalšou metrikou, ktorá bude opisovať texturálne charakteristiky snímku bude **GLCM spolu s Haralickovými vlastnosťami**, ktoré sú opísané v časti 3.5.2.

Pred výpočtom GLCM a Haralikovych vlastností je za potrebu orezať snímok tak, aby neobsahoval žiadne pozadie. Na toto bola implementovaná **metóda extrakcie vnútorného ohraničujúceho boxu**, ktorá na rozdiel od klasického ohraničujúceho boxu extrahuje najväčší obdĺžnik, ktorý je umiestený každou stranou v maske. Klasický ohraničujúci box obsahuje celý prst s čo najmenším podielom pozadia na finálnej snímke. Snímok, ktorý bude extrahovaný bude vypočítaný z masky získanej v časti 4.2.2 a zo snímky po úprave kontrastu získanej v časti 4.3.1.

V maske prsta bude nájdený obdĺžnik, ktorý má čo najväčší obsah no zároveň je celý v maske. Tento obdĺžnik predstavuje nový ROI ("inner ROI"), ktorý bude vystrihnutý zo snímku po CLAHE a HE úpravách.

GLCM matica je zvolená a implementovaná na celý snímok prsta získaný po "inner ROI" extrakcií. Keďže snímka je pri spracovaní v 8-bitovej hĺbke (256 hodnôt), GLCM matica bude mať rozmer 256x256. Z predpisu GLCM matice P(i,j,d,θ) je v tomto prípade hodnota d nastavená na 3, čo značí že opisovaný pixel bude pri výpočte používať hodnoty z troch susedných pixelov z každej strany (teda 6 pixelov dokopy). Následne parameter θ, čo značí naklonenie GLCM. Za θ je dosadená viac ako jedna hodnota, keďže pri rôznom naklonení snímku sú získané matice odlišné. Vo všeobecnosti sa **GLCM otáča, aby sa dosiahla invariantnosť otáčania**, teda boli získané hodnoty z rôznych uhlov. Na získanie výslednej GLCM matice sú hodnoty zpriemerované. V tomto prípade ale budú `použité hodnoty z každého uhla a nie len výsledná matica`. Keďže GLCM je symetrická matica, preferované uhly sú v rozsahu $< 0°, 180° >$. Zvolené hodnoty uhlov pre tento prípad sú $0°, 30°, 45°, 60°, 90°, 120°, 135°, 150°$, čo sú hodnoty rovnomerne pokrývajúce celých $180°$. Výsledné GLCM matice sú znázornené na obrázku 4.9.



Obr. 4.9: GLCM matice pre štyri zvolené uhly – (a) 0°, (b) 30°, (c) 45°, (d) 60°, (e) 90°, (f) 120°, (g) 135°, (h) 150°.

Zo získaných GLCM matíc je vypočítaných 6 Haralickových vlastností, ktoré boli zadefinované v rovniciach 3.9-3.14. Tieto vlastnosti sú vypočítané pre matice v každom natočení. Výsledkom je **48 metrík**, ktoré sú vložené do výslednej sady prvkov.

Výsledná sada prvkov

Všetky metriky získané v časti 4.3.3 sú spojené do jednej finálnej sady prvkov. Sada pre snímok jedného prsta obsahuje 48 metrík získaných z GLCM a Haralickových vlastností, následne 10 metrík opisujúcich percento prezencie žíl v prste, 3 metriky opisujúce dĺžku, počet dlhých a krátkych žíl. Ako posledná metrika pripočítaná k sade prvkov bude priemerná hodnota intenzity prsta, ktorá je získaná z vnútra masky.

Celková sada prvkov pre každý sledovaný prst bude predstavovať **62 jedinečných hodnôt**, ktoré slúžia na vyhodnotenie prezentačného útoku zo snímku. Sada prvkov je uložená na opakované použitie pri trénovaní a klasifikácií.

4.4 Klasifikácia

Táto časť sa bude zaoberať postupom použitým pri trénovaní klasifikátora. Klasifikátor zvolený pre túto prácu bol SVM, opísaný v časti 3.6.1. Pred použitím tohto klasifikátora je potrebné pripraviť a rozdeliť sady prvkov na **trénovacie** a **testovacie**, čo bude opísané v tejto časti.

4.4.1 Predpríprava sady prvkov

Prvým krokom ku vytvoreniu vektoru prvkov na trénovanie je predpríprava sady prvkov. Každá sada prvkov získaná zo snímku prsta je načítaná do **jedného dátového rámca**

("dataframe-u"[1]). Z tohto rámca sú následne odstránené polia, ktoré neobsahujú údaje (názvy stĺpcov, index riadka). Rámec je po tejto operácií stále reprezentovaný ako 2D pole, čo klasifikátor nevie spracovať, preto rámec prejde procesom serializácie, čoho výsledkom je rámec v 1D.

Každý riadok vo výslednom dátovom rámci reprezentuje metriky `práve o jednom zázname`.

Predbežné spracovanie sady prvkov

Na predbežné spracovanie sady prvkov pred trénovaním SVM klasifikátora bude použitá **technika škálovania** (scaler). Technika škálovania `štandardizuje hodnoty jednotlivých stĺpcov odčítaním priemeru a delením štandardnou odchýlkou`. Výsledok tejto techniky predstavuje hodnoty s **nulovým priemerom** a **jednotkovým rozptylom**. Tento krok predspracovania dátovej sady pomáha zlepšiť výkon modelu SVM tým, že zaisťuje, že všetky funkcie sú v podobnom rozsahu a bráni určitým prvkom, aby pri trénovaní dominovali v modeli kvôli ich väčším veľkostiam.

Rozdelenie sady prvkov

Na overenie presnosti klasifikácie vrámci vývoja je za potrebu rozdeliť dáta medzi trénovacie a testovacie. Tieto dáta je potrebné rozdeliť tak, aby bol každý typ falzifikátu obsiahnutý v oboch sadách. Dáta je možné rozdeliť v *rôznych pomeroch*. Vhodný pomer musí byť zvolený tak, aby bol `zaistený dostatok dát na trénovanie ako aj na dostatočné testovanie`.

4.4.2 Trénovanie klasifikátora a klasifikácia snímku

Dáta, ktoré sú vyhradené na trénovanie sú vložené do SVM klasifikátora, ktorý je následne na tejto časti natrénovaný. Následne je do klasifikátora vložený ľubovoľne zvolený riadok, ktorý je binárne klasifikovaný. Pre zvýšenie úspešnosti klasifikácie je možné v SVM nastaviť rôzne parametre, ako typ jadra, ktorý sa použije na oddelenie dát (ako bolo ukázané v časti 3.6.1). Takisto sa dá nastaviť parameter C, pri ktorom zvyšovaní sa nepriamo-úmerne zníži počet odľahlých hodnôt (outliers[2]).

[1] Dátový rámec (dataframe) je 2D dátová štruktúra používaná na analýzu a manipuláciu s údajmi, kde riadky predstavujú pozorované dáta a stĺpce predstavujú hodnoty. Poskytuje štruktúrovaný a účinný spôsob, ako organizovať, transformovať a analyzovať dáta.

[2] Odľahlé hodnoty sa týkajú bodov v dátach, ktoré sa neriadia všeobecným vzorom a sú ďaleko od väčšiny bodov.

Kapitola 5

Implementácia

Táto kapitola bude opisovať detaily implementácie metódy detekcie prezentačného útoku. Kapitola sa bude zameriavať hlavne na programovú časť v ktorej bola metóda navrhnutá, keďže pri snímací dátovej sady nebol použitý žiadny externý softvér.

5.1 Implementačné detaily

Implementácia a testovanie metódy detekcie prezentačného útoku prebiehalo v jazyku `Python 3.10.6`. Jazyk Python bol zvolený kvôli možnosti rýchleho prototypovania, čo umožňovalo rýchle vytváranie funkčných prototypov s minimálnym množstvom prepísania kódu. Tým sa zjednodušil iteratívny proces vývoja metódy.

V práci bola použitá knižnica `bob.bio.vein`[1], z ktorej boli použité metódy extrakcie prvkov Maximálneho zakrivenia, Opakovaného sledovania čiary a Hlavného zakrivenia, ako aj rôzne metódy prahovania.

Práca bola testovaná a ladená v prostredí `Jupyter Notebook`[2]. Notebook umožňuje jednotlivé spúšťanie samostatných buniek kódu a zobrazovanie výstupov v reálnom čase, čo uľahčovalo rýchle zisťovanie chýb alebo nepresností v implementácii.

Na paralelizáciu výpočtu sady prvkov bol použitý modul knižnice `Dask`, `delayed`[3]. Na spracovanie a zobrazené dát boli použité rôzne knižnice, hlavne `padnas` a `pickle`.

Knižnica `scikit-learn`[4] bola použitá na natrénovanie a klasifikáciu za pomoci klasifikátora, keďže obsahuje implementácie rôznych klasifikátorov, menovite klasifikátora SVM.

[1] https://www.idiap.ch/software/bob/docs/bob/bob.bio.vein/stable/index.html
[2] https://jupyter.org/
[3] https://docs.dask.org/en/stable/delayed.html
[4] https://scikit-learn.org/stable/modules/svm.html

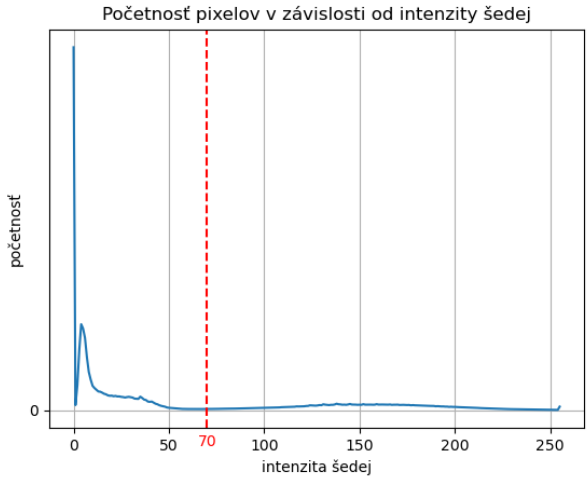
Kapitola 6

Meranie a testovanie

Táto kapitola sa bude venovať testovaním a hodnotením výslednej metódy na detekciu prezentačných útokov. Takisto tu budú popísané a odôvodnené zvolené metódy a konštanty, ktoré vedú na výslednú presnosť a funkčnosť metódy detekcie.

Nastavenie prahovej hodnoty

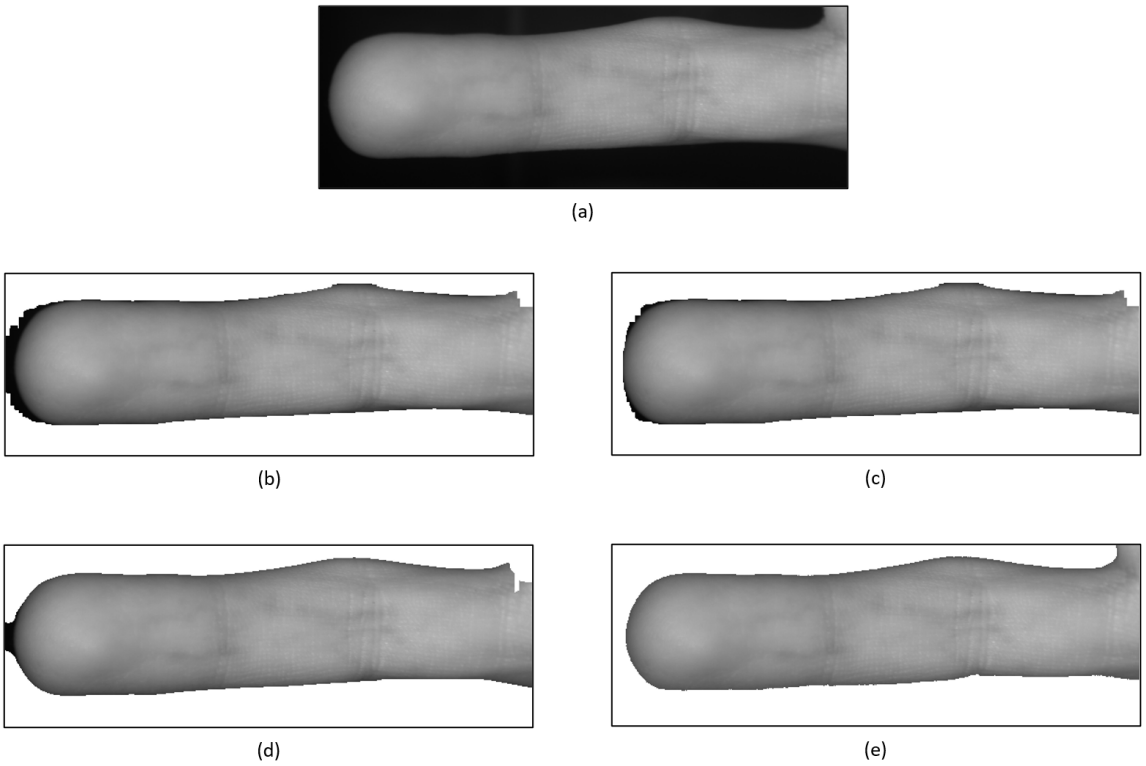
V časti 3.3 je potrebná dobre zvolená prahová hodnota, aby bolo možné presne určiť a ohraničiť ruku od jej okolia. Na to bolo na všetkých snímkoch v databáze vykonané **prahovanie šedej úrovne**. Zo všetkých získaných hodnôt bol vypočítaný výskyt jednotlivých úrovní šedej (od 0 do 255), ktorý je zobrazený na grafe na obrázku 6.1. Tento graf zobrazuje početnosť výskytu (osa y) rôznych hodnôt na snímkoch (osa x). Na grafe je vidno že v snímkoch je veľká prevaha tmavých pixelov (predstavujúce okolie) a menšia špička okolo hodnoty 150. Medzi týmito dvoma vrchmi je úsek veľmi malého výskytu pixelov (50 – 100). Z tohto úseku bola **zvolená hodnota 70**, ktorá najlepšie odlišuje predpokladané hodnoty pozadia od hodnôt popredia.



Obr. 6.1: Hodnoty získané z **prahovania úrovne šedej**. Červenou zobrazený prah, ktorý bude v prahovacej funkcii použitý.

Metóda maskovania prstov

Na maskovanie prstov z časti 4.2.4 boli použité metódy z časti 3.3.1. Konkrétne medzi uvažované metódy patrili Lee, TomesLee, Kono a Otsu (názvy metód podľa mien autorov).



Obr. 6.2: Rôzne typy maskovania aplikované na obrázok (a). Na obrázkoch je ukázaný extrahovaný prst z masiek získaných rôznymi metódami prahovania (b) Lee, (c) TomesLee, (d) Kono, (e) OTSU.

Na snímkoch 6.2b,c, kde sú použité metódy od Lee je vidno mierne nepresné odlíšenie pri špičke prstov, čo sa ale u metódy TomesLee zlepšilo. Napriek tomu pri oboch metódach prevládajú nerovnomerné výsledky. U snímku 6.2d, na ktorý bola použitá metóda Kono sú výsledky vynikajúce až na nedostatok pri špičke prsta, kde metóda nedokáže správne rozoznať pozadie. Metóda OTSU (obrázok 6.2e) dosahuje veľmi dobré výsledky a eliminuje nedostatky ostatných troch metód. S metódou Kono sú ale náročnejšie (o ≈100 ms viac) na výpočet oproti ostatným metódam. Napriek tomuto nedostatku bude vo finálnej metóde používaná metóda OTSU prahovania na maskovanie prsta.

Metóda extrahovania žilového vzoru

Extrahovanie žíl zo snímku prsta bolo sa potrebu previesť tak, aby použitá metóda našla dostatočný počet žíl zo snímka prstu, no zároveň aby zvýraznila čo najmenej šumu alebo iných artefaktov. Zvolená bola metóda, ktorá predstavovala `najlepší pomer medzi týmito vlastnosťami`.

Metóda hlavného zakrivenia má dva parametre – *sigma* a *prah*. Sigma bola nastavená na hodnotu 5, výsledky pod touto hodnotou ukazovali na priamoúmernú schopnosť sledovania vzoru bez zanášania šumu. Nad túto hodnotu klesal počet získaných žíl. Hodnota prahu

bola stanovená na 10, pričom od hodnoty 1 mapa obsahovala porovnateľné výsledky zo sledovania žily. Zvyšovaním tejto hodnoty až po hodnotu 10 priamo-úmerne klesal zachytený šum. Od hodnoty 10 ale metóda strácala schopnosť správneho rozpoznania žily a nebola ďalej testovaná.

Opakované sledovanie čiary má dva parametre – r a počet iterácií, ktoré boli v rámci testovania upravované. Nastavenie hodnoty r na 1 vykazovalo veľmi zlé sledovacie schopnosti. Zvyšovaním hodnoty sa tieto schopnosti zlepšovali až po hodnotu 10, po ktorej metóda fungovala veľmi nepresne až vôbec. Počet iterácií bol testovaný od hodnoty 100. To ukázalo malý počet šumu a malý počet detailov. Zvýšením sa obe tieto charakteristiky priamo-úmerne zlepšovali. Od hodnoty 500 do 1000 boli získané výsledky porovnateľné. Vyššími hodnotami sa `zvyšoval pomer šumu bez zvýšenia presnosti rozoznania`.

Nakoniec metóda maximálneho zakrivenia ktorá má jediný parameter – sigma. Testované od hodnoty 1, metóda znižovala prevahu šumu a zvyšovala úspešne rozpoznané žily. Od hodnoty 10 do 15 sa metóda stáva extrémne citlivou a rozpoznáva len veľmi výrazné žily, no bez žiadneho šumu. Od hodnoty 20 metóda nedokáže rozpoznať žiadne žily. Veľkým problémom bol exponenciálny nárast času potrebného na výpočet s rastúcou hodnotou parametru sigma (40 sekúnd pri sigma=20). Z toho dôvodu bola vo výsledku zvolená hodnota 8, ktorá potrebuje ≈ 7 sekúnd na vypočítanie.

Na všetky snímky ukázané na obrázkoch 6.3b-d boli použité *najlepšie nájdené parametre* pre dané metódy extrakcie, preto tieto snímky budú opisované ako referenčné pre daný extraktor.

Ako je vidno na obrázku 6.3b, metóda hlavného zakrivenia ukazuje priemerné schopnosti na extrakciu žilového vzoru z daného snímku. Do snímku zanáša minimum šumu, no nedokáže správne sledovať dlhšie žily.

Na obrázku 6.3c je výstup z metódy opakovaného sledovania čiary. Táto metóda narozdiel od vyššie spomínanej zanáša do snímku veľa šumu. Pri úprave parametrov tejto metódy **problém pretrváva a není možné získať vzor, ktorý je čistejší**. Metóda ale napriek tomu vykazuje známky správneho získania a zvýraznenia žily.

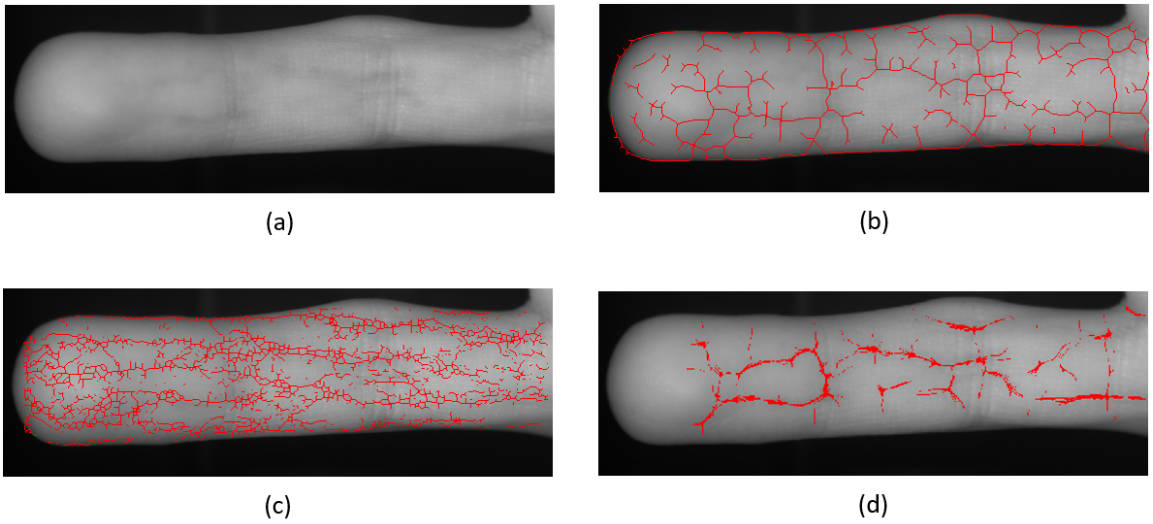
Posledná metóda maximálneho zakrivenia ukázaná na obrázku 6.3d dosahuje na tento typ snímku zďaleka najlepšie výsledky. Vykazuje **veľmi dobrú schopnosť nájdenia žily a jej následného sledovania**. Zároveň do mapy zanáša minimum šupu, na rozdiel od metódy opakovaného sledovania čiary.

Kvôli týmto vlastnostiam bola zvolená metóda **maximálneho zakrivenia**.

GLCM charakteristiky

Extrahovanie texturálnych charakteristík GLCM bolo zvolené oproti HOG kvôli schopnosti extrahovať viacero typov metrík v rôznych konfiguráciách. Týchto metrík bolo vo výsledku natoľko veľa, že bolo za potrebu z metrík vybrať len metriky, ktoré majú `najväčšiu klasifikačnú hodnotu`. Ako prvý krok výberu bolo obmedzenie počtu charakteristík, čo je opísané v časti 3.5.2. Zo šiestich zvolených Haralickových charakteristík a GLCM matíc vypočítaných vo všetkých často používaných uhloch, ktoré sú opísané na jednotkovej kružnici by výsledná sada obsahovala 110 prvkov, čo je ako vstup do SVM klasifikátora považované ako veľké množstvo.

Keďže ale nezáleží na smere, v ktorom je prevádzaný GLCM výpočet je možné obmedziť počet prvkov na polovicu, 48 z pôvodných 96. Táto vlastnosť bola testovaná a potvrdená výpočtom charakteristík vo všetkých uhloch a následné porovnanie hodnôt z uhlov, ktoré ležia oproti sebe na jednotkovej kružnici.



Obr. 6.3: Rôzne typy extrakčných metód aplikované na obrázok (a). Na obrázkoch je ukázaný žilový vzor získaný rôznymi metódami prahovania, ktorý je následne položený na originálny obrázok (b) Hlavné zakrivenie, (c) Opakované sledovania čiary, (d) Maximálne zakrivenie. (Pred aplikovaním metód bola na na snímok aplikovaná ekvalizácia histogramu HE + CLAHE).

Hodnoty v uhloch $60°, 90°, 120°$ vykazovali veľmi podobné výsledky pri všetkých testovaných snímkoch živého prsta, čo je pravdepodobne zapríčinené tým, že žily vo veľmi málo prípadoch dosahovali takéhoto uhlu. Napriek tomu boli vložené do výslednej sady prvkov, keďže pri aplikovaní metód na falzifikáty výsledky z týchto uhlov naberali dôležitejšie hodnoty.

Výsledným vektorom prvkov získaných z GLCM je teda vyššie spomínaných **48 hodnôt z pôvodných 96**, čo znižuje veľkosť celkovej sady prvkov a zrýchľuje čas na spracovanie a klasifikáciu snímku.

6.1 Zhodnotenie výkonnosti navrhnutej metódy

Po zaistení a implementovaní celej metódy boli prevedené testy a zaznamenané časové hodnoty ktoré ukazujú, ako optimálne je metóda navrhnutá.

Priemerná doba výpočtu sady prvkov pre jednu ruku, ktorá obsahuje 3 použiteľné prsty nadobúdala `30 sekúnd`, pričom snímky z ktorých bolo použiteľných prstov menej trvali o 7 sekúnd menej pre každý chýbajúci prst. Pri celkovej veľkosti databázy obsahujúcej 143 snímkov rúk, z ktorej metóda dokáže extrahovať a spracovať 294 samostatných prstov sa doba spracovania sady prvkov pre jednotlivé prsty bez použitia paralelného spracovania pohybovala v rozmedziach 100-110 minút. Priemerná doba na **výpočet jednej ruky sa teda v priemere pohybuje na 25 sekundách**. Pri použití paralelného spracovania rozdeleného na štyri vlákna bola doba spracovania štyri-krát kratšia, teda v rozmedzí 25-27 minút. Testovanie na viacerých vláknach z dôvodu stability systému nebolo prevedené, no jednalo by sa o dobu, ktorá sa dá vyjadriť pomocou rovnice 6.1,

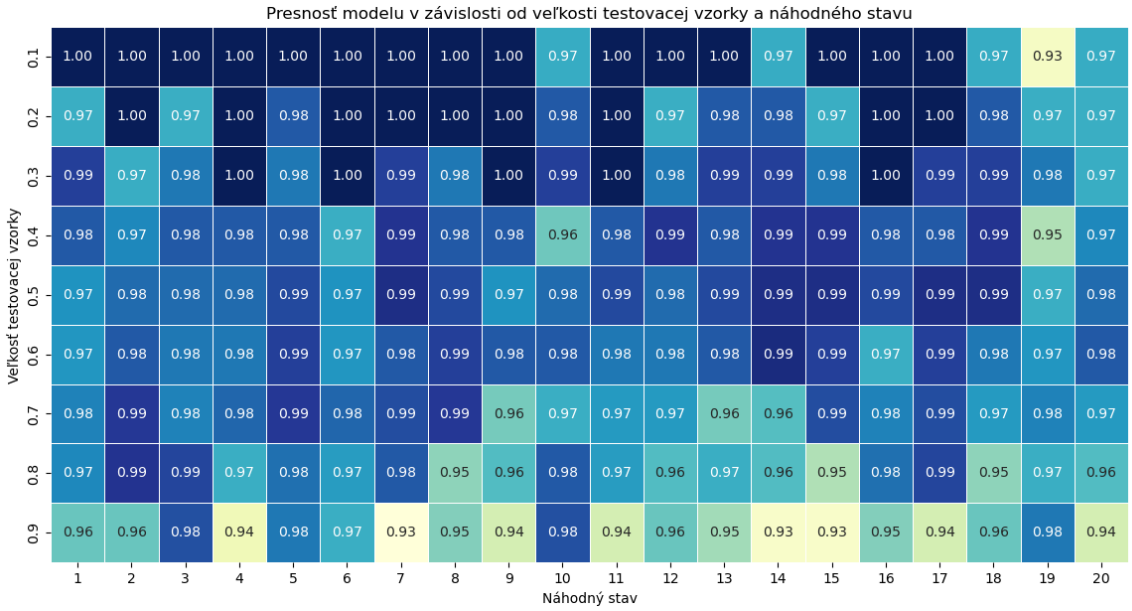
$$\approx time\_to\_process = \frac{n\_hands * \approx 25\ sec}{n\_of\_threads} \tag{6.1}$$

kde *n_hands* je počet snímkov rúk a *n_of_threads* je počet jadier použitých pri paralelizácií.

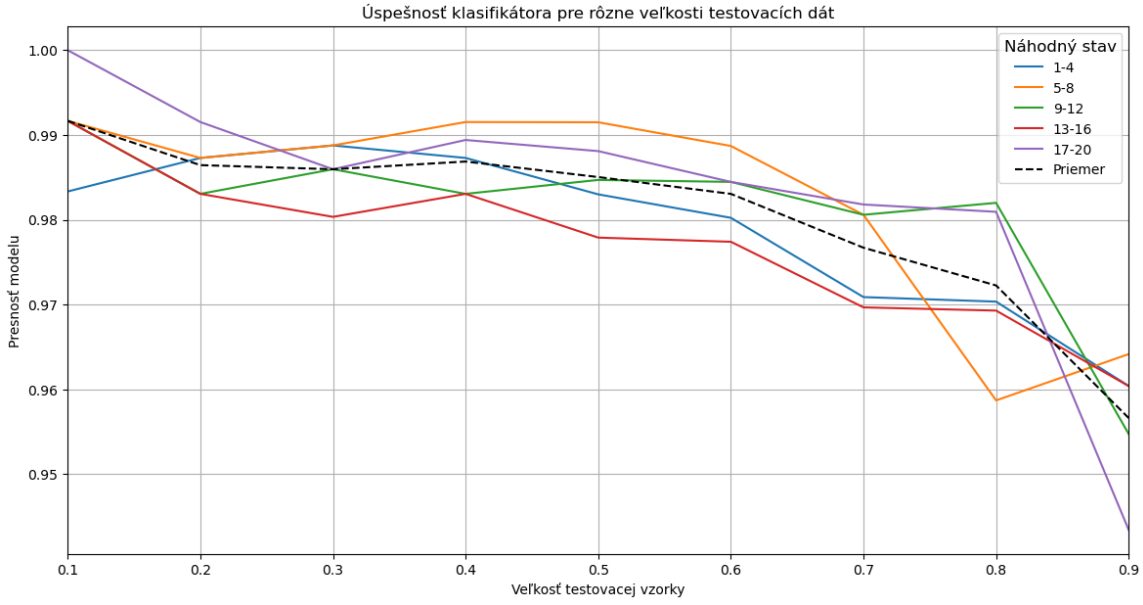
Celková úspešnosť detekcie prezentačných útokov je **závislá na pomere testovacích a trénovacích dát**, ako bolo popísané v časti 4.4.1. Na zistenie vhodného pomeru pre trénovanie klasifikátora a overenie úspešnosti klasifikácie bola sada prvkov rozdelená na rôzne pomery. Tieto pomery boli v rozsahu od 0,1 do 0,9 s krokom 0,1, teda deväť rôznych pomerov medzi trénovacími a testovacími dátami. Funkcia na rozdelenie dát používa parameter "random state", ktorý sa používa na inicializáciu generátora náhodných čísel. Zadaním čísla za tento parameter je zaistené, že výber prvkov v oboch sadách bude rovnaký pri opakovanom prevedení rozdelenia. V testovaní bolo použitých 20 čísel z intervalu <1,20>, ktoré boli dosadené za tento parameter. Na klasifikátor bolo použité lineárne jadro. Pri testovaní polynomického a RBF jadra bez použitia škálovania sady prvkov dosahovali `porovnateľných výsledkov` ako lineárne jadro, no po použití škálovania výsledky pri lineárnom jadre vykazovali priemerne lepšej úspešnosti ako u ostatných typov. Napriek tomu použitie škálovania pri všetkých typoch jadier vykazovalo v priemere 18 % zlepšenie.

Z každého rozdelenia sady prvkov bol natrénovaný a otestovaný SVM klasifikátor s lineárnym jadrom, ktorého úspešnosť bola zaznamenaná a zapísaná do grafu na obrázku 6.4, ktorá znázorňuje presnosť klasifikácie pri zvolených parametroch pomeru rozdelenia a "random state". Z grafu závislosti rozdelenia sady na obrázku 6.5 je vidno, že výsledky z klasifikátora vykazujú pozorovateľný trend, kde zvyšovanie veľkosti trénovacej sady koreluje s vyššou úspešnosťou klasifikácie. Priemerná hodnota ACER zo všetkých testovaných kombinácií parametrov dosiahla 97 %. Problematickejšie pre klasifikátor bolo zamenenie prezentačného útoku oproti prezentácií v dobrej viere, keďže v priemere APCER dosahoval 96 %, čo je o 2 % menej ako BPCER, ktoré dosahuje 98 %. Najväčší problém so zamenením prezentácie v dobrej viere a prezentačným útokom nastáva na snímkoch prsta, v ktorom *nie je dobre zaznamenaný žilový vzor* (nízky kontrast medzi žilou a prstom aj po ekvalizácií histogramu). V opačnom prípade mal klasifikátor problém s falzifikátmi ruky vytvorenými výtlačkom ruky na papieri, presnejšie na snímkoch obsahujúcich aj falzifikát žily.

Ako bolo spomínané v časti 4.4.1, pri veľkom pomere trénovacích dát klasifikátor nemusí byť dostatočne otestovaný a jeho relatívna úspešnosť nemusí byť taká vysoká, ako ukazuje meranie. Z toho dôvodu bola nastavená hranica rozdelenia, ktorá považuje klasifikátor za **dobre otestovaný pod hranicou 0,6**, teda pod 60 % pomeru sady prvkov použitej na trénovanie a nad 40 % sady prvkov použitej na testovanie. Pri rozdelení na 0,6 je pre testovanie v prípade 294 veľkej sady prvkov použitých 118 prstov na testovanie. Keďže je v sade prvkov veľký počet typov falzifikátov, početnosť jednotlivých snímkov rôznych typov týchto falzifikátov je malá a preto sa môže stať, že klasifikátor nemusí byť na daný falzifikát natrénovaný, alebo daný typ falzifikátu nemusí byť otestovaný. Napriek tomu ale klasifikátor `dokáže vo väčšine prípadov tieto snímky vyhodnotiť správne` ako prezentačný útok.



Obr. 6.4: Heatmapa ukazujúca úspešnosť klasifikátora pri rôznom rozdelení sady na trénovaciu a testovaciu a náhodného stavu (random state).



Obr. 6.5: Graf dokazujúci trend klasifikátora: Zväčšovaním testovacej sady sa znižuje úspešnosť klasifikácie, keďže sa zmenšuje veľkosť trénovacej sady.

Kapitola 7

Záver

Vďaka rýchlo rastúcemu záujmu používania biometrickej autentifikácie priamo úmerne rastie záujem o oklamanie biometrických systémov. V tejto práci boli priblížené možnosti prieniku do takýchto systémov spoločne s možnosťami ochrany pred týmito útokmi. Priblížené boli taktiež rôzne metódy na spracovanie a klasifikáciu použité pri návrhu biometrického systému obohatenom o detekciu prezentačných útokov, ktorej sa táto práca venovala.

Cieľom práce bolo nasnímať databázu falzifikátov a živých odtlačkov prstov obohatených o informácie žilového riečiska použitím experimentálneho zariadenia, ktoré je schopné zachytávať vzory žíl v prste za pomoci NIR nasvietenia. K tejto databáze bola navrhnutá metóda detekcie prezentačného útoku na experimentálne zariadenie. Pri riešení práce som si naštudoval literatúru zaoberajúcu sa spracovaním snímkov obsahujúce odtlačok prsta a žilové riečisko, rôzne algoritmy zaoberajúce sa detekciou živosti a prezentačných útokov na dané typy snímkov. Po získaní vstupných dát zo zariadenia som navrhol metódu, ktorej úlohou je zistiť, či bol pred snímač predložený falzifikát alebo vierohodný prst.

V rámci snímania bolo do databázy vložených 143 snímkov rúk, z ktorých bolo po prevedení segmentácie získaných 294 jednotlivých prstov, ktoré boli spracované a použité či už na trénovanie alebo na testovanie klasifikátora.

Po dôkladnom výbere a testovaní rôznych vhodných metód bola získaná metóda, ktorá vykazovala najlepšie výsledky. Táto metóda dosahovala presnosť ACER až do 97 % pri natrénovaní klasifikátora pomocou 178 spracovaných či už živých alebo umelých snímkov prstov (60 % dátovej sady). Metóda v priemere dosahovala úspešnosť APCER 96 % a BPCER 98 %.

Vytvorenú metódu by bolo možné naďalej upravovať a vylepšovať. Bolo by možné vytvoriť hardvérové a softvérové riešenie pre konštantné nasvietenie senzora NIR lúčmi zmenou intenzity NIR LED diód, prípadne zabráneniu prenikania vonkajšieho svetla pri snímaní, čím by boli dosiahnuté lepšie podmienky pre klasifikáciu. Rozšírením charakteristík získaných pri extrakcií prvkov by bolo možné presnejšie opísať predložený prst, čím by sa mohla zvýšiť úspešnosť klasifikácie. Ako posledné navrhnuté vylepšenie by bolo ku navrhnutej metóde implementovať modul na registráciu a verifikáciu daného snímku, čím by sa z navrhnutej metódy mohol stať plnohodnotný biometrický systém.

Literatúra

[1] Information technology—biometric presentation attack detection—part 1: framework. *International Organisation for Standardisation (2017) ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-1.* 2017.

[2] Information technology—biometric presentation attack detection—part 3: testing and reporting. *International Organisation for Standardisation (2017) ISO/IEC JTC1 SC37 Biometrics: ISO/IEC 30107-3.* 2017.

[3] Albregtsen, F., Nielsen, B. a Danielsen, H. Adaptive gray level run length features from class distance matrices. In: *Proceedings 15th International Conference on Pattern Recognition. ICPR-2000.* 2000, sv. 3, s. 738–741 vol.3. DOI: 10.1109/ICPR.2000.903650.

[4] Allinson, N., Sivarajah, J., Gledhill, I., Carling, M. a Allinson, L. Robust Wireless Transmission of Compressed Latent Fingerprint Images. *Information Forensics and Security, IEEE Transactions on.* Október 2007, zv. 2, s. 331 – 340. DOI: 10.1109/TIFS.2007.902684.

[5] Bansal, R., Sehgal, P. a Bedi, P. Minutiae Extraction from Fingerprint Images - a Review. *IJCSI International Journal of Computer Science Issues* [online]. arXiv. 2012, zv. 8, s. 74–85, [cit. 22-11-2022]. DOI: 10.48550/ARXIV.1201.1422. Dostupné z: https://arxiv.org/abs/1201.1422.

[6] Bhan, B. a Patel, S. Efficient Medical Image Enhancement using CLAHE Enhancement and Wavelet Fusion. *International Journal of Computer Applications.* Jún 2017, zv. 167, s. 1–5. DOI: 10.5120/ijca2017913277.

[7] Blanc, N. CCD versus CMOS – has CCD imaging come to an end? December 2003, s. 131–137.

[8] Cervantes, J., Garcia Lamont, F., Rodríguez Mazahua, L. a Lopez, A. A comprehensive survey on support vector machine classification: Applications, challenges and trends. *Neurocomputing* [online]. 2020, zv. 408, s. 189–215, [cit. 20-3-2023]. DOI: https://doi.org/10.1016/j.neucom.2019.10.118. ISSN 0925-2312. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0925231220307153.

[9] Chi Qin, L. a Teoh, S. S. An efficient method of HOG feature extraction using selective histogram bin and PCA feature reduction. *Advances in Electrical and Computer Engineering.* 2016, zv. 16, č. 4, s. 101–108.

[10] Cristianini, N. a Shawe Taylor, J. *An Introduction to Support Vector Machines and Other Kernel-based Learning Methods*. Cambridge University Press, 2000. ISBN 9780511801389.

[11] Davide, M., Dario, M., K., J. A. a Salil, P. *Handbook of Fingerprint Recognition*. 1. vyd. Springer, 2003. ISBN 978-0-387-21587-7.

[12] Davide, M., Dario, M., K., J. A. a Salil, P. *Handbook of Fingerprint Recognition*. 2. vyd. Springer, may 4 2009. ISBN 978-1-84882-254-2.

[13] Furumiya, M., Hatano, K., Nakashiba, Y., Murakami, I., Yamada, T. et al. A 1/2-in, 1.3 M-pixel progressive-scan CCD image sensor employing 0.25-μm gap single-layer poly-Si electrodes. *Solid-State Circuits, IEEE Journal of*. Január 2000, zv. 34, s. 1835 – 1842. DOI: 10.1109/4.808908.

[14] Haralick, R. M., Shanmugam, K. a Dinstein, I. Textural Features for Image Classification. *IEEE Transactions on Systems, Man, and Cybernetics*. 1973, SMC-3, č. 6, s. 610–621. DOI: 10.1109/TSMC.1973.4309314.

[15] Hartung, D. Vascular Pattern Recognition: And its Application in Privacy-Preserving Biometric Online-Banking Systems. In:. 2012. ISBN 978-82-93269-01-4. Dostupné z: http://hdl.handle.net/11250/144366.

[16] Himaga, H. O. M. *Encyclopedia of Biometrics*. 2. vyd. Boston, MA: Springer US, april 2015. 1626 s. ISBN 978-1-4899-7487-7. Dostupné z: https://doi.org/10.1007/978-1-4899-7488-4.

[17] Hsu, C.-w., Chang, C.-c. a Lin, C.-J. A Practical Guide to Support Vector Classification Chih-Wei Hsu, Chih-Chung Chang, and Chih-Jen Lin. [online]. November 2003, s. 1–16, [cit. 01-04-2023]. Dostupné z: https://www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf.

[18] Jain, A. K., Flynn, P. a Ross, A. A. *Handbook of Biometrics*. 1. vyd. Springer, 2008. ISBN 978-0-387-71041-9.

[19] Jain, A. K., Ross, A. A. a Nandakumar, K. *Introduction to Biometrics*. 1. vyd. Springer, Nov 2011. 312 s. ISBN 978-0-387-77326-1.

[20] Jain, R. a Kant, C. Attacks on Biometric Systems: An Overview. *International Journal of Advances in Scientific Research*. September 2015, zv. 1, s. 283–288. DOI: 10.7439/ijasr.v1i7.1975.

[21] Jiang, R., Al Maadeed, S., Bouridane, A., Crookes, D. a Beghdadi, A. *Biometric Security and Privacy*. 1. vyd. Springer, 2017. ISBN 978-953-307-489-4.

[22] Kauba, C., Prommegger, B. a Uhl, A. Combined Fully Contactless Finger and Hand Vein Capturing Device with a Corresponding Dataset. *Sensors*. November 2019, zv. 19, s. 5014. DOI: 10.3390/s19225014.

[23] Kaushal, N. a Kaushal, P. Human Identification and Fingerprints: A Review. *Journal of biometrics and biostatistics*. Január 2011, zv. 2, s. 5. DOI: 10.4172/2155-6180.1000123.

[24] Kolas, O., Farup, I. a Rizzi, A. Spatio-Temporal Retinex-Inspired Envelope with Stochastic Sampling: A Framework for Spatial Color Algorithms. *Journal of Imaging Science and Technology* [online]. Júl 2011, zv. 55, [cit. 12-3-2023]. DOI: 10.2352/J.ImagingSci.Technol.2011.55.4.040503. Dostupné z: https://doi.org/10.2352/j.imagingsci.technol.2011.55.4.040503.

[25] Kolberg, J., Gomez Barrero, M., Venkatesh, S., Ramachandra, R. a Busch, C. Presentation Attack Detection for Finger Recognition. In: *Handbook of Vascular Biometrics*. Springer International Publishing, 2020, s. 435–463. ISBN 978-3-030-27731-4. Dostupné z: https://doi.org/10.1007/978-3-030-27731-4_14.

[26] Löfstedt, T., Brynolfsson, P., Asklund, T., Nyholm, T. a Garpebring, A. Gray-level invariant Haralick texture features. *PLOS ONE* [online]. Public Library of Science. Február 2019, zv. 14, č. 2, s. 1–18, [cit. 20-3-2023]. DOI: 10.1371/journal.pone.0212110. Dostupné z: https://doi.org/10.1371/journal.pone.0212110.

[27] May Sanjaya, I. M., Kesiman, M. a I Made, P. Evaluation of contrast enhancement methods on finger vein NIR images. *Journal of Physics: Conference Series*. Marec 2021, zv. 1810, s. 012035. DOI: 10.1088/1742-6596/1810/1/012035.

[28] Miura, N., Nagasaka, A. a Miyatake, T. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. *Machine Vision and Applications* [online]. Springer Science and Business Media LLC. Oct 2004, zv. 15, č. 4, s. 194–203, [cit. 11-2-2023]. DOI: 10.1007/s00138-004-0149-2. Dostupné z: http://dx.doi.org/10.1007/s00138-004-0149-2.

[29] Miura, N., Nagasaka, A. a Miyatake, T. Extraction of Finger-Vein Patterns Using Maximum Curvature Points in Image Profiles. In:. Január 2005, E90D, s. 347–350. DOI: 10.1093/ietisy/e90-d.8.1185.

[30] Mohanaiah, P., Sathyanarayana, P. a GuruKumar, L. Image Texture Feature Extraction Using GLCM Approach. In: *International Journal of Scientific and Research Publications*. Marec 2013, sv. 3. ISSN 2250-3153.

[31] Msiza, I., Mistry, J., Leke Betechuoh, B., Nelwamondo, F. a Marwala, T. *On the Introduction of Secondary Fingerprint Classification*. Júl 2011. ISBN 978-953-307-489-4.

[32] Nguyen, D. T., Yoon, H. S., Pham, T. D. a Park, K. R. Spoof Detection for Finger-Vein Recognition System Using NIR Camera. *Sensors* [online]. 2017, zv. 17, č. 10, [cit. 12-12-2022]. DOI: 10.3390/s17102261. ISSN 1424-8220. Dostupné z: https://www.mdpi.com/1424-8220/17/10/2261.

[33] O'Gorman, L. An overview of fingerprint verification technologies. *Information Security Technical Report* [online]. 1998, zv. 3, č. 1, s. 21–32, [cit. 23-11-2022]. DOI: https://doi.org/10.1016/S1363-4127(98)80015-0. ISSN 1363-4127. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1363412798800150.

[34] Otsu, N. A Threshold Selection Method from Gray-Level Histograms. *IEEE Transactions on Systems, Man, and Cybernetics*. 1979, zv. 9, č. 1, s. 62–66. DOI: 10.1109/TSMC.1979.4310076.

[35] Patel, O., Maravi, Y. a Sharma, S. A Comparative Study of Histogram Equalization Based Image Enhancement Techniques for Brightness Preservation and Contrast Enhancement. *Signal & Image Processing : An International Journal*. November 2013, zv. 4, s. 11–25. DOI: 10.5121/sipij.2013.4502.

[36] Pisano, E., Zong, S., Hemminger, B., DeLuca, M., Johnston, R. et al. Contrast limited adaptive histogram equalization image processing to improve the detection of simulated spiculations in dense mammograms. *Journal of digital imaging* [online]. November 1998, zv. 11, č. 4, s. 193—200, [cit. 12-3-2023]. DOI: 10.1007/bf03178082. ISSN 0897-1889. Dostupné z: https://europepmc.org/articles/PMC3453156.

[37] Rossi, V. *Digital Fourier Holographic Microscopy and Potential Applications Towards the Design of Photodynamic Therapy of Osteosarcoma*. 2015. Dizertačná práca. Oregon State University. https://ir.library.oregonstate.edu/concern/graduate_thesis_or_dissertations/6h440x00s.

[38] Sastry, S., Kumari, T., Rao, C., Mallika, K., Lakshminarayana, S. et al. Transition Temperatures of Thermotropic Liquid Crystals from the Local Binary Gray Level Cooccurrence Matrix. *Advances in Condensed Matter Physics*. Január 2012, zv. 2012. DOI: 10.1155/2012/527065.

[39] Seitz, P. Solid-State Image Sensing. In:. December 2000, s. 111–151. DOI: 10.1016/B978-012379777-3/50006-6. ISBN 9780123797773.

[40] Sidiropoulos, G. K., Kiratsa, P., Chatzipetrou, P. a Papakostas, G. A. Feature Extraction for Finger-Vein-Based Identity Recognition. *Journal of Imaging*. 2021, zv. 7, č. 5. DOI: 10.3390/jimaging7050089. ISSN 2313-433X. Dostupné z: https://www.mdpi.com/2313-433X/7/5/89.

[41] Wang, K., Ma, H., Popoola, O. a Liu, J. Finger vein recognition. In:. Jún 2011. DOI: 10.5772/18025. ISBN 978-953-307-618-8.

[42] Yousefi, J. Image binarization using Otsu thresholding algorithm. *Ontario, Canada: University of Guelph*. 2011, zv. 10, s. 4. DOI: 10.13140/RG.2.1.4758.9284.

[43] Zhang, K., Zeng, Q. a Yu, X. ROSD: Refined Oriented Staged Detector for Object Detection in Aerial Image. *IEEE Access*. Apríl 2021, PP, s. 11. DOI: 10.1109/ACCESS.2021.3076596.

Príloha A

Obsah přiloženého paměťového média

Priložené pamäťové médium má nasledujúcu štruktúru:

- priečinok `/app`, obsahujúci zdrojové súbory navrhnutej metódy spoločne s databázou použitou pri implementácií a testovaní. Priečinok má nasledujúcu štruktúru:
  - súbor `/app/BP.ipynb`, obsahujúci vzorové volania funkcií navrhnutej metódy spoločne s popisom jednotlivých častí.
  - priečinok `/app/src/`, obsahujúci zdrojové súbory, ktoré obsahujú implementáciu metódy detekcie prezentačného útoku.
  - priečinok `/app/results/`, obsahujúci natrénovaný SVM klasifikátor a spracované snímky z priečinku `/app/db/`.
  - priečinok `/app/db/`, obsahujúci snímky použité na prezentáciu v dobrej viere a pri prezentačnom útoku. Priečinok má nasledujúcu štruktúru:
    - priečinok `/app/db/bona_fide`, obsahujúci snímky reprezentujúce prezentáciu v dobrej viere.
    - priečinok `/app/db/presentation_attack`, obsahujúci snímky reprezentujúce prezentačný útok.
  - súbor `/app/README.md`, obsahujúci popis inštalácie a popis jednotlivých zdrojových súborov v priečinku `/app/src/`.
  - súbor `/app/requirements.txt`, obsahujúci externé knižnice použité v práci.
- priečinok `/doc`, obsahujúci zdrojové súbory a texty v jazyku LaTeX pre vytvorenie správy vo formáte *PDF*.
- súbor `xondru18.pdf`, obsahujúci technickú správu.