



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

DEPARTMENT OF INTELLIGENT SYSTEMS

ANALÝZA FALZIFIKÁTŮ OTISKŮ PRSTŮ VYTVOŘENÝCH Z VYPALOVANÉ FORMY

ANALYSIS OF FINGERPRINT SPOOFS CREATED FROM MOLD DONE BY BURNING TECHNIQUE

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

TERÉZIA SOCHOVÁ

VEDOUcí PRÁCE

SUPERVISOR

Ing. ONDŘEJ KANICH, Ph.D.

BRNO 2021

Zadání bakalářské práce



Studentka: **Sochová Terézia**
Program: Informační technologie
Název: **Analýza falzifikátů otisků prstů vytvořených z vypalované formy**
Analysis of Fingerprint Spoofs Created from Mold Done by Burning
Technique
Kategorie: Bezpečnost
Zadání:

1. Prostudujte literaturu týkající se biometrického rozpoznávání podle otisků prstů a falzifikátů otisků prstů, soustředte se na metody tvorby formy pro falzifikáty. Seznamte se s generováním syntetických otisků prstů.
2. S využitím vhodných materiálů vytvořte několik forem pro tvorbu falzifikátů otisků pomocí laserového vypalování.
3. Formy z předchozího kroku využijte na tvorbu falzifikátů, ty nasnímejte s využitím dostupných senzorů (např. SecuGen, DinoLite).
4. Navrhněte metodu analýzy rozdílů mezi zdrojovým otiskem prstu a nasnímaného falzifikátu.
5. Implementujte navržený algoritmus z předchozího bodu.
6. Otestujte algoritmus z předchozího bodu na vytvořené sadě z bodu 3. Pomocí vhodného algoritmu na zjištění kvality otisků prstů (např. VeriFinger, NFIQ) dále analyzujte kvalitu falzifikátů.
7. Dosazené výsledky shrňte a diskutujte. Uveďte možná 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.
- Kanich, O., Mézl, M., Drahanský, M.: *Creative Materials Used for Fingerprint Spoofs*, Proceedings of International Workshop on Biometrics and Forensics 2018, IEEE, Sassari, 2018, p. 8.
- Champod, C., Espinoza, M.: *Forgeries of Fingerprints in Forensic Science*, Handbook of Biometrics Anti-Spoofing, Springer, 2014, pp. 13-34, ISBN 978-1-4471-6523-1.

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. listopadu 2020

Datum odevzdání: 12. května 2021

Datum schválení: 11. listopadu 2020

Abstrakt

Táto práca je venovaná výrobe a analýze falzifikátov odtlačkov prstov z vypalovanej formy. Cieľom práce je vytvoriť falzifikáty odtlačkov prstov z rôznych materiálov a následne navrhnuť a implementovať algoritmus, ktorý falzifikáty porovná so vzorovými odtlačkami. Falzifikáty sú vyrobené pomocou foriem z bukového dreva. Na výrobu falzifikátov je použitá plastelína, silikón a tekutý latex. Analýza rozdielov medzi falzifikátmi a vzorovými odtlačkami prebieha na základe extrakcie markantov a ich následným spracovaním. Výsledkom sú tri sledované metriky, konkrétne počet a typ markantov, počet spárovaných markantov a priemerný rozdiel vzdialenosti medzi markantmi falzifikátu a markantmi odtlačku. Vytvorený program je otestovaný pomocou databázy vyrobených falzifikátov. Výsledky aplikácie sú porovnané s výsledkami programu VeriFinger. Oba programy sa zhodujú, že najkvalitnejšie vlastnosti vykazujú falzifikáty zo silikónu.

Abstract

This work is devoted to the production and analysis of fingerprint spoofs created from mold using a burning technique. The aim of this work is to create fingerprints spoofs from different materials and then to design and to implement an algorithm that compares spoofs with model fingerprints. Spoofs are made using beech wood molds. In order to create the fingerprints, plasteline, silicone and liquid latex are used. The analysis of the differences between fingerprint spoofs and their real fingerprints is based on the minutiae extraction and on their subsequent processing. The results of analysis are represented by three monitored metrics: number and type of minutiae, number of paired minutiae and average distance difference between fingerprint spoof minutiae and real fingerprint minutiae. The created program is tested using a database of produced fingerprint spoofs. The results of the program are compared with the results of the VeriFinger application. Both programs agreed that spoofs made by silicone are the ones of the highest quality.

Kľúčové slová

odtlačok prsta, falzifikát odtlačku prsta, markanty, výroba foriem, laser, syntetické odtlačky, analýza falzifikátov

Keywords

fingerprint, fingerprint spoof, minutiae, mold manufacturing, laser, synthetic fingerprints, fingerprint spoof analysis

Citácia

SOCHOVÁ, Terézia. *Analýza falzifikátů otisků prstů vytvořených z vypalované formy*. Brno, 2021. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Ondřej Kanich, Ph.D.

Analýza falzifikátů otisků prstů vytvořených z vypalované formy

Prehlásenie

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně pod vedením pana Ing. Ondřeje Kanicha, Ph.D. Uvedla jsem všechny literární prameny, publikace a další zdroje, ze kterých jsem čerpala.

.....
Terézia Sochová
10. mája 2021

Podakovanie

V prvom rade by som chcela poďakovať svojmu vedúcemu Ing. Ondřejovi Kanichovi, Ph.D. za rady, odbornú pomoc, ústretovosť a čas, ktorý mi venoval pri vypracovaní tejto práce. Rovnako by som chcela poďakovať celej svojej rodine za podporu, nie len pri písaní bakalárskej práce, ale aj počas celej doby štúdia.

Obsah

1	Úvod	2
2	Odtlačky prstov	3
2.1	Úvod do biometrie	3
2.2	Charakteristika odtlačku prsta	6
2.3	Spracovanie odtlačku prsta	10
2.4	Rozpoznávanie odtlačkov prstov	11
3	Falzifikáty a syntetické generovanie odtlačkov prstov	14
3.1	Falzifikáty odtlačkov prstov	14
3.2	SFINGE metóda	16
4	Tvorba foriem a výroba falzifikátov	19
4.1	Tvorba foriem metódou vypalovania	19
4.2	Výroba falzifikátov odtlačkov prstov	23
5	Návrh algoritmov analýzy	27
5.1	Predspracovanie	27
5.2	Extrakcia markantov	30
5.3	Porovnanie odtlačku a falzifikátu	32
6	Implementácia	36
6.1	Implementačný jazyk a vývojové prostredie	36
6.2	Štruktúra programu	36
7	Vyhodnotenie	41
7.1	Vyhodnotenie kvality na základe počtu markantov	41
7.2	Vyhodnotenie kvality na základe priemerného rozdielu vzdialenosti	42
7.3	Vyhodnotenie kvality na základe počtu zhodných markantov	44
7.4	Vyhodnotenie zhody pomocou VeriFingeru	45
8	Záver	47
	Literatúra	49
A	Obsah priloženého pamäťového média	52

Kapitola 1

Úvod

Biometria, ako spôsob identifikácie človeka, sa každým rokom stáva populárnejšou, v porovnaní s tradičnejšími spôsobmi ako sú heslá alebo ID karty, u ktorých dochádza k úpadku. Jeden z hlavných dôvodov, prečo je biometria v poslednej dobe obľúbenou, je fakt, že prináša nové typy technológií, ktoré sú pre používateľov pohodlné na používanie. Na overenie identity sú postačujúce časti ľudského tela. Nie je potrebné, aby používateľ so sebou nosil kartu alebo si pamätal heslo. Spomedzi rôznych techník používaných na overovanie (tvár, dúhovka, odtlačok ruky) patria metódy založené na získavaní odtlačkov prstov k najrozšírenejším a rýchlo sa rozvíjajúcim. Vďaka tomu, že každý prst má vzor, ktorý je jedinečný, môžeme ľudí od seba jednoducho a rýchlo odlíšiť. Ruka v ruke s úspechom a vyvíjaním rôznych inovatívnych spôsobov, ako skvalitniť overovanie pomocou odtlačkov prstov, prichádza aj mnoho pokusov na oklamanie týchto systémov. Odtlačky človek zanecháva pri kontakte s povrchom rôznych materiálov. Pre falšovateľa preto nie je zložité získať odtlačok a následne z neho vytvoriť falzifikát. Motiváciou pre falšovanie odtlačkov je určite aj fakt, že odtlačky prstov sú v dnešnej dobe používané ako prístup do internetového bankovníctva, či k platbám a osobným údajom. Napriek tomu, že kvalita skenerov stúpa a často sa používa detekcia živosti, stále existujú prípady, kedy falšovatelia dokážu vďaka falzifikátom prísť k neoprávneným údajom. Výskum a testovanie odolnosti skenerov voči falzifikátom je preto stále potrebný. Cieľom tejto bakalárskej práce je vytvorenie falzifikátov z rôznych materiálov a ich následné porovnanie voči vzorovému odtlačku prsta.

Kapitola 2 vysvetľuje základnú teóriu potrebnú pre pochopenie ďalšieho textu. V prvej časti sa zameriava na biometriu ako celok. V druhej časti vysvetľuje základné termíny a rozdelenia odtlačkov prstov. Tretia časť opisuje postup spracovania a rozpoznávania odtlačkov prstov. Kapitola 3 je venovaná falzifikátom odtlačkov prstov a metóde SFinGe. Prvá časť podáva prehľad o tom, aké materiály sa dnes používajú na výrobu falzifikátov. Druhá časť ponúka bližší pohľad na syntetické generovanie odtlačkov prstov. V kapitole 4 sa začína praktická časť práce. Čitateľ sa dozvie o príprave a výrobe foriem a o výrobe falzifikátov. V tejto kapitole sú zhrnuté výsledky, ktoré boli odpozorované pri výbere vhodného materiálu na výrobu foriem. Kapitola 5 popisuje návrh, akým spôsobom budú vytvorené falzifikáty spracované a porovnané so vzorovými odtlačkami. Kapitola 6 je venovaná implementácii a používateľskému rozhraniu. Opisuje spôsoby, prostriedky, knižnice a algoritmy, ktoré boli použité na vytvorenie programu ktorý porovnáva falzifikáty a vzorové odtlačky. Kapitola 7 hodnotí a porovnáva výsledky z vytvoreného programu a aplikácie VeriFinger. Kapitola 8 je záverom práce, kde sú zhrnuté výsledky a navrhnuté možné rozšírenia.

Kapitola 2

Odtlačky prstov

Predtým ako budú vytvárané samotné falzifikáty, je potrebné sa zoznámiť so základnou teóriou odtlačkov prstov. Táto kapitola v prvej časti podáva informácie o biometrických systémoch a biometrických technikách. Popisuje výhody a nevýhody v porovnaní s ostatnými technikami a vysvetľuje rozdiel medzi často zamieňanými pojmami identifikácia a verifikácia. Druhá časť kapitoly vysvetľuje základné termíny z oblasti odtlačkov prstov, ktoré budú odrazovým mostíkom pri vytváraní a analýze falzifikátov odtlačkov prstov. Kapitola obsahuje rozdelenia odtlačkov prstov podľa spôsobu získavania či vzoru, ktorý sa na odtlačku nachádza. Koniec kapitoly je venovaný spôsobu nasnímania, spracovania a porovnávanía odtlačkov.

2.1 Úvod do biometrie

Pojem biometria je definovaný ako veda, ktorá určuje identitu človeka na základe rôznych typov vlastností danej osoby. Vlastnosti môžu byť fyzické, chemické alebo behaviorálne [16]. Výraz biometria má pôvod v Grécku. Môžeme ho rozdeliť na dve významové slová. Slovo „bios“ znamená život a slovo „metron“ prekladáme ako mierka, takže hovoríme o takzvanom „meraní života“. [11]

Ako každý systém, tak aj biometrický systém má svoje výhody a nevýhody. Za základné výhody biometrie sa považuje zvýšenie bezpečnosti systému a odradenie útočníka od napadnutia tohto systému. Za ďalšiu výhodu považujeme zníženie počtu pokusov o poprenie vlastnej identity. Biometrické vlastnosti sú pre každého jedinca unikátne. Fyzické a behaviorálne rysy sú súčasťou nášho chovania alebo vzhľadu. Oproti overovaniu pomocou hesla či čipu majú výhodu, že si ich nemusíme pamätať, poprípade, že ich nie je možné stratiť, čím sa zároveň zvyšuje pohodlie používania pre ľudského jedinca. [11]

Biometrické systémy majú aj svoje nevýhody a sú napadnuteľné. Sú vytvárané stále nové spôsoby ako je možné systém oklamať použitím rôznych falzifikátov, čoho dôsledkom je nemožnosť detekcie živosti. V biometrii, ako bolo vyššie spomenuté, sa používajú vlastnosti, ktoré sú súčasťou ľudského tela a identity človeka a tým je porušené súkromie. Poslednými podstatnými nevýhodami sú nejednoznačné skóre porovnania pri výstupe a nemožnosť zmeny alebo anulovania vlastnosti v prípade odhalenia. [11]

2.1.1 Biometrický systém a jeho vlastnosti

Biometrický systém je sústava, ktorá umožňuje rozpoznanie určitej charakteristiky jedinca pomocou biometrických údajov a matematických algoritmov [12]. Systém vyberie množinu

potrebných informácií z danej vlastnosti, porovná extrahované rysy s dátami uloženými v databáze a vykoná akcie na základe výsledku porovnania. Biometrický systém je rozdelený na štyri základné moduly, ktorých práca je popísaná nižšie. [16]

- **Senzorový modul** — prvou úlohou je nasnímať dáta danej biometrickej vlastnosti, k čomu je potrebný skener, poprípade čítačka. S týmto modulom je v styku aj používateľ, preto je podstatné vytvorenie vhodného používateľského rozhrania pre tento modul. Nekvalitné rozhranie môže viesť k odmietnutiu používania. [16]
- **Modul určujúci kvalitu a vykonávajúci extrakciu dát** — najskôr zhodnotí kvalitu nasnímaných biometrických dát, aby sa určila vhodnosť dát pre následné spracovanie. Ak sú nasnímané dáta príliš nekvalitné, tak používateľ je požiadaný o opätovné nasnímanie danej biometrickej vlastnosti. Následne sú dáta spracované tak, aby boli zvýraznené potrebné časti na porovnávanie a nepotrebné časti odstránené. [16]
- **Porovnávací modul** — spracováva už extrahované dáta a porovnáva ich s uloženými šablónami. Výsledkom je skóre, ktoré udáva výšku zhody. Napríklad pri biometrických systémoch založených na odtlačkoch prstov sa porovnáva počet zhodných markantov. Porovnávací modul obsahuje aj modul pre vytváranie rozhodnutí, kde sa na základe vypočítaného skóre potvrdí alebo zamietne identita. [16]
- **Databázový modul** — obsahuje databázu, ktorá uchováva všetky biometrické informácie slúžiace na porovnávanie alebo vyhľadávanie nasnímaných biometrických vlastností. [16]

Pri rozhodovaní, aký biometrický systém bude použitý a s akou kombináciou vlastností sa bude pracovať, je vhodné definovať charakteristiky biometrických vlastností. Existuje 8 základných vlastností, ktoré bývajú použité pri výbere vhodného systému na základe preferencií: [11]

1. **Univerzálnosť** — táto charakteristika biometrickej vlastnosti hovorí o tom, že každý zdravý jedinec je obdarený touto vlastnosťou.
2. **Jedinečnosť** — pre každého jedinca musí byť táto vlastnosť unikátna. Nemôže existovať viacero jedincov z identickou vlastnosťou.
3. **Trvácnosť** — je dôležité, aby sa táto charakteristika nemenila s časom.
4. **Výkonnosť** — je spojená s charakteristikou trvácnosti. Hovorí o tom, že vlastnosť sa s časom a starnutím jedinca nesmie zmeniť, inak dôjde k zníženej presnosti systému a zníženiu výkonu.
5. **Merateľnosť** — popisuje, či sa dá vlastnosť získať jednoducho a či existujú spôsoby a prístroje, ktorými sa dá zachytiť a preniesť do digitálnej formy.
6. **Bezpečnosť** — určuje v akej miere je vlastnosť odolná voči falšovaniu.
7. **Nákladnosť** — medzi charakteristiky je zaradená aj finančná náročnosť vybraného biometrického systému.
8. **Prijateľnosť** — charakteristika, ktorá hovorí o tom, ako sú jedinci ochotní poskytnúť biometrickú vlastnosť.

Na základe týchto charakteristík je vytvorená tabuľka 2.1, ktorá spája v riadkoch biometrické vlastnosti a v stĺpcoch definované charakteristiky. Ponúka obraz o vhodnom použití jednotlivých vlastností pri vytváraní biometrického systému. Na začiatku sú stanovené ciele, čo sa požaduje od biometrického systému. Podľa potrieb je vybraná biometrická vlastnosť, ktorá spĺňa najväčší počet podmienok. Ak je systém zameraný na bezpečnosť na najvyššej úrovni, medzi najvhodnejšie vlastnosti budú podľa tabuľky 2.1 patriť odtlačok prsta alebo sietnica oka. Naopak, ak sa bude zameriavať na ochotu jedincom nasnímať biometrickú vlastnosť, tak sietnicu oka, aj keď je bezpečná, nemôžeme brať do úvahy. [11]

Tabuľka 2.1: Charakteristiky biometrických vlastností (o - vysoká, x - nízka, * - stredná). Prevzaté a upravené z [11].

	U	J	T	V	M	B	N	P
Tvár	o	x	*	x	o	x	x	o
Odtlačok prsta	*	o	o	o	*	o	x	*
Ruka	*	*	*	*	o	*	*	*
Sietnica oka	o	*	*	o	x	o	o	x
Podpis	x	x	x	x	o	x	x	o
Hlas	*	x	x	x	*	x	x	o

2.1.2 Identifikácia a verifikácia

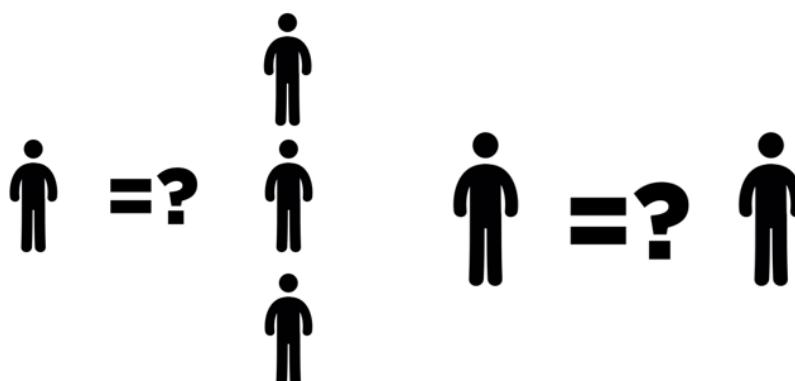
Každý človek má vlastnosti ako je tvar postavy, farba očí, intonácia hlasu, špecifické črty tváre či chôdza, na základe ktorých ho vedia iní jedinci spoznať. Tieto vlastnosti tvoria identitu človeka. Identita pochádza z latinského slova „identitas“, ktoré je odvodené z „idem“, čo znamená rovnaký. Identita je definovaná ako jednoznačná charakteristika každého jedinca. Súčasťou identity je aj DNA, pretože neexistujú na svete dvaja jedinci, ktorým by sa DNA na 100 % zhodovala. [11] [23]

Vďaka tomu, že každého identita je jedinečná, môže byť použitá na overovanie. Pri overovaní identity je dôležité vedieť rozdiel medzi pojmi autentizácia a autorizácia. Autentizácia je proces, ktorý overuje, či je daná osoba tou, za ktorú sa v systéme vydáva. Autorizácia sa vykonáva po úspešnej autentizácii, kedy sú danej osobe pridelené práva a prístupy na prácu s daným systémom. [31]

Pri overovaní identity, existujú dva spôsoby autentizácie. Je to identifikácia a verifikácia. Identifikácia, ako názov naznačuje, slúži k zisteniu identity osoby. V procese identifikácie sa porovnáva nasnímaná biometrická vlastnosť so všetkými referenčnými vzorkami, ktoré už sú uložené v databáze. Ak sa zhoduje s nejakou referenčnou vzorkou, tak identifikácia bola úspešná, inak končí neúspechom. Identifikácia môže byť vyjadrená vzťahom 1:N, kde 1 zodpovedá nasnímanej vlastnosti a N predstavuje všetky referenčné vzorky. Identifikácia odpovedá na otázku „Kto to je?“. Nevýhodou identifikácie je časová náročnosť, ktorá sa prejavuje hlavne pri rozsiahlych databázach. Takéto databázy sú často rozdelené na podkategórie podľa určitej biometrickej vlastnosti. [11] [31]

Pod pojmom verifikácia sa rozumie proces porovnávania nasnímanej vlastnosti s jednou referenčnou vzorkou. Systému je poskytnutá elektronická identita. Vďaka poskytnutej identite je v databáze vyhladaný záznam a na základe verifikácie dôjde k overeniu fyzickej identity. Výsledkom je potvrdenie nájdenia zhody alebo zamietnutie identity a odoprenie prístupu. Tento pojem môžeme vysvetliť aj vzťahom 1:1, kde je porovnávaná jedna vstupná

nasnímaná vlastnosť s jedným záznamom z databázy. Rozdiel medzi identifikáciou a verifikáciou je znázornený na obrázku 2.1. [11] [31]



Obr. 2.1: Rozdiel medzi identifikáciou (vľavo) a verifikáciou (vpravo)

2.2 Charakteristika odtlačku prsta

Odtlačky prstov sú rozdelené podľa druhu. Druh určuje, akým spôsobom bol odtlačok získaný. Prvý druh je odtlačok *rolovaný* [17], ktorý vzniká nafarbením prsta z vnútornej strany farbivom a jeho následným odtlačením. Pri odtlačení sa prstom pohybuje v smere od tela. Týmto spôsobom je získaný rozsiahly odtlačok prsta zo všetkých jeho strán. Druhý druh je odtlačok *pichaný* [17], ktorý je založený na odtlačení iba prednej strany prsta. Na zanechanie stopy sa ako v predchádzajúcom spôsobe využíva pofarbenie kontrastnou farbou. Tento spôsob sa najviac používa na snímanie odtlačkov prstov. Posledným druh je *latentný*. Je získavaný z odtlačku, ktorý bol zanechaný na skúmaných predmetoch [17]. Tieto odtlačky sa získavajú pomocou naprašovacích materiálov a používajú sa hlavne v oblasti kriminalistiky. Obrázok 2.2 zobrazuje všetky tri druhy odtlačkov. [17]

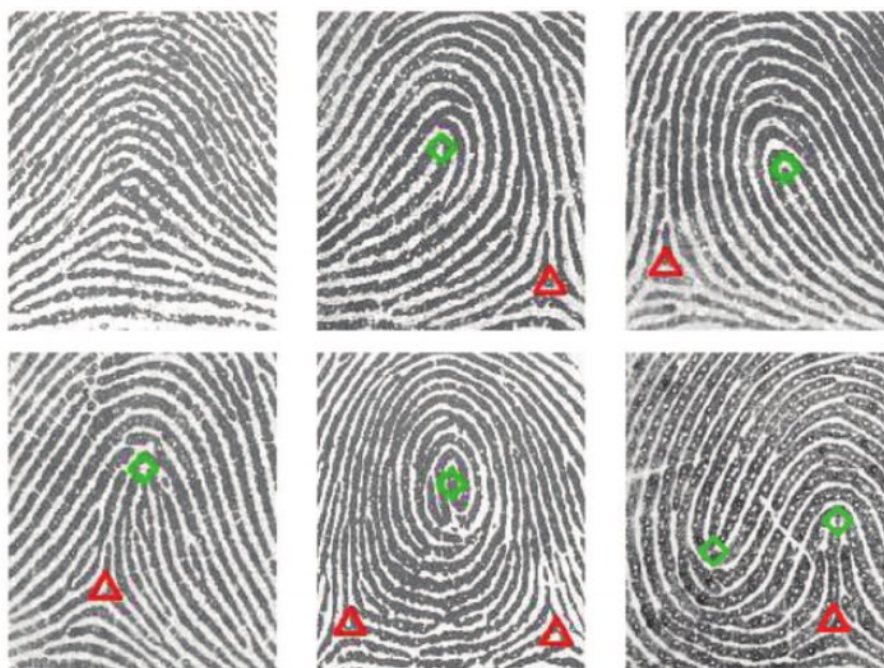


Obr. 2.2: Druhy odtlačkov prstov zľava rolovaný, pichaný, latentný. Prevzaté z [17]

Za jeden z najdôležitejších pojmov je v oblasti odtlačkov prstov považovaný pojem *papilárna línia* [19]. Papilárne línie vznikajú v štvrtom mesiaci vývoja dieťaťa a po zvyšok

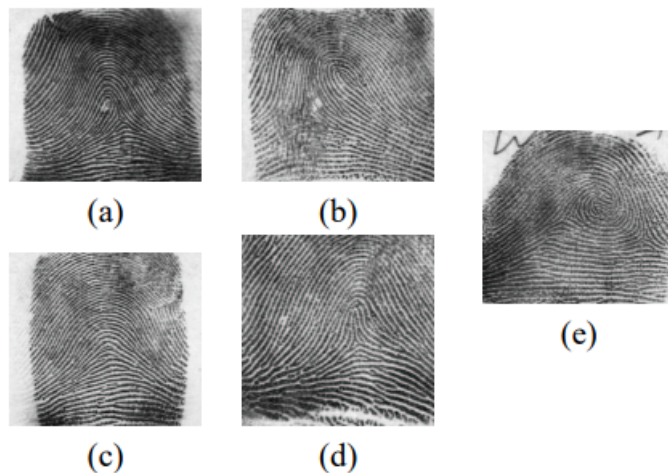
života ostávajú rovnaké [7]. Odtlačok prsta je tvorený zachytením niekoľkých desiatok papilárnych línií [19]. Papilárne línie sú ryhy na brušku prsta, ktoré sú viditeľné voľným okom. Nachádzajú sa v najvrchnejšej vrstve kože, nazývanej epidermis. Šírka papilárnej línie je v rozmedzí od 0,2 do 0,6 milimetrov a jej výška je od 0,1 do 0,4 milimetrov. [19]

Odtlačok prsta obsahuje špeciálne body nazývané body singularity. Základné pochopenie týchto pojmov je dôležité, aby mohla byť pri odtlačku prsta definovaná trieda. Body singularity tvoria 2 základné pojmy: *delta* a *jadro* [11]. Delta je bod na odtlačku prsta, v ktorom sa papilárne línie rozdeľujú do troch smerov. Delta sa často nachádza na okrajoch odtlačku prsta. Každý odtlačok môže obsahovať viac ako jednu deltu. Jadro je definované ako stred odtlačku prsta, aj keď nemusí zodpovedať stredu nasnímaného obrázku. Jadro sa nachádza na najviac spodnej konkávnej papilárnej línii. Obrázok 2.3 zobrazuje body singularity na rôznych odtlačkoch prstov. Pre úplnosť je definovaný aj pojem *typové línie* [11]. Typové línie ohraničujú priestor medzi papilárnou líniou, ktorá patrí k delte a zároveň je k delte najspodnejšiou a papilárnou líniou, ktorá je najvrchnejšou a stále patrí k jadrú. [11]



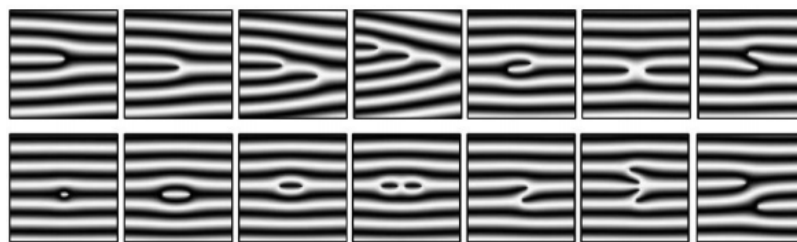
Obr. 2.3: Zachytené body singularity na rôznych snímkach odtlačkov prstov. Delta – červený trojuholník, jadro – zelená kružnica. Prevzaté z [15].

Po pospájaní jednotlivých papilárnych línií vznikajú obrazce. Podľa týchto obrazcov sú odtlačky prstov rozdelené do určitých tried. Vďaka rozdeleniu odtlačkov prstov do tried je jednoduchšie odhaliť, že dve vzorky nie sú zhodné. Ak odtlačok patrí do inej triedy, je okamžite odmietnutý [19]. Klasifikácie tried vznikli podrobným skúmaním geometrických vlastností papilárnych línií. Podľa Henryho klasifikácie sú odtlačky prstov rozdelené do 5 základných tried. Sú nimi *oblúk* (arch), *klenutý oblúk* (tended arch), *špirála* (whorl), *ľavá slučka* (left loop) a *pravá slučka* (right loop). Týchto 5 tried je ukázaných na obrázku 2.4. Všetkých tried je oveľa viac, ale pre nasnímanie odtlačkov prstov sa používa iba tento výber, pretože určiť triedu v automatickom systéme je veľkou výzvou, keďže obsahuje nespočetne mnoho variácií. [29]



Obr. 2.4: Triedy odtlačkov prstov: (a) ľavá slučka, (b) pravá slučka, (c) oblúk, (d) klenutý oblúk, (e) špirála. Prevzaté z [9].

Rozdelenie odtlačkov prstov do vyššie spomínaných tried nie je dostačujúcou podmienkou na identifikáciu človeka, preto je zavedený ďalší termín, ktorým je markant. *Markant* je definovaný ako detail odtlačku prsta, ktorý stačí na rozpoznanie, či sa jedná o danú osobu alebo nie [11]. Bol to práve Francis Galton, ktorý si ako prvý všimol, že odtlačok prsta je veľmi bohatý na detaily nazvané markanty. Rovnako spozoroval, že markanty sa s časom nemenia, a preto patria k jednému zo základných spôsobov, ako porovnať nasnímaný odtlačok so vzorom v databáze. Najznámejšie markanty, ktoré sa najčastejšie objavujú na odtlačkoch prstov sú: ukončenie, jednoduchá vidlička, dvojité vidlička, trojitá vidlička, hák, kríženie, bočný kontakt, bod, interval, jednoduchá slučka, dvojité slučka, jednoduchý most, dvojité most a priesečná línia. Postupne zľava doprava sú zobrazené na obrázku 2.5. [11] [5]



Obr. 2.5: Typy markantov. Prevzaté z [11].

Pre ľudí nie je obtiažne si zapamätať a identifikovať veľké množstvo typov markantov. No na rozpoznanie sú v dnešnej dobe používané počítače a už pri vyššie spomínaných vzoroch sa získavanie odtlačku príliš komplikuje. Preto sa v prístupových systémoch používajú len dva typy markantov: ukončenie a jednoduchá vidlička. [11] [19]

Po zadefinovaní vyššie spomínaných pojmov je vysvetlené ako rozoznať jednotlivé triedy. Sú uvedené tri hlavné triedy:

Oblúk – typ odtlačku, ktorý sa v prevažnej väčšine prejavuje vlastnosťou, že neobsahuje bod delty ani jadro. Jadro obsahuje iba klenutý oblúk. [13]

Špirála – typ odtlačku, ktorý obsahuje najmenej dve delty. Papilárne línie medzi deltami sú oválneho alebo špirálovitého tvaru, pripomínajúce vír. [13]

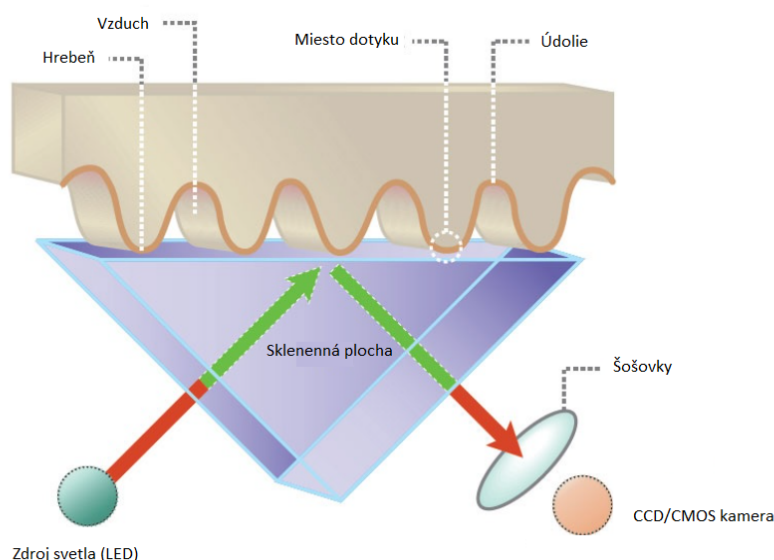
Slučka – typ odtlačku, kde sa väčšina papilárnych línií nachádza medzi typovými líniami. Papilárne línie sa začínajú na jednej strane, obtáčajú sa okolo priamky medzi jadrom a deltou. Koniec papilárnych línií je na rovnakej strane ako ich začiatok. [13]

Zaujímavosťou je, že jednotlivé triedy nemajú štatisticky rovnomerné rozloženie medzi ľuďmi. Približne 60-65 % odtlačkov patrí do triedy *slučka*. Okolo 30-35 % sú odtlačky so vzorom *špirála* a len 5 % ľudí má odtlačky typu *oblúk*. [13]

2.2.1 Senzory na snímanie odtlačkov prstov

Na získanie elektronickej podoby odtlačkov prstov sú známe rôzne technológie. Napríklad kapacitná technológia, ktorej senzor je zložený z malých vodíkových častí pokrytých vrstvou nevodivého oxidu kremičitého. Termická technológia obsahuje tepelné zariadenie. Pracuje na základe faktu, že papilárne línie majú vyššiu teplotu ako údolia medzi nimi. Ultrazvuková technológia je založená na rotujúcom ultrazvukovom vysielači s prijímačom. Ultrazvukové vlny preniknú pod povrch kože a tak snímajú odtlačok prstu. Pri tlakovej technológii má senzor dve vodivé a medzi nimi jednu nevodivú vrstvu. Priložením prsta vznikne tlak, ktorý vytlačí nevodivú vrstvu, vodivé vrstvy sa spoja, a zaznamenajú papilárnu líniu. Pre účely tejto práce bola využitá optická technológia. [11] [20]

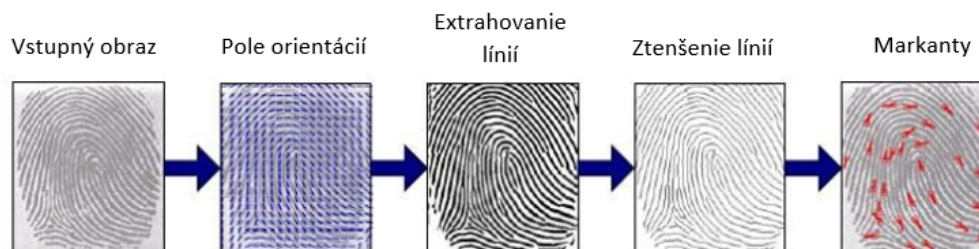
Pri optickom senzore je prst položený na sklenenú priesvitnú plochu. Svetelná dióda osvieti prst. Kamera uložená v spodnej časti nasníma vzniknutý obraz, čím je získaný požadovaný odtlačok. Časti prsta, známe ako hrebene, sú v priamom kontakte so sklenenou plochou, preto sú na výslednom obraze tmavé. Údolia vytvárajú medzeru medzi sklenenou plochou a prstom, čím dovoľia svetlu preniknúť ďalej. Výsledkom sú svetlé časti odtlačku. Celý princíp optického senzora popisuje obrázok 2.6. [11] [20]



Obr. 2.6: Princíp fungovania optického senzora. Prevzaté a upravené z [30].

2.3 Spracovanie odtlačku prsta

Po vysvetlení základných pojmov týkajúcich sa odtlačkov prstov a rozdelení odtlačkov do tried bude ďalšia podkapitola venovaná spracovaniu. To, akými krokmi prechádza odtlačok pri spracovaní, je zobrazené na obrázku 2.7. Zmyslom tohto procesu je zo vstupného obrazu získať markanty. Vzor markantov odtlačku prsta je reprezentácia samotného odtlačku a je používaný v ďalšom spracovaní a porovnávaní. [20]



Obr. 2.7: Kroky spracovania odtlačku prsta. Prevzaté a upravené z [26]

2.3.1 Nasnímanie odtlačku prsta

Celý proces začína nasnímaním odtlačku prsta pomocou senzora. Na prvý pohľad jednoduchá úloha, avšak je veľmi dôležité, aká je nasnímaná kvalita odtlačku prsta. Nedostatočná kvalita sa prejaví pri nasledujúcich krokoch procesu. Prejaviť sa môže aj na výsledku v podobe nedostatočného počtu markantov. Po nasnímaní je potrebná úprava šumu a odstránenie nadbytočne nasnímaných informácií. Pri snímaní je dôležité rozlišovať medzi jednotlivými druhmi odtlačkov prstov. Ďalšie sledované aspekty sú: živosť prstu, ochorenia kože, ale aj miera čistoty senzora. [11]

2.3.2 Vytvorenie poľa orientácií

Po nasnímaní sa dostáva na rad vytvorenie poľa orientácií. Orientované pole $O(i,j)$ je definované ako obraz veľkosti $M \times N$, kde M je šírka a N je dĺžka nasnímaného obrazu. V každom bode obrazu je vypočítaná lokálna orientácia línie. Pokračuje sa so špecifikáciou orientácie línie pre celý blok, kedy je obraz rozdelený na neprekrývajúce sa bloky. Výsledok je namapovaný na pôvodný snímok odtlačku prsta. [11] [20]

2.3.3 Extrakcia a stenčenie papilárnych línií

Tretím krokom v rámci celého procesu získavania markantov, je vytvorenie čierneho-bieleho obrazu. Čiernou sú zobrazené hrebene (ridges) a bielou údolia (valleys). Na vytvorenie čierneho-bieleho obrazu sa najčastejšie využívajú metódy prahovania. Po dokončení binarizácie je k dispozícii čierno-biela snímka obsahujúca papilárne línie, ktoré majú rôznu hrúbku. V ďalšom kroku sú získané papilárne línie rovnakej hrúbky, konkrétne v hrúbke práve jedného pixelu. Je známych viacero metód používaných na tento účel. Účelom je znížiť počet bodov, ktoré vytvárajú papilárne línie, pričom je podstatné, aby neubúdali v žiadnom smere. Mohlo by dôjsť k problému so zmenou smeru markantov. [19] [11]

2.3.4 Detekcia markantov

Posledným a najdôležitejším krokom je odhalenie jednotlivých markantov a ich následná extrakcia. Jedna z často používaných metód na nazýva *Hongova metóda* [14]. Metóda extrahuje dva typy už vyššie spomínaných markantov: ukončenie a jednoduchá vidlička. Ak má pixel, aspoň tri susedné pixely línie, tak spolu tvoria jednoduchú vidličku. Ak má pixel línie práve jedného suseda, tak je detekované ukončenie.[11] [20]

2.4 Rozpoznávanie odtlačkov prstov

Proces rozpoznávania je základom pre nájdenie dvoch zhodných odtlačkov prstov. Porovnaný je nasnímaný odtlačok prsta a reprezentácia odtlačku prsta nazývaná šablóna. Šablóna je uložená a spracovaná v databáze. Na základe použitej metódy sú skúmané prislúchajúce vlastnosti. Pri porovnávacích algoritmoch porovnávame dva zadané odtlačky. Výsledkom je stupeň podobnosti odtlačkov alebo porovnanie v tvare zhodné/nezhodné. Porovnanie dvoch odtlačkov je veľmi zložitý problém, pretože pri každom novom nasnímaní jedného odtlačku prsta vzniká rozdielny obraz. Faktory, ktoré sa musia pri porovnávaní brať do úvahy sú nasledovné: [20]

- **Posunutie** — k posunutiu dochádza, keď je ten istý prst pri nasnímaní položený na inú pozíciu na senzore. Posunutie prsta o 2 mm na senzore znamená posunutie o približne 40 pixelov na nasnímanom odtlačku pri rozlíšení 500 dpi. [20]
- **Rotácia** — k rotácii dochádza, keď je ten istý prst počas snímania otočený o určitý uhol a senzor nezmenil svoju pozíciu. [20]
- **Nelineárne skreslenie** — ku skresleniu dochádza, keď počas snímania prenášaný vzor z trojrozmerného prsta na dvojrozmerný povrch senzora. Skreslenie vzniká kvôli plasticite kože. Vďaka, ktorej je koža vplyvom vonkajších síl tvarovaná. [20]
- **Tlak a stav kože** — štruktúra odtlačku je správne nasnímaná, ak má prst rovnomerný kontakt s plochou senzora na všetkých miestach. Ak je vyvíjaný príliš veľký alebo naopak malý tlak, zhoršuje sa kvalita nasnímaného odtlačku a zhoršujú sa podmienky na jeho spracovanie. Na zníženej kvalite snímky sa môže podieľať veľa ďalších faktorov, ako napríklad kožné choroby, poranenia prstov, vlhkosť kože, pot či rôzne nečistoty. [20]
- **Nedostatočné prekrytie** — posunutie a rotácia môžu spôsobiť, že niektoré časti odtlačku prstu sú mimo plochu senzora a nie sú nasnímané. Pri porovnaní môže dojsť k situácii, kedy nasnímaný odtlačok a šablóna v databáze majú malú plochu prekrytia. [20]
- **Šum** — vzniká hlavne na senzore. Môže sa stať, že senzor obsahuje nečistoty alebo zvyšky predošlých odtlačkov. Obrázok 2.8 zobrazuje rozdielne možnosti nasnímania jedného odtlačku. [20]

Keďže pri porovnávaní odtlačkov vzniká veľké množstvo problémov spojených s posunutím, rotáciou či kvalitou obrazu, existuje viacero metód, ktoré riešia možné ťažkosti pri nasnímaní svojim vlastným spôsobom. Metódy založené na korelácii porovnávajú dve snímky odtlačkov prstov na základe výpočtu korelácie zodpovedajúcich pixelov pre rôzne zarovnania snímok. Metódy založené na vlastnostiach papilárnych línií môžu byť využité,

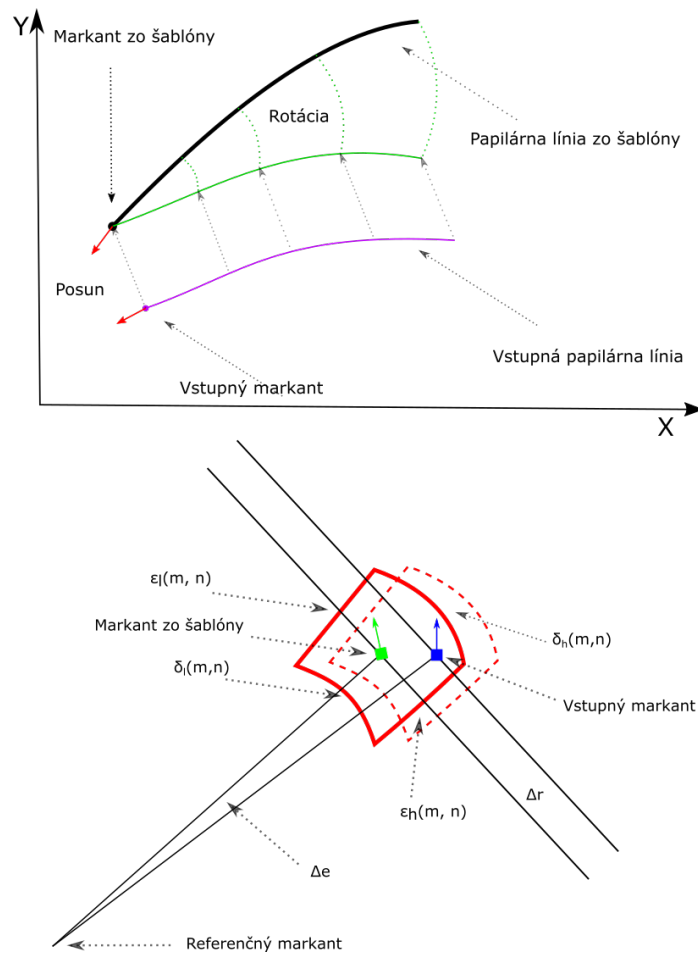


Obr. 2.8: Rôzne nasnímania jedného odtlačku prsta.

keď má snímka odtlačku nízku kvalitu a markanty nie sú viditeľné. Pre porovnanie sa používa veľkosť a tvar odtlačku prsta, počet, tvar a pozícia singulárnych bodov, priestorové a geometrické vlastnosti papilárnych línií. Metódy založené na vlastnostiach papilárnych línií majú nízku rozlišovaciu schopnosť a záleží pri nich, ktorá časť odtlačku prsta je nasnímaná. V tejto podkapitole je vysvetlený princíp najčastejšie používaných metód, ktoré sú založené na markantoch. [11] [20]

2.4.1 Metódy založené na markantoch

Metódy založené na markantoch patria medzi najpopulárnejšie metódy rozpoznávania. V prvom kroku sú získané markanty zo šablóny uloženej v databáze a z odtlačku prsta. Extrahované markanty z obidvoch snímok sú uložené v poli. O každom markante sú uložené informácie: pozícia, uhol a typ. Tieto metódy sa skladajú z generovania globálneho prekrytia, kedy sú snímky odtlačkov zarovnané, a z hľadania lokálneho prekrytia, kedy sú extrahované markanty porovnané. Znázornenie zarovnanie a porovnanie opisuje obrázok 2.9. Ak sú vlastnosti markantov v rozmedzí určených hodnôt, tak sú považované za zhodné. Z jednotlivých dvojíc markantov sa vytvára skóre. Na základe tohto skóre je určené, či je snímka a šablóna považovaná za jeden odtlačok prsta. Konkrétnejšie vysvetlenie rozpoznávania na základe markantov je popísané v podkapitole 5.3. [11] [20]



Obr. 2.9: Hore je znázornené zarovnanie markantov na základe posunu a rotácie. Dole je znázornené porovnanie markantov na základe povolenej odchýlky uhlu a pozície. Prevzaté a upravené z [11].

Kapitola 3

Falzifikáty a syntetické generovanie odtlačkov prstov

Vďaka unikátnosti odtlačkov prstov, relatívne nízkej cene čítačiek na snímanie odtlačkov prstov a kvalitnému vyhodnocovaniu, sa rozpoznávacie systémy založené na odtlačkoch prstov stali jednými z najrozšírenejších pri overovaní identity. So zvyšujúcou sa popularitou týchto systémov sa začala zvyšovať snaha o ich prelomenie. Na to, aby mohli byť vytvorené kvalitné rozpoznávacie systémy, ktoré vedia rozlíšiť reálny odtlačok od falzifikátu a majú nízku mieru chybovosti, je vhodné ich otestovať pomocou falzifikátov a takéto prístupy zamietnuť. Na testovanie a optimalizáciu je potrebná databáza s veľkým počtom odtlačkov prstov. Vytváranie takýchto databáz je náročné na časové aj finančné zdroje. Z pohľadu ľudských zdrojov je táto práca monotónna, čo môže viesť k strate sústredenia a k nasnímaniu nekvalitných odtlačkov a problematická, z dôvodu porušenia súkromia osôb, ktoré odtlačky poskytujú. Práve v prípadoch, kedy je potrebné vytvoriť rozsiahlu databázu odtlačkov, je používané syntetické generovanie odtlačkov prstov.

Táto kapitola sa preto venuje materiálom na výrobu falzifikátov a popisuje popisuje syntetický generátor SFINGE, ktorý vytvára vysoko kvalitné a použiteľné syntetické odtlačky.

3.1 Falzifikáty odtlačkov prstov

Vytvoriť si falzifikát, pomocou ktorého sa podarí prelomiť zabezpečovací prístupový systém, je túžba rovnako stará ako samotné systémy. S príchodom osobných zariadení, ktoré vymenili používanie hesiel a PIN kódov za odtlačky prstov na overenie prístupu, sa počet pokusov ako tieto systémy prelomiť stále zvyšuje [19]. Tieto útoky môžu byť realizované pomocou množstva metód. Najpoužívanejšími sú vytvorenie objektu, ktorý sa podobá prstu a obsahuje odtlačok alebo 2D/3D vytlačené odtlačky prstov [8]. Okrem týchto metód sa vytvárajú rôznorodé formy, ktoré slúžia na vytvorenie falzifikátu. Táto podkapitola popisuje materiály, ktoré sú všeobecne používané na tvorbu falzifikátov. [10]

3.1.1 Materiály na výrobu falzifikátov

Na svete sú desiatky materiálov, ktoré môžu byť použité na výrobu falzifikátov. Vhodnosť materiálu pre výrobu falzifikátu závisí na jeho fyzikálnych vlastnostiach. Najvhodnejší materiál by mal mať vlastnosti podobné ľudskej koži a mal by byť ľahko spracovateľný. Najdôležitejšie vlastnosti sú trvácnosť, elasticita a masťnosť. Ďalšie vlastnosti ako farba,

pulz, vodivosť, odpor sú dôležité na skúmané len pri špeciálnych typoch senzorov. Pohľad, ktorý rovnako treba brať do úvahy je výroba falzifikátu, kde je dôležité odpovedať na tieto 4 otázky:

- Aké úsilie je vynaložené pre skopírovanie odtlačku z formy?
- Aké úsilie je potrebné pre odstránenie falzifikátu z formy?
- Ako dlho proces vytvárania trvá?
- Či sú potrebné nejaké špeciálne nástroje alebo prístupy?

V článku [18] autori testovali 21 materiálov na výrobu falzifikátov. Po výrobe falzifikátov zo všetkých materiálov bolo na základe vizuálnej kontroly a ich nasnímaní do digitálnej podoby vybraných 7, ktoré boli ďalej skúmané. Záverom článku [18] je, že z vybraných materiálov preukázali najlepšiu kvalitu vosk, latex a siligum (silikónová pasta). Na základne vyššie spomínaných vlastností a výsledkov z článku je opísaných 7 materiálov na výrobu falzifikátov: [10] [18]

Vosk – vosk je pred naplnením formy potrebné roztopiť. Podobne ako pri plastelíne sa vosk ľahko prispôbi forme. Zložitejšou časťou je odstraňovanie z formy. Vosk je krehký, a tým náchylný, že sa rozlomí na viac kúskov. [10]

Farby na sklo – sú špeciálnym typom farby, ktoré sú vhodné na maľovanie na sklo, porcelán alebo keramiku. Do formy sa vleje tenká vrstva farby na sklo. Ak je vrstva príliš tenká, pri vyschnutí sa farba natiahne a praskne. Po zaschnutí je falzifikát opatrne odstránený z formy. Pri načítaní falzifikátu je vhodné dať medzi prst a falzifikát nepriehľadnú vrstvu, aby neboli zachytené papilárne línie reálneho odtlačku. [18]

Plastelína – je materiál dobre známy od detstva. Medzi prínosné vlastnosti patrí, že plastelína je mäkká a poddajná, ľahko sa prispôbi forme a jednoducho sa z nej odstraňuje. Medzi nevýhody patrí, že nespĺňa podmienku trvácnosti a je jednoducho deformovateľná. [10]

Želatína – pre vytvorenie je potrebné pridať vodu, roztopiť a nechať stuhnúť. Materiál je typický pre svoju krehkosť. Preto sa stáva, že pri odstraňovaní sa falzifikát roztrhne. Pre jednoduchšie odstránenie nebýva falzifikát z formy oddelený priamo, ale pomocou špeciálnej pásky s lepidlom. Výsledný falzifikát je elastický, ale opäť nie trvácny. [10]

Silikón – tento materiál má všetky vlastnosti vhodného materiálu pre falzifikát. Je trvácny a flexibilný. Výzvou je však vytvoriť silikónový falzifikát bez vzduchových bublín. Rovnako ťažkou úlohou je oddeliť falzifikát od formy, keďže po zaschnutí pevne drží vo forme. [10]

Tekutý latex – je biela tekutina, ktorá sa dá nájsť v niektorých typoch rastlín. Pri tomto type materiálu, je najzložitejšou časťou vytvoriť falzifikát, ktorý má rovnakú hrúbku vo všetkých svojich častiach. Falzifikát z latexu by mal byť, čo najtenší, ale taký aby sa dal oddeliť od formy. Falzifikáty z tohto materiálu sú trvácne a elastické, ale je ich ťažko pripraviť. [10]

Siligum – je dvojzložková silikónová pasta. Obe zložky (modrá a biela) sú zmiešané v pomere 1:1. Vzniknutá hmota je vtlačaná do formy. Po 5 až 15 minútach vzniká pevný falzifikát. S týmto materiálom sa jednoducho narába a pri vtláčaní do formy môže byť použitá väčšia sila. [18]

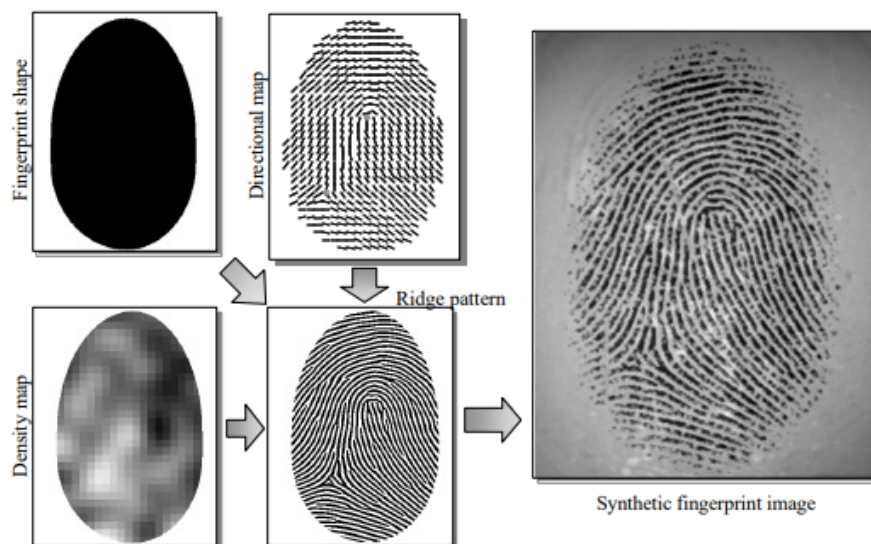
3.2 SFINGE metóda

SFINGE (Synthetic Fingerprint Generation) je metóda, ktorá patrí k najstarším a najpoužívanejším technikám svojho druhu [19]. Hlavným cieľom je vytvárať veľké databázy, ktoré by slúžili na hodnotenie výkonu rôznych rozpoznávacích systémov. Syntetické generovanie odtlačkov šetrí čas a financie potrebné na výrobu databázy a rieši problém so súkromím osôb. Jednou z podstatných vlastností je aj možnosť z jedného odtlačku pomocou posunu, rotácie, skreslenia, hrúbky papilárnych línií a iných faktorov, vytvoriť nový odtlačok. [10]

3.2.1 Metóda generovania syntetického odtlačku

V podkapitole 2.3 je opísaný postup spracovania odtlačku prsta. Odtlačok je najskôr oddelený od pozadia, následne je vypočítané pole orientácií a lokálna frekvencia. Nakoniec dochádza k extrahovaniu a stenčeniu línií a extrakcii markantov. Pri generovaní syntetického odtlačku prsta je postup opačný. Vygenerovanie syntetického odtlačku invertuje poradie niektorých spomínaných krokov. [10]

V prvom kroku je vygenerovaný tvar odtlačku. Ďalej je vygenerované pole orientácií a lokálna frekvencia. Ich kombináciou sú vygenerované papilárne línie. Do výsledného odtlačku je pridaný šum. Obrázok 3.1 zobrazuje základný princíp generovania syntetických odtlačkov. [20]



Obr. 3.1: Základná myšlienka syntetického generovania odtlačkov. [6]

Aby mohlo byť z jedného syntetického odtlačku vytvorených viacero snímok, tak sa používa zložitejší postup. Je vygenerovaný hlavný odtlačok (master-fingerprint) od ktorého môžu byť odvodené vedľajšie odtlačky zmenou určitých vlastností. Pri generovaní hlavného odtlačku je proces vytvárania nasledovný:[10]

1. **Generovanie tvaru odtlačku** — je vygenerovaná silueta, ktorá má tvar reálneho prsta.[20]
2. **Generovanie poľa orientácií** — definovaná trieda odtlačku, s čím súvisí určenie pozície základných bodov ako je jadro a delta. Na generovanie vierohodného poľa orientácií sa využíva matematický model. [20]

3. **Generovanie frekvencie obrazu** — v tomto kroku je generovaná frekvencia papilárnych línií, ktorá odpovedá kritériám odvodeným z pozorovania skutočných odtlačkov prstov. [20]
4. **Generovanie vzoru papilárnych línií** — na základe používania iteratívneho filtrovania je vytvorený vzor papilárnych línií a markantov. [6]

Vygenerovaný hlavný odtlačok je ďalej použitý na vytvorenie jeho odvodených odtlačkov. Zmenou určitých vlastností je vytvorený dojem, že ide o iný odtlačok. Faktory ovplyvňujúce vytváranie odvodených odtlačkov prstov sú:

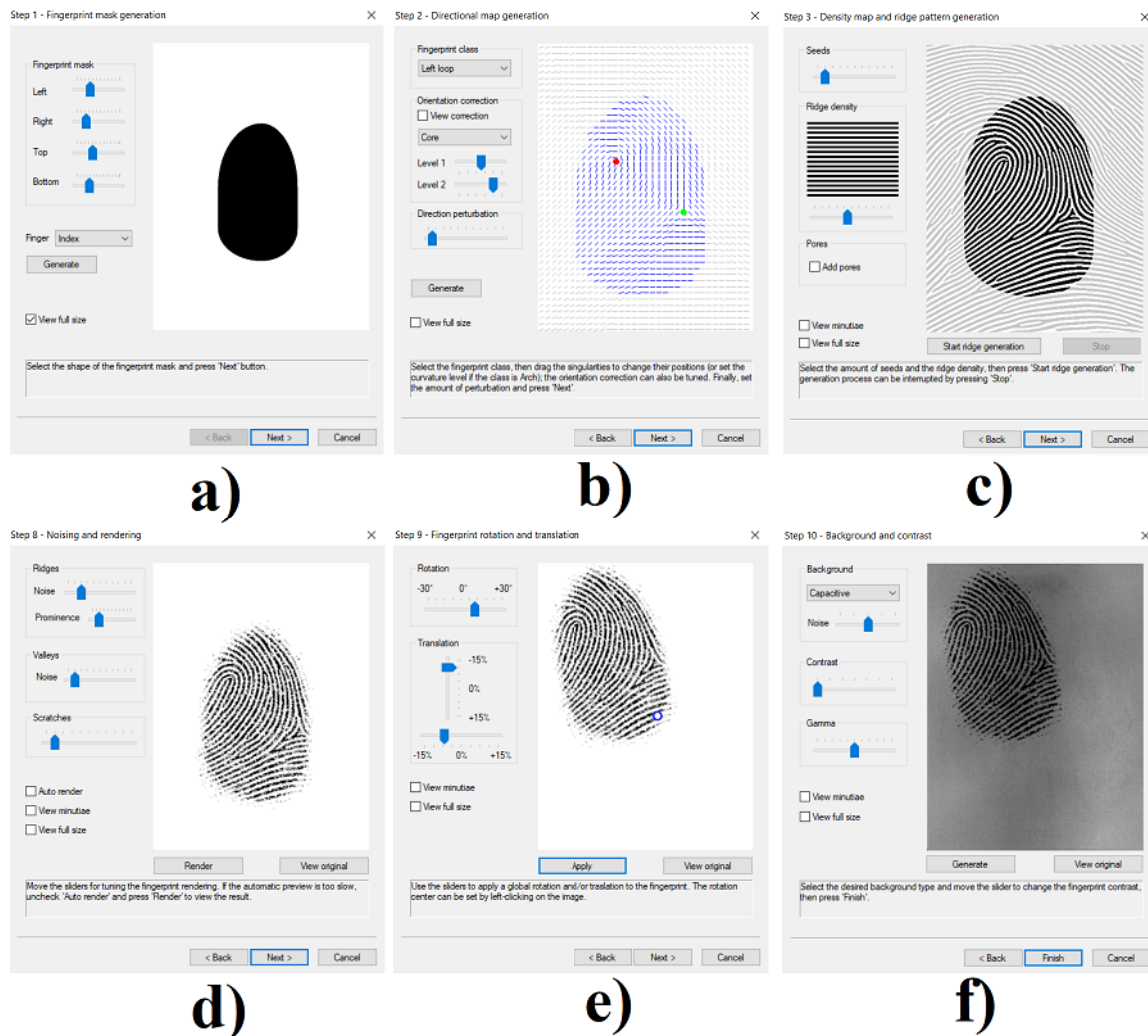
- posun na x-osi a y-osi a rotácia,
- rôzne oblasti dotyku,
- zmena hrúbky papilárnej línie
- šum pozadia alebo iný náhodný šum,
- nelineárne skreslenie,
- malé rany alebo škrabance pridané do odtlačku.

Pre vytvorenie odvodeného odtlačku prsta sa za sebou vykonávajú nasledujúce kroky. Všetky operácie sú aplikované na vytvorený hlavný odtlačok. Na začiatku je vybraná kontaktná oblasť. Pri výbere kontaktnej oblasti so sensorom je posúvaný vygenerovaný vzor odtlačku, pričom tvar odtlačku sa nemení. V druhom kroku je zmenená priemerná hrúbka papilárnej línie. Na hlavný odtlačok sú aplikované morfológické operátory. Operátor erózie namodeluje suchú pokožku alebo slabý tlak pri snímaní odtlačku. Operátor dilatácie vytvorí dojem vlhkej pokožky alebo použitia veľkého tlaku, čím sa mení hrúbka papilárnych línií. Tretím krokom je skreslenie odtlačku prsta. Jeden z hlavných bodov pri vytváraní odvodených odtlačkov a rozlíšenie sa od ostatných, je aplikácia nelineárneho skreslenia. Vytvára deformácie kože spôsobené rôznym umiestnením prsta na sensor. Skreslenie je vytvárané pomocou *Langerovej interpolácie*. Štvrtým krokom je pridanie šumu. Pre vytvorenie pórov alebo nedokonalostí v papilárnych líniách sa do hlavného odtlačku pridáva šum v podobe bielych bodov, ktoré sú rozdielnej veľkosti a tvaru. V piatom bode dochádza ku globálnemu posunu a rotácii. Pri reálnom odtlačku väčšinou nie je prst umiestnený presne v strede senzora. Takýto dojem je docielený aj pri syntetických odtlačkoch. V tomto kroku je vzniknutý obraz náhodne rotovaný o určitý uhol a posunutý na osi x a osi y. V poslednom bode sa generuje pozadie odtlačku prsta. Vygenerovaný hlavný odtlačok vyzerá realisticky, ale má biele pozadie. Na vygenerovanie pozadia ktoré je podobné ako pri nasnímaní odtlačku zo skenera, sa používa *Karhunen-Loève transformácia*. Vygenerované pozadie sa vloží za obrázok odtlačku. [20] [10]

3.2.2 SFINGE nástroj

Spoločnosť BioLab vyvinula nástroj na syntetické generovanie snímok odtlačkov prstov, ktorý pracuje na základe spôsobov opísaných metódou SFINGE. Tento nástroj používateľovi poskytuje možnosť vygenerovať si databázu odtlačkov prstov na základe zvolených vstupov, ako je počet vygenerovaných odtlačkov, veľkosť obrázka, maximálna hodnota posunu a rotácie či maximálne množstvo pridaného šumu. Pri generovaní pozadia môže byť

zvolený typ snímača, vďaka čomu vygenerovaný odtlačok umocňuje dojem, že ide o ručne nasnímaný odtlačok. Tento nástroj bol použitý aj pri vytváraní foriem pre falzifikáty v praktickej časti tejto práce. Obrázok 3.2 zobrazuje kroky pri generovaní syntetického odtlačku pomocou aplikácie SFINGE. [20]



Obr. 3.2: Proces generovania syntetických odtlačkov prstov pomocou nástroja SFINGE: a) generovanie masky odtlačku, b) generovanie mapy orientácií, c) generovanie frekvencie a vzoru papilárnych línií, d) generovanie šumu, e) generovanie rotácie a posunu, f) generovanie pozadia.

Kapitola 4

Tvorba foriem a výroba falzifikátov

Jedným z najpodstatnejších krokov pri tvorbe falzifikátov je príprava foriem, z ktorých sa budú falzifikáty vyrábať. Formy sa môžu vytvárať rôznymi spôsobmi, ale pri všetkých spôsoboch by mali formy spĺňať rovnaké podmienky. Forma by mala byť viacnásobne použiteľná a odolná voči deformácii.

Touto kapitolou začína praktická časť práce. Prvá časť kapitoly sa zaoberá tvorbou foriem pomocou laserovej gravírovačky, správnym nastavením parametrov a výberom vhodného materiálu pre formy. Po vytvorení foriem je na rade výroba falzifikátov. Druhá časť kapitoly je preto venovaná výrobe falzifikátov z troch materiálov.

4.1 Tvorba foriem metódou vypalovania

Na vytvorenie foriem bol použitý prenosný laser Laser Pecker Pro, ktorý je zobrazený na obrázku 4.1. Laser má jednoduché ovládanie cez mobilnú aplikáciu. Ako vstupné súbory je možné použiť obrázky formátu G-Code, bmp a jpg. Následne si používateľ vyberie veľkosť vypáleného obrázku a má možnosť si zvoliť parametre sily a hĺbky laseru, ktoré sa vyberajú na základe materiálu, do ktorého sa bude vypalovať. Laser pracuje s teplotou 0 °C - 65 °C. Laser je umiestnený na stojane, ktorý má nastaviteľnú vzdialenosť od podložky. Pre účely tejto práce boli použité obrázky vo formáte bmp. Dĺžka výsledných foriem je 20mm a šírka bola doplnená automaticky pomerom k dĺžke. Táto hodnota bola určená na základe veľkosti snímačej plošky čítačky odtlačkov prstov, ktorá je 15,2 mm x 20,3 mm. Vzdialenosť laseru od podložky bola nastavená na 200 mm na základe manuálu. Sila a hĺbka laseru bola nastavená individuálne pre jednotlivé formy a materiály. Výroba jednej formy trvala 2 - 20 minút čistého času vypalovania. Dĺžka doby vypalovania závisela na nastavených parametroch a hustote materiálu. Čím vyššie percento sily a hĺbky bolo použité, tým viacej času bolo potrebné na vytvorenie formy. [27]



Obr. 4.1: Laser používaný pri vytváraní foriem.

4.1.1 Výber materiálov pre formy

Výber vhodného materiálu pre formu bola jednou z časovo najnáročnejších častí práce. Materiály pre formy boli vyberané na základe vyššie spomenutých podmienok, viacnásobnej použiteľnosti a nedeformovateľnosti. Pri výbere materiálu bolo brané do úvahy aj to, že laser nie je určený na vypalovanie do kovov. Pre každý vybraný materiál bol zopakovaný rovnaký postup. V prvom kroku bol na materiál vypálený vzorový odtlačok s počiatočnou silou a hĺbkou. Podľa toho, ako vyzeral odtlačok bola sila a hĺbka pridávaná alebo odoberaná. Po niekoľkých opakovaní bol materiál vyhlásený za nevhodný alebo vhodný na základe toho, či bol vypálený výsledok podobný vzorovému odtlačku a obsahoval viditeľné papilárne línie alebo nie. Pri vhodných materiáloch bola ďalej skúmaná optimálna kombinácia sily (P) a hĺbky (D) laseru tak, aby bola vytvorená forma čo najpresnejšia v porovnaní s pôvodným odtlačkom. Pre každú kombináciu a materiál bol vytvorený falzifikát z plastelíny. Falzifikáty boli porovnané medzi sebou. Parametre formy z ktorej bol vytvorený falzifikát, ktorý sa najviac podobal vzorovému odtlačku, boli použité ako vzorové pre daný materiál. Pre overenie, či forma vytvára vhodné falzifikáty, bola ich kvalita vyhodnotená pomocou nástroja od spoločnosti SecuGen. Na základe tohto postupu sú testované materiály rozdelené do dvoch skupín opísaných v nasledujúcich podkapitolách. Za nevhodné materiály pre výrobu foriem vypalovaním sú považované také, do ktorých sa nepodarilo vypáliť formu odtlačku podobnú vzorovému odtlačku.

4.1.2 Nevhodné materiály

Prvým nevhodným materiálom je mäkký plast. Ako skúšobný materiál bol použitý vrchnák od plastovej nádoby. Súhrn všetkých skúšaných kombinácií sily a hĺbky pre tento materiál je zobrazený v tabuľke 4.1. Prvý pokus prebiehal so silou a hĺbkou nastavenou na 60 %. Výsledok bol nedostatočný, niektoré časti formy neboli vypálené. Preto boli zvýšené obe hodnoty na plný výkon. Tu sa časť materiálu, vystavená laseru roztopila a papilárne línie sa zliali dokopy. Preto nasledovalo zníženie sily aj hĺbky o 20 %. Výsledkom boli viditeľné papilárne línie, no forma bola v niektorých miestach stále zliata. Pri znížení sily aj hĺbky na 70 % výsledná forma nebola zliata, ale papilárne línie neboli pospájané a forma bola príliš plytká. Ako posledná možnosť bola zvolená vyššia hĺbka a sila postupne znižovaná. Táto cesta sa zdala ako najlepšia. Pri nastavení sily na 50 % a hĺbky na 90 % bola forma dostatočne hlboká, papilárne línie boli pospájané, no nie zliate. Avšak po vytvorení falzifikátu z plastelíny, mal výsledný falzifikát deformované papilárne línie a na niektorých častiach boli zliate. Tento trend nasledovali aj ostatné kombinácie so zníženou silou a zvýšenou hĺbkou.

Tabuľka 4.1: Kombinácie hodnôt sily (P) a hĺbky (D) použitých na vytvorenie formy z mäkkého plastu

Sila (P)	Hĺbka (D)	Výsledok
30 %	30 %	žiadny výsledok
60 %	60 %	príliš slabý
70 %	70 %	nepospájané papilárne línie, plytká
70 %	90 %	forma je zliata
50 %	90 %	falzifikát mal deformované papilárne línie
40 %	90 %	falzifikát mal deformované papilárne línie
30 %	90 %	falzifikát mal deformované papilárne línie, menšia hĺbka
30 %	80 %	slabá hĺbka formy
80 %	80 %	zliaty v niektorých častiach, plytká
100 %	100 %	forma je zliata

Ďalší testovací materiál bol silikón. Pre vypalovanie poslužil silikónový obal na mobilný telefón. Pri tomto materiáli bolo skúšaných menej kombinácií sily a hĺbky ako v predošlom prípade, pretože už pri kombinácii P: 50 % a D: 100 %, laser nezanechal v silikóne požadovanú hĺbku formy. Preto každé zníženie sily, znamenalo príliš plytkú formu. Ani jedna z odskúšaných kombinácií nevytvorila vhodnú formu. Pri kombinácii P: 100 % a D: 100 % bola forma v častiach z najväčšou hustotou papilárnych línií zliata a papilárne línie boli neostré. V ostatných prípadoch bola výsledná silikónová forma príliš plytká hlavne na okrajoch formy. Po vytvorení falzifikátu z foriem, ktoré neboli zliate, bol falzifikát jemný v niektorých prípadoch takmer neviditeľný. V tabuľke 4.2 sú zhrnuté odskúšané kombinácie s výsledným hodnotením.

Ďalším materiálom, ktorý treba spomenúť, je balzové drevo. Pôvodne bol plán mať balzové drevo ako hlavný materiál pre vypalovanie foriem, ale prax ukázala, že tento materiál nepatrí k najvhodnejším. Balza je mäkké a ľahké drevo s malou hustotou. Balzové drevo sa často používa na výrobu modelov. Formy vykazovali lepšie vlastnosti ako formy zo silikónu, či plastu. Papilárne línie boli vo väčšine skúšaných kombinácií viditeľné, bola dosiahnutá aj dostatočná hĺbka formy. Prvý problém nastal v častiach otlaku, kde bola najväčšia hustota papilárnych línií. Laser dokázal vypáliť papilárne línie, ale úzke časti dreva, ktoré medzi nimi ostali, sa nedokázali udržať pri forme a odpadli. Pri niektorých kombináciách sa do

Tabuľka 4.2: Kombinácie hodnôt sily (P) a hĺbky (D) použitých na vytvorenie formy zo silikónu

Sila (P)	Hĺbka (D)	Výsledok
60 %	100 %	neostré papilárne línie, príliš plytká
70 %	100 %	neostré papilárne línie, plytká
80 %	100 %	neostré papilárne línie, plytká
90 %	100 %	neostré papilárne línie, plytká
100 %	100 %	časť zliata

falzifikátu prenášala aj štruktúra dreva. Po pritlačení plastelíny k forme niektoré časti dreva ostali vo falzifikáte a tlak formu deformoval. Pri vytváraní falzifikátov z tekutých materiálov ako silikón alebo tekutý latex sa po odstránení forma poškodila a už nebola znovu použiteľná. Výsledný falzifikát mal v sebe prilepenú odtrhnutú formu. Balzové drevo, ktoré bolo použité, nemalo rovnakú tvrdosť vo všetkých častiach, čo znižovalo kvalitu foriem. Celkové zhodnotenie foriem z balzového dreva je popísané v tabuľke 4.3.

Tabuľka 4.3: Kombinácie hodnôt sily (P) a hĺbky (D) použitých na vytvorenie formy zo silikónu

Sila (P)	Hĺbka (D)	Výsledok
45 %	60 %	rozpadnutý stred odtlačku po vytvorení falzifikátu
50 %	25 %	plytká, prevažuje štruktúra dreva
50 %	50 %	rozpadnutý stred, nepresné papilárne línie vo falzifikáte
50 %	60 %	rozpadnutý stred
50 %	70 %	spálený stred
60 %	20 %	viditeľná štruktúra dreva, pokazený stred
60 %	30 %	plytká na okrajoch, vytvára falošné papilárne línie na falzifikáte
70 %	20 %	rozpadnutý stred
70 %	30 %	rozpadnutý stred, vrchná vrstva zničená silikónovým falzifikátom
70 %	40 %	vypálený stred

4.1.3 Vhodné materiály

Po neúspešnom pokuse s balzovým drevom boli otestované tvrdšie typy dreva. Po pozorovaní bolo zistené, že drevené formy vykazujú najlepšie výsledky. Nedostatkom bolo, že do falzifikátov sa odtlačala štruktúra dreva, konkrétne pozostatky po letokruhoch, ktoré sú vo falzifikátoch nežiadúce. Preto bolo potrebné vybrať drevo, ktoré bude mať hladký obrúsený povrch s čo najjemnejšou štruktúrou. Po viacerých pokusoch a rôznych typoch dreva bolo vybraté bukové drevo. Bukové drevo patrí medzi tvrdé dreva s rovným a hladkým povrchom. Obe vlastnosti sú vyhovujúce pre formu. Vďaka tvrdosti je forma pevná a nedeformovateľná. Vďaka hladkému povrchu falzifikát obsahuje minimum nežiadúcich drobných častí, ktoré by mohli znížiť kvalitu falzifikátu. Do bukového dreva boli formy vypalované rôznou silou a hĺbkou laseru. Najoptimálnejší výsledok, kedy forma nebola spálená, bola dosiahnutá pri nasledujúcich hodnotách: $P = 75 \%$ a $D = 85 \%$. Do vybratého materiálu bolo vytvorených celkovo 10 výsledných foriem. Podklad pre formy tvoria odtlačky

zobrazené na obrázku 4.2. Odtlačky v hornom riadku sú reálne odtlačky nasnímané pomocou optického senzora na odtlačky prstov, ktorého princíp je opísaný v podkapitole 2.2.1. Na obrázky odtlačkov bol aplikovaný Gaborov filter a binarizácia, pre dosiahnutie lepších výsledkov. Dolný riadok zobrazuje odtlačky, vygenerované pomocou aplikácie SFINGE. Výsledné formy sú zobrazené na obrázku 4.3.



Obr. 4.2: Odtlačky použité na výrobu foriem. Horný riadok Real1 - Real5. Dolný riadok Sfinge1 - Sfinge5.



Obr. 4.3: Výsledné formy.

4.2 Výroba falzifikátov odtlačkov prstov

Na výrobu falzifikátov v tejto práci z drevených vypálených foriem bolo odskúšaných 5 zo 7 opísaných materiálov v kapitole 3.1 a to plastelína, želatína, vosk, tekutý latex a silikón. Pri

želatíny a vosku sa nepodarilo dosiahnuť očakávané výsledky. Po naliatí želatíny do formy, sa želatína pri každom pokuse vpila do dreva. Voskové falzifikáty sa nepodarilo oddeliť bez toho, aby falzifikát ostal v jednom celku. Pri voskových falzifikátoch bol použitý nevhodný typ vosku zo sviečky. Vhodnejšie by bolo použiť gélový vosk alebo voskovú hmotu, ktorá sa používa v stomatológii. S týmito dvomi materiálmi nebolo ďalej pracované. Výsledné falzifikáty vznikali z troch materiálov: plastelína, silikón a tekutý latex.

4.2.1 Falzifikáty z plastelíny

Na výrobu falzifikátov bola použitá detská plastelína, ktorá sa dá kúpiť v papiernictve. Z plastelíny bola pomocou rovného povrchu vytvorená plocha, o niečo väčšia ako forma s hrúbkou približne 2mm. Plocha z plastelíny bola položená a jemne pritlačená do formy. Keďže plastelína je poddajná, okopírovala formu a do niekoľkých sekúnd vznikol výsledný falzifikát. Vzniknutý falzifikát bol z formy jednoducho odstránený bez použitia špeciálnych nástrojov. Po odstránení bol falzifikát orezaný po obryse vzniknutého odtlačku. Pre lepšie výsledky boli falzifikáty odložené do studenej miestnosti, vďaka čomu jemne stvrdli a držali svoj tvar. Pri snímaní falzifikátov bolo zistené, že niektoré farby plastelíny sú vhodnejšie ako iné. Modrá a zelená plastelína vytvárali snímky, ktoré boli intenzitou čiernej, podobné reálnemu odtlačku prsta. Falzifikáty z červenej plastelíny vytvárali príliš svetlé snímky. Každý falzifikát z plastelíny bol nasnímaný maximálne dvakrát. Pri každom nasnímaní strácal svoju kvalitu. Obrázok 4.4 zobrazuje výrobu plastelínových falzifikátov.



Obr. 4.4: Výroba plastelínových falzifikátov.

4.2.2 Falzifikáty zo silikónu

Na výrobu falzifikátov bol použitý transparentný silikón odolný voči vode, používaný na opravu kúpeľní. Z tuby bol vytlačený silikón v tekutom stave. Pomocou príborového noža bol rozprestretý po celej ploche formy. Forma naplnená silikónom odpočívala nasledujúcich 8 hodín. Po zaschnutí bol silikón silno prilepený k forme. Pri formách z mäkkých materiálov (balzové drevo) môže odstránenie falzifikátu zničiť celú formu. Pri formách z tvrdého dreva bol falzifikát odstránený pomocou pilníka na nechty. Postupne od okrajov až ku stredu. Niektoré silikónové falzifikáty boli vo forme ponechané po dobu dvoch dní. Takéto falzifikáty sa už nepodarilo z formy odstrániť. Preto je dôležité nenechať silikónový falzifikát vo forme príliš dlho. Pre jednoduchšie nasnímanie a prácu s falzifikátom bol falzifikát upravený pomocou nožničiek. Obrázok 4.5 zobrazuje výrobu silikónových falzifikátov.



Obr. 4.5: Výroba silikónových falzifikátov.

4.2.3 Falzifikáty z tekutého latexu

Na výrobu bol použitý tekutý latex, používaný na maľovanie na telo a výrobu masiek. Do formy bolo vyliate primerané množstvo, aby zakrylo celú formu a okolie o veľkosti pol centimetra. Ako tekutý latex tuhne, tak znižuje svoj objem, preto sa netreba báť naliať väčšie množstvo. Doba tuhnutia je približne 12 hodín. Falzifikáty, ktoré boli odstránené skôr, nemali tuhú konzistenciu a dali sa ľahko zdeformovať. Podobne ako pri silikónových falzifikátoch, bol na oddelenie okrajov použitý pilník. Stred odtlačku sa dal odlepiť pomocou rúk. Pre lepšie nasnímanie bola z latexu vystrihnutá iba časť s odtlačkom. Pri práci s tekutým latexom je dôležité, zvýšiť opatrnosť a jemnosť pohybov pri odstraňovaní falzifikátu. Obrázok 4.6 zobrazuje výrobu falzifikátov z tekutého latexu.



Obr. 4.6: Výroba latexových falzifikátov.

Na nasnímanie pravých odtlačkov a falzifikátov bola použitá čítačka Hamster Pro 20 (HU20-A) od spoločnosti SecuGen zobrazená na obrázku 4.7. Ide o vysoko kvalitnú optickú čítačku odtlačkov prstov, ktorá sa dá pripojiť k zariadeniu cez USB kábel. Veľkosť snímacieho okna je 15.2 mm x 20.3 mm. Na zobrazenie snímaných odtlačkov bola použitá aplikácia SecuGen Device Diagnostic Utility. Výsledná snímka má rozlíšenie 300×400 pixelov.



Obr. 4.7: Čítačka odtlačkov prstov HU20-A.

Kapitola 5

Návrh algoritmov analýzy

Táto kapitola je venovaná popisu návrhu algoritmov analýzy rozdielov medzi zdrojovým odtlačkom prsta a nasnímaným falzifikátom. V podkapitole Predspracovanie je opísaný postup, akým budú snímky upravené ešte pred tým, ako dôjde k porovnávaniu. Postup predspracovania je obvyklým postupom, ktorý sa používa pri vylepšení kvality obrazu odtlačkov prstov. V podkapitole Extrakcia markantov je opísaný spôsob, akým sú z upravených snímok získané markanty, ktoré budú najdôležitejšími prvkami pri porovnaní. V podkapitole Porovnanie odtlačku a falzifikátu, je vysvetlený algoritmus zarovnania, ktorý je potrebný vykonať pred porovnaním. Ďalej je opísaný spôsob samotného porovnávania vzorového odtlačku a falzifikátu.

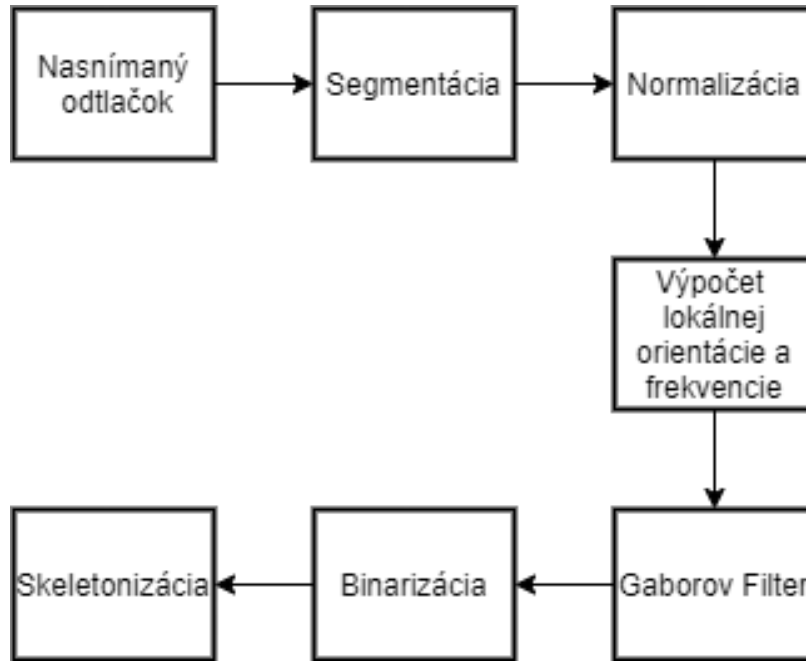
5.1 Predspracovanie

Predspracovanie obrazu slúži na zlepšenie kvality odtlačku a následné jednoduchšie spracovanie. Vďaka úprave obrazu, je odtlačok zbavený pórov a šumu medzi papilárnymi líniami, ktoré sú súčasťou papilárnych línii. Taktiež sú odstránené nečistoty a fragmenty nachádzajúce sa v okolí odtlačku, ale nie sú jeho súčasťou. Vstupom je šedo-tónový obraz a výstupom čiernobiela kostra odtlačku. Celý postup úpravy obrazu je naznačený na obrázku 5.1.

5.1.1 Segmentácia

Prvým krokom pri zlepšení kvality nasnímaného odtlačku je segmentácia. Pri procese segmentácie je oddelené popredie obrázku odtlačku od jeho pozadia. Popredie zodpovedá odtlačku prsta, ktorý obsahuje hrebene a údolia. Pozadie zodpovedá častiam obrázku, ktoré nie sú súčasťou oblasti odtlačku prsta a neobsahujú platné informácie pre jeho ďalšie spracovanie. Pri segmentácii je na začiatku určený globálny prah. Obrázok je rozdelený na bloky o veľkosti $W \times W$. Pre každý blok je vypočítaná stredná hodnota úrovne šedej, označenej ako $M(k)$. V ďalšom kroku je pre každý blok vypočítaný rozptyl úrovne šedej $V(k)$ pomocou rovnice 5.1. $I(i, j)$ vo vzorci je šedo-tónová hodnota pixelu na pozícii i a j . Výsledná hodnota rozptylu je porovnaná s vopred určenou hodnotou prahu. Ak je hodnota rozptylu menšia ako prah, blok je vyhodnotený ako pozadie, inak je blok vyhodnotený ako popredie obrázku. [25] [3]

$$V(k) = V(k) + \left(\frac{1}{W^2} * (I(i, j) - M(k))^2 \right) \quad (5.1)$$



Obr. 5.1: Proces predspracovania nasnímaného odtlačku.

5.1.2 Normalizácia

Normalizácia je proces, ktorý sa používa na standardizáciu intenzity hodnôt v danom obraze, a to úpravou rozsahu hodnôt úrovne šedej. Normalizácia je pixelová operácia, ktorej hlavnou úlohou je znížiť odchýlku v hodnotách úrovne šedej hrebeňov a údolí. Výpočet hodnoty pixela normalizovaného obrázku zobrazuje rovnica 5.2. Hodnoty M_0 a V_0 sú požadované hodnoty priemeru a rozptylu. [25] [3]

$$G(i, j) \equiv \begin{cases} M_0 + \sqrt{\frac{V_0(I(i, j) - M)^2}{V}}, & \text{ak } I(i, j) > M \\ M_0 - \sqrt{\frac{V_0(I(i, j) - M)^2}{V}}, & \text{inak,} \end{cases} \quad (5.2)$$

5.1.3 Výpočet lokálnej orientácie

Ďalším krokom je výpočet lokálnych orientácií odtlačku prsta. Výsledok výpočtu lokálnych orientácií je jeden zo základných vstupov pri výpočte Gaborovho filtru. Orientácia reprezentuje uhol papilárnej línie v danej časti obrázku. Na začiatku je celý obrázok rozdelený do blokov o veľkosti $W \times W$ (16 x 16). Ako druhý krok si vypočítaný gradient $\partial_x(i, j)$ a gradient $\partial_y(i, j)$ pre každý pixel v bloku. $\partial_x(i, j)$ reprezentuje gradient v smere osi x a $\partial_y(i, j)$ v smere osi y. Na výpočet gradientov sa používa vertikálny a horizontálny Sobelov operátor. Následne je vypočítaná lokálna orientácia pre daný blok v bode (i, j) , ktorý je centrálnym pixelom pre každý blok. Výpočet prebieha pomocou rovníc 5.3, 5.4 a 5.5,

$$V_x(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u, v)\partial_y(u, v), \quad (5.3)$$

$$V_y(i, j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (\partial_x^2(u, v) - \partial_y^2(u, v)), \quad (5.4)$$

$$\theta(i, j) = \frac{1}{2} \tan^{-1} \left(\frac{V_y(i, j)}{V_x(i, j)} \right) \quad (5.5)$$

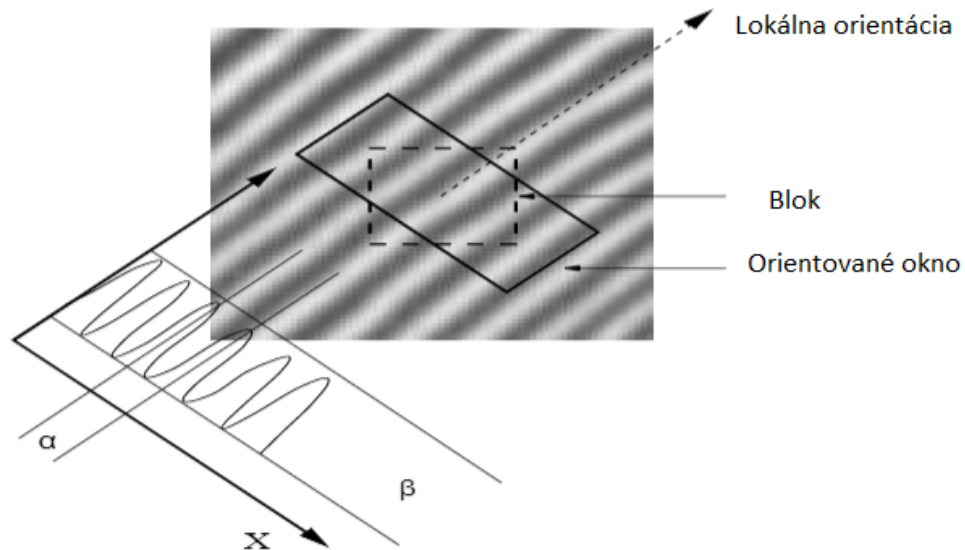
kde $\theta(i, j)$ je odhad lokálnej orientácie pre blok a centrálnym pixelom je (i, j) . Hodnota $\theta(i, j)$ je len najmenším štvorcovým odhadom a nemusí vždy reprezentovať správnu orientáciu v danom bloku. Na spresnenie výsledkov sa používa filter dolnej priepusti, medzi ktoré patrí napríklad Gaussov filter. [14]

5.1.4 Výpočet lokálnej frekvencie

Pred výpočtom samotného Gaborovho filtru na odstránenie šumu a zlepšenia kvality obrázku ostáva vypočítať lokálnu frekvenciu pre každý blok obrázku. Lokálna frekvencia predstavuje priemernú vzdialenosť hrebeňov v počítanom bloku. Lokálnu frekvenciu je vyjadrená pomocou rovnice 5.6, kde $\tau(i, j)$ predstavuje priemerný počet pixelov medzi každými dvoma hrebeňmi bloku.

$$f(i, j) = \frac{1}{\tau(i, j)} \quad (5.6)$$

Lokálnu frekvenciu je definovaná ako vlnu sínusového tvaru v smere kolmom k lokálnej orientácii v bloku. Tento jav zobrazuje obrázok 5.2. Na obrázku 5.2 je blok, ku ktorému je vytvorené orientované okno otočené o 90° voči bloku. V orientovanom okne je následne počítaný priemerný počet pixelov medzi dvoma hrebeňmi vyjadrený v podobe periodicky sa opakujúcej sínusovej vlny. [14]



Obr. 5.2: Princíp výpočtu lokálnej frekvencie. Upravené a prevzaté z [14].

5.1.5 Gaborov filter

Definovaním frekvencie a orientácie pre jednotlivé bloky odtlačku boli získané potrebné informácie pre odstránenie šumu. Na odstránenie šumu a zachovanie reálnych hrebeňov a údolí bol použitý filter pásovej prepusti, ktorým je Gaborov filter. Gaborov filter aplikuje na obrázok vlastnosti frekvencie aj orientácie. Vyznačuje sa spoločným rozlíšením v priestorovej a frekvenčnej doméne. Aby mohol byť Gaborov filter aplikovaný na obrázok, je potrebné mať k dispozícii frekvenciu, orientáciu a štandardné odchýlky Gaussovej obálky. Gaborov filter je obecné definovaný podľa rovnice 5.7:

$$V(x, y : \phi, f) = \exp\left\{-\frac{1}{2}\left[\frac{(x \cos \phi)^2}{\theta_x^2} + \frac{(x \sin \phi)^2}{\theta_y^2}\right]\right\} \cos(2\pi f x \cos \phi) \quad (5.7)$$

kde ϕ je orientácia Gaborovho filteru, f je frekvencia sinusoidy, θ_x a θ_y sú konštanty Gaussovej obálky pozdĺž osi x a osi y . Určujú veľkosť Gaborovho filteru. [14]

5.1.6 Binarizácia

Ďalším krokom v spracovaní obrazu je binarizácia. Pri binarizácii je šedotónový obrázok obsahujúci 256 rozdielnych stupňov intenzity farby, zmenený na čierno-biely. Pri procese binarizácie sa pracuje s prahom. Podľa hodnoty prahu sa rozhodne, či bude daný pixel zmenený na hodnotu 0 (čierna) alebo 255 (biela). Existuje viacero typov prahovania. Medzi najpoužívanejšie patrí jednoduché prahovanie, kedy je pre každý pixel nastavená rovnaká hodnota prahu. Nastavenie globálneho prahu nemusí byť správne vo všetkých prípadoch, napríklad ak má obrázok rôznu intenzitu svetla z jednotlivých častiach. Vtedy sa používa adaptívne prahovanie, kde je hodnota prahu pre daný pixel vypočítaná na základe jeho okolia. Pre každý pixel môže byť určená rozdielna hodnota prahu. Poslednou spomenutou bude Otsu metóda. Pri Otsu binarizácii nie je určená vopred hodnota prahu, ale je automaticky vypočítaná podľa hodnôt na obrázku, kedy sa prejdú všetky možné hodnoty prahu a nájde sa optimálna hodnota pre vstupný obraz. Otsu metóda pracuje so štatistickými dátami obrazu. Pre nájdenie prahu sa používa histogram obrázku. V tejto práci bola použitá posledná spomenutá metóda. [25] [1]

5.1.7 Skeletonizácia

Posledným krokom predspracovania obrazu je skeletonizácia. Skeletonizácia je morfológická operácia, ktorá zúži všetky papilárne línie na hrúbku jedného pixela. Skeletonizácia uľahčuje následnú extrakciu markantov z odtlačku prsta. Na skeletonizáciu sa používa napríklad algoritmus *Zhang-Suen* vymyslený v roku 1984. Algoritmus pri každej iterácii vykoná dve sady podmienok na odstránenie pixelov z obrázku. Prvá sada podmienok slúži na odstraňovanie bodov z juhovýchodu, druhá zo severozápadu. Algoritmus končí, keď neexistuje žiadny pixel, ktorý by vyhovoval aspoň jednej sade podmienok. [28]

5.2 Extrakcia markantov

Existuje mnoho spôsobov ako získať potrebné markanty z odtlačku prsta. Je možné ich rozdeliť do dvoch hlavných skupín: metódy pracujúce s binarizovaným odtlačkom prsta a metódy, ktoré pracujú s pôvodným šedotónovým odtlačkom. Každá z týchto metód má ešte svoje pod rozdelenia. Táto práca sa bližšie venuje jednej z metód, ktorá pracuje s binarizovaným odtlačkom. Opäť, aj táto metóda sa delí na techniky extrakcie markantov nad

zúženým a nezúženým odtlačkom. V kapitole 5 bol obrázok najskôr binarizovaný a potom zúžený na šírku jedného pixela. V tomto trende sa bude pokračovať, a teda vybratá metóda extrakcie markantov bude vykonávaná nad binarizovaným a zúženým obrázkom odtlačku prsta. Metóda *Crossing number* je často používaná pre extrakciu markantov. Patrí medzi obľúbené, kvôli svojej efektívnosti počítania a jednoduchosti implementácie. Markanty sú získavané pomocou prehľadávania okolia každého pixelu, ktorý je súčasťou papilárnej línie. Pre každý takýto pixel je skúmané okolie 3x3 pixely, ako ukazuje obrázok 5.3. P je skúmaný pixel a $P_1 - P_8$ tvoria okolie pixelu. [14] [3]

P_1	P_2	P_3
P_8	P	P_4
P_7	P_6	P_5

Obr. 5.3: Okolie pixelu.

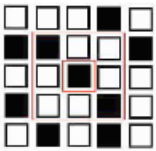
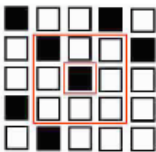
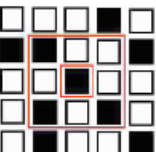
Podľa rovnice 5.8 sa vypočíta hodnota CN v každej matici. Rovnica je definovaná ako polovica súčtu rozdielov medzi susednými pixelmi v 8-okolí. Na základe výsledku, môže byť pixel klasifikovaný ako ukončenie, vidlička alebo pixel nepatriaci markantu. Tento výpočet sa dá jednoducho vysvetliť. Ak je pixel súčasťou hrany, je mu priradená hodnota 1. Je prechádzané po okraji matice od pozície P_1 po P_8 v smere hodinových ručičiek. Ak je rozdiel dvoch nasledujúcich pixelov 1, je možné určiť, že bola zachytená hrana. Podľa toho, koľko má pixel hrán v bezprostrednom okolí, je možné určiť, či a o aký markant sa jedná. Ak pixel okolo seba nemá žiadne iné pixely ležiace na hrane je označený ako izolovaný bod. Ak pixel susedí iba s jedným pixelom ležiacim na hrane, tak je možné určiť, že ide o ukončenie. Ak má okolo seba 3 pixely ležiace na hranách, ide o vidličku. Pre ilustráciu sú jednotlivé prípady zobrazené na obrázku 5.4. [3]

$$CN = \frac{1}{2} \sum_{i=1}^8 |P_i - P_{i+1}| \quad (5.8)$$

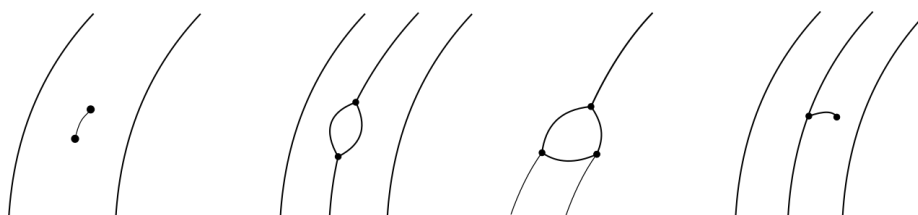
5.2.1 Falošné markanty

Po spracovaní markantov sa medzi pravými markantmi objavajú aj falošné markanty. Falošné markanty vznikajú napríklad, ak odtlačok obsahuje šum, alebo boli čítačkou zachytené póry prsta. Falošné markanty sa vytvárajú ako artefakty pri procese skeletonizácie. Obrázok 5.5 ukazuje niektoré typy falošných markantov. Je možné vidieť, že falošný markant naľavo vytvára falošné ukončenie. Ostatné falošné markanty sú spracované ako vidličky. Tieto falošné markanty je potrebné odstrániť. Existuje viacero spôsobov ako na to. Jeden spôsob je založený na vzdialenosti markantov. Vypočíta sa vzdialenosť medzi každými dvoma markantami a jej hodnota sa porovná s určeným prahom. Ak je vzdialenosť markantov pod určenou hodnotou, oba markanty sú považované za falošné. Iný prístup nepoužíva vzdiale-

nosť markantov, ale preskúma ich okolie. Prvý so spomínaných prístupov je použitý v práci. [4]

	CN = 2 pixel je súčasťou hrebeňu
	CN = 1 ukončenie
	CN = 3 vidlička

Obr. 5.4: Typ markantu na základe výsledku CN. Prevzaté a upravené z [24].



Obr. 5.5: Falošné markanty.

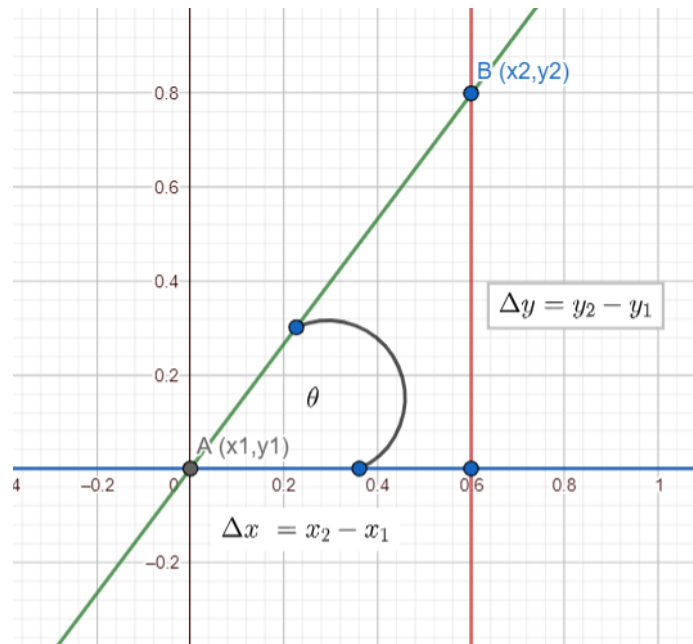
5.3 Porovnanie odtlačku a falzifikátu

Porovnanie reálneho odtlačku s falzifikátom je založené na rozpoznaní obrazov na základe extrahovaných markantov. Algoritmus najprv nájde na oboch odtlačkoch markanty, pomocou metódy *Crossing number* opisovanej v podkapitole 5.2. Pre všetky markanty vypočíta uhol. Následne zarovná snímok s falzifikátom, podľa snímku s reálnym odtlačkom. Ako ďalší krok nájde spoločné markanty, na základe ich zarovnanej pozície, typu markantu a uhlu. Nakoniec vypočíta priemerný rozdiel vzdialenosti medzi markantami reálneho odtlačku a falzifikátu.

5.3.1 Výpočet uhlu

Po extrahovaní markantov je známa pozícia a typ markantu, ale to nie je dostačujúce pri porovnaní dvoch odtlačkov. Aby bolo možné určiť, či sú dva markanty zhodné, je nutné vedieť uhol markantu. Hodnotu uhla je možné zistiť na blokovej úrovni. Tento spôsob je

vysvetlený v podkapitole 5.1.3, kde je opísaný výpočet lokálnej orientácie. Uhol je možné získať aj na pixelovej úrovni, kedy pracuje priamo z pixelom a jeho okolím. Na výpočet sú potrebné dva body. Je nájdená pozícia pixelu markantu, čo je bod A . Následne v smere hodinových ručičiek je prechádzané 8-okolie pixelu. Prvý nájdený čierny pixel je bod B . Uhol θ je uhol medzi vektorom z bodov A a B a horizontálnou osou x . Uhol je vypočítaný dosadením hodnoty smernice priamky do inverznej funkcie tangens. Smernica priamky je pomer medzi zmenou na vertikálnej osi a zmenou na horizontálnej osi. Spôsob nájdenia uhlu je zobrazený na obrázku 5.6. [11]



Obr. 5.6: Výpočet uhlu medzi bodom A a B.

5.3.2 Zarovnanie markantov

Posledný krok pred určením zhody dvoch odtlačkov je ich zarovnanie. Existujú dva odtlačky, ktoré pochádzajú z jedného prsta. Keď sa na odtlačky pozrie človek, tak dokáže nájsť zhodu. Človek vidí, že obsahujú rovnaké markanty, ktoré sú obkolesené ďalšími markantami, ktoré sa zhodujú. Aby túto zhodu vedel zistiť aj počítačový program, potrebuje jednotlivé markanty zarovnať na rovnakú pozíciu a potom ich porovná. V práci bude porovnávaný vzorový odtlačok s jeho falzifikátom. Preto je možné predpokladať, že tieto dva odtlačky sa budú na seba podobať. Avšak pri nasnímaní odtlačku a falzifikátu môže dôjsť k posunu a rotácii jednotlivých snímok. Táto podkapitola vysvetľuje spôsob zarovnania odtlačkov pomocou základných vlastností markantov, ktorými sú uhol a pozícia. Na zarovnanie podľa markantov sa používa *Houghova transformácia*.

Pri Houghovej transformácii sú vstupom dve množiny. Množina R obsahuje všetky markanty vzorového odtlačku. Množina F obsahuje markanty zachytené na falzifikáte. Výstupom sú Δ_x , Δ_y a Δ_Θ , ktoré určujú posun na osi x , osi y a rotáciu. Pri Houghovej transformácii je začínané s predpokladom, že všetky body z množiny R a F sú budúce možné zhodné body. V každom kroku vypočítame novú hodnotu pre Δ_x a Δ_y . Hodnoty sú vypočítané pomocou afinnej transformácie a rozdielu uhlov podľa rovníc 5.9 a 5.10. V ďalšom

kroku je definované akumulované pole A , kde sa ukladajú všetky možné hodnoty Δ_x , Δ_y a Δ_Θ . Pole A obsahuje aj štvrtý parameter, ktorý určuje počet hlasov pre dané parametre. Po prejdení všetkých dvojíc sa v poli A nájde prvok z najvyššou akumulovanou hodnotou. Parametre uložené pod daným indexom sú výsledné hodnoty. [21]

$$\Delta_x = x_R - (\cos \Theta - \sin \theta) * x_F \quad (5.9)$$

$$\Delta_y = y_R - (\sin \Theta + \cos \theta) * y_F \quad (5.10)$$

5.3.3 Určenie zhody dvoch markantov

Po zarovnaní snímok je možné predpokladať, že markanty vzorového odtlačku ako aj falzifikátu, ktoré majú byť označené za zhodné, sa nachádzajú na rovnakej pozícii, respektíve v jeho blízkom okolí. Markanty spĺňajúce túto vlastnosť, môžeme avšak nájsť aj na dvoch odtlačkoch, kde každý patrí inému prstu. Preto, aby boli dva markanty vyhlásené za zhodné nestačí porovnať ich pozíciu. Preto je vytvorená kombinácia viacerých parametrov, ktoré sa všetky musia zhodovať, tým sa zníži šanca na vyhlásenie rozdielnych markantov za zhodné. Okrem pozície markantu bude preto kontrolovaný aj uhol a typ markantu. Pri nasnímaní tých istých odtlačkov sa nemusia hodnoty troch vyššie spomínaných parametrov zhodovať na 100 %. Každý z parametrov má povolenú odchýlku, v ktorej sa môže líšiť a markanty sa budú stále považovať za zhodné. Markant môžeme definovať ako trojicu $M = (X, \Theta, t)$ kde:

- X – bod X určuje polohu markantu, obsahuje súradnice x a y ,
- Θ – orientácia Θ určuje uhol markantu s vodorovnou osou x ,
- t – typ t určuje, či sa jedná o ukončenie alebo vidličku.

Existuje markant M_1 , ktorý patrí do množiny markantov vzorového odtlačku prsta a markant M_2 patriaci do množiny markantov falzifikátu. Tieto dva markanty je možné považovať za zhodné, ak spĺňajú nasledujúcu rovnicu:

$$X_1 = X_2 \cup \Theta_1 = \Theta_2 \cup t_1 = t_2 = 1 \quad (5.11)$$

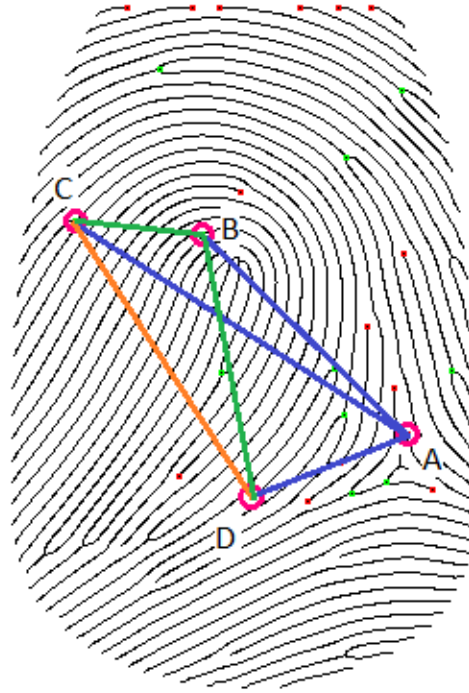
výraz $X_1 = X_2$ je považovaný za pravdivý, ak je hodnota X_2 v rozsahu povolenej odchýlky vzdialenosti o . Čo je možné vyjadriť vzťahom $|X_1 - X_2| \leq o$. Analogicky je postupované aj pri vyhodnotení pravdivosti ostatných dvoch výrazov z rovnice 5.11. Ak sú všetky tri výrazy zároveň vyhodnotené ako pravdivé, markanty M_1 a M_2 sú zhodné. [3]

5.3.4 Výpočet priemerného rozdielu vzdialenosti

Priemerný rozdiel vzdialenosti slúži ako ďalšia metrika pre porovnanie rozdielov reálneho odtlačku prsta a falzifikátu. Čím menší priemerný rozdiel vzdialenosti je dosiahnutý, tým vernejšou kópiou je daný falzifikát. Pre výpočet priemerného rozdielu vzdialenosti je potrebné mať zoznam zhodných markantov z prechádzajúceho kroku. Všetky operácie sú prevádzané nad zoznamom zhodných markantov. V prvom kroku sú vypočítané priemerné vzdialenosti medzi spárovanými markantami reálneho odtlačku prsta. Obrázok 5.7 ukazuje spôsob spájania markantov. Ružovým krúžkom sú naznačené spárované markanty. Pri výpočte je treba brať do úvahy, že úsečka \overline{AB} je identická z úsečkou \overline{BA} . Každé dva markanty v zozname sú spojené, a podľa rovnice 5.12 na výpočet vzdialenosti medzi dvoma bodmi,

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (5.12)$$

kde x_1 a y_1 sú súradnice začiatočného bodu úsečky a x_2 a y_2 je pozícia koncového bodu. Na získanie priemeru je podelený súčet vzdialeností počtom všetkých úsečiek. Rovnaký postup je zopakovaný aj pre spárované markanty falzifikátu. Počet úsečiek na oboch snímkoch sa musí zhodovať. Priemerné vzdialenosti z reálneho odtlačku a falzifikátu sú odčítané. Výsledok je priemerný rozdiel vzdialenosti.



Obr. 5.7: Spárované markanty a vzdialenosť medzi nimi.

Kapitola 6

Implementácia

Výstupom tejto práce je okrem vytvorených foriem a falzifikátov aj desktopová aplikácia, ktorá pripraví obrázok na extrakciu markantov a následne porovná polohu, uhol markantov a vypočíta priemerný rozdiel vzdialenosti markantov vzorového odtlačku prsta voči falzifikátu. Cieľom je implementovať postupy na predspracovanie obrazu a analýzu rozdielov spomínaných v kapitole 5. V tejto kapitole je popísané, aký implementačný jazyk a prostredie boli používané pri vývoji aplikácie, ako boli implementované jednotlivé časti predspracovania od segmentácie až po skeletonizáciu. Ďalej je uvedený postup extrakcie markantov a optimalizácia ich počtu. Nakoniec je vykonané zarovnanie markantov a nájdenie zhodných markantov. Všetky zdrojové súbory spomínané v nasledujúcom texte, spolu s návodom na spustenie programu, sú súčasťou priloženého pamätového média. Obsah média je popísaný v prílohe A.

6.1 Implementačný jazyk a vývojové prostredie

Aplikácia bola implementovaná v jazyku Java. Java je objektovo-orientovaný jazyk, ktorého syntax je založená na jazykoch C/C++. Jedným z dôvodov, prečo bola vybratá Java, ako implementačný jazyk je skutočnosť, že na ňu nadväzuje platforma JavaFX, ktorá slúži na vytváranie vizuálnych okenných aplikácií. Pomocou JavaFX bolo vytvorené používateľské rozhranie aplikácie. V kóde sa dá pomocou vytvorených objektov pristupovať k vizuálnym prvkom aplikácie. Celý projekt bol vyvíjaný v prostredí IntelliJ IDEA. Výsledný program je spustiteľný na operačnom systéme Windows 10. [2]

Pre jednoduchšie spracovanie obrazu bola použitá knižnica OpenCV. OpenCV je multiplatformová open-source knižnica napísaná v jazyku C++, ktorá dokáže komunikovať aj s jazykmi Python, Matlab alebo Java. OpenCV obsahuje viac ako 2500 optimalizovaných algoritmov používaných na riešenie problémov z oblasti počítačového videnia a strojového učenia. Algoritmy, ktoré sú v tejto knižnici, bývajú použité na rozpoznanie tvári, detekciu objektov vo videu a spracovanie obrazu. [22]

6.2 Štruktúra programu

Po spustení programu sa zobrazí okno aplikácie, kde si používateľ vyberie vzorový odtlačok prsta a falzifikát na porovnanie. Beh programu sa spustí stlačením tlačidla „Analyze“, kedy program vojde do triedy `Controler.java`. `Controler.java` je hlavnou triedou, ktorá komunikuje s rozhraním a určuje logický prechod programom. Postupne je každá snímka

predspracovaná a následne sú vzájomne porovnané. Metódy zabezpečujúce predspracovanie obsahuje trieda `Preprocess.java`. Metódy zabezpečujúce extrakciu markantov a porovnanie sa nachádzajú v triede `Postprocess.java`. Okrem už spomínaných tried, implementácia obsahuje aj triedy `Minutiae.java`, `MinutiaeImage.java` a `AlignmentObject.java`, ktoré slúžia na vytvorenie pomocných objektov. Implementácia všetkých tried je bližšie popísaná v nasledujúcich podkapitolách.

6.2.1 Úprava odtlačku prsta

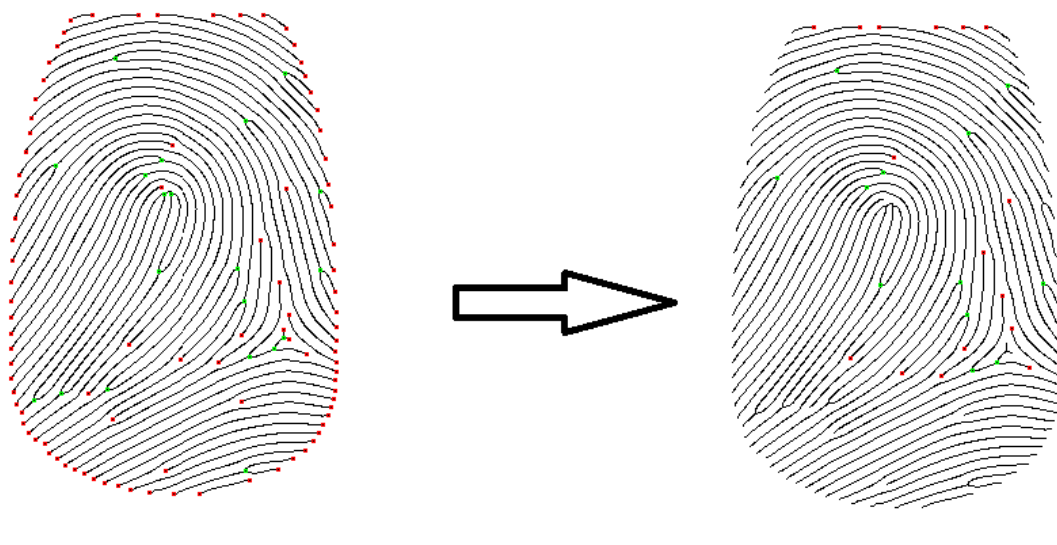
Úprava snímku odtlačku prsta začína segmentáciou. Metóda `fingerprintSegmentation()` má tri parametre. Prvý je vstupný obrázok, druhý je parameter `B` určuje veľkosť bloku a parameter `threshold` je hodnota prahu. Segmentácia je vykonávaná po blokoch. Výpočet prebieha na základe postupu z podkapitoly 5.1.1. Veľkosť bloku `B` je určená na 20 a hodnota prahu je nastavená na 300. Ak sú papilárne línie príliš svetlé, tak segmentácia sa postará o to, že svetlé časti odtlačku sa stanú pozadím. Normalizácia je implementovaná na základe vzorcov z podkapitoly 5.1.2. Hodnoty `M0` a `V0` sú nastavené podľa článku [14] od pána Honga. Ďalším krokom je výpočet lokálnej orientácie, frekvencie a Gaborovho filtra. Tieto funkcie neboli implementované v programe. Na spracovanie obrazu pomocou Gaborovho filtra bol využitý kód tretej strany napísaný v jazyku Python. Do skriptu je posielaný normalizovaný obrázok. Skript je volaný z triedy `Controller.java`, po procese normalizácie. Na jeho spustenie je použitý príkaz `getRuntime().exec()`, ktorý skript zavolá pomocou príkazového riadku. Výstupom skriptu je uložená snímka upravená Gaborovým filtrom. Implementovaný program pokračuje prístupím k uloženému obrázku. Na binarizáciu je použitá funkcia `threshold()` z knižnice `opencv`. Typ použitej binarizácie je definovaný ako `CV_THRESH_BINARY_INV | CV_THRESH_OTSU`. Poslednou metódou, ktorá zabezpečuje úpravu obrazu je `fingerprintSkeletonization()`, ktorá zabezpečuje zúženie papilárnych línií na jeden pixel. V tejto metóde sa pre jednoduchšiu prácu s odtlačkom, vstupný parameter typu `BufferedImage` zmení na 2D pole. Pracuje sa s binarizovaným obrázkom, ktorý obsahuje iba dve farby bielu a čiernu. Do poľa sú uložené biele pixely pod hodnotou 0 a čierne pod hodnotou 1. Obrázok 6.1 zobrazuje vstupný odtlačok a výsledný odtlačok po úprave obrazu.



Obr. 6.1: Vľavo sa nachádza vstupná snímka, vpravo snímka po úprave, pripravená na extrakciu markantov.

6.2.2 Extrakcia markantov a porovnanie

Implementácia metód na extrakciu porovnanie, sa nachádza v súbore `Postprocess.java`. Extrakcia markantov je implementovaná v metóde `minutiaeExtraction()`. Na začiatku je inicializovaná premenná `sum` na hodnotu 0. V cykle sa prechádza každý pixel, ak má pixel hodnotu 1 (je čierny), kontrolujú sa hodnoty na súradniciach okolo bodu. Do premennej `sum` sa pripočíta absolútna hodnota rozdielu dvoch za sebou idúcich pixelov. Nakoniec sa hodnota premennej `sum` zmenší na polovicu. Ak je `sum` rovný 3 alebo 1, pixel je pridaný do zoznamu markantov. Pre markant je vytvorená vlastná trieda `Minutiae.java`. Konštruktor tejto triedy má tieto parametre: `x` a `y` (poloha), typ markantu (1 = ukončenie, 3 = vidlička) a uhol. Celý postup je inšpirovaný vzorcami z podkapitoly 5.2. Ku extrakcii markantov sa viažu dve ďalšie funkcie `removeFalseMinutiae()` a `removeBorderMinutiae()`, ktoré odstránia nepotrebné markanty. V prvej funkcii nazvanej `removeFalseMinutiae()` sa kontroluje vzdialenosť medzi markantami. Ak je vzdialenosť menšia ako 10, tak markanty sú odstránené zo zoznamu. Funkcia `removeBorderMinutiae()` odstraňuje najmä ukončenia na okrajoch odtlačku. Prechádza obrázok po riadkoch, prvý a posledný markant na každom riadku odstráni. Obrázok 6.2 ukazuje počet markantov pred a po odstránení falšných a okrajových markantov. Pre následné porovnanie je potrebné zistiť uhly markantov. To vykonáva metóda `calculateAngle()`, ktorá pracuje so zoznamom markantov. V cykle v smere hodinových ručičiek hľadá, ktorým smerom markant pokračuje, ak zachytí ďalší čierny bod, poznačí si jeho polohu a z cyklu vyskočí. Následné vypočíta rozdiel na osi `x` a osi `y`. Pomocou funkcie `atan(yRozdiel, xRozdiel)`, ktorá je súčasťou matematickej knižnice, vypočíta uhol v radiánoch, ktorý je prepočítaný na stupne pomocou funkcie `toDegrees()`



Obr. 6.2: Počet markantov pred (vľavo) a po odstránení nepotrebných markantov (vpravo).

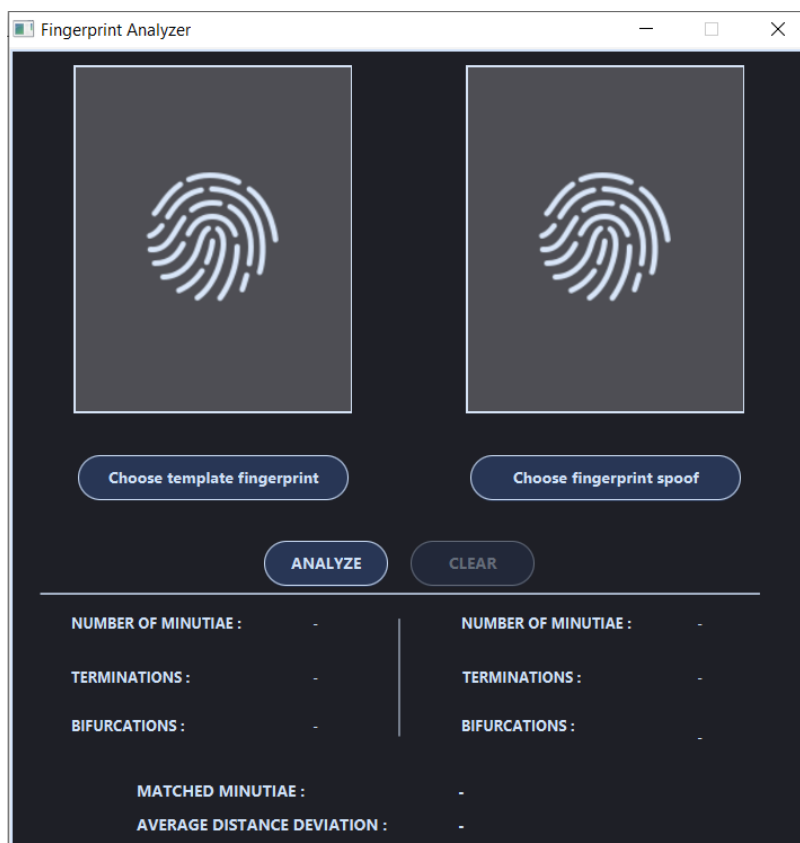
Zatiaľ všetky opísané funkcie spracovávali snímky osobitne. Pri porovnaní bude pracované s oboma snímkami súčasne. Metóda `ProcessImage()` vracia vztvorený objekt typu `MinutiaeImage`, ktorý obsahuje spracovaný obrázok a zoznam markantov. Oba obrázky sa najskôr zarovnajú vo funkcii `fingerprintsAlignment()`. Proces zarovnávania je implementovaný pomocou Houghovej transformácie z podkapitoly 5.3.2. Následne sú vo funkcii `fingerprintsMatching()` nájdené vhodné dvojice markantov. Funkcia obsahuje pevne sta-

novené odchýlky kedy sa markanty ešte považujú za vhodné. Odchýlka uhlu je 45° , čo je rozdiel jedného pixela. Odchýlka vzdialenosti bola experimentálnym spôsobom určená na hodnotu 10. Poslednou funkciou, pred ukončením programu je `averageLinesDeviation()`, ktorá vypočíta priemernú vzdialenosť zhodných markantov na reálnom odtlačku a vzdialenosť na falzifikáte. Tieto hodnoty následne odčíta. Na koniec programu sa vypíšu vypočítané hodnoty do používateľského prostredia programu a program je pripravený na ďalšie porovnávanie.

6.2.3 Grafické rozhranie

Na obrázku 6.3 je zobrazené vytvorené grafické rozhranie. Grafické rozhranie pozostáva zo vstupnej a výstupnej časti, ktoré sú rozdelené horizontálnou čiarou. Vo vstupnej časti vyberie používateľ požadované dáta. Vo výstupnej časti sa zobrazia výsledky po prebehnutí programu. Používateľ vyberie súbory, ktoré chce nahráť. Po kliknutí na tlačidlá `Choose template fingerprint` a `Choose fingerprint spoof` sa používateľovi zobrazí adresárová štruktúra. Predvolený adresár, v ktorom sa vyhľadáva, má názov *fingerprints*, ktorý obsahuje databázu odtlačkov a nachádza sa pri spustiteľnom súbore. Ak tento adresár neexistuje, začne sa prehľadávať v domovskom adresári. Vyhľadávajú sa súbory vo formáte `bmp`. Pred spustením behu programu musia byť vybraté obe snímky, ak tomu tak nie je, používateľ je na to upozornený. Po stlačení tlačidla `Analyze` používateľ čaká na výpis výsledkov. Údaje špecifické pre snímku sa vypíšu do stĺpca pod obrázkom. Týmito údajmi sú: celkový počet nájdených markantov na obrázku, ich rozdelenie na ukončenia a vidličky. Výsledky porovnania, ktoré sú spoločné pre oba snímky nájdeme v posledných dvoch riadkoch. Vstupné obrázky sa zmenia na výstupné, ktoré budú obsahovať upravené snímky so zaznačenými markantmi. Zelenou sú zaznačené vidličky a červenou ukončenia. Ak chce používateľ pokračovať, stačí tlačidlo `Clear`. Všetky hodnoty sa vynulujú a používateľ môže nahráť ďalší vzorový odtlačok a falzifikát na porovnanie.

Grafické rozhranie bolo vytvorené pomocou platformy JavaFX. Implementáciu rozhrania sa nachádza v súbore `sample.fxml`. Hlavným prvkom je `GridPane`, ktorý vytvára mriežku stĺpcov a riadkov. Má určenú šírku a dĺžku. Všetky ostatné prvky sa stávajú jeho potomkami. Potomkovia sa môžu rozprestierať cez viacero stĺpcov a riadkov, ale vždy sa musia nachádzať v rozmedzí definovaným dĺžkou a šírkou. Na výber obrázkov zo súboru bol použitý prvok `FileChooser`, ktorý poskytuje podporu štandardných dialógových okien súborov. Prvok `ImageView` slúži na zobrazenie vybraných súborov. Prvky na popis a zobrazenie vypočítaných dát pochádzajú z triedy `Label`. Na nahratie súborov, spustenie behu programu a jeho vynulovanie bol použitý prvok `Button`.



Obr. 6.3: Grafické rozhranie aplikácie. Horná časť slúži na vstupy od používateľa, dolná na výstupy z programu.

Kapitola 7

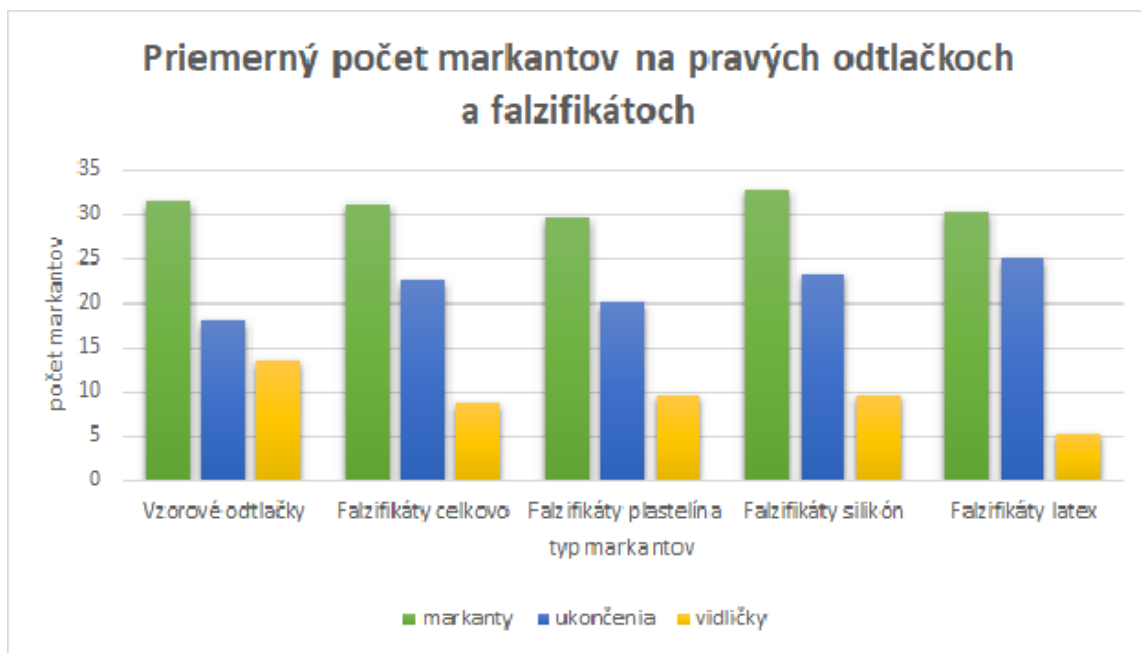
Vyhodnotenie

Táto kapitola sa zaoberá vyhodnotením kvality vytvorených falzifikátov a implementovanej aplikácie. Vyhodnotenie je založené na dátach zo 75 falzifikátov odtlačkov prstov, ktoré boli vytvorené z 10 foriem. Falzifikáty boli vytvorené z troch materiálov. Celkovo vzniklo 28 falzifikátov z plastelíny, 31 zo silikónu a 16 z tekutého latexu. Vyhodnotenú sú tri charakteristiky falzifikátov získané ako výsledok implementácie. V prvej časti je zhodnotená kvalita falzifikátov na základe porovnania počtu markantov na falzifikáte a na reálnom odtlačku. V druhej časti sa hodnotí kvalita falzifikátov, na základe priemerného rozdielu vzdialenosti medzi markantami falzifikátu a vzorového odtlačku. Posledný experiment je zameraný na počet identifikovaných spoločných dvojíc markantov na falzifikáte a zdrojovom odtlačku. Pri poslednom experimente sa výsledky zhodného počtu markantov porovnávajú s výsledkami z nástroja VeriFinger. Pri niektorých experimentoch boli porovnané aj vzorové odtlačky s ich reálnymi odtlačkami. To znamená, že pre každý reálny vzorový odtlačok bolo okrem falzifikátov nasnímaných niekoľko ďalších snímok vzorového odtlačku.

7.1 Vyhodnotenie kvality na základe počtu markantov

Prvým pozorovaným javom je počet markantov a pomer jednotlivých typov markantov zachytených na vzorových odtlačkoch a falzifikátoch, ako je vidieť na obrázku 7.1. Priemerný počet markantov (zelené stĺpce) pre vzorové odtlačky (prvý zelený stĺpec) a falzifikáty celkovo (druhý zelený stĺpec) je na podobnej hodnote. Konkrétne priemerný počet markantov pri vzorových odtlačkoch je 31,5 markanta a pri falzifikátoch 31,11 markanta. Rozdiel je 0,39 markantu, preto je možné z tohto pohľadu konštatovať, že počet markantov sa pri výrobe falzifikátov nezmenil. Čo sa však zmenilo, je pomer medzi zachytenými ukončeniami a vidličkami. Pri vzorových odtlačkoch je vidieť vyšší priemerný počet vidličiek (žlté stĺpce) zachytených na jednom odtlačku ako pri falzifikátoch. Rozdiel je 4,9 markanta. Pre podrobnejšiu analýzu, posledné tri troj-stĺpce zobrazujú priemerný počet markantov, priemerný počet ukončení a priemerný počet vidličiek pre falzifikáty rozdelené podľa materiálu. Najväčší pokles v počte vidličiek je pri latexových falzifikátoch. Po preskúmaní snímok falzifikátov bolo zistené, že pokles počtu vidličiek je spôsobený rozpojením markantu typu vidlička na dva markanty typu ukončenie. Čo vysvetľuje priamo úmerný nárast ukončení v porovnaní s poklesom vidličiek (modré a žlté stĺpce). Toto rozpojenie mohlo vzniknúť z viacerých dôvodov. Rozpojenie mohlo byť spôsobené nasnímaním, kedy falzifikát obsahuje vidličku, no nie je dostatočne výrazná a čítačka ju vyhodnotí ako dve odlišné čiary. Druhou možnosťou je, že rozpojenie bolo spôsobené úpravou snímky pri vylepšení pomocou

Gaborovho filtra, najmä v oblasti singulárnych bodov, kde môže dojsť k zlému vyhodnoteniu orientácie a frekvencie. Obrázok 7.2 zobrazuje jav rozpojenia vidličiek na konkrétnom príklade z databázy odtlačkov.



Obr. 7.1: Graf zobrazujúci priemerný počet markantov nájdených vo vzorových odtlačkoch, všetkých falzifikátoch a falzifikátoch vytvorených z jednotlivých materiálov.

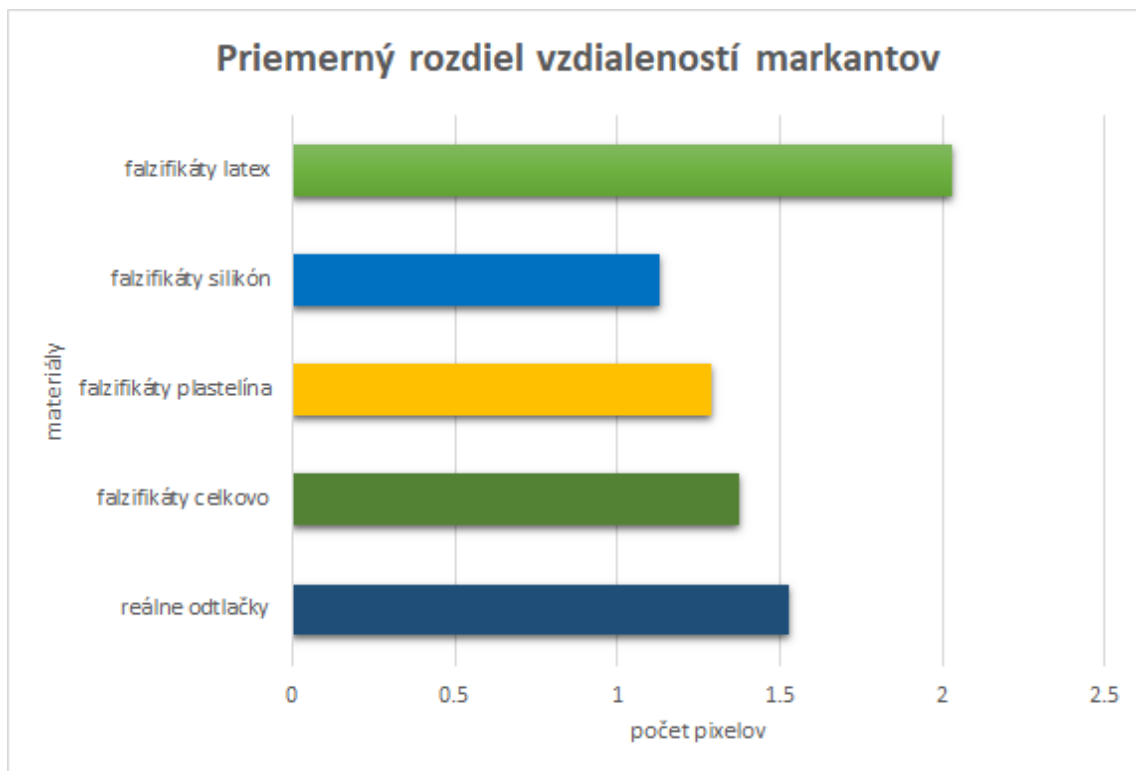


Obr. 7.2: Vidlička (ľavý obrázok) rozpojená na dve ukončenia (pravý obrázok)

7.2 Vyhodnotenie kvality na základe priemerného rozdielu vzdialenosti

Hodnota rozdielu určuje presnosť, s akou bol falzifikát vytvorený. V ideálnom prípade by sa hodnota rozdielu mala rovnať 0. Vtedy by bolo možné konštatovať, že falzifikát je presnou kópiou reálneho odtlačku. Obrázok 7.3 zobrazuje, že priemerný rozdiel vzdialenosti medzi markantmi všetkých falzifikátov a ich vzorových odtlačkov je 1,37 pixela (tmavozelený stĺpec). Rozdiel vo vzdialenosti, ktorý vznikol, je spôsobený tlakom pri nasnímaní vzorového odtlačku a falzifikátu. Každý materiál má iné vlastnosti, ktoré tiež vytvárajú

rozdiel vzdialeností. Plastelína je ľahko deformovateľná. Po odstránení z formy sa aj jemným pritlačeníím alebo natiahnutím môže falzifikát jemne rozšíriť, čo má za dôsledok zmenu vzdialenosti medzi markantmi. Ako aj pri predošlom experimente, graf zobrazuje viditeľné rozdiely pri porovnaní rôznych materiálov. Falzifikáty vyrobené z tekutého latexu majú vyšší priemerný rozdiel vzdialenosti ako plastelína či silikón. Falzifikáty vyrobené zo silikónu sa z pohľadu priemernej odchýlky javia ako najkvalitnejšie, keďže ich priemerný rozdiel v porovnaní so vzorovými odtlačkami je 1,13 pixela, pričom najmenší rozdiel dosahuje hodnotu iba 0,0212 pixela. Pri plastelínových falzifikátoch je pozorovaný podobný trend ako pri silikóne. Ako je možné vidieť v tabuľke 7.1. Minimum a maximum pri plastelínových falzifikátoch dosahujú ešte o niečo lepšie hodnoty ako pri silikónových falzifikátoch. Pri tomto experimente bola porovnaná aj priemerná vzdialenosť markantov medzi vzorovým odtlačkom a jeho rozličnými nasnímaniami. Priemerný rozdiel vo vzdialenosti markantov v tomto prípade dosiahol hodnotu 1,52 pixela. Pri falzifikátoch bola táto hodnota vyčíslená na 1,37 pixela. Čo dokazuje, že priemerný rozdiel vzdialenosti markantov je pri falzifikátoch menší ako pri reálnych odtlačkoch prstov.



Obr. 7.3: Graf zobrazujúci priemerný rozdiel vzdialenosti spárovaných markantov pre reálne odtlačky (tmavomodré), falzifikáty celkovo (tmavozelené), falzifikáty z plastelíny (žlté), falzifikáty zo silikónu (modré) a falzifikáty z latexu (zelené).

Tabuľka 7.1: Minimálne a maximálne hodnoty priemerného rozdielu vzdialenosti markantov pre falzifikáty

	Minimálna hodnota	Maximálna hodnota
Falzifikáty plastelína	0,0119	4,4059
Falzifikáty silikón	0,0212	4,7929
Falzifikáty latex	0,2769	5,2333
Reálne odtlačky	0,0177	4,1539

7.3 Vyhodnotenie kvality na základe počtu zhodných markantov

Na obrázku 7.4 je zobrazený graf, ktorý vyjadruje počet zachytených spoločných markantov na vertikálnej osi a vzorku falzifikátu (žltá, zelená a modrá krivka) alebo vzorku reálneho odtlačku (tmavozelená krivka) na horizontálnej osi. Napríklad, modrá krivka zobrazuje počet spárovaných markantov pre všetky falzifikáty vyrobené zo silikónu. Najvyššiu hodnotu zhodných markantov dosiahol falzifikát vytvorený z plastelíny. Predlohou bol reálny odtlačok prsta *Real4*. Falzifikáty s najmenším počtom zachytených spoločných markantov boli dva. Oba boli vytvorené z tekutého latexu. Pre lepšiu prehľadnosť bola vytvorená tabuľka 7.2, ktorá poskytuje základné štatistické údaje získane z grafu. Pri pohľade na priemernú hodnotu zhodných markantov majú znovu najmenšiu úspešnosť falzifikáty vyrobené z tekutého latexu. Priemerná hodnota zhodných markantov sa u plastelíny a silikónu približuje ku kvalite reálnych odtlačkov. Podľa kritéria zhodných markantov sú najkvalitnejšie falzifikáty vyrobené z plastelíny.



Obr. 7.4: Graf zobrazuje hodnoty zhodných markantov pre falzifikáty z plastelíny (zelená), zo silikónu (modrá), z tekutého latexu (žltá) a pre reálne odtlačky (tmavozelená)

Tabuľka 7.2: Minimálna, maximálna a priemerná hodnota zhodných markantov pre materiály: plastelína, silikón, tekutý latex a reálne odtlačky.

	Minimálna hodnota	Maximálna hodnota	Priemerná hodnota
Plastelína	4	26	11.71
Silikón	4	25	10.83
Tekutý latex	3	15	8.06
Reálne odtlačky	4	25	12.63

7.4 Vyhodnotenie zhody pomocou VeriFingeru

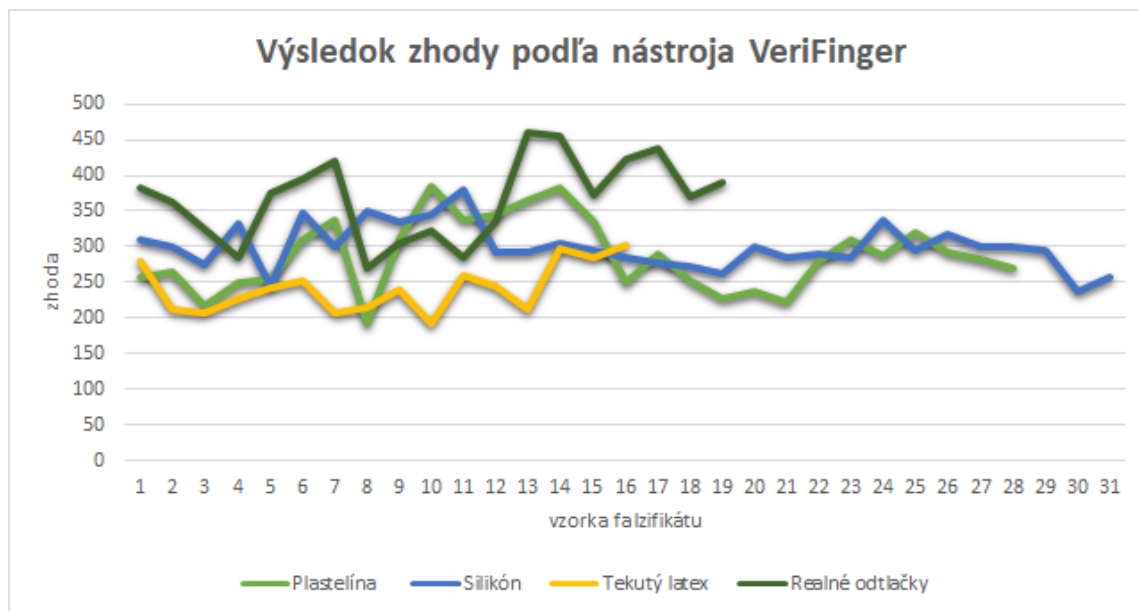
Databáza falzifikátov bola po vyhodnotení vytvoreným programom vyhodnotená aj pomocou nástroja VeriFinger, ktorý slúži na identifikáciu a verifikáciu odtlačkov. Pred spracovaním snímok programom VeriFinger bola u všetkých odtlačkov nastavená hodnota DPI na 500, aby VeriFinger dokázal so snímkami pracovať. U každého falzifikátu je vypočítané skóre zhody voči vzorovému odtlačku. V tomto experimente boli porovnané so vzorovým odtlačkom aj jeho iné reálne nasnímaná. Výsledky pre jednotlivé prsty sú uvedené v tabuľke 7.3. Syntetické odtlačky (začínajúce na Sfinge) boli porovnané iba s falzifikátmi. Priemerné hodnoty pre všetky falzifikáty sa pohybujú v rozpätí 239-341. Pri reálnych odtlačkoch je priemerná zhoda medzi 311 až 421. Reálne odtlačky majú o niečo vyššiu priemernú zhodu. Tento jav sa dá vysvetliť výsledkom z prvého experimentu, kde sa ukázalo, že pri falzifikátoch dochádza k premene vidličiek na ukončenia. Pri porovnaní nie sú takéto markanty považované za rovnaké, čím sa znižuje hodnota celkovej zhody. Najvyššiu hodnotu zhody z vyrobených falzifikátov dosiahol falzifikát z plastelíny, ktorého predlohou bol odtlačok *Real4*. Na porovnanie zhody sa je možné pozrieť aj z iného pohľadu. Tabuľka 7.4 zobrazuje minimálnu, maximálnu a priemernú hodnotu zhody na základe použitých materiálov. Výsledky zhody na základe materiálov sú spracované aj graficky na obrázku 7.5, kde falzifikáty z tekutého latexu neprekvapili a dosahujú najnižšie hodnoty. Hodnoty reálnych odtlačkov, falzifikátov z plastelíny a falzifikátov zo silikónu dosahujú podobné výsledky. Z falzifikátov mali podľa nástroja VeriFinger najvyššiu úspešnosť falzifikáty vyrobené zo silikónu.

Tabuľka 7.3: Výsledky zhody vypočítané pomocou nástroja VeriFinger z pohľadu prstov

	Falzifikáty			Reálne odtlačky		
	Min	Max	Priemer	Min	Max	Priemer
Real1	206	311	257	285	383	339
Real2	226	347	292	271	421	365
Real3	192	309	249	385	334	311
Real4	253	385	335	370	437	399
Real5	292	383	341	373	460	427
Sfinge1	207	304	262	-	-	-
Sfinge2	192	227	239	-	-	-
Sfinge3	213	309	277	-	-	-
Sfinge4	285	337	306	-	-	-
Sfinge5	269	299	289	-	-	-

Tabuľka 7.4: Výsledky zhody vypočítané pomocou nástroja VeriFinger z pohľadu materiálov

	Minimálna hodnota	Maximálna hodnota	Priemerná hodnota
Plastelína	192	385	287
Silikón	238	380	300
Tekutý latex	192	303	242
Reálne odtlačky	271	460	366



Obr. 7.5: Graf zobrazujúci hodnotu zhody falzifikátov z nástroja VeriFinger.

Po vyhodnotení falzifikátov implementovaným programom a nástrojom VeriFinger môže byť konštatovaných niekoľko záverov. Za najmenej kvalitné falzifikáty oba programy vyhodnotili falzifikáty vyrobené z tekutého latexu. Tento trend môžeme pozorovať vo všetkých vyhodnotených kategóriách. Latexové falzifikáty mali najmenšiu priemernú zhodu, najväčší rozdiel vzdialeností markantov medzi vzorovým odtlačkom a falzifikátom a najmenší počet zhodných markantov. Falzifikáty z tekutého latexu vykazovali aj najvýraznejšiu zmenu pomeru medzi ukončeniami a vidličkami. Ďalším záverom je, že reálne odtlačky v porovnaní s falzifikátmi dosahovali pri vyhodnotení počtu zhodných markantov a pri vyhodnotení nástrojom VeriFinger o pár jednotiek vyššiu zhodu, čo je dôsledok zníženia počtu vidličiek na falzifikátoch. Posledným záverom je, že podľa oboch programov majú falzifikáty z plastelíny a silikónu podobnú kvalitu. Na základe priemerného rozdielu vzdialenosti markantov, počtu markantov a výsledkov z nástroja VeriFinger majú lepšiu kvalitu silikónové falzifikáty. Na základe počtu zhodných markantov sa javia o niečo kvalitnejšie falzifikáty z plastelíny.

Kapitola 8

Záver

Hlavným cieľom tejto bakalárskej práce bolo vytvoriť a analyzovať falzifikáty odtlačkov prstov vytvorených z foriem, ktoré vznikli pomocou vypalovania. Pre všeobecné zorientovanie sa v téme bola najskôr naštudovaná literatúra z oblasti biometrie, odtlačkov prstov a výroby foriem a falzifikátov. Ďalším krokom bolo vyrobenie foriem, z ktorých boli falzifikáty vytvorené. Pri výrobe foriem pomocou vypalovania bolo otestovaných viacero materiálov. Z kombinácie materiálov a sily laseru sa najviac osvedčilo tvrdé bukové drevo. Do dreva bolo vypálených 10 finálnych foriem. Z týchto foriem boli vytvorené falzifikáty z plastelíny, silikónu a tekutého latexu. Po ich nasnímaní bola vytvorená databáza 75 falzifikátov.

Následne bol implementovaný program, ktorý porovnával vzorové odtlačky s falzifikátmi. V prvom kroku program predspracoval nasnímané odtlačky a falzifikáty odtlačkov prstov. Tento krok zabezpečil vylepšenie kvality ich obrazu. Predspracovanie obrazu bolo zložené z viacerých procesov. Začínalo sa procesom segmentácie, po segmentácii nasledovala normalizácia, výpočet lokálnej orientácie a frekvencie, a aplikovanie Gaborového filtra. Posledné dva kroky v predspracovaní boli binarizácia a skeletonizácia. Po úprave boli zo snímok extrahované markanty a snímky vzorových odtlačkov a falzifikátov boli na základe extrahovaných markantov porovnané. Program vyhodnotil pri načítaných snímkach počet markantov a určil typ markantov. Pri porovnaní dvoch snímok určil zhodné markanty a priemerný rozdiel vzdialenosti spoločných markantov.

Na overenie práce implementovaného programu boli snímky falzifikátov vyhodnotené pomocou nástroja VeriFinger, ktorý dokáže porovnať odtlačky. Podľa výsledkov implementovaného programu a nástroju VeriFinger bolo vyhodnotené, že v priemere najviac kvalitné falzifikáty boli vyrobené zo silikónu. Na základe výsledkov z kapitoly Vyhodnotenie bolo zistené, že vytvorené falzifikáty obsahujú o 36 % menej vidličiek ako vzorové odtlačky. Falzifikát s najvyšším počtom zhodných markantov patril odtlačku *Real4* a bol vytvorený z plastelíny. Pri porovnaní vzorových odtlačkov s falzifikátmi a vzorových odtlačkov s reálnymi odtlačkami bolo zistené, že priemerný rozdiel vzdialenosti markantov pri falzifikátoch je nižší ako pri reálnych odtlačkoch.

Úspešné porovnanie výsledkov implementovaného programu s výsledkami z programu VeriFinger dokazuje, že ciele práce boli splnené. Boli vypálené formy, pomocou ktorých boli vytvorené falzifikáty. Falzifikáty boli pomocou skeneru načítané do digitálnej formy. Následne bol implementovaný program na analýzu rozdielov. Všetky nasnímané odtlačky boli analyzované pomocou implementovaného programu a nástroju VeriFinger. Správnu funkčnosť programu dokazujú podobné výsledky z nástroju VeriFinger. V budúcnosti by mohol byť program rozšírený o ďalšie funkcionality ako pridanie používateľského vstupu na upravenie prahových hodnôt pri segmentácii a normalizácii, integrácia čítačky odtlačkov

prstov, čo by umožnilo priame načítavanie odtlačkov prstov do programu, možnosť analýzy viacerých odtlačkov súčasne a optimalizovanie rýchlosti aplikácie. Okrem zlepšenia programu je ďalším možným rozšírením práce preskúmanie iných materiálov, či už na výrobu foriem alebo falzifikátov.

Literatúra

- [1] *Image Thresholding* [online]. [cit. 2021-04-12]. Dostupné z: https://docs.opencv.org/master/d7/d4d/tutorial_py_thresholding.html.
- [2] *Open CV* [online]. [cit. 2021-04-12]. Dostupné z: <https://opencv.org>.
- [3] ADEWOLE, S. K., JIMOH, G. R. a ABIKOYE, C. O. A Review of Algorithms for Fingerprint Image Acquisition, Preprocessing and Minutiae Extraction. *Lorin Journal of Science*. 2014, zv. 1, č. 2, s. 245–263. ISSN 2408 – 4840.
- [4] BANSAL, R., SEHGAL, P. a BEDI, P. Minutiae Extraction from Fingerprint Images - a Review. *International Journal of Computer Science Issues*. September 2011, zv. 8, č. 3. ISSN 1694-0814.
- [5] BARTŮNĚK, J. S. *Minutiae Extraction from Fingerprint with Neural Network and Minutiae based Fingerprint Verification*. Karlskrona, SWE, 2005. Diplomová práce. Blekinge Institute of Technology, School of Engineering, Department of Signal Processing. Dostupné z: <http://www.diva-portal.org/smash/get/diva2:833407/FULLTEXT01.pdf>.
- [6] CAPPELLI, R. SFinGe: an Approach to Synthetic Fingerprint Generation. *International Workshop on Biometric Technologies*. Január 2004. DOI: 10.1007/978-3-642-27733-7_8-2.
- [7] CHALOUPKA, R. *Generátor otisků prstů*. Brno, 2007. Diplomová práce. FIT VUT v Brně. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=115874.
- [8] CHUGH, T., CAO, K. a JAIN, A. K. Fingerprint Spoof Buster. *CoRR*. 2017, abs/1712.04489. Dostupné z: <http://arxiv.org/abs/1712.04489>.
- [9] DASS, S. C. a JAIN, A. K. Fingerprint Classification Using Orientation Field Flow Curves. In: *Proceedings of the Fourth Indian Conference on Computer Vision, Graphics and Image Processing*. Kolkata, India: DBLP, 2004. ICVGIP. ISBN 978-1-4503-1660-6.
- [10] DRAHANSKÝ, M., ed. *Hand-based biometrics: Methods and Technology*. London: The Institution of Engineering and Technology, 2018. ISBN 978-1-78561-224-4.
- [11] DRAHANSKÝ, M., ORSÁG, F. a KOL. *Biometrie*. Brno: Computer Press, 2011. ISBN 978-80-254-8979-6.

- [12] GUENNOUNI, S., MANSOURI, A. a AHAITOUF, A. Biometric Systems and Their Applications. In: GIUDICE, G. L. a CATALÁ, A., ed. *Visual Impairment and Blindness - What We Know and What We Have to Know*. London: IntechOpen, 2020, kap. 20. DOI: 10.5772/intechopen.84845. ISBN 978-1-83880-258-5.
- [13] HONG, L. *Automatic Personal Identification Using Fingerprints*. East Lansing, Michigan, 1998. Dizertačná práca. Michigan State University. Dept. of Computer Science.
- [14] HONG, L., WAN, Y. a JAIN, A. K. Fingerprint Image Enhancement: algorithm and performance evaluation. *IEEE Transactions on pattern analysis and machine intelligence*. 1998, zv. 8, č. 20, s. 777–789. DOI: 10.1109/34.709565.
- [15] HUCKEMANN, S., HOTZ, T. a MUNK, A. Global Models for the Orientation Field of Fingerprints: An Approach Based on Quadratic Differentials. *IEEE Transaction on Pattern Analysis and Machine Intelligence*. 2008, zv. 30, č. 1. DOI: 10.1109/TPAMI.2007.70826.
- [16] JAIN, A. K., FLYNN, P. a ROSS, A. A. *Handbook of biometrics*. New York: Springer, 2008. ISBN 978-0-387-71040-2.
- [17] JUREK, J. *Biometrické rozpoznání živosti prstu*. Brno, CZ, 2016. Diplomová práca. Vysoké učení technické v Brne, Fakulta elektrotechniky a komunikačních technologií.
- [18] KANICH, O., MÉZL, M. a DRAHANSKÝ, M. Use of Creative Materials for Fingerprint Spoofs. In: *2018 International Workshop on Biometrics and Forensics (IWBF)*. Institute of Electrical and Electronics Engineers, 2018, s. 1–8. DOI: 10.1109/IWBF.2018.8401565. ISBN 978-1-5386-1366-5. Dostupné z: <https://www.fit.vut.cz/research/publication/11185>.
- [19] KANICH, O. *Fingerprint damage simulation: a simulation of fingerprint distortion, damaged sensor, pressure and moisture*. Saarbrücken: Lambert academic publishing, 2014. ISBN 978-3-659-63942-5.
- [20] MALTONI, D., MAIO, D., JAIN, A. K. a PRABHAKAR, S. *Handbook of Fingerprint Recognition*. Springer, 2003. ISBN 0-387-95431-7.
- [21] MLAMBO, C. S., MATHEKGA, M. E. a NELWAMONDO, F. V. A Study of Hough Transform-based Fingerprint Alignment Algorithms. *International Journal of Computer Applications*. October 2014, zv. 103, č. 8. DOI: 10.5120/18091-9158.
- [22] ORACLE. *JavaFX: Getting Started with JavaFX* [online]. [cit. 2021-04-12]. Dostupné z: <https://docs.oracle.com/javase/8/javafx/get-started-tutorial/jfx-overview.htm#JFXST784>.
- [23] RAK, R., MATYÁŠ, V. a ŘÍHA, Z. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. ISBN 978-80-247-2365- 5.
- [24] RAVI, J., RAJA, K. B. a VENUGOPAL, K. R. Fingerprint recognition using minutia score matching. *International Journal of Engineering Science and Technology*. 2009, zv. 1, č. 2, s. 35–42. ISSN 0975-5462.

- [25] RAYMOND, T. *Fingerprint Image Enhancement and Minutiae Extraction*. Perth, 2003. Diplomová práce. University of Western Australia. Dostupné z: <https://www.peterkovesi.com/studentprojects/raymondthai/RaymondThai.pdf>.
- [26] ROSS, A. A. *Information Fusion in Fingerprint Authentication*. East Lansing, Michigan, 2003. Dizertačná práce. Michigan State University. Department of Computer Science and Engineering.
- [27] SHENZHEN HINGIN TECHNOLOGY COMPANY. *L1 Pro Instruction manual*. 2019. Dostupné z: <https://fccid.io/2ATNE-L1PV12/User-Manual/User-Manual-4582687.pdf>.
- [28] SUDARMA, M. a SUTRAMIANI, N. P. The Thinning Zhang-Suen Application Method in the Image of Balinese Scripts on the Papyrus. *International Journal of Computer Applications*. Apríl 2014, zv. 91, č. 1. DOI: 10.5120/15844-4726.
- [29] TAN, X., BHANU, B. a LIN, Y. Fingerprint Classification Based on Learned Features. *IEEE Transactions on Systems Man and Cybernetics Part C (Applications and Reviews)*. 2005, zv. 3, č. 35, s. 287–300. DOI: 10.1109/TSMCC.2005.848167.
- [30] TRIGGS, R. *How fingerprint scanners work: Optical, capacitive, and ultrasonic explained* [online]. [cit. 2021-03-24]. Dostupné z: <https://www.androidauthority.com/how-fingerprint-scanners-work-670934/>.
- [31] TUMIN, S. a ENCHEVA, S. A Closer Look at Authentication and Authorization Mechanisms for Web-Based Applications. In: *Proceedings of the 5th WSEAS Congress on Applied Computing Conference, and Proceedings of the 1st International Conference on Biologically Inspired Computation*. Stevens Point, Wisconsin, USA: World Scientific and Engineering Academy and Society (WSEAS), 2012, s. 100–105. BICA'12. ISBN 9781618040893.

Príloha A

Obsah priloženého pamäťového média

Priložené pamäťové médium obsahuje:

- **xsocho14.pdf** - textová časť bakalárskej práce
- **xsocho14.zip** - zdrojové súbory k textovej časti bakalárskej práce
- **src.zip** - zdrojové súbory k programu
- **FingerprintAnalyzer.zip** - obsahuje spustiteľnú verziu programu, sadu nasnímaných falzifikátov a `readme.txt`, kde je popísaný návod na spustenie programu
- **results.zip** - výsledky a grafy použité v práci
- **readme.txt** - súbor s bližším popisom obsahu adresára