



**VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ**

BRNO UNIVERSITY OF TECHNOLOGY

**FAKULTA INFORMAČNÍCH TECHNOLOGIÍ**

FACULTY OF INFORMATION TECHNOLOGY

**ÚSTAV INTELIGENTNÍCH SYSTÉMŮ**

DEPARTMENT OF INTELLIGENT SYSTEMS

**POKROČILÉ GENEROVÁNÍ ARTEFAKTŮ FALZIFIKÁTŮ  
DO SYNTETICKÝCH OTISKŮ PRSTŮ**

ADVANCED GENERATION OF SPOOF ARTEFACTS INTO SYNTHETIC FINGERPRINTS

**DIPLOMOVÁ PRÁCE**

MASTER'S THESIS

**AUTOR PRÁCE**

AUTHOR

**Bc. ŽOFIA VRÁBL'OVÁ**

**VEDOUCÍ PRÁCE**

SUPERVISOR

**Ing. ONDŘEJ KANICH, Ph.D.**

BRNO 2021

## Zadání diplomové práce



23942

Studentka: **Vrábl'ová Žofia, Bc.**  
Program: Informační technologie  
Obor: Informační systémy a databáze  
Název: **Pokročilé generování artefaktů falzifikátů do syntetických otisků prstů**  
**Advanced Generation of Spoof Artefacts into Synthetic Fingerprints**  
Kategorie: Zpracování obrazu  
Zadání:

1. Prostudujte literaturu týkající se rozpoznávání podle otisků prstů, syntetického generování otisků prstů a tvorby falzifikátů. Seznamte se z možnými artefakty, které jsou typické při snímání falzifikátů otisků prstů a jejich simulacemi do syntetických otisků prstů.
2. Navrhněte vylepšení stávajícího modelu či úplně nový přístup a posléze algoritmus pro generování minimálně dvou artefaktů (např. prasklina, nerovnoměrnosti papilárních linií, artefakty mimo plochu otisku, apod.) do syntetických otisků prstů. Řešení bude umožňovat anotaci provedeného poškození a její export.
3. Navržený algoritmus z předchozího bodu implementujte.
4. Proveďte otestování Vašeho řešení pomocí vhodných algoritmů (např. IDkit, VeriFinger, FiQiVi, apod.). Prozkoumejte vliv artefaktů na porovnávání otisků prstů, na určení jejich kvality a posuďte rozdíl mezi původním a vylepšeným řešením.
5. Dosažené výsledky shrňte a diskutujte. Uveďte možná rozšíření Vašeho řešení.

### Literatura:

- Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S.: *Handbook of Fingerprint Recognition*. Springer, 2009, pages 512. ISBN 978-1-8488-2254-2.
- 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.
- Kanich, O.: *Research in Fingerprint Damage Simulations*, Doctoral thesis, FIT BUT in Brno, Brno, 2018, p. 148.
- Vrábl'ová, Ž.: *Generování projevu falzifikátů do syntetických otisků prstů z generátoru SFinGe*, Bakalářská práce, FIT VUT v Brně, Brno, 2019.

Při obhajobě semestrální části projektu je požadováno:

- Body 1 a 2.

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

Vedoucí práce: **Kanich Ondřej, Ing., Ph.D.**

Vedoucí ústavu: Hanáček Petr, doc. Dr. Ing.

Datum zadání: 1. listopadu 2020

Datum odevzdání: 19. května 2021

Datum schválení: 11. listopadu 2020

## Abstrakt

Cielom práce je rozšírenie aplikácie pre generovanie prejavov falzifikátov do syntetických odtlačkov prstov o možnosť generovania nových prejavov falzifikátov spolu s anotáciami vytvorených poškodení. Prejavy falzifikátov vybrané pre rozšírenie aplikácie sú oblasti papilárnych línií s nižšou jasnosťou a projekcia praskliny v materiáli falzifikátu. Vybrané prejavy boli analyzované, bol vytvorený návrh metód pre ich generovanie a metódy boli následne implementované. Vygenerovaním implementovaných prejavov falzifikátov sa na základe testovania preukázateľne znížila kvalita syntetických odtlačkov prstov, aj skóre podobnosti určované pri identifikácii. V porovnaní s pôvodnými implementovanými prejavmi sa kvalita odtlačkov prstov znížila v rozšírenom riešení viac, skóre podobnosti pri generovaní samostatných prejavov falzifikátov sa celkovo znížilo približne rovnako.

## Abstract

The goal of this thesis is to extend the application for spoof effects generation into synthetic fingerprints with the possibility of generation of two new spoof effects together with annotations of generated damages. Spoof effects chosen for this thesis are areas with lower clarity and defects in spoof material. Those effects were analyzed, methods to generate those effects were designed and then implemented. According to testing, generation of two new added spoof effects led to reduction in quality of fingerprint images, as well as the value of the similarity score determined during identification. In comparison with the original solution, the quality of the fingerprints decreased more in the extended solution, the similarity score in the generation of separate spoof effect decreased overall approximately equally.

## Klíčové slová

odtlačky prstov, falzifikáty odtlačkov prstov, syntetické odtlačky prstov, prejavy falzifikátov

## Keywords

fingerprints, spoofed fingerprints, synthetic fingerprints, spoof effects

## Citácia

VRÁBLOVÁ, Žofia. *Pokročilé generování artefaktů falzifikátů do syntetických otisků prstů*. Brno, 2021. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Ondřej Kanich, Ph.D.

# Pokročilé generování artefaktů falzifikátů do syntetických otisků prstů

## Prehlásenie

Prehlasujem, že som túto diplomovú prácu vypracovala samostatne pod vedením pána Ing. Ondřeja Kanicha, Ph.D. Uviedla som všetky literárne pramene, publikácie a ďalšie zdroje, z ktorých som čerpala.

.....  
Žofia Vráblová  
16. mája 2021

## Podakovanie

Chcela by som sa poďakovať môjmu vedúcemu doktorovi Ondřejovi Kanichovi za jeho rady, obsiahle odpovede na otázky a časté konzultácie.

# Obsah

<b>1</b>	<b>Úvod</b>	<b>3</b>
<b>2</b>	<b>Odtlačky prstov</b>	<b>4</b>
2.1	Biometria . . . . .	4
2.2	Biologické pozadie odtlačkov prstov . . . . .	5
2.3	Vlastnosti odtlačkov prstov . . . . .	8
2.4	Získavanie odtlačkov prstov . . . . .	10
2.5	Rozpoznávanie odtlačkov prstov . . . . .	12
2.6	Porovnávanie odtlačkov prstov . . . . .	14
<b>3</b>	<b>Falzifikáty odtlačkov prstov</b>	<b>18</b>
3.1	Nebezpečenstvo falšovania odtlačkov prstov . . . . .	18
3.2	Metódy výroby falzifikátov . . . . .	20
3.3	Artefakty falzifikátov . . . . .	24
3.4	Detekcia živosti . . . . .	26
3.5	Detekcia falzifikátov . . . . .	29
<b>4</b>	<b>Generátor syntetických odtlačkov</b>	<b>31</b>
4.1	Syntetické odtlačky prstov . . . . .	31
4.2	SFinGe . . . . .	32
4.3	Chaloupkov generátor odtlačkov prstov . . . . .	34
4.4	SyFDaS . . . . .	36
4.5	Anguli . . . . .	37
4.6	SYnFi . . . . .	38
<b>5</b>	<b>Návrh</b>	<b>39</b>
5.1	Opis aktuálnej aplikácie . . . . .	39
5.2	Výber artefaktov falzifikátov pre rozšírenie aplikácie . . . . .	41
5.3	Nižšia jasnosť papilárnych línií . . . . .	41
5.4	Prasklina . . . . .	44
5.5	Anotácie poškodení . . . . .	48
<b>6</b>	<b>Implementácia</b>	<b>49</b>
6.1	Celkové úpravy aplikácie . . . . .	49
6.2	Trieda FingerprintMask . . . . .	51
6.3	Trieda LowerClarity . . . . .	52
6.4	Trieda Defect . . . . .	57

<b>7 Testovanie</b>	<b>65</b>
7.1 Vytvorené dátové sety . . . . .	65
7.2 Vyhodnotenie testovania nástrojom FiQiVi . . . . .	66
7.3 Vyhodnotenie testovania nástrojom VeriFinger . . . . .	70
<b>8 Záver</b>	<b>75</b>
<b>Literatúra</b>	<b>77</b>

# Kapitola 1

## Úvod

V súčasnosti sú odtlačky prstov najpoužívanější biometrickou charakteristikou využívanou pre zabezpečenie v biometrických systémoch, pretože vhodným spôsobom spĺňajú kritériá kladené na potenciálne použiteľné biometrické vlastnosti. Každá osoba má jedinečný odtlačok prsta, ktorý sa počas života nemení, dá sa kvantitatívne merať jednoduchým snímaním a ako metóda zabezpečenia je medzi užívateľmi všeobecne akceptovaný. Najslabšou vlastnosťou odtlačku prsta je vysoká miera rizika sfalšovania v dôsledku jeho zanechávania na mnohých povrchoch a relatívne jednoduchých metód výroby falzifikátov vhodných pre oklamanie digitálnych senzorov odtlačkov prstov.

Z tohto dôvodu je vynakladaná veľká snaha o neustále zlepšovanie detekcie živosti, ktorá by v súčasnosti mala byť nutnou súčasťou senzorov odtlačkov prstov. Aj v dnešnej dobe sa však nájdu senzory bez detekcie živosti, napríklad v niektorých mobilných telefónoch. Detekcia falzifikátov je niekedy považovaná za metódu patriacu pod detekciu živosti, niekedy je kladená na rovnakú úroveň ako detekcia živosti. Ide o opačný princíp, v rámci ktorého sú v obrázkoch odtlačkov prstov hľadané prejavy falzifikátov na rozdiel od prejavov živého prsta. Aktuálne je zavedený nový názov pre detekciu živosti, a síce detekcia prezenčného útoku, ktorý pod seba zahŕňa oba uvedené spôsoby odhalenia falzifikátov.

Algoritmy vznikajúce v oblasti rozpoznávania odtlačkov prstov vyžadujú pre testovanie obrovské databázy odtlačkov prstov, často vytvárané pomocou generátorov syntetických odtlačkov prstov. Motiváciou pre túto prácu je umožnenie generovania realisticky vyzera-  
júcich syntetických odtlačkov prstov s prejavmi falzifikátov, čím môže byť zlepšený vývoj a testovanie algoritmov pre detekciu falzifikátov, alebo môžu byť použité pri tréningu daktyloskopických expertov, ktorí odhaľujú falzifikáty len na základe ich znalostí a skúseností, nie len v oblasti informatiky. Aplikácia, ktorá umožňuje takéto generovanie, vznikla ako bakalárska práca [1] a v tejto práci je rozširovaná o generovanie ďalších prejavov falzifikátov, ako aj anotácií vytvorených poškodení. Vďaka anotáciám bude možné vytvoriť tréningovú množinu pre strojové učenie, prípadne bude podľa nich možné vyhodnotiť presnosť algoritmov pre detekciu falzifikátov.

V kapitole 2 sú uvedené teoretické základy nutné pre porozumenie práci s odtlačkami prstov. V kapitole 3 sú priblížené falzifikáty odtlačkov prstov. Kapitola 4 sa zaoberá syntetickými odtlačkami prstov a ich generátormi. V kapitole 5 je uvedený výber prejavov falzifikátov, ktoré sú spracovávané v tejto práci, spolu s výsledkami analýzy ich vzhľadu a návrhom algoritmov pre generovanie. V kapitole 6 je uvedený spôsob a výsledky implementácie generovania prejavov falzifikátov. V kapitole 7 sú opísané dátové sety vytvorené prostredníctvom rozšírenej aplikácie spolu s priebehom testovania a jeho výsledkami.

## Kapitola 2

# Odtlačky prstov

Odtlačky prstov sú v súčasnosti najpoužíwanejšou biometrickou charakteristikou slúžiacou pre rozpoznávanie ľudí [2]. Pre pochopenie práce s nimi je najskôr nutné všeobecne sa zoznámiť s metódami rozpoznávania osôb, tzv. biometrickými údajmi. Okrem toho je potrebné pochopiť aj to, ako funguje samotné rozpoznávanie založené na odtlačkoch prstov. V úvode kapitoly je stručne predstavená biometria, biometrické charakteristiky a vlastnosti, ktoré sú používané pre opis biometrických charakteristík a ich vhodnosti použitia pre biometrické systémy. Ďalej je v kapitole priblížené biologické pozadie odtlačkov prstov. Následne sú uvedené vlastnosti odtlačkov prstov, ktoré sú používané pri automatizovanom rozpoznávaní odtlačkov prstov, ale aj pri porovnávaní daktyloskopmi. Posledné časti kapitoly približujú jednotlivé kroky automatizovaného rozpoznávania odtlačkov prstov a rôzne prístupy k samotnému porovnávaniu, ktoré je kľúčovým prvkom celého rozpoznávania.

### 2.1 Biometria

Slovo biometria pochádza z gréčtiny a môže byť preložené ako meranie života [2]. Z pohľadu informačných technológií je biometria definovaná ako automatické rozoznávanie individuí založené na ich fyzických a behaviorálnych vlastnostiach [3]. Rozpoznávané biometrické vlastnosti musia byť rozlišovacie, čiže s určenou presnosťou musí byť možné odlíšiť na základe nich rozdielne osoby [4].

Použitie biometrie pre zabezpečenie zariadení či informácií má niekoľko výhod, napríklad odrádza útočníkov od útokov, zvyšuje bezpečnosť, zvyšuje pohodlie užívateľa [2]. Na druhej strane prináša aj určité nevýhody, napríklad nemôže byť anulovaná v prípade poškodenia, jej výstupom je skóre porovnania, ktoré je nejednoznačné, nezachováva súkromie, biometrický systém je napadnutelný. [2].

Alternatívou k biometrii je zabezpečenie použitím hesiel alebo pin kódov. Tento druh zabezpečenia nie je ideálny, najmä vzhľadom na to, že užívatelia majú tendenciu zabúdať a používať rovnaké heslo opakovane. Experimentmi bolo už v roku 2007 zistené, že typický internetový užívateľ má približne 25 účtov chránených heslom a pre prístup do nich využíva 6,5 hesiel, z čoho vyplýva, že každé heslo používa na 3,9 odlišných webových stránkach. [5]

Ďalšou alternatívou je používanie identifikačných kariet, ktoré ale môžu byť jednoducho odcudzené alebo stratené. Spoľahlivý systém pre identifikáciu osôb by mal používať biometriu [5]. Biometrická charakteristika užívateľa nemôže byť stratená ani zabudnutá, užívateľ ju nemôže poprieť a pre útočníkov nie je úplne jednoduché jej falšovanie [6].



V biometrickom systéme sa pre zabezpečenie používa jedna alebo viac biometrických charakteristík. Biometrické charakteristiky sú rozdelené do dvoch skupín, podľa toho, či sa jedná o fyzické vlastnosti alebo behaviorálne vlastnosti. Medzi fyzické vlastnosti je zaradený odtlačok prsta, tvár, dúhovka oka, sietnica oka, atď. Medzi behaviorálne vlastnosti patrí reč, mimika tváre, dynamická forma podpisu, chôdza, atď. [2].

Pri výbere biometrickej charakteristiky vhodnej pre zabezpečenie určitého systému sa zohľadňujú najmä nasledujúce vlastnosti [7] [8]:

- Univerzálnosť – každá osoba by mala mať danú biometrickú charakteristiku,
- jedinečnosť – žiadne dve osoby nemôžu mať danú biometrickú charakteristiku rovnakú,
- konštantnosť – biometrická charakteristika je v čase nemenná,
- získateľnosť – biometrická charakteristika musí byť kvantitatívne merateľná,
- akceptácia – ochota ľudí nechať biometrickú charakteristiku nasnímať,
- výkonnosť – biometrická charakteristika sa nemôže zmeniť ani zostarnúť, čo máva vplyv na výkonnosť systému,
- odolnosť proti falšovaniu – náročnosť vytvorenia falzifikátu danej biometrickej charakteristiky.

Posledné tri vlastnosti sa viažu k praktickému použitiu biometrického systému [6] [8]. Z tohto pohľadu môže byť uvažované aj o ďalšej vlastnosti, ktorou sú finančné náklady na zabezpečenie [2]. Neexistuje biometrická charakteristika, ktorá by absolútne spĺňala niektorú z vlastností, ani biometrická charakteristika, ktorá by ich spĺňala simultánne, preto sa pri výbere vhodnej biometrickej charakteristiky berie do úvahy kompromis medzi danými vlastnosťami [4].

V biometrii sú rozoznávané dve základné metódy autentifikácie [2] [4]:

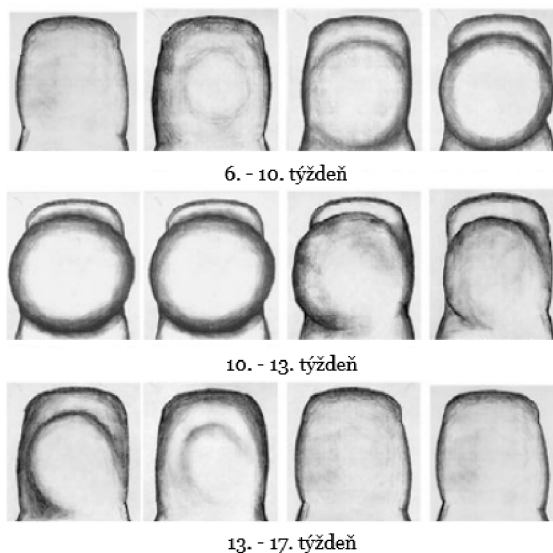
- Identifikácia – slúži k zisteniu identity osoby, biometrickému systému je poskytnutá len biometrická charakteristika, prehľadáva sa celá databáza a výsledkom je nájdená alebo nenájdená identita osoby.
- Verifikácia – slúži k potvrdeniu identity osoby, biometrickému systému je poskytnutý unikátny identifikátor osoby a jej biometrická charakteristika, v databáze sa porovná len jeden záznam a výsledkom je potvrdenie alebo nepotvrdenie identity.

## 2.2 Biologické pozadie odtlačkov prstov

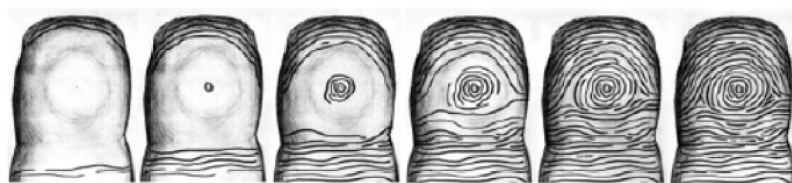
Odtlačok prsta sa počas vývinu plodu objavuje, keď sa pokožka na špičkách prstov začína diferencovať a plne sformovaný je okolo siedmeho mesiaca vývinu. Vzor odtlačku prsta od svojho sformovania ostáva nemenný počas celého života. Výnimkou sú poranenia, ako napríklad odreniny alebo rezné rany, ktoré vytvorený vzor môžu dočasne alebo trvale zmeniť. [8]

Diferenciácia pokožky je spôsobená rastom *volar pads* na dlaniach, prstoch a chodidlách [8]. *Volar pads* sú prechodné opuchy tkaniva pod pokožkou, ktoré sa vyskytujú dočasne počas vývinu plodu na špičkách prstov a najviac ovplyvňujú formáciu papilárnych línií a ich počet (papilárne línie budú opísané podrobnejšie v ďalšom texte) [9]. Ich meniacia sa podoba

počas rôznych týždňov vývinu plodu je pre predstavu znázornená na obrázku 2.1. Výskyt a tvar *volar pads* má dopad najmä na základný tvar vzoru odtlačku prsta. Na obrázku 2.2 je schematicky naznačená uvedená spojitosť medzi *volar pads* a základným tvarom vzoru odtlačku prsta. Konkrétny tvar vzoru je tvorený na oveľa jemnejšej úrovni [9]. Povrch špičky prsta sa postupne zväčšuje, čím sa papilárne línie oddeľujú a vytvárajú miesto pre vznik nových [7]. Týmto spôsobom vznikajú markanty (markanty budú podrobnejšie písané v ďalšej podkapitole) [7].



Obrázok 2.1: *Volar pads*, dočasné opuchy tkaniva pod pokožkou, vyskytujúce sa počas vývinu plodu na špičkách prstov. Na obrázku je znázornená ich meniac sa podoba počas rôznych týždňov vývinu plodu. Výskyt *volar pads* ovplyvňuje formáciu celkového tvaru papilárnych línií a ich počet. Obrázok bol prebraný a modifikovaný z [9].



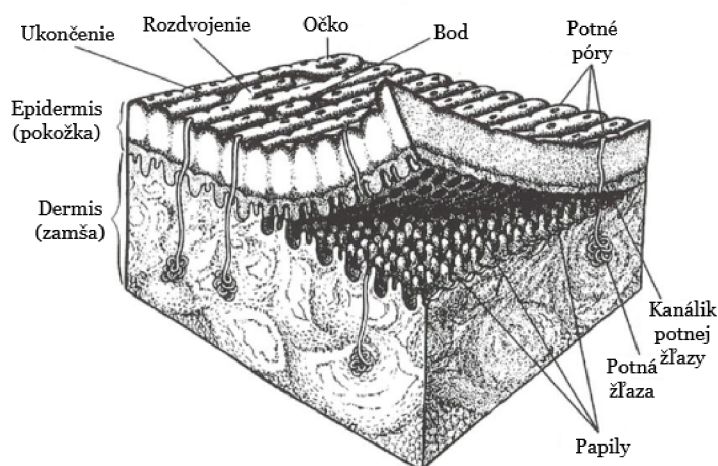
Obrázok 2.2: Výskyt a tvar *volar pads* má dopad najmä na základný tvar vzoru odtlačku prsta. Na obrázku je schematicky znázornená súvislosť medzi *volar pads* a formovaním základného vzoru odtlačku prsta. Obrázok bol prebraný z [9].

Plodová voda a poloha plodu sa počas procesu diferenciácie mení. Bunky na špičke prsta rastú v mikroprostredí, ktoré je iné pre každú ruku, aj pre každý prst. Details vzoru odtlačkov prstov sú určené týmto meniacim sa mikroprostredím, ovplyvnené sú náhodnými fyzickými sťahmi a uvoľneniami. Počas vytvárania odtlačkov existuje toľko variácií, že je prakticky nemožné, aby pre dvoch odlišných ľudí vznikli úplne rovnaké odtlačky prstov. [7] [8]

Genetika zapríčiňuje, že odtlačky prstov jedinca sú diferenciovane z rovnakých génov, nejedná sa preto o vytváranie náhodných vzorov. Zároveň však absolútne neurčuje vytvorenie konkrétneho vzoru, ako bolo opísané vyššie. Z tohto dôvodu sú odtlačky prstov iné aj pre jednovaječné dvojčatá a sú vhodnou biometrickou vlastnosťou na ich rozlíšenie. Jedinosť odtlačkov prstov však nie je matematicky dokázaný fakt, je výsledkom empirického pozorovania. [8] [9]

Papilárne línie sú vyvýšené reliéfy kože, ktoré tvoria vzor odtlačku prsta [10] [11]. Majú výšku v rozmedzí 0,1 – 0,4 mm a ich šírka sa pohybuje v rozmedzí 0,2 – 0,5 mm [2] [12]. Papilárne línie je možné vidieť na obrázku 2.3 spolu s dvomi najvrchnejšími vrstvami kože, epidermis a dermis. Papilárne línie sa nachádzajú vo vrstve epidermis [13]. Ich súčasťou sú potné póry a svojím zakrivením vytvárajú rôzne markanty (na obrázku sa jedná o ukončenie, rozdzvenie, očko, bod, ktoré budú podrobnejšie opísané v nasledujúcej podkapitole) [10] [11]. Zakrivenie papilárnych línií je formované v nižšej vrstve, dermis, ktorá obsahuje papily a potné žľazy prepojené s potnými pórnymi v epidermis kanálikmi [10] [11].

Koža je konštantne regenerovaná, pričom nová bunka začína svoj život v najspodnejšej vrstve a postupne sa dostáva do vrchnejších vrstiev, čím vytláča odumreté staršie bunky. Papilárne línie, ktoré vidíme na povrchu, sú len projekciou nižšej vrstvy. V dôsledku toho papilárne línie nemôžu byť jednoducho zmenené alebo odstránené poškodením vrstvy epidermis, pretože sa vplyvom regenerácie obnoví ich pôvodný vzor. Pre trvalé poškodenie či odstránenie odtlačkov prstov by bolo potrebné poškodiť vrstvu dermis. [10] [11] [13]



Obrázok 2.3: Štruktúra kože s papilárnymi líniami a vrstvami epidermis a dermis. Obrázok bol prebraný a upravený z [2].

Z kriminalistického a daktyloskopického hľadiska sa vznik a existencia obrazcov papilárnych línií riadi takzvanými daktyloskopickými zákonmi [14]:

1. Obrazce papilárnych línií sú relatívne nemenné v priebehu života človeka.
2. Papilárne línie sú neodstrániteľné, ak nie je odstránená alebo zničená zárodočná vrstva kože (dermis).
3. Na svete nie sú dvaja ľudskí jedinci, ktorí by mali zhodné obrazce papilárnych línií.

Z daktyloskopických zákonov a biologických skutočností uvedených v tejto podkapitole vyplýva, že odtlačky prstov veľmi vysoko uspokojujú charakteristiky univerzálnosť, jedinečnosť, konštantnosť a výkonnosť [6], ktoré boli uvedené v podkapitole 2.2.

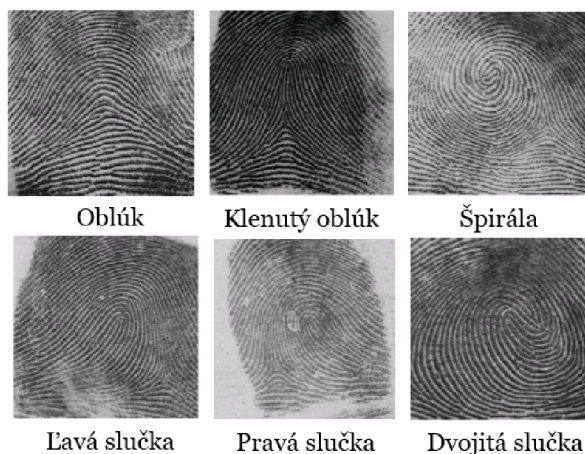
## 2.3 Vlastnosti odtlačkov prstov

S odtlačkami prstov pracujú dva typy systémov. Prvým typom sú prístupové systémy – bežné systémy, používané pre riadenie prístupu k zariadeniu, do miestnosti, a pod. Druhým typom sú forenzné systémy – systémy používané v kriminalistike, nazývané aj daktyloskopické systémy. Odtlačok prsta je v tomto prípade získaný z miesta činu alebo od osoby s neznámou identitou. V oboch typoch systémov je potrebné digitálne rozpoznávanie odtlačkov prstov. Prístupové systémy obvykle vykonávajú verifikáciu, forenzné systémy obvykle vykonávajú identifikáciu spojenú s verifikáciou (dôkaz proti konkrétnemu páchatelovi) [13] [15].

Na globálnej úrovni vytvárajú papilárne línie vzor, ktorý nazývame trieda odtlačkov prstov [2]. Klasické porovnávanie dvoch obrázkov odtlačkov prstov je výpočtovo náročné, preto je pri identifikácii použitá klasifikácia do tried. Pri procese identifikácie sa určí trieda porovnávaného odtlačku prsta a následne sú vylúčené odtlačky prstov z iných tried. Identifikácia prebieha len nad časťou databázy obsahujúcou určenú triedu, čím sa významne zníži výpočtová náročnosť aj čas porovnávania [11].

Vo veľkých databázach, ako napríklad v FBI<sup>1</sup> v systéme AFIS<sup>2</sup> [16] sa používa Henryho klasifikačný systém, ktorý je založený na rozdelení odtlačkov do troch základných tried – oblúk (*arch*), slučka (*loop*) a vír (*whorl*) [2]. Odtlačky prstov v daných triedach nie sú rovnomerne zastúpené. Najčastejšie sa vyskytuje trieda slučka, a to v 65,5 % odtlačkov prstov, najmenej často oblúk v 6,6 % odtlačkov prstov, vír je uprostred, nachádza sa v 27,9 % odtlačkov prstov [10] [11].

Dnes sa používajú aj rozšírené verzie, v ktorých sú tri triedy z Henryho klasifikácie rozdelené do viacerých špecifickejších tried [11]. Nové triedy sú napríklad klenutý oblúk (*tented arch*), ľavá slučka (*left loop*), pravá slučka (*right loop*), dvojité slučka (*twin loop*). Na obrázku 2.4 sú znázornené odtlačky prstov reprezentujúce uvedené triedy.



Obrázok 2.4: Triedy odtlačkov prstov. Obrázok bol prebraný a upravený z [17].

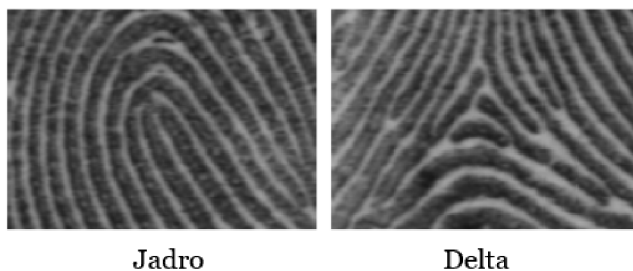
<sup>1</sup> *Federal Bureau of Investigation*

<sup>2</sup> *Automated Fingerprint Identification System*

Pri klasifikácii odtlačkov prstov do tried sa používajú dva typy radiacich bodov nazývané singulárne body [8] [11]:

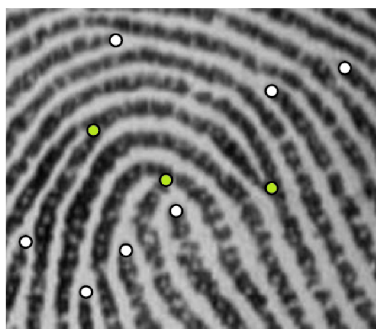
- Delta – miesto, v ktorom papilárne línie prebiehajú do troch smerov [2] [12],
- jadro – stred odtlačku prsta, nachádza sa v najspodnejšom vykľutí v priebehu papilárnych línií, neodpovedá stredú odtlačku prsta [2] [12]. Ak odtlačok prsta nemá žiadne singulárne body, za jadro je väčšinou považovaný bod maximálneho zakrivenia papilárnych línií [7].

Triedy odtlačkov prstov sa odlišujú na základe počtu alebo smeru singulárnych bodov [10]. Delta a jadro sú znázornené na obrázku 2.5.



Obrázok 2.5: Singulárne body. Obrázok bol prebraný a upravený z [7].

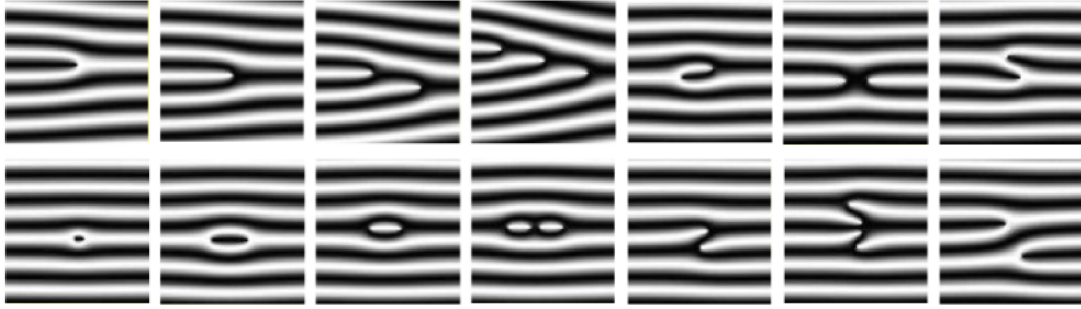
Na lokálnej úrovni sú odtlačky prstov rozlišované na základe špeciálnych útvarov vytváraných papilárnymi líniami, nazývaných markanty (*minutiae*) [2] [8]. Jedná sa o miesta v odtlačku prsta, kde sú papilárne línie ukončené, rozdelené alebo spojené [7]. Medzi markantmi rozlišujeme dva základné typy – ukončenie (*termination*) a vidlička (*bifurcation*) [7]. Okrem umiestnenia majú markanty dve ďalšie ukladané vlastnosti, a to orientáciu a typ [7]. Orientácia markantu je smer, v ktorom by pokračovala papilárna línia v bode markantu [2]. Ukončenie je bod, v ktorom papilárna línia náhle končí [8]. Vidlička je bod, v ktorom sa papilárna línia rozdeľuje do dvoch vetiev [8]. Na obrázku 2.6 je ukončenie znázornené bielou farbou a vidlička zelenou farbou.



Obrázok 2.6: Základné typy markantov. Ukončenie je znázornené bielou farbou, vidlička zelenou farbou. Obrázok bol prebraný a upravený z [18].

Okrem dvoch základných typov markantov existuje mnoho ďalších, z ktorých nie všetky sú používané pre rozpoznávanie odtlačkov prstov. Prístupové systémy si vystačia so spomí-

nanými dvomi základnými typmi markantov [2]. Rozpoznávanie zložitých vzorov by zbytočne predĺžilo celý proces [10] [11]. Pre kriminalistické účely sa používa väčšie množstvo markantov, ktoré sú odvodené od základných typov [2]. Niektoré z nich sú uvedené na obrázku 2.7. V hornom rade zľava je to ukončenie (*termination*), vidlička (*bifurcation*), dvojitá vidlička (*double bifurcation*), trojitá vidlička (*triple bifurcation*), hák (*hook*), kríženie (*cross*), bočný kontakt (*side contact*) [2] [12]. V dolnom rade pokračuje zľava bod (*point*), interval (*interval*), jednoduchá slučka (*single loop*), dvojitá slučka (*double loop*), jednoduchý most (*bridge*), dvojitý most (*twin bridge*), priesečná línia (*intersection*) [2] [12].



Obrázok 2.7: Rôzne typy markantov. Obrázok bol prebraný a upravený z [17].

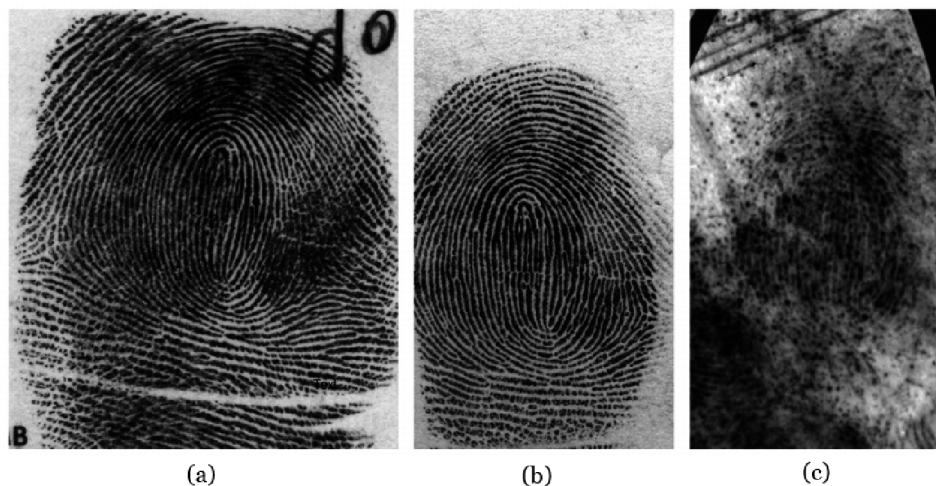
## 2.4 Získavanie odtlačkov prstov

Základným predpokladom pre získavanie odtlačkov prstov je ochota užívateľov poskytnúť ich odtlačky prstov pre snímanie. Odtlačky prstov sú jednou z najrozvinutejších biometrických technológií používaných pre kriminálne vyšetrovania vo forenzných oddeleniach na celom svete, v dôsledku čoho je s nimi pevne spätá stigma kriminality [19]. V dnešnej dobe sa užívatelia stretávajú so zabezpečením pomocou odtlačkov prstov v každodennom živote, napríklad v mobilných telefónoch či notebookoch. Kvôli asociácii odtlačkov prstov s kriminálnym vyšetrovaním mali užívatelia tendenciu vnímať toto zabezpečenie negatívne [12]. Je nutné doplniť, že tento typ obáv medzi užívateľmi sa dnes už vytráca. Ďalšia časť ľudí má oprávnený strach zo zneužitia ich odtlačkov prstov, nakoľko je odtlačok veľmi jednoducho získateľný z mnohých povrchov, ktorých sa dotkne [12]. Z uvedených skutočností vyplýva, že odtlačky prstov spĺňajú požadovanú vlastnosť akceptáciu užívateľmi, definovanú v podkapitole 2.2, len priemerne [6]. Užívateľská akceptácia rozpoznávania tváre alebo geometrie ruky je vyššia [6].

Odtlačky prstov môžu byť získané viacerými spôsobmi. Na základe spôsobu získania odtlačku prsta sú v daktyloskopickej praxi rozoznávajú tri kategórie odtlačkov prstov [20]:

- Rolovaný – je získaný rolovaním prsta z jednej strany na druhú s cieľom zachytiť čo najväčšiu plochu odtlačku prsta,
- pichaný – pri jeho získavaní je odtlačok prsta len pritlačený k povrchu,
- latentný – je získaný zodvihnutím z povrchu alebo objektu, ktorého sa osoba dotkla bez zámeru zanechať odtlačok prsta. Na prvý pohľad nie je viditeľný, pre zviditeľnenie je nutné použitie chemikálií alebo prášku [21]. Latentný odtlačok prsta je vytvorený potom alebo inou chemickou látkou [14].

Uvedené typy odtlačkov prstov sú znázornené na obrázku 2.8: (a) rolovaný, (b) pichaný, (c) latentný.



Obrázok 2.8: Tri typy odtlačkov prstov: (a) rolovaný, (b) pichaný a (c) latentný. Obrázok bol prebraný a upravený z [20].

Pôvodnou technikou pre získavanie odtlačkov prstov bolo používanie atramentu. Špička prsta bola priložená najskôr k čiernemu atramentu a následne na papier, kde zanechala odtlačené papilárne línie. Táto metóda bola využívaná najmä pri vytváraní daktyloskopických kariet [14], ktoré boli používané pre manuálne porovnávanie odtlačkov prstov. Daktyloskopická karta poskytovala na rozdiel od dnes používaných skenerov rolované aj pichané odtlačky prstov. [13]

S rapidným rozšírením používania odtlačkov prstov vo forenzných vedách začali rásť aj databázy odtlačkov prstov a manuálne rozpoznávanie začalo byť nerealizovateľné. Vznikla potreba automatického rozpoznávania odtlačkov prstov a s tým spojená potreba digitálnej reprezentácie obrázka odtlačku prsta. Medzi prvými systémami takéhoto typu vznikol AFIS, ktorý bol vytvorený na základe poznatkov expertov v manuálnom rozpoznávaní odtlačkov prstov a dodnes je používaný na celom svete. [8] [21] [22]

Typicky je digitálny obrázok rolovaného alebo pichaného odtlačku prsta získaný jedným z dvoch spôsobov, naskenovaním atramentového odtlačku prsta alebo použitím skenera odtlačkov prstov [19] [20]. Historicky sa v aplikáciách používal práve prvý spôsob, takzvaná atramentová technika [8]. Prst osoby bol s použitím atramentu otláčený na papier, ktorý bol následne naskenovaný klasickým skenerom pre papier [8]. Tento spôsob je nazývaný aj *off-line* získavanie odtlačkov prstov [8].

Dnes väčšina civilných systémov a napríklad aj kriminálny systém AFIS akceptujú digitálne obrázky odtlačkov prstov získané takzvanou *live-scan* metódou. V tomto prípade nie je pre získanie odtlačku prsta použitý žiaden atrament, osoba len položí prst na plochý povrch skenera. Takto vzniknuté obrázky musia spĺňať určité špecifikácie, ktoré určujú ich kvalitu a formát, za účelom maximalizovať kompatibilitu medzi rozličnými aplikáciami využívajúcimi odtlačky prstov pochádzajúce z rôznych skenerov. [8]

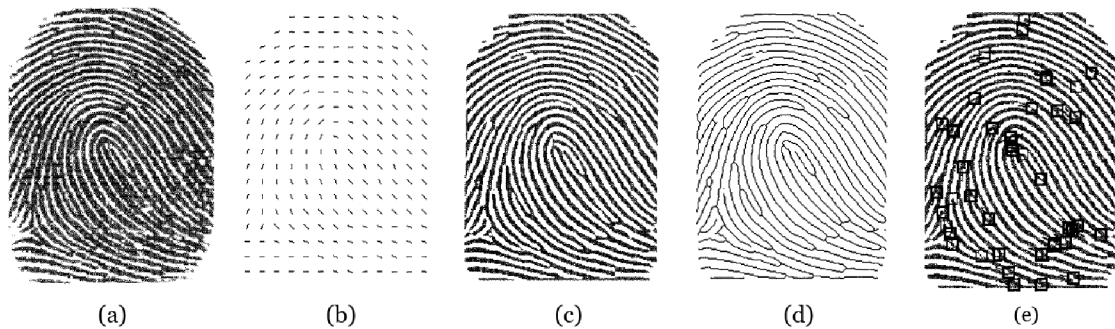
Existujú rozličné spôsoby získania digitálneho obrázka vzoru papilárnych línií, z ktorých každá má silnejšie aj slabšie stránky. Jedná sa najmä o optickú technológiu, používajúcu vhodné osvetlenie a kameru, kapacitnú technológiu, ultrazvukovú, elektrooptickú, tlakovú

a termickú technológiu. Na základe daných technológií existujú analogicky k nim rôzne typy skenerov odtlačkov prstov. Pôvodné získavanie odtlačkov prstov pomocou atramentu je zaradené medzi mechanické technológie. [2] [22]

## 2.5 Rozpoznávanie odtlačkov prstov

Biometrické systémy obvykle pracujú v dvoch režimoch – registrácia a verifikácia/identifikácia. Pri registrácii užívateľ prikladá registrovaný prst k senzoru viackrát, systém pri tom vytvára priemernú reprezentáciu snímaných odtlačkov a vytvára šablónu vysokej kvality. Druhý režim, verifikácia/identifikácia, funguje podobne, ale vykonáva sa v rámci neho aj porovnanie uloženej šablóny s práve snímaným odtlačkom prsta. Proces rozpoznávania odtlačkov prstov nie je jednoduchý a skladá sa z viacerých krokov, ktoré budú podrobnejšie opísané v ďalších sekciách. Problémy sťažujúce rozpoznávanie odtlačkov prstov budú priblížené v nasledujúcej podkapitole. Výstupy jednotlivých krokov procesu rozpoznávania sú znázornené na obrázku 2.9. [2] [12]

Zo skutočností uvedených v tejto podkapitole vyplýva, že odtlačky prstov je možné kvantitatívne merať, avšak zložitosť procesu má vplyv na to, že uspokojujú charakteristiku získateľnosť, ktorá bola uvedená v podkapitole 2.2, vzhľadom k ostatným biometrikám len priemerne [6].



Obrázok 2.9: Výstupy krokov procesu rozpoznávania odtlačku prsta: (a) vstupný obrázok, (b) pole orientácií, (c) extrahované čierno-biele papilárne línie, (d) stenčené papilárne línie, (e) extrahované markanty. Obrázok bol prebraný a upravený z [19].

### 2.5.1 Snímanie odtlačku prsta a jeho predspracovanie

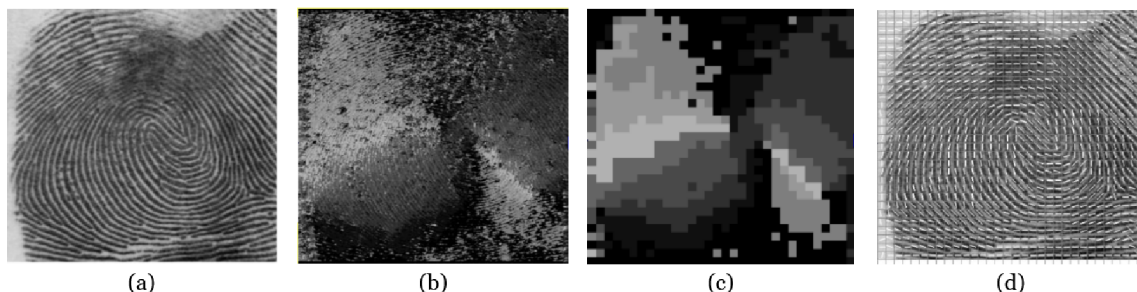
V prvom rade je potrebné získať digitálnu formu obrázka odtlačku prsta zo senzoru alebo z inej predlohy. Nutnosťou je počiatočné predspracovanie obrázka, aby z neho bol odstránený šum, ktorý je v obrázkoch odtlačkov prstov značne prítomný. Jedná sa o segmentáciu oblasti odtlačku prsta od pozadia, pričom je potrebné použiť robustné techniky, nakoľko odtlačok prsta je pruhovaný vzor, na ktorý sa nedá jednoducho použiť globálne či lokálne prahovanie. [2] [12] [18]

### 2.5.2 Vytvorenie poľa orientácií

Pre získanie poľa orientácií je potrebné v každom bode obrázka spočítať smer papilárnej línie. Výpočet prebieha na základe odtieňa sivej v pixeloch v okolí daného bodu. Ak sa



bod nachádza priamo na papilárnej línii, má čiernu farbu a s maximálnou pravdepodobnosťou určuje smer papilárnej línii v konkrétnom bode. Po vypočítaní smeru v každom bode obrazu je vykonaná transformácia na blokové pole orientácií. Následne je blokové pole mapované na pôvodný obrázok. Výstupy jednotlivých medzikrokov vytvorenia poľa orientácií sú znázornené na obrázku 2.10. [2] [12]



Obrázok 2.10: Výstupy medzikrokov vytvorenia poľa orientácií: (a) vstupný obrázok, (b) výpočet orientácií v každom bode obrázka, (c) blokové pole orientácií, (d) mapovanie blokového poľa na pôvodný obrázok. Obrázok bol prebraný a upravený z [17].

### 2.5.3 Extrahovanie papilárnych línií

Zmyslom celého opisovaného procesu je nájdenie markantov v rámci obrázka odtlačku prsta. Markanty sú súčasťou papilárnych línií, preto je potrebné najskôr z obrázka extrahovať papilárne línie. Na obrázkoch odtlačkov prstov sú papilárne línie tmavé, údolia – medzery medzi papilárnymi líniami sú svetlé. Na základe uvedenej vlastnosti je pre extrakciu papilárnych línií vhodné použiť binarizáciu obrazu pomocou prahovania. Táto metóda je citlivá na potné póry na papilárnych líniiach, ako aj na nespojitosti v papilárnych líniiach zapríčinené záhybmi alebo rezmi, ktoré majú tiež svetlú farbu. Pre vyriešenie daných problémov je obrázok znova upravený, používa sa pri tom škálovanie histogramu a 2D Gáborová funkcia pre filtrovanie. Následne je už možné použiť binarizáciu a získať tým potrebnú čierno-bielu reprezentáciu papilárnych línií. [2] [7] [12]

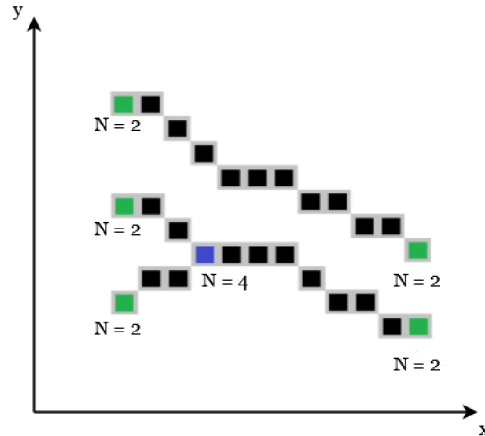
### 2.5.4 Stenčenie papilárnych línií

Výsledkom predchádzajúceho kroku je obrázok papilárnych línií, ktoré môžu mať všeobecne rôznu šírku. Pre získanie markantov je potrebné stenčiť papilárne línie na šírku jedného pixelu. V nasledujúcej sekcii bude uvedené, ako stenčenie uľahčuje detekciu markantov. Pre stenčenie papilárnych línií býva použitý pomerne jednoduchý algoritmus, ktorý ale musí zabezpečiť, aby papilárna línia neubúdala v žiadnom smere a tým pádom nedošlo ku problémom s polohou markantov. Medzi najpoužívanejšie metódy patrí metóda Emyroglu, dnes už je nahradená inými algoritmi, ktoré sa líšia presnosťou a dobou výpočtu. Patria medzi ne napríklad algoritmy Zhang-Suen či Guo-Hall. [2] [12] [23]

### 2.5.5 Detegovanie a extrahovanie markantov

Pre detekciu a extrahovanie markantov sa používa takzvaná Hongova metóda [2]. Podľa súčtu bodov v okolí na obrázku stenčenej papilárnej línii sa detegujú základné markanty,

ktorými sú ukončenie a vidlička. Ich kombináciou vznikajú ostatné, zložitejšie markanty. Metóda deteguje ukončenie, keď je súčet bodov v okolí rovný dvom, o vidličku sa jedná, keď je súčet bodov v okolí väčší ako tri. Detekcia markantov je schematicky znázornená na obrázku 2.11. Modrou farbou je označená vidlička, zelenou farbou ukončenie. Počet bodov v okolí jednotlivých markantov udáva  $N$ . [2] [12]



Obrázok 2.11: Schematicky znázornená detekcia markantov v stenčených papilárnych líniách. Obrázok bol prebraný a upravený z [1].

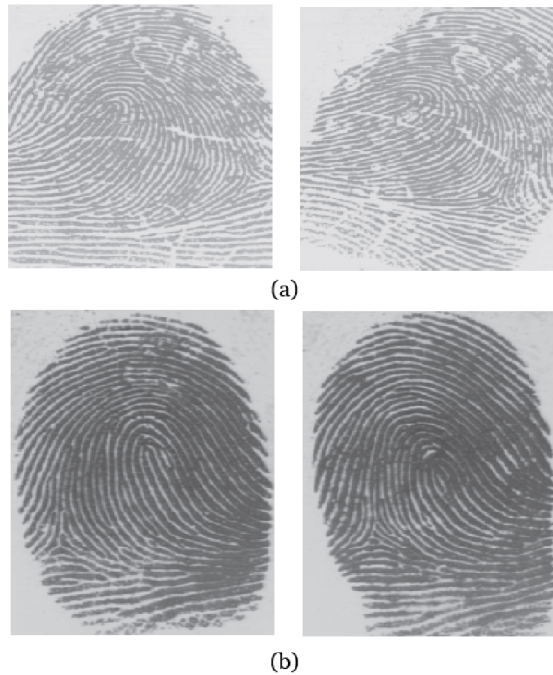
## 2.6 Porovnávanie odtlačkov prstov

Dva odtlačky sú v daktyloskopickej praxi považované za rovnaké, keď sa v nich vyskytuje určité množstvo zhodných markantov. V rôznych krajinách je minimálny počet markantov rozličný. V Českej republike je možné vykonať identifikáciu človeka na základe odtlačku prsta, ak obsahuje minimálne 10 markantov zhodných so šablónou. V súčasnej dobe sa diskutuje o tom, či je potrebné určovať minimálny počet markantov, alebo sa v každom prípade má postupovať individuálne, napríklad na základe početnosti jednotlivých markantov, ako je to napríklad v USA. [14]

Rozhodnutie, či sú dva odtlačky prstov rovnaké, nie je jednoduché najmä kvôli dvom faktorom. Prvým z nich je vysoká variabilita v rôznych reprezentáciách jedného odtlačku prsta, takzvaná vnútrotriedna variabilita. Vnútrotriedna variabilita znamená, že obrázky odtlačkov rovnakého prsta snímané v rôznych časoch alebo okolnostiach, môžu vďaka niektorým faktorom, ako napríklad posunutie, rotácia, šum, pôsobiť tak, akoby išlo o odtlačky dvoch rôznych prstov. [8]

V opačnom prípade môžu odtlačky rôznych prstov pôsobiť akoby sa jednalo o odtlačok totožného prsta. Tento jav sa nazýva mimotriedna variabilita a spôsobuje ho najmä podobná pozícia singulárnych bodov či orientácia papilárnych línií. Pravdepodobnosť, že v odlišných odtlačkoch prstov by bolo skutočne veľké množstvo markantov rovnakých, je veľmi malá. Pri porovnávaní odtlačkov prstov je ešte pred porovnaním snaha obrázky odtlačkov čo najlepšie zarovnať a znížiť tým možnosť nesprávneho porovnania. [8]

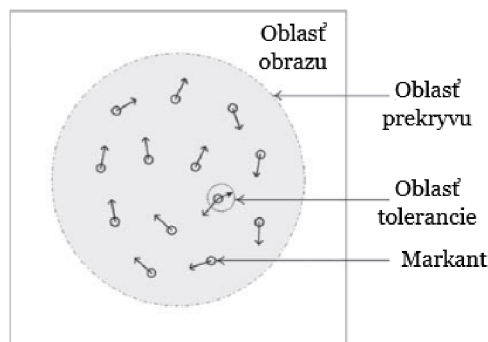
Vnútrotriedna a medzitriedna variabilita sú znázornené na obrázku 2.12. V nasledujúcich sekciiach budú opísané jednotlivé metódy používané pri automatizovanom porovnávaní odtlačkov prstov.



Obrázok 2.12: Variabilita odtlačkov prstov: (a) vnútrotriedna variabilita, na obrázkoch sú rôzne snímky odtlačku rovnakého prsta, (b) medzitriedna variabilita, na obrázkoch sú snímky rôznych odtlačkov prstov. Obrázok bol prebraný a upravený z [22].

### 2.6.1 Porovnávanie založené na markantoch

Najpoužívanejším spôsobom porovnávania odtlačkov prstov je porovnávanie založené na markantoch. Rozšírenosť metódy vyplýva z jej spojitosti so spôsobom, akým odtlačky prstov porovnávajú forenzní experti, ktorých spôsob porovnávania je akceptovaný ako dôkaz identity na súdoch po celom svete. Z obrázka odtlačku prsta sú extrahované informácie o markantoch (postup extrakcie vysvetlený v kapitole 2.5) a uložené sú v dvojrozmernom poli. Porovnávanie potom spočíva v nájdení takého prekrytia dvoch polí, v ktorom je maximálny počet zhodných markantov. [8]



Obrázok 2.13: Oblasť prekrytia a tolerancie používaná pri porovnávaní na základe markantov. Obrázok bol prebraný a upravený z [12].

Všeobecne sa jedná o problematiku rozpoznávania vzorov. Príkladom dvoch metód porovnávania s využitím markantov sú Honghova metóda a Rathova metóda. Obidve metódy pracujú v dvoch krokoch. V prvom kroku riešia zarovnanie, generujú globálny prekryv. V druhom kroku riešia porovnanie, hľadajú lokálny prekryv. Väčšinou je pri porovnávaní markantov zvolená určitá tolerancia a aj veľmi podobné markanty, ktoré však nie sú úplne zhodné, sú považované za rovnaké. Oblasť prekryvu a oblasť tolerancie vo vzťahu k celkovému obrazu a markantom je znázornená na obrázku 2.13. [2] [12]

### 2.6.2 Porovnávanie založené na korelácii

Porovnávanie založené na korelácii používa obrázky odtlačkov prstov v odtieňoch sivej. Korelácia je počítaná medzi uloženým obrázkom odtlačku prsta, ktorý je šablónou a medzi obrázkom snímaného odtlačku prsta. Merítkom ich rozdielnosti je súčet štvorcov rozdielov hodnôt medzi intenzitami každej príslušnej dvojice pixelov. Porovnávané obrázky sú prekryté a korelácia je počítaná lokálne pre rôzne prekrytia obrázkov (ich posuny, rotácie, atď.). Na záver je korelácia lokálnych regiónov kombinovaná do jedného výsledku celkovej korelácie. Táto metóda porovnania je výpočtovo náročná, avšak je implementovateľná v hardware. [2] [8] [12]

Jeden z najťažších problémov všeobecne pri identifikácii pomocou odtlačkov prstov je to, že porovnávanie je veľmi výrazne ovplyvnené stavom povrchu špičky prsta, na ktorý vplýva prostredie a vlastnosti danej osoby (napr. príliš suchý prst, rôzne choroby). Existujú algoritmy, ktoré sú vysoko robustné voči degradovanému obrázku odtlačku prsta a umožňujú identifikáciu aj takýchto odtlačkov prstov. Jedným z nich je algoritmus využívajúci koreláciu, konkrétne funkciu POC<sup>1</sup>. Uvedeným algoritmom je možné úspešne porovnávať aj odtlačky prstov, ktoré nie je možné správne porovnať bežnými konvenčnými algoritmami. [24]

### 2.6.3 Porovnávanie založené na vlastnostiach papilárnych línií

Porovnávanie založené na vlastnostiach papilárnych línií je používané najmä z dôvodov, že spoľahlivá extrakcia markantov z obrázkov nízkej kvality je veľmi náročná a všeobecne sa jedná o časovo náročnú operáciu. Častokrát sú vlastnosti papilárnych línií používané ako doplnok ku markantom pre zvýšenie presnosti a robustnosti. [8]

Medzi vlastnosti papilárnych línií používané pre porovnávanie patria [8]:

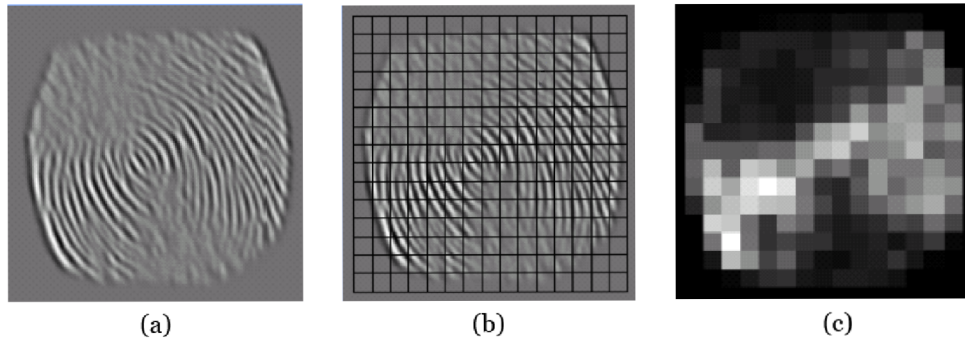
- veľkosť a externá silueta odtlačku prsta,
- počet, typy a umiestnenie singulárnych bodov,
- geometrické atribúty papilárnych línií,
- globálna a lokálna textúra,
- potné póry.

Prvá a druhá uvedená vlastnosť nie sú v odtlačkoch prstov veľmi stabilné, líšia sa na základe konkrétnej časti prstu priloženej k ploche senzora [8]. Potné póry sú naopak veľmi vysoko rozlišujúcou vlastnosťou, avšak ich získanie vyžaduje použitie skenerov s vysokým rozlíšením [8]. Textúra je definovaná fixnou orientáciou a frekvenciou papilárnych línií [25].

---

<sup>1</sup>Phase-Only Correlation

Na obrázku 2.14 je znázornené použité textúry pre porovnávanie. Vstupný obrázok odtlačku prsta je filtrovaný použitím ôsmich Gáborových filtrov [25]. Následne je každý výstup filtrovania rozdelený štvorcovou mriežkou [25]. Reprézntácia každého výstupu je vytvorená na základe hodnôt intenzít pixelov v jednotlivých bunkách mriežky a je použitá pre rozpoznávanie [25].



Obrázok 2.14: Reprézntácia odtlačku založená na textúre: (a) výstup Gáborovho filtra aplikovaného na vstupný obrázok odtlačku prsta, (b) rozdelenie štvorcovou mriežkou, (c) reprézntácia vypočítaná na základe intenzít buniek mriežky. Obrázok bol prebraný a upravený z [25].

## Kapitola 3

# Falzifikáty odtlačkov prstov

Odtlačky prstov sú biometrickou vlastnosťou náchylnou na prezentačné útoky, ktoré sú pre biometriu jednou z najväčších a najničivejších hrozieb [26]. V dobre navrhnutom biometrickom systéme musí byť zaistené, že len autorizované osoby môžu pristupovať k chráneným prostriedkom [26]. Táto kapitola sa zaoberá teóriou spojenou s falzifikátmi odtlačkov prstov, pričom sú používané dva termíny, ktoré je nutné explicitne vymedziť.

Termín „odtlačok“ (*print*) je rezervovaný pre atramentovú reprezentáciu odtlačku prsta, alebo reprezentáciu získanú *live-scan metódou*. Termín „stopa“ (*mark*) je používaný pre označenie vrstvy zanechanej na materiáli v dôsledku tvorby mastného sekrétu na povrchu odtlačkov prstov, či už sa jedná o dôsledok kontaktu povrchu s pravým prstom alebo falzifikátom. Všeobecne je tento termín spájaný s kriminálnou aktivitou. Hlavný rozdiel medzi stopou a odtlačkom je ten, že odtlačok je zanechávaný v kontrolovaných podmienkach (pod dohľadom, alebo na základe presných inštrukcií), zatiaľ čo stopa je zanechaná v nekontrolovanom prostredí a častokrát je latentná. [26]

V úvode kapitoly sú uvedené príklady zneužitia odtlačkov prstov pri kriminálnom vyšetrowaní, ako aj príklady zneužitia pre oklamanie biometrických sensorov a jednotlivé typy útokov na biometrický systém. Ďalej sú v kapitole uvedené metódy výroby falzifikátov a následne artefakty, ktoré sú vo falzifikátoch odtlačkov prstov prítomné. Záver kapitoly je venovaný detekcii falzifikátov v biometrických systémoch, či už detekciou živosti alebo inými metódami opísanými v poslednej podkapitole.

Zo skutočností uvedených v tejto kapitole vyplýva, že odtlačky prstov len veľmi málo uspokojujú vlastnosť požadovanú od biometrickej charakteristiky, a to odolnosť proti falšovaniu [6], uvedenú v podkapitole 2.2.

### 3.1 Nebezpečenstvo falšovania odtlačkov prstov

Na začiatku 20. storočia, keď sa odtlačky prstov začali používať na súdoch ako dôkazový materiál z miest činu, vznikla možnosť čeliť pri vyšetrowaní falošným odtlačkom prstov. Falošné odtlačky prstov sú používané osobami, ktoré páchajú trestný čin a snažia sa pozornosť strhnúť na nezainteresovanú osobu alebo ich použitím odkloniť smer vyšetrowania. V dnešnej dobe sú používané aj pre oklamanie biometrických systémov. Pod termín falošné odtlačky prstov spadajú umelo vyrobené falzifikáty, ale aj zranené alebo iným spôsobom modifikované živé prsty. [13] [26]

Známym prípadom falošných odtlačkov prstov, figurujúcich vo vyšetrowaní kriminálneho prípadu, je vražda Harryho Oakesa, svojho času najbohatšieho muža Britského kráľovstva,

na Bahamách v roku 1943. Dvaja skorumpovaní policajti premiestnili odtlačok podozrivého z pohára, z ktorého pil počas policajného výsluchu a umiestnili ho na nábytok na mieste činu. Obhajoba bola schopná preukázať nezhodu medzi pozadím na odtlačku prsta vzhľadom k materiálu, z ktorého bol vyrobený nábytok, na ktorom sa odtlačok prsta našiel. [27]

Louis J. van der Meulen vo svojom článku opisuje okolnosti, ktoré ho priviedli k nápadu použiť odtlačky prstov na nohách ako falošné odtlačky prstov. Počas druhej svetovej vojny bol nútený podstúpiť trinástmesačný útek z Holandska až do Turecka. S jeho spoločníkom si počas prechodu cez Alpy zabezpečili falošné francúzske doklady, ktoré bolo potrebné doplniť o odtlačky prstov. Nechceli, aby odtlačky boli v prípade komplikácií spájané s nimi ani s ich priateľmi. Použili preto odtlačky z prstov na nohách. [28]

Výroba falošných odtlačkov prstov má aj *law-enforcement* opodstatnenie, čiže použitie za účelom presadzovania práva. Známym prípadom je snaha FBI dostať sa teroristom do telefónu, ktorá vyvolala spor so spoločnosťou Apple. FBI sa podarilo odomknúť telefón Syed Rizwan Farooka, ktorý počas útoku v Kalifornii zabil 14 ľudí. Telefón bol odomknutý bez pomoci spoločnosti Apple, ktorá ho vyrobila. Apple odmietla poskytnutie pomoci pri odomknutí vzhľadom na udržanie statusu privátnosti a bezpečnosti. V článku je uvedené, že telefón bol odomknutý alternatívnou metódou, pričom je možné špekulovať, že namiesto lámania kryptografických algoritmov mohol byť použitý falzifikát odtlačku prsta. FBI neprezradila, akým spôsobom sa podarilo do telefónu dostať, presadzuje však názor, že získanie kritických digitálnych informácií má svoj význam, keď ide o všeobecnú bezpečnosť. [29]

Akt obchádzania biometrického systému útočníkmi je nazývaný útok. Aj keď je štandardné použitie kryptografie väčšinou užitočné pre prevenciu útoku, v biometrickej doméne je niekoľko nových typov útokov, na ktoré je potrebné použiť iné mechanizmy. Celkovo existujú dva typy útokov, nepriamy a priamy útok [26] [30].

Nepriamy útok je vykonaný vo vnútri systému, počítačovo-kriminálnym *hackerom*, napríklad upravením šablóny v databáze, upravením extrakcie rysov, upravením porovnávaní, a i. Prevenciou voči tomuto typu útoku je šifrovanie, *firewall*, antivírusový software [26] [30].

Priamy útok je vykonaný mimo digitálnych limitov systému, na senzore, a preto voči nemu nemôžu byť použité prostriedky digitálnej ochrany. Priamy útok môže byť vykonaný použitím falšovanej umelej biometriky alebo opätovným odoslaním biometrického signálu zo senzora (*replay attack*). Tento typ útoku je potenciálne veľmi nebezpečný, keďže nevyžaduje pokročilé programovacie schopnosti na rozdiel od nepriameho útoku [26] [30].

Motiváciou útočníka pri priamom útoku je buď vyhnutie sa identifikácii, alebo tvrdenie, že má identitu autorizovaného používateľa. Pri vyhnutí sa identifikácii mení svoju biometrickú vlastnosť, aby pôvodná ostala utajená (*obfuscation*). Pri tvrdení, že má identitu autorizovaného používateľa, môže buď jednoducho predložiť svoju vlastnú biometrickú vlastnosť, a veriť, že dostatočne oklame biometrický systém (*zero-effort attack*), alebo prezentuje sfalšovanú biometrickú vlastnosť daného autorizovaného užívateľa (*spoofing/presentation attack*). [7]

Bolo preukázané, že odtlačky prstov sú náchylné na vykonanie priameho útoku. Takzvané gumené prsty, čiže umelé prsty, ktoré môžu byť jednoducho vyrobené z lacného a dostupného jedlého želé, je možné použiť pre oklamanie optických aj kapacitných sensorov. Gumené prsty sú vyrobené ako odliatky, ktoré sú následne živým prstom pritlačené k senzoru. Na obrázku 3.1 je znázornené porovnanie odtlačku prsta, ktorý slúžil ako zdroj na vyrobienie formy (a) s obrázkom z kapacitného senzoru, ktorý vznikol po priložení formy k ploche senzoru (b). [31]

Na internete je možné nájsť množstvo novinových článkov zachytávajúcich falšovanie odtlačkov prstov pre oklamanie biometrického systému bežnými ľuďmi. Napríklad v roku



Obrázok 3.1: Gumené umelé prsty: (a) odtlačok prsta, ktorý bol použitý ako vzor pri výrobe formy z jedlého želé, (b) obrázok získaný z kapacitného senzoru po nasnímaní formy pritlačenej na povrch senzora živým prstom. Obrázok bol prebraný a modifikovaný z [31].

2008 bola na letisku v Japonsku chytená žena, ktorá sa snažila oklamať kontrolný systém využitím špeciálnej pásky s odtlačkami prstov niekoho iného, ktoré mala na svojich prstoch. [32]

Podobne bola v roku 2013 políciou zadržaná brazílska doktorka, ktorá používala protézy prstov na oklamanie systému zachytávajúceho dochádzku zamestnancov do nemocnice. Následné policajné vyšetrovanie ukázalo, že v danom meste okolo 300 verejných zamestnancov dostávalo plat bez toho, aby chodili do práce. [33]

## 3.2 Metódy výroby falzifikátov

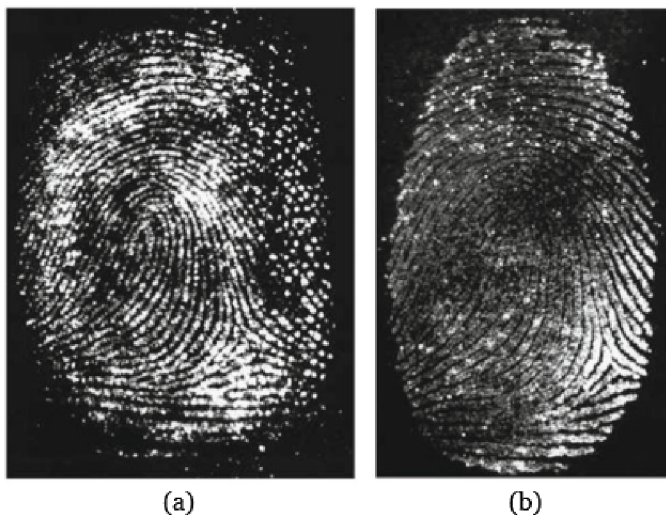
Falzifikáty odtlačkov prstov môžu byť vyrobené viacerými metódami, niektoré z nich budú podrobnejšie opísané v nasledujúcich podkapitolách. Metódy výroby sú uvedené tak, ako sú opisované vo forenzej literatúre, čiže sú zamerané na zanechanie stopy odtlačku prsta na mieste činu s úmyslom znemožniť alebo odvrátiť smer vyšetrovania. Pre oklamanie biometrických sensorov sú používané rovnaké metódy výroby falzifikátov, avšak po vyrobení stačí priložiť falzifikát k povrchu senzora, nie je potrebné nanášať naň špeciálny materiál ako je to v prípade potreby zanechania stopy na mieste činu. [26]

### 3.2.1 Výroba pečiatky

Na základe obrázka papilárnych línií alebo stopy odtlačku prsta odobratej z nejakého povrchu je možné vyrobiť pečiatku (*stamp*). Pečiatka býva zhotovená z gumy alebo polyméru prostredníctvom bežne komerčne dostupných metód, ako je napríklad laserové gravírovanie. Takto vyrobený falzifikát stráca flexibilitu, ale je možné vytvoriť ním značku odtlačkov prstov na povrchoch. Stopa musí pozostávať z masného materiálu, ktorý pripomína sekret zanechaný papilárnymi líniami pri dotyku s povrchom. Môže byť použitý napríklad prirodzený sekret vylučovaný na povrchu čela človeka. [26]



DFO<sup>1</sup> je aminokyselinové činidlo používané na získanie latentných či krvavých stôp zo semi-pórovitých a pórovitých materiálov [34]. Keď sú odtlačky detegované použitím DFO, v prípade falzifikátov býva odhalený rozdiel medzi distribúciou a množstvom mastného sekrétu [26]. V pravom odtlačku prsta sekrét kopíruje štruktúru potných pórov, a tým pádom aj papilárnych línií, ale v prípade falošného odtlačku je distribuovaný odlišným spôsobom. Rozdiel je znázornený na obrázku 3.2, (a) pravý odtlačok prsta zanechaný na papieri a detegovaný použitím DFO, (b) rovnakým spôsobom detegovaný falošný odtlačok prsta. Na obrázku vidieť rozdielny výskyt bodiek reprezentujúcich mastný sekrét, ktoré sú zvýraznené použitím fotoluminescentného režimu.



Obrázok 3.2: Rozdiel medzi pravým a falošným odtlačkom prsta zanechaným pečiatkou: (a) pravý odtlačok prsta, (b) falzifikát. Odtlačky boli detegované použitím DFO. Obrázok bol prebraný a modifikovaný z [26].

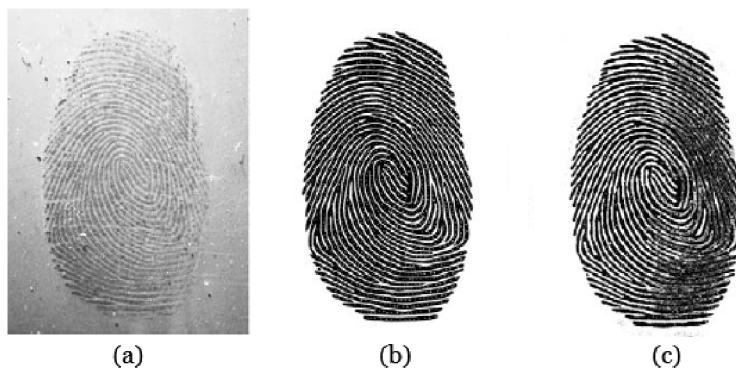
### 3.2.2 Výroba odliatku

Táto metóda vedie k výrobe 3D odliatku (*cast*), ktorým je následne možné za pomoci mastného materiálu zanechávať stopy na povrchu. Základná technika výroby odliatku vyžaduje použitie reálneho prsta človeka pre vytvorenie prvotného odliatku. Vhodným materiálom pre jeho výrobu je termoplastický materiál [35]. Iné materiály vykazujú nízku hĺbku papilárnych línií, alebo vznik vzduchových bublín [26]. Na základe prvotného odliatku je použitím rôznych materiálov, ako napríklad silikónové biele lepidlo alebo latex, vyrobený opačný odliatok [26]. Alternatívne je možné vyrobiť odliatok aj bez použitia reálneho prsta, v tomto prípade je potrebný invertovaný obrázok odtlačku prsta, ktorý sa vytlačí na 3D tlačiarňu na acetátový hárok (priesvitná fólia) a opačná forma je potom naplnená želatínou, lepidlom alebo latexom [26]. Experimentmi bolo preukázané, že odliatok vysokej kvality môže byť vyrobený aj s použitím lacných a dostupných materiálov [36]. Materiály pochádzajúce z potravinárskeho priemyslu nepreukázali najlepšie výsledky, naopak, použitie akvariálneho silikónu alebo epoxidovej živice viedlo k vytvoreniu kvalitných falzifikátov odtlačkov prstov [36].

<sup>1</sup>z anglického názvu – 1,8-diazafluoren-9-one

Odliatky môžu byť vyrobené veľmi kvalitne a rozlíšenie pravej stopy odtlačku prsta od falošnej je v tom prípade veľmi náročné. Kvalita falzifikátu závisí najmä od použitého materiálu, ktorého výber ovplyvňuje aj schopnosť reprodukovat potné póry. Pri vhodne zvolenom materiáli sú znaky falzifikátu pozorovateľné len vo veľmi kvalitných obrázkoch odtlačkov prstov. V menej kvalitných pripomínajú šum, ktorý sa v obrázkoch odtlačkov prstov bežne vyskytuje. [26]

Bolo dokázané, že touto metódou výroby je možné oklamať senzor odtlačkov prstov. V rámci danej štúdie boli vyrobené falzifikáty odtlačkov prstov 12 rôznych osôb, ktoré viedli k zisteniam, že skóre podobnosti získané skenerom pri porovnávaní pravých odtlačkov prstov je najvyššie, v prípade výroby odliatku s dostupným prstom je nižšie a v prípade výroby odliatku bez použitia prsta je najnižšie. Záver je v súlade s logickým predpokladom, že kvalita odtlačku najviac klesá pri použití metódy bez dostupného prsta, kedy je nutné urobiť v rámci výroby väčšie množstvo činností. Pokles skóre však nie je dostatočný pre detekciu falzifikátu, pre ktorú je nutné použitie ďalších mechanizmov. Na obrázku 3.3 je uvedený rozdiel medzi zviditeľneným latentným odtlačkom prsta (a), upraveným obrázkom latentného odtlačku (b) a obrázkom získaným zo skenera po priložení vyrobeného odliatku (c). [35]

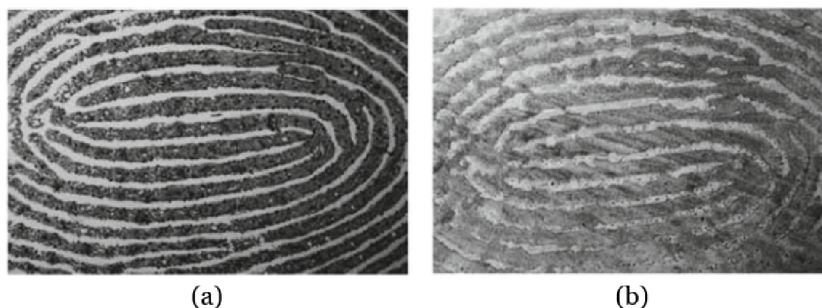


Obrázok 3.3: Metóda výroby odliatku: (a) zviditeľnený latentný odtlačok prsta, (b) upravený obrázok latentného odtlačku prsta zdvihnutého z povrchu, (c) obrázok zo skenera odtlačkov prstov získaný priložením odliatku z lepidla, ktorý bol vyrobený na základe obrázka (b) vytlačenom na acetátovom hárku. Obrázok bol prebraný a modifikovaný z [35].

### 3.2.3 Výroba plošných spojov

Pre výrobu falzifikátov odtlačkov prstov je možné využiť aj techniky používané pri výrobe plošných spojov. Táto metóda nevyžaduje použitie reálneho prsta, stačí obrázok odtlačku prsta, ktorý je potrebné invertovať, vytlačiť na priehľadný materiál a priložiť na medený povrch. Medzery medzi papilárnymi líniami sú na invertovanom obrázku tmavé a po osvetlení UV svetlom ochránia medený povrch. Cez priehľadné miesta UV svetlo prejde a procesom chemického leptania vytvorí na medenom povrchu 3D tvar papilárnych líní. Následne je možné vzniknutú formu využiť napríklad pri výrobe odliatku odtlačku prsta. [26]

Na stopách odtlačkov prstov zanechaných takto vytvoreným falzifikátom sú v porovnaní s obrázkami pravých odtlačkov prstov porušené okraje papilárnych líní [26]. Rozdiel medzi originálnym odtlačkom prsta (a) a stopou zanechanou falzifikátom vyrobeným metódou výroby plošných spojov s viditeľne porušenými okrajmi papilárnych líní (b), je znázornený na obrázku 3.4.



Obrázok 3.4: Metóda výroby plošných spojov: (a) pravý odtlačok prsta, (b) stopa zanechaná falzifikátom vyrobeným metódou výroby plošných spojov s porušenými okrajmi. Obrázok bol prebraný a modifikovaný z [26].

### 3.2.4 Výroba premiestnením odtlačku s pomocou adhézneho materiálu

Už v roku 1937 bolo ukázané, že odtlačok prsta je možné preniesť z jedného povrchu na druhý, pričom po takomto prenese stálo stále obsahuje markanty a je od pravého odtlačku rozlíšiteľný len po dôkladnom preskúmaní pod mikroskopom. Predtým bolo úspešné falšovanie odtlačkov prstov touto metódou daktyloskopickými expertmi považované za nemožné. [37]

V tejto metóde je odtlačok prsta zodvihnutý z povrchu s použitím adhézneho materiálu – lepidla (napríklad lepiacej pásky) a následne prenesený na iný povrch. V podstate sa nejedná o skutočný falzifikát, ale ak bol odtlačok prenesený na iné miesto s úmyslom podvodu, je zaň považovaný [37]. Metóda pôsobí jednoducho, v podstate sa ani nejedná o výrobu, avšak úspešnosť takejto operácie v praxi je nízka [26]. Aby bolo možné stopu odtlačku prstu preniesť, je vyžadované, aby bola dvíhaná z hladkého povrchu, prenesená na čistý povrch, a navyše, aby obsahovala dostatočné množstvo masného sekrétu na prenos [26].

Na takto vyrobenom falzifikáte odtlačku prsta môžu byť pozorované vzduchové bubliny vzniknuté pri prenose, zvláštny tvar okrajov odtlačku spôsobený dvíhaním pásky a taktiež zvyšky lepidla. Obrázok 3.5 zobrazuje falzifikát odtlačku vyrobený prenosením pravého odtlačku prsta. V uvádzanom falzifikáte sú prítomné vzduchové bubliny aj stopy po dvíhaní pásky v ľavom okraji odtlačku.



Obrázok 3.5: Falzifikát odtlačku prsta vyrobený prenosením stopy odtlačku prsta pomocou lepidla a detegovaný hliníkovým práškom. Obrázok bol prebraný a modifikovaný z [26].

### 3.3 Artefakty falzifikátov

Vo falzifikátoch odtlačkov prstov sú prítomné určité stigmy, ktoré forenzní experti využívajú pre rozlíšenie pravých odtlačkov prstov od falzifikátov. Neexistuje štrukturovaný dokumentovaný spôsob, ktorý na základe daných znakov vedie k rozhodnutiu, či sa jedná o falzifikát, alebo nie. Tvoria len časť dôkazov v procese rozhodovania. Naopak, finálne rozhodnutie je založené na tréningu a skúsenostiach forenzného experta. [26]

Vo všeobecnosti sa rozlišujú vnútorné a vonkajšie znaky falzifikátov. Vnútorné znaky je možné pozorovať priamo na odtlačku prsta, pričom vonkajšie znaky sú badateľné z kontextu, v ktorom sa odtlačok prsta nachádza [26]. V tomto texte budú bližšie predstavené len vnútorné znaky falošných odtlačkov prstov. Medzi ne patrí:

- Šum v pozadí (druh haló efektu) okolo odtlačku prsta alebo vo vnútri odtlačku prsta v oblastiach bez papilárnych línií. Vzniká pri dotyku odliatku s povrchom, v miestach, kde na odliatku už nie sú papilárne línie, len hladký povrch. [26]
- Celkový tvar falzifikátu je neprirodený, odlišný od tvaru, ktorý vznikne pri odtlačaní skutočného prsta [26]. Na obrázku 3.6 je neprirodený celkový tvar prítomný vo falzifikáte (f), ale napríklad aj (c), aj keď daný falzifikát bol vybraný pre ukážku iného artefaktu.
- Externé obrysy odtlačku prsta sú veľmi jasné. Na konci odliatku papilárne línie náhle končia, čo sa prejaví okamžitým ukončením papilárnej línie v odtlačku falzifikátu, zatiaľ čo v pravom odtlačku papilárne línie na okrajoch miznú postupne. Náhle ukončenie papilárnych línií je prítomné na obrázku 3.6 v každom falzifikáte. [26]
- Chýbajúce oblasti papilárnych línií alebo oblasti papilárnych línií, ktoré sú v porovnaní s ich okolím menej jasné [26]. Chýbajúci región papilárnych línií je na obrázku 3.6 vo falzifikáte (g), oblasti papilárnych línií s nižšou jasnosťou vo falzifikáte (b).
- Rozmazané alebo skreslené papilárne línie v oblastiach, v ktorých sa to neočakáva vzhľadom na prirodzené odtlačenie prsta na povrchu [26]. Skreslené okraje papilárnych línií sú prítomné na obrázku 3.6 vo falzifikáte (d), skreslené a rozmazané papilárne línie vo falzifikáte (g), v hornej časti falzifikátu.
- Neočakávaný výskyt papilárnych línií vzhľadom na použitú techniku detekcie odtlačku prsta [26], ako bolo podrobnejšie uvedené v kapitole 3.2.1.

V kvalitných obrázkoch odtlačkov prstov môžu byť pozorované nasledujúce konkrétne znaky falzifikátov:

- Absencia potných pórov, ktoré však pri vhodnom výbere materiálu môžu byť prítomné aj vo falzifikáte [26]. Na obrázku 3.6 je absencia potných pórov prítomná vo všetkých falzifikátoch.
- Vzduchové bubliny, ktoré sú v prípade použitia odliatku taktiež prítomné len v prípade nevhodne zvoleného materiálu. Okrem toho sa vzduchové bubliny vyskytujú vo falzifikátoch, ktoré boli vytvorené premiestnením pravého odtlačku pomocou adhézneho materiálu. Na obrázku 3.6 sú vzduchové bubliny zobrazené vo falzifikáte (a). [26]
- Defekty v materiáli projektované do obrázku falzifikátu [26]. Na obrázku 3.6 je vo falzifikáte (e) prítomná projekcia praskliny vzniknutej v materiáli pri výrobe odliatku.

- Veľmi úzke medzery medzi papilárnymi líniami v porovnaní so šírkou papilárnych líní alebo nerovnomerné šírky papilárnych líní a medzier medzi nimi [26]. Tento artefakt je na obrázku 3.6 prítomný vo falzifikáte (c).
- Prítomnosť rovnakých artefaktov v rôznych odtlačkoch zobrazujúcich rovnakú oblasť papilárnych líní [26].



Obrázok 3.6: Artefakty falzifikátov odtlačkov prstov: (a) vzduchové bubliny, (b) oblasti papilárnych líní s nižšou jasnosťou, (c) nerovnomerné šírky papilárnych líní a medzier medzi nimi, (d) skreslené papilárne línie, (e) defekt v materiáli, (f) neprirodzený celkový tvar, (g) oblasť s chýbajúcimi papilárnymi líniami. V niektorých obrázkoch falzifikátov je prítomných viac artefaktov, v opise je uvedený vždy len jeden artefakt, pre ktorý bol falzifikát vybraný ako reprezentujúci zástupca. Obrázky falzifikátov pochádzajú z databázy výskumnej skupiny STRaDe<sup>1</sup> [38], ktorá pôsobí na Fakulte informačných technológií Vysokého učení technického v Brne.

### 3.3.1 Vzduchové bubliny

Vzduchové bubliny sú viditeľné v samotnom falzifikáte, ako aj v obrázku vzniknutom po snímaní falzifikátu skenerom. V obrázkoch sa potom javia ako prázdne miesta, ktoré majú odtieň približne rovnaký, ako je odtieň medzi papilárnymi líniami. Bubliny sa vo falzifikátoch nachádzajú v rôznom počte, rozličných tvaroch a na rôznych miestach v rámci plochy odtlačku. Veľkosť bublín sa líši od úplne malých, ktoré môžu byť zameniteľné s medzerami medzi papilárnymi líniami, až po relatívne veľké bubliny, ktoré prekrývajú väčší počet papilárnych líní. Tvar bubliny väčšinou pripomína kruh alebo elipsu s rôznou mierou porušenia okraja. Závažnejšie porušenie tvaru bublín je častejšie viditeľné v menších bublinách, väčšie

<sup>1</sup>Security Technology Research and Development

bublíny majú častokrát len mierne porušený okraj. Nie je jednoduché vymedziť interval s minimálnym a maximálnym počtom bublín, ktoré sa nachádzajú v odtlačkoch prstov. [1]

Pre potreby podrobnejšieho pozorovania boli počas analýzy vzduchových bublín v [1] vyrobené falzifikáty z materiálov, ktoré vykazujú vysoký výskyt vzduchových bublín. Konkrétne sa jednalo o farbu na sklo a gél na výrobu sviečok. V experimente boli zistené súvislosti medzi tvarom bublín vo falzifikáte a na obrázku vzniknutom po snímaní falzifikátu skenerom. Okrem toho z experimentov vyplynulo, že vzduchové bubliny, ktoré sa vo vyrobených falzifikátoch dotýkajú, po snímaní skenerom ostávajú oddelené a nevytvoria jeden spoločný útvar. [1]

### 3.3.2 Neprirodzený tvar

Pri použití niektorých materiálov a metód na výrobu falzifikátov je náročné zachovať prirodzený tvar odtlačku. V rámci experimentov počas analýzy vzduchových bublín v [1], bolo možné pozorovať aj neprirodzený tvar falzifikátov. Liatie roztopeného gélu na výrobu sviečok alebo aplikovanie farby na sklo neumožnili zachovať tvar odtlačku prsta, aj keď bol znázornený na podložke. Vznikali falzifikáty s rôznymi bočnými výčnelkami a celkovo iným tvarom. Keď je pre výrobu falzifikátu dostupný len latentný odtlačok, prirodzený tvar odtlačku, ktorý by sa dal napodobniť, nie je ani k dispozícii. Ďalšími dôvodmi vzniku neprirodzeného tvaru môže byť orezanie alebo odstrihnutie častí falzifikátu, aby ho bolo možné umiestniť na plochu skenera, vytvorenie príliš tenkého falzifikátu, ktoré pri odlepovaní z podložky vedie k pozdĺžnemu natiahnutiu falzifikátu, atď. Z uvedeného vyplýva, že počas výroby falzifikátov na celkový tvar odtlačku vplývajú viaceré faktory. [1]

V analýze falzifikátov s neprirodzeným tvarom sa vyskytovali najmä nasledovné vlastnosti – príliš rovné okraje, konkávny tvar, strany odtlačku prsta preličené dovnútra, tvar porušeného obdĺžnika, tvar lichobežníka s príliš rovnými hranami. Naopak, tvary prirodzených odtlačkov prstov môžu byť prirovnané k elipse alebo k oválu, neobsahujú rovné hrany, majú konvexný tvar. [1]

### 3.3.3 Ostatné artefakty

Vzduchové bubliny a neprirodzený celkový tvar boli v predchádzajúcich častiach opísané podrobnejšie, nakoľko bol ich vzhľad a výskyt pozorovaný v rámci výroby a analýzy obrázkov z databáz v práci, ktorá sa zaoberá konkrétne danými dvomi artefaktmi [1]. Ostatné artefakty v odbornej literatúre nie sú podrobnejšie opísané, dostupné sú len všeobecné informácie a obrázky.

## 3.4 Detekcia živosti

Detekcia živosti je schopnosť biometrického systému odlišiť neživý prst, ktorý je napríklad vyrobený zo syntetického materiálu, od živého prsta, pričom jej hlavným účelom je odhaliť falzifikát. Zisťovanie pravosti detekciou živosti je relevantné len pri získavaní odtlačku prsta *live-scan* metódou. [12]

Pri odtlačkoch prstov má detekcia živosti podstatnú úlohu najmä kvôli zanechávaniu stopy odtlačku prsta na mnohých povrchoch, ktorých sa dotkne [2]. Rovnako sa takmer zo všetkých materiálov dajú odtlačky prstov jednoducho získať použitím určitých fyzikálnych, chemických, fyzikálno-chemických, či špeciálnych metód [14]. Medzi fyzikálne techniky patrí použitie rôznych daktyloskopických práškov, v rámci chemických metód sa pre

získanie odtlačku prsta z povrchu využíva určitá chemická reakcia. Fyzikálno-chemické metódy zahŕňajú naparovanie a medzi špeciálne metódy patrí napríklad použitie laserových metód [14].

Nakoľko je výroba falzifikátov podľa kapitoly 3.2 nenáročná a možná aj v domácich podmienkach, detekcia živosti je nutnou súčasťou biometrického zariadenia. Výrobcovia senzorov sa snažia neustále vylepšovať svoje technológie, v dôsledku čoho je metód detekcie živosti odtlačkov prstov pomerne veľa. Niektoré metódy sú jednoduché a cenovo dostupné, iné sú náročnejšie na realizáciu, ale po funkčnej stránke sú veľmi spoľahlivé. [2]

Rôzne technológie senzorov odtlačkov prstov sú náchylné na použitie falzifikátov v rôznej miere. Jednoduché senzory môžu byť oklamané aj čierno-bielym vytlačeným obrázkom odtlačku prsta, pokročilejšie senzory umelo vyrobeným falzifikátom odtlačku prsta autorizovanej osoby. Z tohto pohľadu sú najzraniteľnejšie optické senzory, ktoré je v niektorých prípadoch možné oklamať aj obrázkom odtlačku prsta. Nasledované sú senzormi založenými na tlaku, na ktoré teoreticky stačí pritlačiť 3D odliatok odtlačku prsta. Za uvedenými senzormi sú umiestnené kapacitné, termálne a ultrazvukové snímače, ktoré už pre oklamanie vyžadujú sofistikovanejšie použitie falzifikátu. [39]

V závislosti na zvolenej metóde detekcie živosti testovanie prebieha buď počas zachytávania odtlačku prsta, kedy by neživý prst mal byť automaticky odmietnutý, alebo počas procesu rozpoznávania, kedy neživý prst musí byť zachytený, ale mal by byť odhalený počas procesu rozpoznávania a nebyť ďalej spracovávaný [13]. Získanie biometrických dát a dát pre testovanie živosti by však malo prebehnúť simultánne, inak má útočník možnosť urobiť dva separátne útoky [12].

Detekcia živosti odtlačkov prstov môže byť vykonávaná rôznymi metódami, ktoré budú uvedené v ďalšom texte. Okrem uvedených metód existujú aj ďalšie, špecifické metódy, alebo metódy chránené firemným tajomstvom [2].

### 3.4.1 Detekcia potu

Rovnako ako väčšina ľudského tela aj prsty sú pokryté potnými pórami ako bolo uvedené v kapitole 2.2 a na obrázku 2.3, vyskytujú sa na papilárnych líniách. Zachytením aktivity potných pórov je možné detegovať živosť prsta. Pre túto metódu je potrebné držať prst na ploche senzora približne 5 sekúnd. Počas danej doby dôjde k výronu kvapôčiek potu z potných pórov, čím sa farba papilárnych línií zmení na tmavšiu. Zmena farby papilárnych línií v čase v dôsledku výronu potu je znázornená na obrázku 3.7. [2]

Pre detekciu potu je vyžadované použitie skenera s vysokým rozlíšením. Nie je potrebné použitie dodatočného hardware. [12]

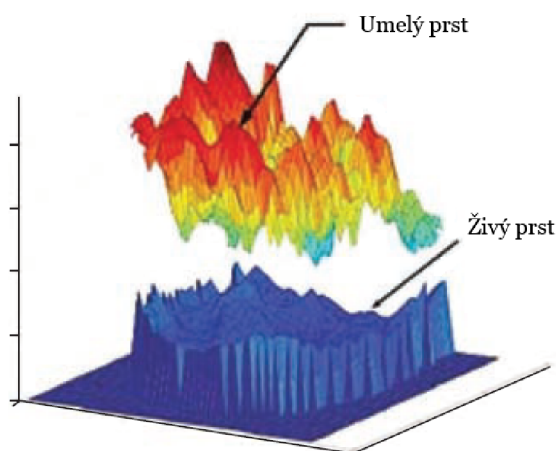


Obrázok 3.7: Tmavnutie papilárnych línií v čase v dôsledku výronu potu. Obrázok bol prebraný a upravený z [40].

### 3.4.2 Spektroskopické vlastnosti

Táto metóda detekcie živosti je založená na multispektrálnych vlastnostiach kože. Koža je z hľadiska priepustnosti svetla polopriepustným materiálom. Pri osvetlení povrchu prsta svetelnými zdrojmi s rôznymi vlnovými dĺžkami dôjde k čiastočnému pohlteniu a odrazeniu rôznych vlnových dĺžok. Navyše, koža každého užívateľa reaguje na dané osvetlenie iným spôsobom. Reakcia však kvôli vysokej vnútrotriednej variabilite nebýva použitá ako samostatná biometrická vlastnosť pre rozpoznávanie. [2] [40]

Pri použití tejto metódy je nutné, aby bol konvenčný senzor odtlačkov prstov doplnený o multispektrálny senzor. Vzhľadom na odlišné multispektrálne vlastnosti kože a materiálov pre výrobu falzifikátov tento skener dokáže jednoznačne rozlíšiť skutočný prst od falzifikátu. Rozdiel v grafe vytvorenom pri snímaní reálneho prsta a falzifikátu je znázornený na obrázku 3.8. [12]



Obrázok 3.8: Multispektrálne obrazové dáta jednoznačne rozlišujú medzi živým prstom a realisticky vyrobeným falzifikátom. Grafy znázorňujú odlišnosť spektrálneho obsahu obrázka umelého prsta s tým, aký sa očakáva pri živom prste. Obrázok bol prebraný a upravený z [41].

### 3.4.3 Ultrazvuková technológia

Ultrazvuková metóda detekcie živosti je založená na fakte, že ultrazvukové vlny prenikajú pod povrch prsta. Využitím tohto princípu je možné odhaliť nalepený falzifikát. Ultrazvukové vlny odrazené od povrchu falzifikátu neodpovedajú charakteristikám vln odrazených od živého prsta bez ďalších vrstiev. Existujú senzory odtlačkov prstov, ktoré týmto spôsobom získavajú aj obrázok odtlačku prsta. Najväčším problémom tejto metódy je analýza a rekonštrukcia signálov, ktoré sú ťažko interpretovateľné. [2] [12]

### 3.4.4 Fyzické vlastnosti

Fyzické vlastnosti patria medzi najjednoduchšie metódy detekcie živosti. Sú založené na rôznych merateľných javoch súvisiacich s kožou, ktorých úspešnosť je rôzna. [2]



Menej vhodnými fyzickými vlastnosťami pre detekciu živosti sú teplota prsta, teplý a studený podnet, zmeny pri prítlaku, elektrické vlastnosti kože. Teplota prsta nie je ideálnou vlastnosťou pre detekciu živosti, nakoľko sa významne mení v závislosti od vlastností prostredia. Teplý a studený podnet znamená, že užívateľ počas snímania odtlačku stláča rôzne tlačidlá, podľa pocitu tepla a chladu. Útočník má však polovičnú šancu uhádnuť. Zmeny pri prítlaku zachytávajú vlastnosť, že pri pritlačení prsta na senzor sa papilárne línie rozširujú. Koža reaguje na prítlak vytlačením krvi, jej farba sa teda zmení na svetlejšiu. [2] [12]

Vďaka elektrickým vlastnostiam kože je možné merať odpor či impedanciu, keďže koža je vodivým materiálom [2] [12]. Medzitriedna variabilita medzi živým prstom a falzifikátom je nízka, vnútrotriedna variabilita je vysoká [2] [12]. Vodivosť však môže byť použitá ako základný a lacný spôsob pre detekciu živosti, minimálne sa nedá obísť nevodivým materiálom.

Úspešne môže byť pre detekciu živosti využitá srdcová aktivita. Srdce pumpuje do tela okysličenú krv, smerom do srdca je privádzaná neokysličená krv. Pumpovanie spôsobuje objemové zmeny v tepnách a žilách, čo zapríčiňuje aj pulzovanie kože na končekoch prstov. Tento pohyb je voľným okom nerozoznateľný, je merateľný laserovým senzorom pre meranie vzdialenosti, alebo vďaka významnému zväčšeniu obrázka bruška prsta. [2] [12]

V súvislosti so srdcovou činnosťou je použitá aj ďalšia metóda detekcie živosti, ktorá je založená na fakte, že v prste sú dva typy krvi – okysličená a neokysličená. Oba typy je možné detegovať použitím infračerveného svetla. Za živý prst je potom považovaný ten, ktorý obsahuje oba typy krvi. [2] [12]

## 3.5 Detekcia falzifikátov

Detekcia falzifikátov je úloha pozostávajúca z rozlíšenia medzi tým, či je snímaná skutočná biometrika, alebo podvrh. Detekcia živosti, ktorá bola opísaná v časti 3.4, je zameraná na overenie živosti biometriky predkladanej senzoru. Niekedy je považovaná za synonymum detekcie falzifikátov, niekedy za konkrétnu metódu jej vykonania. V nasledujúcom texte budú bližšie predstavené niektoré ďalšie metódy používané pre detekciu falzifikátov.

### 3.5.1 Schopnosť detekcie falzifikátov forenznými expertmi

Z vedeckého hľadiska bola obava, či je odtlačky prstov možné falšovať, potvrdená v roku 1934 [42]. Už vtedy vznikla vo forenznej vede nutnosť overovať pravosť odtlačkov prstov, pričom táto kontrola prebiehala vizuálne a bola vykonávaná vyškoleným špecialistom [26]. Schopnosť odlíšiť reálny odtlačok prsta od falošného forenznými expertmi bola prvýkrát overená v rovnakom roku [43]. Experimentu sa vtedy zúčastnilo 8 expertov, ktorí skúmali 4 odtlačky prstov. Celkovo z 32 rozlišovaní medzi pravým a falošným odtlačkom prsta bolo 20 správnych, 11 nesprávnych a 1 neurčený. Falzifikáty boli precízne vyrobené v prísnych podmienkach.

Pre určenie falzifikátu forezným expertom je kľúčová metóda použitá pri výrobe a z nej vyplývajúca kvalita falzifikátu odtlačku prsta, pričom odhalenie kvalitných falzifikátov je veľmi náročné. Určenie pravosti odtlačku prsta je individuálne pre každý skúmaný odtlačok, preto celý proces rozlišovania neprebíha systematicky, závisí na skúsenostiach a tréningu forezného experta, ktorý býva väčšinou limitovaný. [26]

Vykonaných bolo viacero podobných experimentov, ktoré potvrdili predpoklad, že v niektorých prípadoch je takáto kontrola náročná a rozlíšenie pravého odtlačku od falzifikátu nie je jednoduché ani jednoznačné. [26]

### 3.5.2 Detekcia imitácie

V dnešnej dobe je nutné čeliť aj falzifikátom odtlačkov prstov vhodným pre oklamanie digitálnych senzorov. S rozmachom digitálnych senzorov sa zväčšila aj potreba algoritmov, ktoré umožnia softwarovo, poprípade v spojení s dodatočným hardware, rozlíšiť pravý odtlačok prsta od falošného. [26]

Detekcia imitácií funguje na opačnom princípe ako detekcia živosti. V tomto prípade je systém chránený tým, že sú v odtlačku prsta hľadané znaky falzifikátov odtlačkov prstov, ktoré boli uvedené v časti 3.3. Tento prístup je najdlhšie zavedeným protiopatrením pre falšovanie z hľadiska forenzných aplikácií. Vznikol na základe spôsobu vizuálneho hodnotenia odborníkov, ktoré vylepšuje v tom, že dokáže hodnotiť aj znaky voľným okom neviditeľné. [26]

### 3.5.3 Detekcia na základe posúdenia kvality obrázka odtlačku prsta

Táto metóda vznikla na základe predpokladu, že obrázok odtlačku zachytený so zámerom napodobniť pravý odtlačok, má inú kvalitu ako obrázok pravého odtlačku prsta zachytený počas klasického scenára. Existuje množina kritérií, ktoré tvoria klasifikátor. Môže medzi ne patriť napríklad porucha štruktúry, prítomnosť artefaktov falzifikátov, stupeň ostrosti obrázka, úroveň farieb a svetla, množstvo informácií získaných z obrázka. Po vyhodnotení daných kritérií z obrázka odtlačku prsta je určená pravdepodobnosť živosti a následne je obrázok priradený do jednej z dvoch tried — falzifikát alebo pravý odtlačok prsta. [26]

V metóde FQA<sup>1</sup> sú kritériá na posúdenie kvality obrázka prispôbené priamo odtlačkom prstov. Kvalita obrázka odtlačku prsta je posúdená napríklad na základe sily a smerovania papilárnych línií, ich spojitosti, jasnosti či integrity štruktúry papilárnych línií a medzier medzi nimi. Informácie o daných vlastnostiach môžu byť extrahované z poľa orientácií, alternatívne pomocou filtrov, z intenzity pixelov v odtieňoch sivej, zo silového spektra alebo pomocou neurónových sietí. Kvalita obrázka býva vyhodnotená buď holistickým spôsobom z celého obrázka, alebo v jednotlivých častiach obrázka osobitne a následným zjednotením výsledkov. Táto metóda využíva pre detekciu falzifikátu len jeden vstupný obrázok. [26]

V metóde IQA<sup>2</sup> sa jedná o celkové posúdenie kvality obrázka bez zamerania na odtlačky. V rámci metódy existujú dva spôsoby posúdenia kvality. V prvom z nich je dostupný aj obrázok pravého odtlačku prsta, v druhom sa vychádza len z jedného obrázka. Metóda pracuje s celým obrázkom, nesleduje žiadne znaky špecifické pre odtlačky prstov a pre posúdenie kvality používa štatistické modely. [26]

---

<sup>1</sup>*Fingerprint-Specific Quality Assessment*

<sup>2</sup>*General Image Quality Assessment*

## Kapitola 4

# Generátor syntetických odtlačkov

V akademickej aj industriálnej oblasti je vyvíjané obrovské úsilie pre vynájdenie nových algoritmov v oblasti rozpoznávania odtlačkov prstov, avšak menšia snaha je vynakladaná pre vyhodnotenie ich výkonu a správnosti [44]. Dôvodom je fakt, že takéto testovanie musí byť uskutočnené na rozsiahlej databáze odtlačkov prstov, ktorá častokrát nie je k dispozícii [44]. Riešením daného problému je použitie syntetických odtlačkov prstov. Priama pozornosť biometrie je zameraná na verifikáciu a identifikáciu, generovanie syntetických biometrických dát je inverzný biometrický problém [45]. Tieto syntetické dáta replikujú možné instance biometrických dát, ktoré by inak neboli dostupné [45].

V úvode kapitoly sú bližšie opísané syntetické odtlačky prstov. V súčasnosti existuje viacero prístupov pre generovanie syntetických odtlačkov prstov, vo výskume aj v aplikáciách je najpoužívanejšia metóda SFinGe<sup>1</sup> [12]. Okrem tejto metódy sú v samostatných podkapitolách priblížené aj ďalšie generátory, Chaloupkov generátor odtlačkov prstov, SyFDaS<sup>2</sup>, Anguli a SYnFi<sup>3</sup>.

### 4.1 Syntetické odtlačky prstov

Presnosť novovzniknutých algoritmov v oblasti odtlačkov prstov je potrebné overovať na rozsiahlych databázach odtlačkov prstov, kvôli potenciálnym malým chybám, ktoré iným spôsobom nemôžu byť odhalené. Tento fakt spôsobuje mnohé problémy, nakoľko dostupné databázy sú častokrát malé a súkromné. Algoritmus potom nie je otestovaný objektívne, naopak, je takzvané vysoko dátovo závislý. Znamená to, že algoritmus nie je otestovaný pre odtlačky pochádzajúce z rôznych aplikácií a prostredí. V dôsledku dátovej závislosti sa potom môže stať, že algoritmy sú veľmi presné, keď je na vstupe bežný odtlačok prsta (napríklad z triedy slučka) a naopak, ich presnosť je chabá, keď sú na vstupe zvláštne alebo menej časté odtlačky prstov (napríklad z triedy dvojité slučka). Ďalším problémom spojeným s databázami odtlačkov prstov je fakt, že akonáhle je databáza použitá pre otestovanie niektorého algoritmu, ďalej už nemôže byť používaná. [8] [10] [46]

---

<sup>1</sup>*Synthetic Fingerprint Generation*

<sup>2</sup>*Synthetic Fingerprint Damage Simulator*

<sup>3</sup>*Automatic Synthetic Fingerprint Generation*

Aby bol algoritmus otestovaný objektívne, je potrebná databáza s tisícami až desiatimi odličkami odličkov prstov [10] [44]. Zhromažďovanie obrázkov odličkov prstov do takýchto obrovských databáz je [44]:

- Drahé po finančnej aj časovej stránke,
- nezáživné pre ľudí, ktorí odličky zbierajú, aj pre dobrovoľníkov, ktorí sa väčšinou musia odobratia odličkov zúčastniť viackrát,
- chúlóstivé z dôvodov ochrany osobných údajov.

Riešením uvedených problémov je generovanie obrovských databáz syntetických odličkov prstov. Syntetické odličky prstov napodobňujú obrázky odličkov prstov získané z digitálnych skenerov, pretože väčšina komerčných aplikácií využíva *online* získavanie digitálnej reprezentácie odličkov prstov. Je možné vytvárať aj také syntetické odličky prstov, ktoré napodobňujú odličky získané *offline* metódou. Pri vytváraní generácie syntetických odličkov prstov sa vyžaduje, aby odličky v nej obsahovali vnútrotriadnu aj medzitriadnu variabilitu tak, ako je to prirodzené. Mala by obsahovať viac realistických odličkov rovnakého „virtuálneho prsta“ simulovaním rozličných plôch dotyku, nelineárnych deformácií vzniknutých nepravouhlým priložením prsta k ploche senzoru, variácií v šírke papilárnych línií kvôli intenzite pritlačenia prsta alebo vlhkosti pokožky, malých porezaní na prste alebo iných druhov šumu/porušení. [8] [44]

Databázy syntetických odličkov prstov sú užitočným nástrojom pre optimalizáciu, vyhodnocovanie a certifikovanie biometrických systémov. V súčasnosti existuje snaha pre generovanie databáz syntetických odličkov prstov s počtom odličkov porovnateľným ku veľkosti svetovej populácie, ktoré by slúžili pre vyhodnocovanie rôznych experimentov s odličkami prstov. Takéto vyhodnocovanie by vyžadovalo výkonnú *hardware*, v niektorých prípadoch by boli potrebné aj mesiace výpočtového času. Vzhľadom na vznikajúce technológie a očakávané trendy by v nasledujúcich rokoch mohli byť možné aj experimenty takéhoto typu. [12]

## 4.2 SFinGe

Typickým postupom pri extrahovaní znakov z obrázkov odličkov prstov je prvotná segmentácia odličku z pozadia, následne sú približne určené mapy orientácie a frekvencie papilárnych línií. Na základe týchto informácií je vytvorený vzor papilárnych línií a nakoniec sú detegované markanty [12]. Tieto operácie boli podrobnejšie vysvetlené v časti 2.5.

Metóda SFinGe využíva pri generovaní syntetických odličkov prstov niektoré inverzované kroky z vyššie uvedených [12]. Najskôr je potrebné vygenerovať hlavný odličok (*master fingerprint* – perfektný odličok [10], v procese digitálneho spracovania odličkov prstov je ekvivalentný k fáze, v ktorej sú extrahované papilárne línie, znázornenej na obrázku 2.9 (c)). Postup generovania hlavného odličku sa delí do štyroch krokov [8]:

1. Generovanie tvaru odličku,
2. generovanie mapy orientácií,
3. generovanie mapy frekvencie papilárnych línií,
4. generovanie vzoru papilárnych línií.

V prvom kroku je vygenerovaná plocha odtlačku, ktorá je v základnom tvare oválna, jej eliptické segmenty sa však dajú upravovať, vďaka čomu môžu mať syntetické odtlačky rozličné tvary [10].

V druhom kroku sa určuje trieda odtlačku, podľa ktorej je vygenerované umiestnenie singulárnych bodov. Ich pozíciu je taktiež možné meniť. Výstupom druhého kroku je pole orientácií. [10]

V treťom kroku je na základe heuristických kritérií, vytvorených vzhľadom na vizuálnu inšpekciu veľkého množstva odtlačkov prstov, vygenerovaná frekvencia papilárnych línií [8].

Vstupom pre proces generovania papilárnych línií sú výstupy prvých troch krokov, ktoré boli generované samostatne. V štvrtom kroku sa generuje vzor papilárnych línií. V metóde SFinGe je to zabezpečené elegantným spôsobom. Z viacerých počiatočných bodov (*initial seeds*) sa s využitím Gáborových filtrov a znalosti polí orientácie a frekvencie generujú papilárne línie a na náhodné miesta markanty rôznych typov. [8]

Pre generovanie viacerých odtlačkov rovnakého „virtuálneho prsta“ je potrebný komplexnejší prístup [12]. Viaceré syntetické odtlačky môžu byť odvodené z hlavného odtlačku, ktorý predstavuje unikátny a nemeniteľný vzor, napríklad prostredníctvom posunu, rotácie, zmeny stavu kože, pridaním šumu [8]. V metóde SFinGe sú pre získanie odvodených odtlačkov na hlavný odtlačok postupne aplikované nasledujúce štyri úpravy [44]:

1. Zmeny priemernej hrúbky papilárnych línií,
2. skreslenie,
3. pridanie šumu,
4. globálne otočenie/posun.

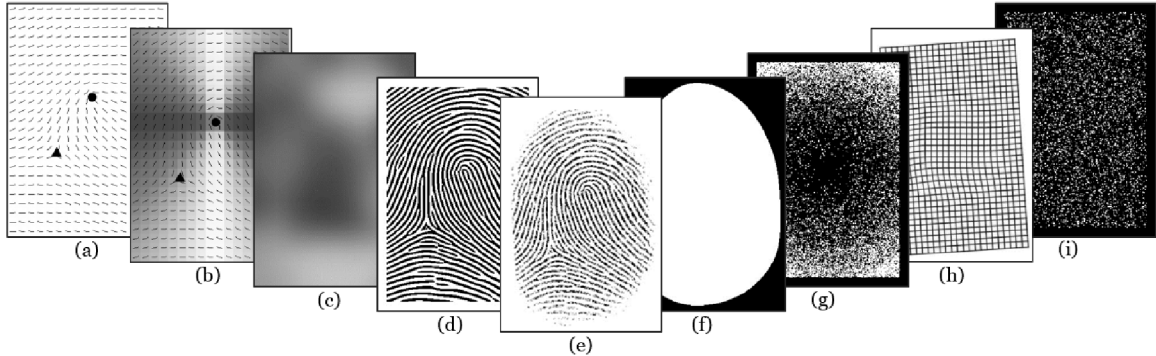
Na obrázky odtlačkov prstov má podobný vplyv vlhkosť prsta a tlak, akým je prst priťlačený k senzoru. Papilárne línie sú na obrázku tenšie, keď je pokožka prsta suchá alebo tlak malý. Naopak, vlhké prsty alebo väčší tlak prsta na senzor spôsobia, že papilárne línie sa na obrázku javia hrubšie. Simulácia rôznej miery vlhkosti a tlaku prsta pri vytváraní odvodených odtlačkov je v generátore SFinGe realizovaná pomocou morfológických operátorov. [8] [10] [47]

Nelineárne skreslenie, ktoré v obrázkoch odtlačkov prstov vzniká kvôli deformáciám pokožky pri rôznom priložení prsta na plochu skenera, je na hlavný odtlačok aplikované v druhom kroku. Je pri tom využitá Lagrangeova interpolácia [8]. Interpolácia je prostriedkom pre aproximáciu funkcií, ktorá umožňuje na základe znalosti ľubovoľnej množiny bodov vytvoriť polynóm približne odpovedajúci funkcii popisujúcej študovaný jav. Lagrangeov tvar interpolačného polynómu je konkrétny spôsob, akým je interpolačný polynóm možné skonštruovať. [8] [48]

Počas online získavania odtlačku prsta vplyvajú na rušenie snímaného signálu viaceré faktory. Kvôli tomu je na výstupe obrázkov v odtieňoch sivej nedokonalý, obsahuje rôzne porušenia, ako napríklad nepravidelnosť papilárnych línií, rozdielny kontakt papilárnych línií so senzorom, prítomnosť malých pórov vo vnútri papilárnych línií a i. Tieto nedokonalosti sú do obrázka v generátore SFinGe zanášané nasledovne – do osobitnej vrstvy sa izolujú biele pixely reprezentujúce medzery medzi papilárnymi líniami, pridá sa rušivý šum vo forme malých bielych škvŕn, obrázok sa vyhladí oknom veľkosti  $3 \times 3$  a získaný obrázok sa prekryje vrstvou uloženou v prvom kroku. [8] [44]

V poslednom kroku sa na odtlačok aplikuje globálne otočenie alebo posun, ktoré má simulovať neperfektné umiestnenie prsta na plochu senzora. Celý proces generovania syntetického odtlačku prsta generátorom SFinGe je schematicky znázornený na obrázku 4.1, kde

je na obrázku (e) znázornený výsledný syntetický odtlačok prsta, ktorý vznikol vytvorením hlavného odtlačku (kroky znázornené na obrázkoch (a) – (d)), jeho poškodením pre realistickjší vzhľad (kroky (g) – (i)) a orezaním maskou tvaru odtlačku prsta znázorenou na obrázku (f). [10]



Obrázok 4.1: Proces generovania syntetického odtlačku generátorom SFinGe: (a) mapa orientácií, (b) modifikovaná mapa orientácií, (c) mapa hustoty papilárnych línií, (d) hlavný odtlačok, (e) výsledný syntetický odtlačok, (f) maska odtlačku prsta, ktorou je orezaný hlavný odtlačok, (g) náhodný šum, (h) šum spôsobený skreslením, (i) konštantný šum. Obrázok bol prebraný a upravený z [49].

### 4.3 Chaloupkov generátor odtlačkov prstov

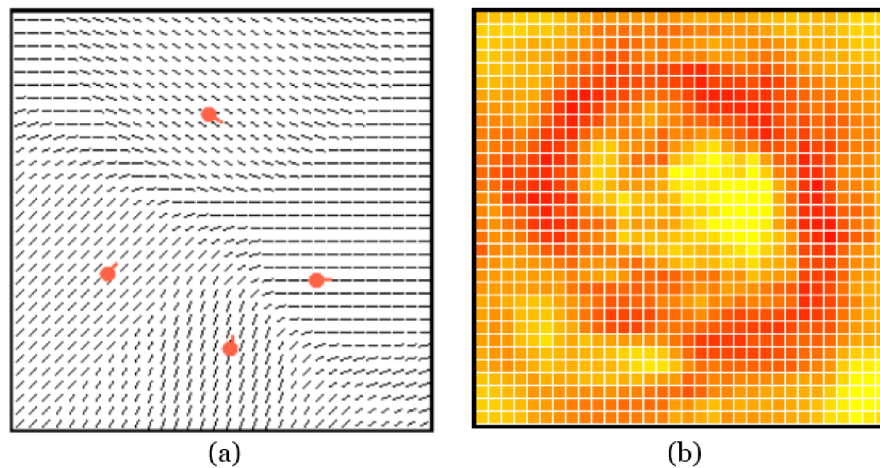
Chaloupkov generátor odtlačkov prstov používa pre generovanie podobné kroky ako generátor SFinGe. Vzor odtlačku prsta s papilárnymi líniami však tvorí na základe vygenerovaných alebo užívateľom zadaných markantov. Okrem toho obsahuje filtre, pomocou ktorých je možné vytvoriť realistickjší vzhľad odtlačku prsta. [50]

V generátore SFinGe dochádza ku kompletnému generovaniu odtlačku prsta podľa zadaného tvaru a triedy odtlačku. V prípade, že sú zadané pozície markantov, nie je možné použiť rovnaký prístup, pretože na základe samotných markantov sa nedá určiť natočenie prsta, čiže ani trieda odtlačku prsta. Okrem toho by v dôsledku generovania na základe triedy odtlačku prsta mohlo dôjsť k vygenerovaniu poľa orientácií, ktoré by nekorešpondovalo so všetkými zadanými markantmi a ich smerom udávajúcim orientáciu papilárnej línie. Hlavný rozdiel voči metóde SFinGe spočíva najmä v jej upravení tak, aby v dôsledku generovania na základe zadaných markantov nevznikli uvedené problémy. [50]

Pri generovaní poľa orientácií je využívaná ako vstupná informácia len množina zadaných markantov, ktoré v rámci neho tvoria pevne dané body. Na základe týchto bodov je vygenerovaný zvyšok poľa orientácií pre každý bod obrázka tak, aby si nimi korešpondoval. Na práve počítaný bod má pritom pre zachovanie správnosti najväčší vplyv najbližší markant. Pole orientácií je následne možné použiť ako základ pre vygenerovanie papilárnych línií prebiehajúcich smermi zodpovedajúcimi orientáciám zadaných markantov. V algoritme sa neberú do úvahy singulárne body, pretože globálne ovplyvňujú pole orientácií, a v tomto prípade by bolo náročnejšie vygenerovať ho tak, aby boli rešpektované pozície a orientácie lokálnych zadaných markantov. Z uvedeného vyplýva, v čom je algoritmus pre generovanie odtlačkov prstov pomocou dopredu zadaných markantov náročnejší ako me-

tóda SFinGe, v ktorej sú markanty vytvárané náhodne až pri generovaní papilárnych línií. Pole orientácií vygenerované na základe vplyvu štyroch zadaných markantov je zobrazené na obrázku 4.2 (a). [50]

Rozloženie hustoty papilárnych línií v odtlačku prsta je v metóde SFinGe konštantné, zvolené na základe rozloženia hustoty pozorovaného vo veľkom množstve skutočných odtlačkov prstov. Tento spôsob môže byť využitý, pretože je dopredu známy tvar odtlačku prsta, pozícia špičky prsta, jeho stred a okraje. V tomto generátore je rozloženie hustoty premenné a pre jeho vytvorenie je potrebné vytvoriť pole s rozmermi veľkosti vytváraného obrázka a v ňom definovať pre všetky miesta premenlivú hodnotu hustoty. Presnosti pritom nemusí byť venovaná príliš veľká pozornosť, rovnako nemusí byť nastavená hodnota hustoty pre každý pixel osobitne. Hustota rozloženia papilárnych línií môže byť upravená užívateľom, preto je v rámci generovania zobrazená ako prepočítaná farebná mapa, aj keď samotný výpočet využíva výškovú reprezentáciu. Farebná reprezentácia hustoty rozloženia papilárnych línií je zobrazená na obrázku 4.2 (b). [50]



Obrázok 4.2: Chaloupek generátor: (a) vygenerované pole orientácií s ohľadom pozície štyroch zadaných markantov, (b) vygenerovaná premenná hustota papilárnych línií, výšková mapa prepočítaná na farebnú. Obrázok bol prebraný a upravený z [50].

Pre samotné generovanie papilárnych línií sú podobne ako v generátore SFinGe použité Gáborové filtre na vstupný obrázok a dopočítané jednotlivé pixely obrázka. Opäť je však tento prístup modifikovaný tak, aby zohľadňoval existujúce zadané markanty. Papilárne línie sú generované do celého obrázka s rozlíšením  $15 \times 15$ , ktorý je následne orezaný do požadovaného tvaru odtlačku prsta. Výsledný obrázok odtlačku prsta vygenerovaný Chaloupekovým generátorom s použitím filtra pre realistickejší vzhľad odtlačku prsta je znázornený na obrázku 4.3 [50]

Nastavitelné parametre Chaloupekovho generátora ovplyvňujúce generovanie odtlačku prsta sú [50]:

- Gáborov filter,
- hustota rozloženia,
- viditeľná plocha odtlačku,
- markanty.



Obrázok 4.3: Výsledný obrázok odtlačku prsta z Chaloupkovho generátora. Obrázok bol prebraný a upravený z [50].

## 4.4 SyFDaS

SyFDaS je generátor odtlačkov prstov slúžiaci pre generovanie syntetických odtlačkov simulujúcich poškodené skutočné odtlačky prstov. Pre jeho vytvorenie bolo najskôr simulované generovanie syntetických odtlačkov prstov použitím Petriho siete. Simulácia bola nazvaná FGN<sup>1</sup> [51]. Petriho siete sú špeciálnou modelovacou technikou, ktorá môže byť reprezentovaná matematickou notáciou alebo grafom [52]. Grafická reprezentácia je lepšie pochopiteľná, matematická zase umožňuje použitie rôznych analýz a dôkazov [52].

Petriho siete sú často používané pre zjednodušenie komplexných distribuovaných systémov. V tomto prípade boli použité podobne, pre poskytnutie jasného pohľadu na zobrazenie všetkých možností, ktoré sa môžu pri generovaní syntetického prsta s poškodeniami vyskytnúť. Vzniknutý scenár bol čiastočne zrekonštruovaný v *software* s implementáciou niektorých simulácií poškodenia uvedených v Petriho sieti. [11] [51]

Aby bola vytvorená Petriho sieť čo najzrozumiteľnejšia, celý proces generovania syntetického odtlačku bol rozdelený do štyroch častí [51]:

1. Simulácia generovania hlavného odtlačku,
2. simulácia stavu prostredia,
3. simulácia stavu užívateľa a jeho prsta,
4. simulácia stavu senzora.

Uvedené časti zachytávajú okruhy všetkých druhov poškodení odtlačku prsta, ktoré je možné simulovať aj vo výslednej aplikácii SyFDaS. Každá časť je v Petriho sieti aj aplikácii ďalej rozčlenená na základe konkrétnych možností spôsobujúcich poškodenia. [11]

Vzniknutá Petriho sieť pokrýva generovanie javov, ktoré môžu ovplyvniť obrázok odtlačku prsta počas získavania jeho digitálnej reprezentácie. V prípade konkrétneho scenára získania odtlačku prsta s konkrétnym sensorom, stavom užívateľa a prostredia môže byť táto sieť redukovaná len na nevyhnutné časti.

Samotná aplikácia SyFDaS vychádza zo simulácie FGN a môže byť rozdelená do dvoch častí – vytvorenie syntetického odtlačku prsta a simulácia poškodení odtlačku prsta. Pre generovanie základného syntetického odtlačku prsta je použitá vylepšená verzia Chaloupkovho

---

<sup>1</sup> *Fingerprint Generation Petri Net*



generátora, ktorý bol opísaný v podkapitole 4.3. Informácie o senzore, type generovaného poškodenia a všetkých informácií potrebných pre simuláciu poškodenia boli integrované do rovnakého rozhrania. Výsledky generovania poškodení v závislosti na stave užívateľa, konkrétne kožných ochorení atopický ekzém (b) a bradavica (c), spolu s vygenerovaným syntetickým odtlačkom prsta bez poškodení (a) sú znázornené na obrázku 4.4 [11]

Okrem integrovania nových prvkov umožňujúcich generovanie poškodení odtlačku prsta bolo vylepšené aj samotné generovanie syntetického odtlačku prsta. Konkrétne bola pridaná možnosť zadať okrem vstupných markantov aj triedu odtlačku prsta, v dôsledku čoho muselo byť zmenené aj generovanie poľa orientácií. Pri generovaní poľa orientácií je v aplikácii najskôr použité pole orientácií pre zadanú triedu odtlačku prsta. Markantom je pridaná významnosť, ktorá určuje ako veľmi daný markant ovplyvňuje inicializáciu poľa orientácií. [11]



Obrázok 4.4: SyFDas: Generovanie syntetického odtlačku prsta bez poškodenia (a) a s poškodeniami spôsobenými kožnými ochoreniami, konkrétne atopický ekzém (b) a bradavica (c). Tieto poškodenia spadajú pod simuláciu stavu užívateľa a jeho prsta. Obrázok bol prebraný a upravený z [11] a z [17].

## 4.5 Anguli

Názov Anguli pochádza z hindčiny, podľa krajiny jeho vzniku, a v preklade znamená prst [53]. Anguli je *open-source* aplikácia implementujúca metódu SFinGe. Jej hlavným účelom je umožniť jednoduché vytvorenie veľkého množstva syntetických odtlačkov prstov. Takéto generovanie môže byť výpočtovo náročné, preto Anguli umožňuje generovať odtlačky prstov paralelne s využitím viacerých jadier. Umožňuje vyprodukovať až milión syntetických odtlačkov prstov za menej než štyri dni, s využitím 8 fyzických procesorových jadier. Aplikácia je navyše kompatibilná so systémom Windows aj Linux. [49] [54]

Anguli poskytuje prívetivé užívateľské rozhranie, ktoré umožňuje generovanie ľubovoľného počtu odtlačkov prstov s rôznymi konfiguráciami. Medzi hlavné funkcie patrí [54]:

- Generovanie viacerých výsledných zobrazení odvodených odtlačkov prstov od hlavného odtlačku prsta,
- ukladanie metadát,

- nastavenie množstva odtlačkov prstov, ktoré majú byť uložené v jednom adresári,
- percentuálne nastavenie pre pridanie šumu a poškodenia papilárnych línií,
- rozsah pixelov, ktorými sú odtlačky prstov transformované.

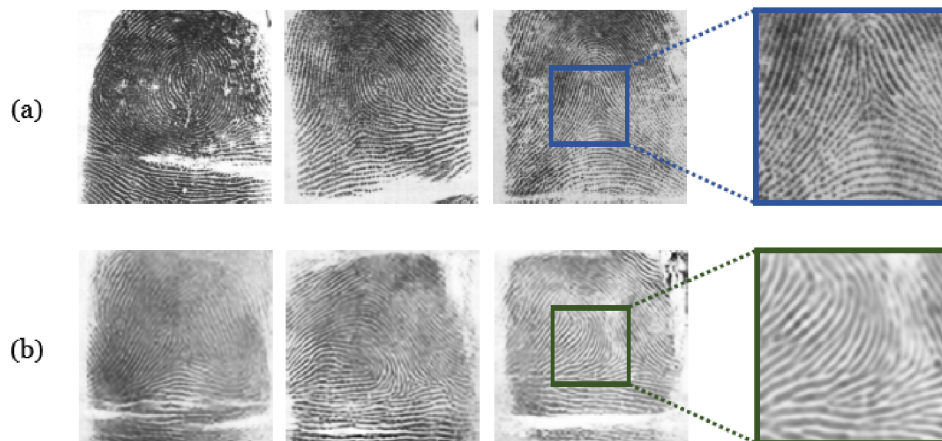
## 4.6 SYnFi

SYnFi je generátor odtlačkov prstov, ktorý na rozdiel od SFinGe a Anguli nepoužíva pre vytváranie odtlačkov prstov matematické modely, ale je založený na neurónových sieťach. Pri jeho vytváraní bolo hlavným cieľom generovanie syntetických odtlačkov prstov, ktoré nie sú rozoznateľné od skutočných odtlačkov prstov. [55]

Najväčšou výzvou v generovaní syntetických odtlačkov prstov s vysokou kvalitou je určenie rozloženia hustoty pravdepodobnosti reálnych odtlačkov prstov. Keď je toto rozloženie známe, vzorkovaním je možné generovať syntetické odtlačky prstov podľa daného rozloženia. Tento problém bol vyriešený použitím GAN <sup>1</sup> na určenie pravdepodobnosti rozloženia reálnych odtlačkov prstov. Použitím tohto prístupu kvôli nedostupnosti veľkých verejne dostupných databáz nie je možné dobre generalizovať a vytvárať realisticky pôsobiace odtlačky prstov. Preto je tento prístup použitý len v prvej fáze generovania, pre vytvorenie obrázka odtlačku prsta s nízkou kvalitou. [55]

V druhej fáze je použitý SR <sup>2</sup> model, ktorý transformuje obrázok nízkej kvality do realistického obrázka odtlačku prsta s vysokou kvalitou. V tejto fáze sú do obrázka pridané detaily a textúra markantov. [55]

Testovaním bolo preukázané, že model strojového učenia dosahujúci v rozpoznávaní odtlačkov prstov najlepšie výsledky mohol rozoznať syntetické odtlačky z generátora SYnFi od skutočných odtlačkov prstov len o 0,43 % lepšie ako pri náhodnom odhade. Uvedená skutočnosť ilustruje efektívnosť SYnFi. Na obrázku 4.5 sú znázornené skutočné odtlačky prstov (a) v porovnaní so syntetickými odtlačkami prstov vytvorenými generátorom SYnFi (b). [55]



Obrázok 4.5: SYnFi: (a) skutočné odtlačky prstov, (b) syntetické odtlačky prstov vytvorené generátorom SYnFi. Obrázok bol prebraný a upravený z [55].

<sup>1</sup>Generative Adversarial Network

<sup>2</sup>Super-Resolution

# Kapitola 5

## Návrh

Obsahom tejto kapitoly je predstavenie návrhu metód pre generovanie niektorých vybraných prejavov falzifikátov do syntetických odtlačkov prstov. Dané prejavy sú dopĺňané do už existujúcej aplikácie pre generovanie prejavov falzifikátov. Aplikácia je bližšie predstavená v úvode kapitoly. Následne je opísaný proces výberu artefaktov falzifikátov, o ktoré bude aplikácia rozširovaná.

Ďalej kapitola obsahuje podkapitoly zahŕňajúce analýzu a návrh algoritmu pre dva vybrané prejavy falzifikátov. Nakoľko je v aplikácii implementované základné spracovanie obrázka syntetického odtlačku prsta, konkrétne detekcia plochy odtlačku v rámci obrázka a detekcia papilárnych línií, tieto operácie už nie sú zahrnuté v uvedených algoritmoch. Predpokladá sa, že v čase použitia algoritmov je maska plochy odtlačku prsta aj maska papilárnych línií k dispozícii pre použitie.

### 5.1 Opis aktuálnej aplikácie

Generátor prejavov falzifikátov do syntetických odtlačkov prstov je implementovaný ako konzolová aplikácia bez užívateľského rozhrania. Implementačným jazykom je C++, s využitím knižnice OpenCV vo verzii 3.4.3 a grafických prvkov jazyka C++. [1]

V aplikácii je možné generovať tri prejavy falzifikátov – vzduchové bubliny, neprirodzený celkový tvar a postupne miznúce okraje. Miznúce okraje nie sú prejavom falzifikátov, naopak, artefaktom vyskytujúcim sa vo falzifikátoch odtlačkov prstov je náhle ukončenie papilárnych línií v externých kontúrach odtlačku prsta. Aplikácia očakáva na vstupe hlavný odtlačok z generátora SFinGe bez generovaných poškodení len orezaný do tvaru odtlačku prsta. Táto reprezentácia obsahuje náhle ukončenie papilárnych línií, preto boli implementované postupne miznúce okraje, aby bolo možné generovať realistickejšie obrázky odtlačkov prstov s prejavmi falzifikátov. [1]

Generovanie prebieha výberom módu pomocou klávesnice. Každý generovaný prejav môže byť skúšobne vytvorený viackrát, výslednú reprezentáciu je však nutné uložiť. Do jedného falzifikátu môže byť vygenerovaná aj kombinácia viacerých artefaktov, jedinou podmienkou pritom je, že ak má výsledný odtlačok obsahovať postupne miznúce okraje, musia byť vygenerované, a najmä uložené ako prvé. Nemalo by zmysel generovať miznúce okraje po tom, ako by bol vygenerovaný neprirodzený celkový tvar. [1]

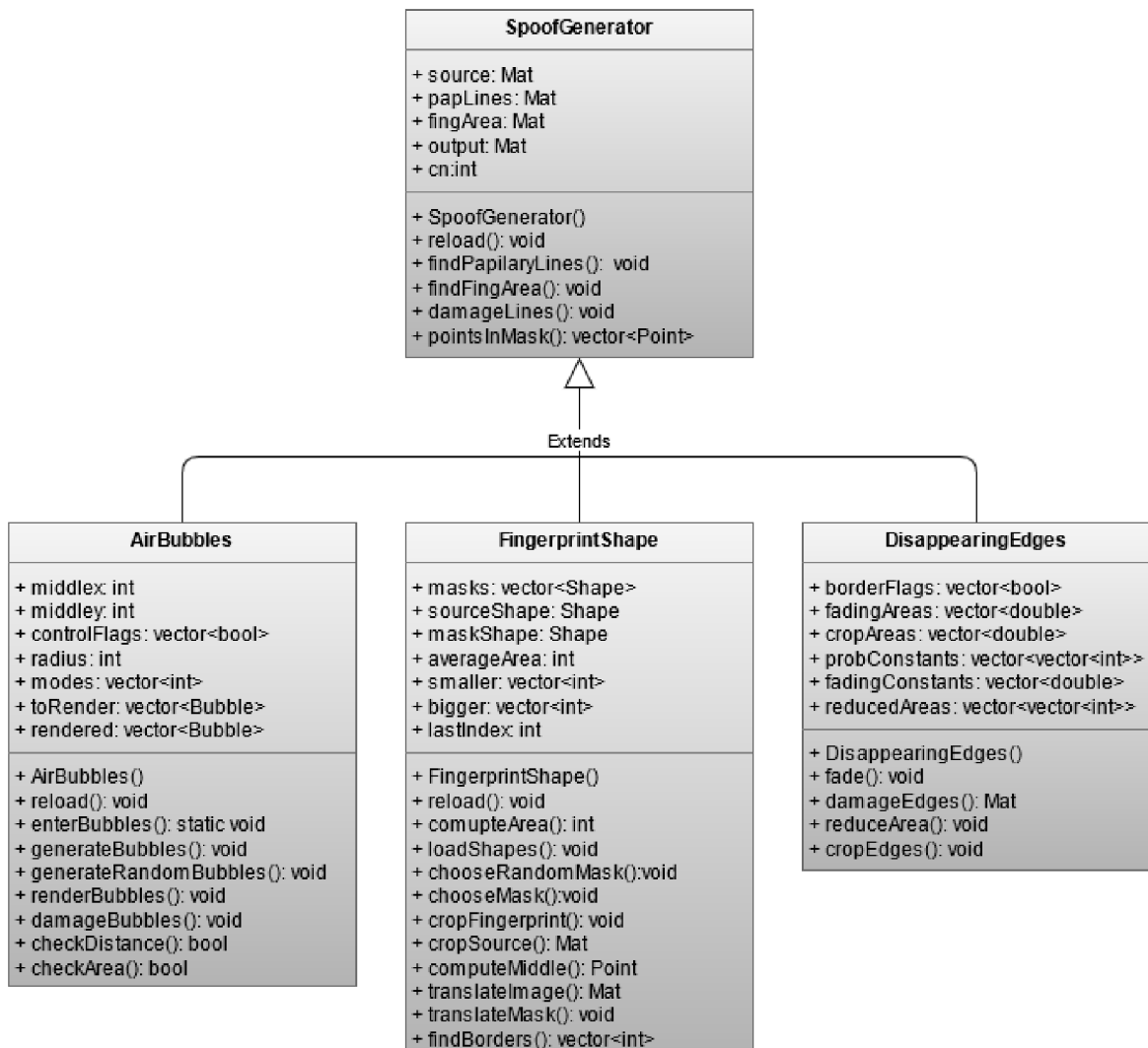
Vzduchové bubliny môžu byť vytvorené v dvoch módoch, a to náhodným generovaním, kedy sú ich pozície, veľkosti a počet vygenerované náhodne programom, alebo môžu byť uvedené atribúty zadané užívateľom pomocou myši. Konkrétny tvar bubliny a poškodenie

jej okraja sú vždy vygenerované náhodne, s určitou pravdepodobnosťou určenou veľkosťou bubliny. [1]

Neprirodzený tvar môže byť taktiež vygenerovaný náhodne, vtedy je programom v závislosti na veľkosti plochy syntetického odtlačku prsta zvolený jeden z dopredu pripravených tvarov, zostrojených podľa tvarov falzifikátov z databázy výskumnej skupiny STRaDe. Okrem toho môže byť tvar zvolený výberom užívateľa, kedy sú mu postupne zobrazované všetky dostupné tvary. [1]

Pri postupne miznúcich okrajoch nie je implementované náhodné generovanie, užívateľ musí zvoliť jeden z piatich dostupných stupňov poškodenia a jednu z troch dostupných širok miznúcich okrajov. [1]

Diagram tried aplikácie pre generovanie prejavov falzifikátov je uvedený na obrázku 5.1. Trieda `SpoofGenerator` reprezentujúca generátor je rozšírená o triedy implementujúce generovanie jednotlivých artefaktov falzifikátov `AirBubbles`, `FingerprintShape` a `DisappearingEdges`.



Obrázok 5.1: Diagram tried pôvodnej aplikácie pre generovanie prejavov falzifikátov. Obrázok bol prebraný a upravený z [1].

## 5.2 Výber artefaktov falzifikátov pre rozšírenie aplikácie

Pre výber prejavov falzifikátov, o ktoré má byť aplikácia rozšírená, bola urobená analýza prejavov falzifikátov vyskytujúcich sa v obrázkoch falzifikátov po snímaní skenerom. Obrázky boli porovnávané so zábermi rovnakých falzifikátov z mikroskopu, aby bolo určené, či sa jedná o skutočný prejav falzifikátov, alebo chybu vzniknutú počas snímania skenerom. Pre analýzu boli použité dve databázy obrázkov falzifikátov pochádzajúce z výskumnej skupiny STRaDe.

V databázach boli nájdené viaceré prejavy falzifikátov, z tých, ktoré sú uvedené v podkapitole 3.3. Celkovo sa v daných databázach v rámci falzifikátov najčastejšie vyskytovala absencia potných pórov, veľmi jasné externé obrysy odtlačkov prstov, neprirodzený celkový tvar a veľmi úzke medzery medzi papilárnymi líniami v porovnaní so šírkou papilárnych líní. Z uvedených prejavov je absencia potných pórov už prítomná v obrázkoch syntetických odtlačkov prstov, nasledujúce dva prejavy sú implementované v základnej aplikácii. Pri prejave veľmi úzke medzery medzi papilárnymi líniami je náročné určiť, či sa skutočne jedná o prejav falzifikátu, alebo sú rozdielne medzery spôsobené prítlakom pri snímaní.

Menej často boli prítomné vzduchové bubliny, defekty v materiáli, rozmazané alebo skreslené papilárne línie. Z prejavov uvedených v tejto kategórii sú vzduchové bubliny taktiež už implementované v základnej aplikácii a pri rozmazaných či skreslených papilárnych líniah je rovnako ako pri nerovnomerných medzerách náročné určiť, či sa jedná o falzifikát, alebo len poškodenie vzniknuté pri snímaní. Defekty v materiáli boli vybrané ako prvý prejav, o ktorý bude základná aplikácia rozširovaná. Konkrétne bola vybraná prasklina, ktorá je medzi rôznymi defektmi vyskytujúcimi sa na obrázkoch najlepšie rozoznatelná.

Len veľmi vzácnne sa medzi falzifikátmi vyskytuje šum v pozadí, chýbajúce oblasti papilárnych líní alebo oblasti papilárnych líní, ktoré sú v porovnaní s ich okolím menej jasné. Z tejto oblasti bol napriek nie až tak častému výskytu zvolený druhý prejav pre rozšírenie aplikácie, a to oblasti papilárnych líní s nižšou jasnosťou. Dôvodom je možnosť na základe distribúcie materiálu viditeľnom vo falzifikáte po snímaní skenerom jednoznačne vylúčiť, že by sa jednalo o chybu pri snímaní. Tento problém pri ostatných prejavoch nie je možné nepochybne vyriešiť.

Prejavy, ktoré vôbec nie sú v databáze prítomné, poprípade ich nie je možné identifikovať, sú neočakávaný výskyt papilárnych líní vzhľadom na použitú techniku detekcie odtlačku prsta a prítomnosť rovnakých artefaktov v rôznych odtlačkoch zobrazujúcich rovnakú oblasť papilárnych líní.

## 5.3 Nižšia jasnosť papilárnych líní

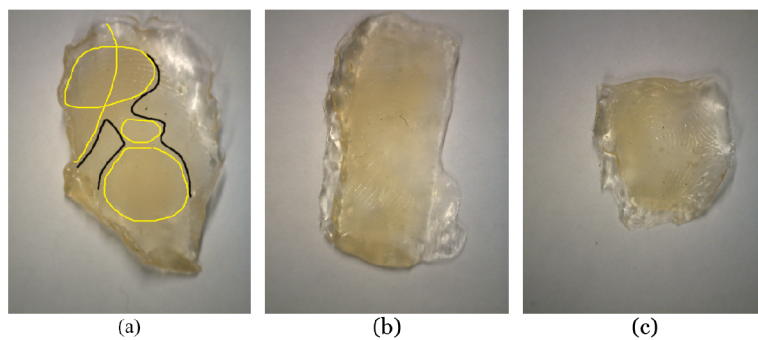
Prvým vybraným prejavom falzifikátov sú oblasti papilárnych líní s nižšou jasnosťou. V rámci prípravy pred vytvorením algoritmu bola urobená analýza obrázkov z databázy výskumnej skupiny STRaDe, ktoré obsahujú daný prejav.

### 5.3.1 Analýza falzifikátov s oblasťami s nižšou jasnosťou papilárnych líní

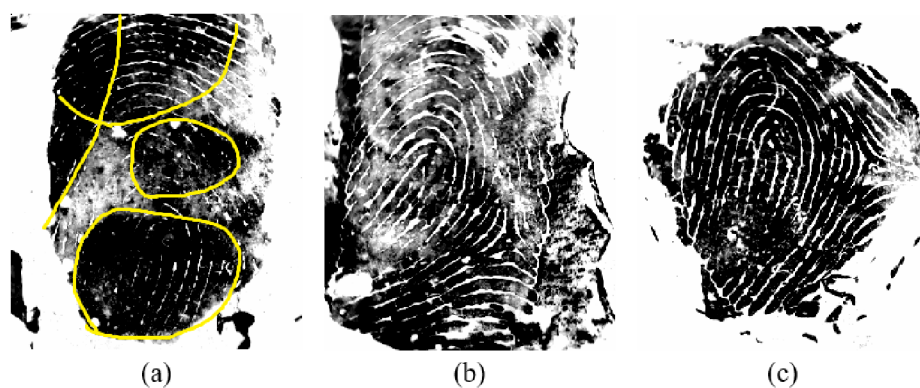
Ako bolo uvedené v kapitole 3.3, v niektorých falzifikátoch odtlačkov prstov je možné pozorovať chýbajúce oblasti papilárnych líní, alebo oblasti papilárnych líní s nižšou jasnosťou. V databáze falzifikátov sa oblasti papilárnych líní s nižšou jasnosťou vyskytujú vo falzifikátoch vyrobených z latexu. V samotnom falzifikáte sa pritom jedná o oblasti, v ktorých je v dôsledku nerovnomernej distribúcie tenšia vrstva materiálu. Artefakt vzniká až pri

snímaní skenerom, kedy sú papilárne línie v tenšej vrstve zachytené s nižším jasom a kontrastom. Toto poškodenie by mohlo byť vnímané ako chyba pri snímaní, avšak, keďže pri snímaní skutočného prsta by k danému poškodeniu nemohlo dôjsť, môže byť považované za znak falzifikátov.

Na obrázku 5.2 sú znázornené falzifikáty odtlačkov prstov vyrobené z latexu po snímaní mikroskopom. Na obrázkoch je viditeľná rôzna distribúcia materiálu v rámci falzifikátov. Hrubšie vrstvy materiálu majú tmavší odtieň a vyskytujú sa v tvare pripomínajúcom elipsy. Pomyselné elipsy pritom nie sú len vo vnútri falzifikátu, môžu zasahovať aj mimo oblasti odtlačku. Tenšie vrstvy majú svetlejší odtieň, sú až priehľadné. Ich tvar je veľmi nepravidelný, nedá sa prirovnať k žiadnemu útvaru. Tvary zrejme súvisia s distribúciou materiálu počas výroby falzifikátov. Hrubšie vrstvy vznikajú v dôsledku väčšieho množstva materiálu, ktorý sa roz distribuuje do elipsovitého tvaru. Tenšie oblasti ostávajú v miestach, kam sa väčšie množstvo materiálu nedostane. Na obrázku 5.2 (a) sú pre lepšiu predstavu čiernou farbou približne naznačené hranice tenších priehľadných oblastí a žltou farbou elipsy ohraničujúce oblasti s hrubšími vrstvami materiálu.



Obrázok 5.2: Falzifikáty odtlačkov prstov vyrobené z latexu po snímaní mikroskopom. Vo falzifikátoch sú viditeľné hrubšie a tenšie vrstvy materiálu, odlišujú sa farebným odtieňom. Hrubšie oblasti sú tmavšie, tenšie oblasti sú svetlé, až priehľadné. Obrázky pochádzajú z databázy výskumnej skupiny STRaDe.



Obrázok 5.3: Obrázky falzifikátov odtlačkov prstov vyrobených z latexu po nasnímaní skenerom. Falzifikáty obsahujú oblasti papilárnych línií s nižšou jasnosťou. Obrázky pochádzajú z databázy výskumnej skupiny STRaDe.

Na obrázku 5.3 sú znázornené falzifikáty z obrázka 5.2 po snímaní skenerom odtlačkov prstov. Príslušné falzifikáty sú na oboch obrázkoch označené rovnakým písmenom. Na týchto obrázkoch je možné pozorovať oblasti papilárnych línií s nižšou jasnosťou pripomínajúce oblaky pary. Odtieň papilárnych línií na vonkajších hraniciach oblastí je svetlejší a postupne je zosvetlovaný až na farbu medzier medzi papilárnymi líniami. V centrálnych častiach týchto oblastí sa vyskytujú útvary pripomínajúce malé biele kruhy. V okrajových častiach sú okrem svetlejšieho odtieňa papilárnych línií prítomné pixely, ktoré sú už v týchto častiach úplne biele. Celkovo majú dané oblasti nepravidelný tvar, ich spojitost je porušená občasnými tmavými miestami vyskytujúcimi sa aj v rámci oblastí so svetlým odtieňom. Na obrázku 5.3 (a) sú žltou farbou približne naznačené hranice hrubších nepriehľadných oblastí, ktoré pripomínajú elipsovité tvar. Hranice tenších oblastí po snímaní skenerom je na tomto obrázku možné porovnať s ich naznačením na obrázku 5.2 (a) z mikroskopu.

### 5.3.2 Algoritmus pre generovanie oblastí s nižšou jasnosťou papilárnych línií do syntetických odtlačkov prstov

Falzifikáty obsahujúce oblasti papilárnych línií s nižšou jasnosťou sú vzhľadom na rozdielnu distribúciu materiálu pri výrobe falzifikátu navzájom odlišné. Je preto žiadúce prispôbiť algoritmus generovania tomuto faktoru a vytvoriť náhodne generované oblasti. Nejedná sa však o náhodné generovanie tvarov, oblasti s nižšou jasnosťou musia spĺňať potrebné vlastnosti, musia byť generované podľa dopredu danej logiky a musia pôsobiť realisticky, podobne ako na obrázku 5.3. V určitých situáciách, napríklad pre potreby testovania, je nutné prispôbovať vzhľad falzifikátu, a preto je metóda náhodného generovania oblastí s nižšou jasnosťou doplnená aj o možnosť zadania ich pozície a približnej veľkosti užívateľom.

Oblasti s nižšou jasnosťou papilárnych línií je náročné prirovnáť k nejakému tvaru, ako bolo opísané v časti 5.3.1. Pri generovaní budú preto vytvárané reprezentácie nepriehľadných oblastí s hrubšou vrstvou materiálu, ktoré môžu byť prirovnané k elipse. V prípade módu, kedy generovanie ovplyvňuje užívateľ, bude taktiež pomocou myši zadávať elipsy reprezentujúce nepriehľadné oblasti a oblasti s nižším jasom budú vytvorené v rámci plochy odtlačku prsta mimo zadaných hrubších vrstiev.

Algoritmus pre náhodné generovanie oblastí papilárnych línií s nižšou jasnosťou:

1. Vypočítaj aproximáciu obsahu odtlačku prsta `fingerArea` určenú počtom bielych pixelov v maske plochy odtlačku prsta.
2. Náhodne vygeneruj parametre elipsy, jej stred, polomer a otočenie.
3. Ulož základnú reprezentáciu vygenerovanej elipsy do poľa `thickerLayersBase`.
4. Vytvor novú masku všetkých vygenerovaných elíps.
5. Poruš kontúry masky vygenerovaných elíps pre dosiahnutie realistickejšieho vzhľadu.
6. Vypočítaj aproximáciu plochy všetkých vygenerovaných elíps `ellipsesArea` určenú počtom bielych pixelov v maske elíps.
7. Podľa zvoleného pomeru plochy medzi hrubšími oblasťami a celej plochy odtlačku urč, či plocha `ellipsesAreas` presiahla definovanú hranicu, ak áno, pokračuj ďalším krokom, ak nie, vráť sa na krok 2.

8. Vygeneruj grafickú reprezentáciu oblastí s nižšou jasnosťou papilárnych línií.
9. Prekry vzniknutý obrázok bielymi pixelmi z reprezentácie papilárnych línií.
10. Vyhľad výsledný obrázok oknom veľkosti  $2 \times 2$ .

Algoritmus v prípade zadania oblastí s hrubšou vrstvou materiálu užívateľom obsahuje len pár odlišností. Namiesto bodov 1 a 2 sú elipsy získané od užívateľa prostredníctvom zadania ich tvaru myšou. Body 6 a 7 sú z algoritmu vypustené, ostatné ostávajú rovnaké. Vygenerovanie realistickej grafickej reprezentácie oblastí s nižšou jasnosťou v bode 8 sa dosiahne:

- zosvetlením odtieňa v celej oblasti mimo zadaných elíps,
- vygenerovaním bielych pixelov pokrývajúcich papilárne línie,
- vygenerovaním tmavého šumu prekrývajúceho zosvetlenú oblasť, a tým narúšajúceho jej spojitosť,
- zavedením rôznych stupňov pre generovanie zväčšujúceho sa poškodenia smerom od okrajov do centrálnejších častí oblastí papilárnych línií s nižšou jasnosťou.

## 5.4 Prasklina

Druhým vybraným prejavom falzifikátov je prasklina v materiáli falzifikátu odtlačku prsta. V rámci prípravy pred vytvorením algoritmu bola urobená analýza obrázkov z databázy výskumnej skupiny STRaDe, ktorá vznikla ako snaha vyrobiť, opísať a porovnať falzifikáty z takzvaných „kreatívnych materiálov“ – materiálov často používaných pri modelovaní [56]. Z celkového počtu dvadsaťjeden vyskúšaných materiálov sú v uvedenej databáze obrázky falzifikátov z ôsmich materiálov, z ktorých vznikli najkvalitnejšie falzifikáty. Dané falzifikáty sú v databáze nasnímané viacerými typmi senzorov a mikroskopom [56].

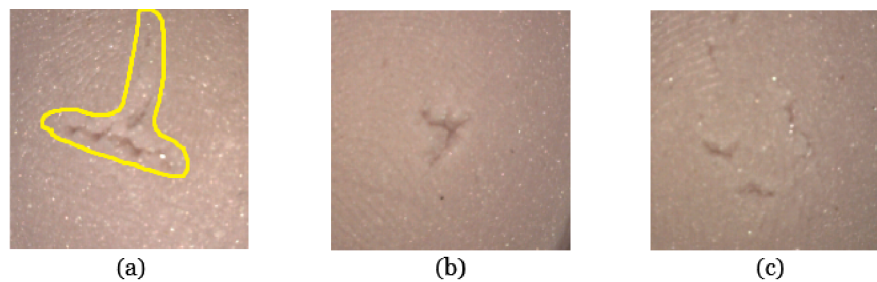
Analýza bola zameraná na obrázky z optického senzora Secugen, ktoré sa najviac podobajú syntetickým odtlačkom prstov, a na obrázky z mikroskopu Dinolite, s ktorými boli čiernobiele obrázky zo senzora porovnávané. V rámci analýzy bolo zistené, že v databáze sa praskliny vyskytujú v troch druhoch materiálov, a to Cernit, Kato a vosk. V každom z uvedených materiálov majú praskliny odlišný, typický tvar. V prípade generovania tohto prejavu je preto žiadúce generovať viac typov prasklín, odpovedajúcich prasklinám v uvedených materiáloch.

### 5.4.1 Analýza falzifikátov z materiálu Cernit

Cernit je polymérová hlina, ktorá je považovaná za jednu z najsilnejších. Po vytvarovaní do požadovaného tvaru materiál stvrdne upečením v rúre. Falzifikáty uložené v databáze boli vytvorené len zo surovej hmoty, bez pečenia v rúre. [56]

Na obrázku 5.4 sú znázornené približené výrezy falzifikátov odtlačkov prstov vyrobených z materiálu Cernit po snímaní mikroskopom. Na obrázkoch (a) a (b) sú prítomné praskliny, ktoré majú zúbkovitý tvar, vychádzajú z jedného bodu a pokračujú do viacerých smerov. Na obrázku (c) je prítomných niekoľko jednoduchších prasklín, ktoré neprebiehajú do viacerých smerov.





Obrázok 5.4: Výrezy z falzifikátov odtlačkov prstov vyrobených z materiálu Cernit po snímaní mikroskopom. Zobrazené sú približené časti falzifikátov obsahujúce praskliny zúbkovitého tvaru. Obrázky pochádzajú z databázy výskumnej skupiny STRaDe.



Obrázok 5.5: Obrázky falzifikátov odtlačkov prstov vyrobených z materiálu Cernit po snímaní skenerom. Obrázky pochádzajú z databázy výskumnej skupiny STRaDe.

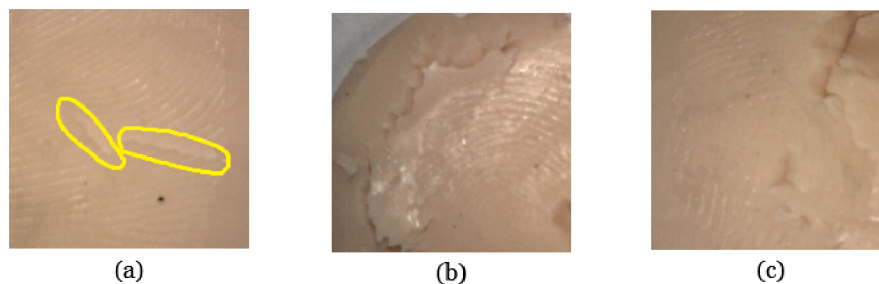
Na obrázku 5.5 sú znázornené falzifikáty odtlačkov prstov z obrázka 5.4 po snímaní skenerom odtlačkov prstov. Príslušné falzifikáty sú na oboch obrázkoch označené rovnakým písmenom. Na obrázkoch (a) je v rámci oboch obrázkov žltou farbou vyznačený výskyt príslušných prasklín pred a po snímaní skenerom. Analogicky sú praskliny pre porovnanie vyznačené aj na obrázkoch z iných materiálov, ktoré sú opísané v nasledujúcich podkapitolách. Praskliny v materiáli Cernit majú po snímaní skenerom zachovaný zúbkovitý tvar a priebeh ako na obrázkoch z mikroskopu. Falzifikát na obrázku (b) je nasnímaný spôsobom, kvôli ktorému nie je možné vidieť celú prasklinu.

#### 5.4.2 Analýza falzifikátov z materiálu Kato

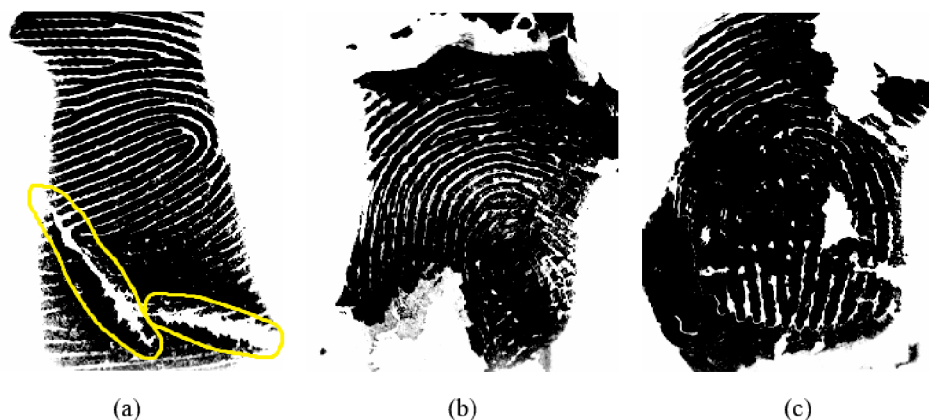
Kato je rovnako ako Cernit polymérová hlina, ktorá je považovaná za úplne najsilnejšiu. Kato tiež môže byť po vytvarovaní pre stvrdnutie upečený v rúre, ale pri výrobe falzifikátov, ktoré sú uložené v databáze, nebola táto fáza uskutočnená. [56]

Na obrázku 5.6 sú znázornené približené výrezy falzifikátov odtlačkov prstov vyrobené z materiálu Kato po snímaní mikroskopom. Na obrázkoch (b) a (c) sú prítomné rozsiahle praskliny, zasahujúce veľmi hlboko. Tieto praskliny majú podobný zúbkovitý tvar ako praskliny v materiáli Cernit, ale sú širšie, hlbšie, neprebiehajú do viacerých smerov, tvoria oblú-

kovitý tvar. Na obrázku (a) sú prítomné dve plytké praskliny iného typu, ktoré sú užšie a majú rovný tvar.



Obrázok 5.6: Výrezy z falzifikátov odtlačkov prstov vyrobené z materiálu Kato po snímaní mikroskopom. Vo falzifikátoch sú viditeľné viaceré druhy prasklín. Obrázky pochádzajú z databázy výskumnej skupiny STRaDe.

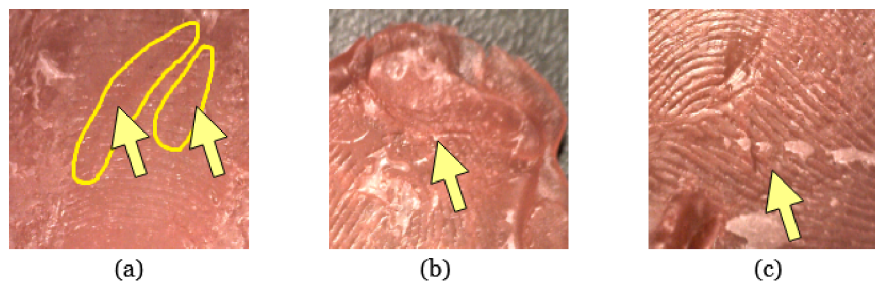


Obrázok 5.7: Obrázky falzifikátov odtlačkov prstov vyrobených z materiálu Kato po snímaní skenerom. Obrázky pochádzajú z databázy výskumnej skupiny STRaDe.

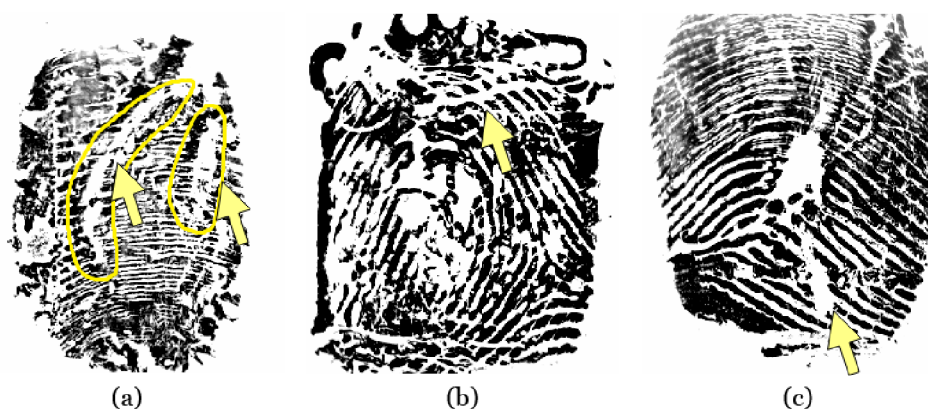
Na obrázku 5.7 sú znázornené falzifikáty odtlačkov prstov z obrázka 5.6 po snímaní skenerom odtlačkov prstov. Praskliny na obrázkoch (b) a (c) majú zachovaný tvar a priebeh ako na obrázkoch z mikroskopu, nie sú však zachytené celé. Na rozdiel od prasklín v materiáli Cernit, na ktoré sa čiastočne podobajú, je ich okraj, najmä na obrázku (b), oveľa súvislejší a menej poškodený. Dve samostatné praskliny na obrázku (a) po snímaní zdánlivo vytvorili jeden útvar v dôsledku ich tesnej blízkosti.

#### 5.4.3 Analýza falzifikátov z vosku

Na obrázku 5.8 sú znázornené približené výrezy z falzifikátov odtlačkov prstov vyrobených z vosku po snímaní mikroskopom. Falzifikáty z vosku obsahujú veľa poškodení, preto sú praskliny na každom obrázku vyznačené šípkami. Na obrázkoch (b) a (c) sú prítomné kratšie praskliny, ktoré nie sú príliš hlboké. Na obrázku (a) sa vyskytujú dve veľmi plytké praskliny, ktoré sú široké a dlhé, pomerne slabo viditeľné aj po zväčšení a úpravách obrázka z mikroskopu.



Obrázok 5.8: Výrezy falzifikátov odtlačkov prstov vyrobené z vosku po snímaní mikroskopom. Vo falzifikátoch sa vyskytuje veľké množstvo poškodení, uvažované praskliny sú vyznačené šípkami. Obrázky pochádzajú z databázy výskumnej skupiny STRaDe.



Obrázok 5.9: Obrázky falzifikátov odtlačkov prstov vyrobených z vosku po snímaní skenerom. V obrázkoch sa vyskytuje veľké množstvo poškodení, uvažované praskliny sú vyznačené šípkami. Obrázky pochádzajú z databázy výskumnej skupiny STRaDe.

Na obrázku 5.9 sú znázornené falzifikáty odtlačkov prstov z obrázka 5.8 po snímaní skenerom odtlačkov prstov. Praskliny na obrázkoch (b) a (c) sú pomerne úzke a ich okraje sú na rozdiel od predchádzajúcich uvedených prasklín neporušené. Praskliny na obrázku (a) sú po snímaní skenerom oveľa lepšie viditeľné, tvoria dlhé oblúkovité útvary s takmer neporušenými okrajmi.

#### 5.4.4 Zhrnutie typov prasklín vyskytujúcich sa v rôznych materiáloch a návrh algoritmu

Z analýzy typov prasklín v jednotlivých materiáloch vyplýva, že praskliny môžu mať zúbkovitý alebo rovný tvar. Celkový priebeh prasklín je buď oblúkovitý, rovný alebo z centrálného bodu prebiehajúci do viacerých smerov. Okraje prasklín môžu byť porušené v rôznej miere. Okrem uvedených vlastností sa praskliny líšia v šírke a dĺžke. Pri rozdielnej hĺbke prasklín nebol pri analýze zaznamenaný výrazný vplyv na vzhľad praskliny.

Algoritmus pre náhodné generovanie prasklín:

1. Náhodne zvol body určujúce koncové body praskliny, prípadne aj riadiaci bod, ktorý je potrebný pri výpočte tvaru paraboly pri oblúkovitej praskline.
2. Nastav typ praskliny a jej šírku podľa vstupu od užívateľa.
3. Podľa typu a šírky praskliny vygeneruj grafickú reprezentáciu praskliny:
  - (a) vygeneruj základnú krivku určujúcu tvar praskliny,
  - (b) vygeneruj zužujúce sa okraje praskliny,
  - (c) vygeneruj poškodenie okrajov praskliny.

V prípade zadávania riadiacich bodov praskliny užívateľom je odlišný len prvý krok algoritmu. V rámci jedného falzifikátu je možné postupne vygenerovať viac prasklín, ktoré sa môžu križovať, a tým napríklad simulovať prasklinu vychádzajúcu z centrálného bodu do viacerých smerov. Dôsledkom tohto riešenia je, že v rámci jedného falzifikátu je možné vygenerovať aj viac typov prasklín. V databáze falzifikátov, v ktorej bola robená analýza, sa väčšinou v jednom falzifikáte vyskytoval len jeden typ praskliny, s miernymi odlišnosťami v dĺžke, či šírke. Navrhnuté riešenie však poskytuje aj vygenerovanie rôznych typov prasklín do jedného odtlačku, nakoľko je na uvážení užívateľa, s akým úmyslom praskliny generuje.

## 5.5 Anotácie poškodení

Uvedené algoritmy sú kvôli prehľadnosti zamerané len na vytvorenie príslušných poškodení v obrázku odtlačku prsta. Okrem toho je nutné, aby po vygenerovaní poškodení bolo možné vytvoriť aj anotácie vhodným spôsobom opisujúce poškodenie.

Anotácie budú slúžiť k vytvoreniu tréningových množín pre neurónové siete prípadne pre overenie, že algoritmy správne detegujú poškodenia. Vytvorené budú prostredníctvom uloženia vstupu a simultánneho generovania poškodení do vstupného obrázka, ako aj do obrázka s čiernym pozadím. Anotáciou bude mapa toho, čo sa zmenilo.

Uvedený spôsob vytvárania anotácií je možné jednoducho skombinovať s algoritmom pre vytváranie oblastí s nižšou jasnosťou, aj s algoritmom pre vytváranie prasklín. Okrem toho je vhodný pre použitie aj pre generovanie artefaktov falzifikátov, ktoré sú v základnej aplikácii už implementované.

## Kapitola 6

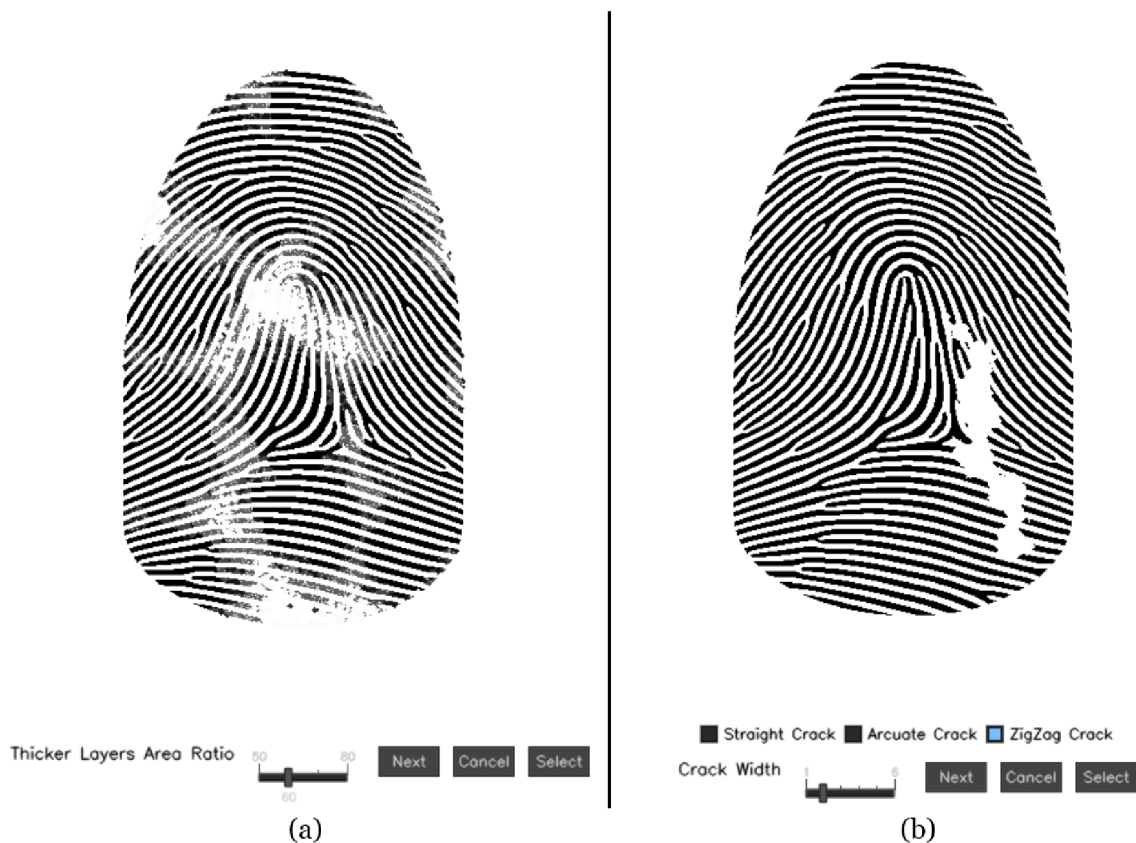
# Implementácia

V tejto kapitole je opísaná implementácia metód navrhnutých v kapitole 5. V jednotlivých podkapitolách sú opísané celkové úpravy aplikácie, v rámci ktorých bola vytvorená aj trieda `FingerprintMask` a priblížené fungovanie tried pre generovanie dvoch hlavných doplnených vybraných prejavov falzifikátov `LowerClarity` a `Defect`. Nakoľko sa jedná o rozšírenie existujúcej aplikácie, výber programovacieho jazyka bol ovplyvnený jazykom pôvodnej aplikácie, ktorým je C++ s využitím knižnice `OpenCV`. Uvedené triedy boli implementované tak, aby korešpondovali s architektúrou danej aplikácie.

### 6.1 Celkové úpravy aplikácie

V rámci rozšírenia aplikácie bolo nutné okrem implementácie dvoch vybraných poškodení aj celkovo upraviť aplikáciu. Ako bolo opísané v kapitole 5.1, generovanie rôznych prejavov bolo v pôvodnej aplikácii ovládané prepínaním módov pomocou klávesnice. Vlastnosti prejavov falzifikátov, ako napríklad šírka a intenzita miznúcich papilárnych línií, boli zadávané taktiež pomocou klávesnice, umiestnenie a rozmery vzduchových bublín boli zadávané pomocou myši. V rozšírenom riešení bolo implementované jednoduché grafické užívateľské rozhranie, pomocou voľne dostupnej knižnice `cvui` [57], ktorá vznikla práve z dôvodu jednoduchšieho zadávania parametrov pri práci s obrázkami prostredníctvom knižnice `OpenCV`.

Prepínanie módov generovania prejavov ostalo realizované pomocou klávesnice, avšak módy boli zjednodušené a ich prepínanie zjednotené. Po prepnutí do módu sa užívateľovi zobrazia grafické prvky umožňujúce jednoduchšie nastavenie parametrov generovaného prejavu. Grafické elementy sa pre každý generovaný prejav líšia a sú prispôsobené pre jeho potreby. Okrem nastavenia parametrov generovania je pomocou grafických prvkov možné vyskúšať vygenerovať každý prejav viackrát, alebo jeho generovanie úplne zrušiť. Po vybratí vyhovujúcej reprezentácie je nutné vygenerovaný prejav trvalo uložiť, po čom už nemôže byť z odtlačku odstránený, ale zmeny ostanú zachované pri generovaní ďalších prejavov. Grafické elementy vykreslené pri náhodnom generovaní oblastí s nižšou jasnosťou a praskliny sú pre ilustráciu zobrazené na obrázku 6.1. Boli pridané pre nastavenie generovania všetkých prejavov falzifikátov, aj tých implementovaných v pôvodnej aplikácii. Okrem zmien pri zadávaní parametrov generovaných prejavov ostalo ponechané zadávanie vzduchových bublín pomocou myši a rovnaký spôsob bol použitý aj pri zadávaní oblastí s nižšou jasnosťou a riadiacich bodov praskliny.



Obrázok 6.1: Prvky jednoduchého grafického užívateľského rozhrania pri náhodnom generovaní oblastí s nižšou jasnosťou (a) a náhodnom generovaní praskliny (b).

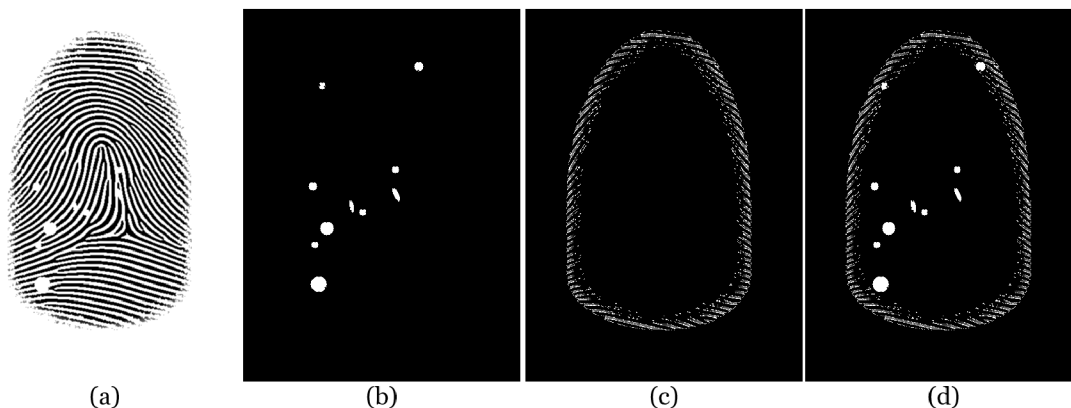
V rozšírenej aplikácii existuje 5 základných módov generovania, medzi ktorými sa prepína pomocou klávesnice:

- A – *Area*, neprirodzený celkový tvar,
- B – *Bubbles*, vzduchové bubliny,
- C – *Clarity*, oblasti s nižšou jasnosťou,
- D – *Defect*, defekt v materiáli, konkrétne prasklina,
- E – *Edges*, postupne miznúce okraje.

Po zvolení generovaného prejavu aplikácia očakáva prechod do módu náhodného generovania alebo generovania ovplyvneného užívateľom. Pre toto zjednotenie prechádzania medzi módmí generovania boli postupne miznúce papilárne línie, implementované v pôvodnej aplikácii, doplnené o možnosť náhodného generovania, kedy je šírka oblasti a intenzita miznutia vygenerovaná náhodne.

Zmenený bol aj spôsob poškodzovania dokonalého odtlačku vygenerovaním poškodenia papilárnych línií. V pôvodnom riešení bolo toto poškodenie generované vždy, v rozšírenej verzii je generované len po spustení s parametrom *-d*. S použitím parametra *-a* sa spolu s prejavmi falzifikátov vygenerujú aj anotácie vykonaných poškodení. Pre každý uložený

prejav falzifikátov je vytvorená osobitná anotácia a uložená je do rovnakého priečinka, kam má byť uložený výstupný obrázok z aplikácie. Vytvorená je navyše aj anotácia obsahujúca všetky uložené poškodenia v jednom obrázku. V prípade, že bolo použitím parametra `-d` vygenerované poškodenie dokonalej reprezentácie papilárnych línií, je aj toto zahrnuté v anotáciách. Na obrázku 6.2 sú znázornené anotácie vygenerovaných vzduchových bublín (b), postupne miznúcich okrajov papilárnych línií (c) a celková anotácia všetkých vygenerovaných poškodení (d) pri vytváraní výstupného obrázka falzifikátu (a).



Obrázok 6.2: Anotácie vygenerovaných poškodení: (a) – výstupný obrázok falzifikátu, (b) – anotácia vzduchových bublín, (c) – anotácia postupne miznúcich okrajov papilárnych línií, (d) – celková anotácia s oboma vygenerovanými prejavmi.

## 6.2 Trieda `FingerprintMask`

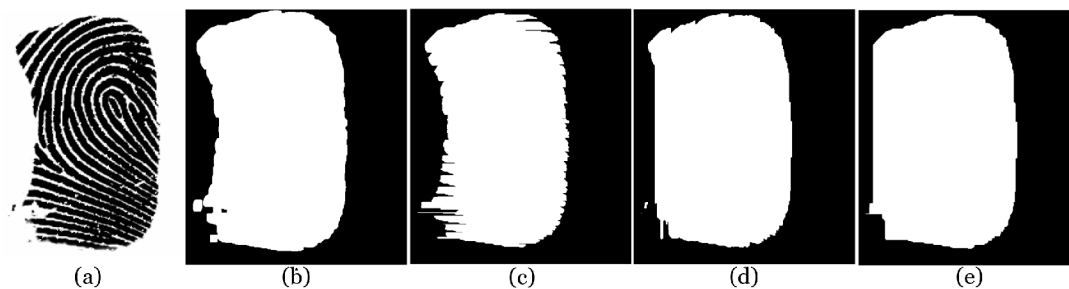
V rozšírenej aplikácii okrem piatich základných módov, uvedených v predchádzajúcej kapitole, existuje ešte šiesty mód, `M – Mask`, ktorý umožňuje zo zadaného vstupného obrázka falzifikátu vygenerovať masku jeho neprirodzeného tvaru a funguje inak ako ostatné módy. Vzniknutá maska neprirodzeného tvaru je po vytvorení zaradená medzi ostatné masky na orezanie odtlačku pri generovaní neprirodzeného celkového tvaru. Jedná sa o rozšírenie prejavu neprirodzený celkový tvar, ktoré vyžadovalo zásadnú zmenu v implementácii, a síce, že počet masiek pre orezanie pred ich načítaním musí byť zistený dynamicky počas behu aplikácie. Toto riešenie implementujú metódy `fileExistenceCheck` a `findMaskCount` triedy `FingerprintShape`.

Samotné vytvorenie masky falzifikátu implementujú metódy triedy `FingerprintMask`. Maska je vytvorená jedným z dvoch hlavných princípov, buď vyplňaním pixelov v maske papilárnych línií, alebo rozmazaním masky papilárnych línií. Vyplňanie je realizované metódou `rowColumnFilling`, ktorá v závislosti na nastavení premennej triedy vykoná riadkové vyplňanie, stĺpcové vyplňanie, alebo kombinované vyplňanie. V aplikácii je pri generovaní masky možné prezrieť si všetky možnosti a zvoliť tú, ktorá najlepšie vyhovuje tvaru daného falzifikátu, nakoľko falzifikáty majú často konkávny tvar, ktorý môže byť s použitím niektorého konkrétneho spôsobu vyplňania úplne znehodnotený.

Rovnako je možné vybrať aj masku, ktorá vznikla použitím jednoduchšej metódy `blurredMethod`, v ktorej je maska papilárnych línií dostatočne rozmazaná oknom veľkosti  $15 \times 15$  a následne je použité prahovanie s prahovou hodnotou intenzity sivej 10, čiže všetky svet-

lejšie pixely sú zmenené na biele a všetky tmavšie na čierne. Po zvolení finálnej podoby masky je maska zväčšená na rozmer  $416 \times 560$ , aby bola kompatibilná s maskami vytvorenými pre pôvodnú aplikáciu, uložená je do priečinka s maskami s názvom reprezentujúcim číselné označenie masky, teda `maskCount + 1`, kde `maskCount` je aktuálny počet masiek pripravených na orezanie. Rovnako je pre kompatibilitu s ostatnými generovanými prejavmi obrázok uložený aj do priečinka, kam má byť uložený výstup z aplikácie. Po vytvorení a uložení masky už nie je možné generovať do vstupného obrázka ďalšie prejavy falzifikátov, čím sa mód M odlišuje od ostatných módov aplikácie, ktoré môžu byť počas behu programu navzájom rôzne kombinované.

Na obrázku 6.3 je zobrazený falzifikát s konkávnym tvarom, z ktorého má byť vytvorená maska (a), maska vytvorená rozmazaním (b), maska vytvorená riadkovým vyplňaním (c), stĺpcovým vyplňaním (d) a kombinovaným riadkovým aj stĺpcovým vyplňaním (e). Je možné vidieť, že pre tento konkrétny tvar falzifikátu je pre vytvorenie masky najlepšie zvoliť rozmazanie alebo riadkové vyplňanie, pričom pri oboch by bolo nutné vykonať dodatočné úpravy. Stĺpcové a kombinované vyplňanie úplne znehodnocujú tvar falzifikátu, čo bola motivácia pre vytvorenie viacerých spôsobov získania masky, aby bolo možné pre každý konkrétny prípad posúdiť viac možností a vybrať najlepšie vyhovujúcu.



Obrázok 6.3: Vytvorenie masky neprirodzeného celkového tvaru falzifikátu: (a) – vstupný obrázok falzifikátu, (b) – maska vytvorená rozmazaním, (c) – maska vytvorená riadkovým vyplňaním, (d) – maska vytvorená stĺpcovým vyplňaním, (e) – maska vytvorená kombinovaným riadkovým aj stĺpcovým vyplňaním.

### 6.3 Trieda LowerClarity

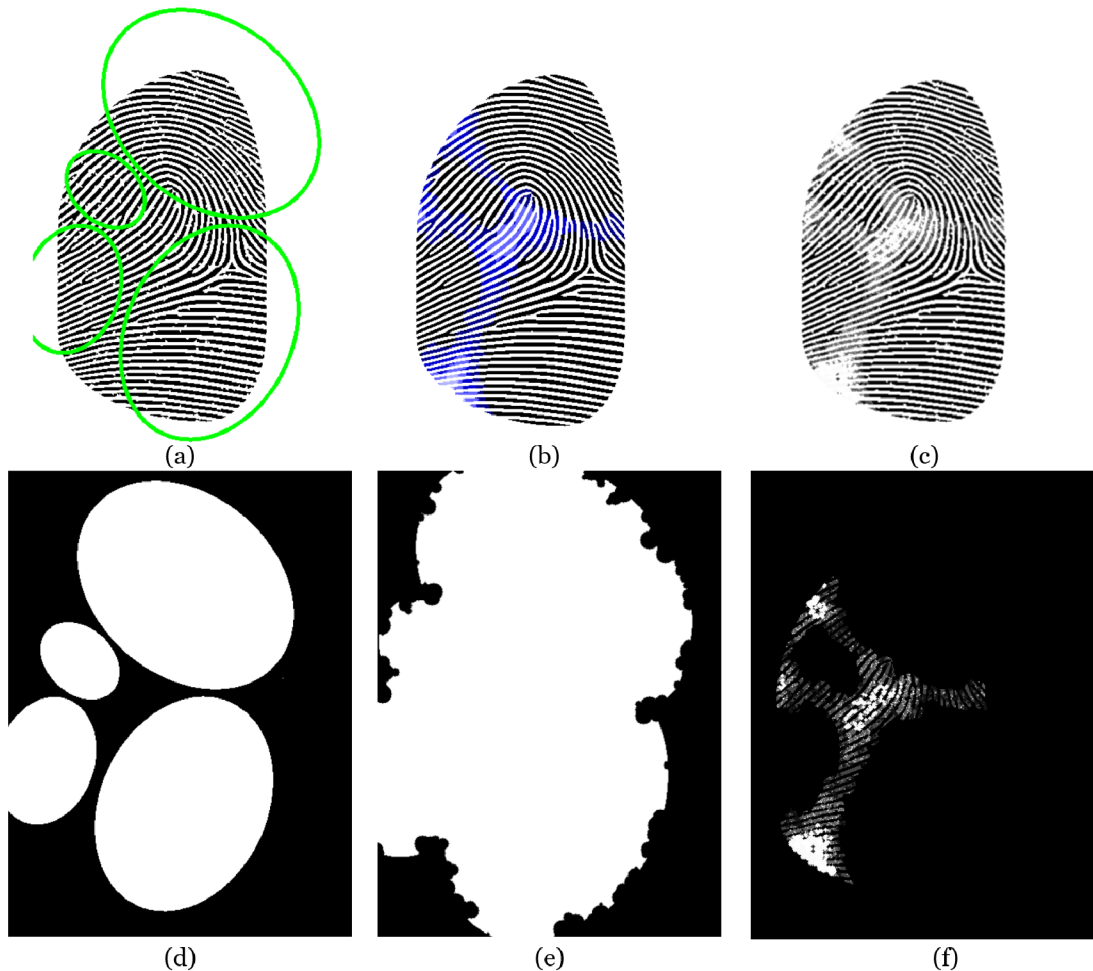
Trieda `LowerClarity` obsahuje metódy pre generovanie grafickej reprezentácie oblastí papírnych línií s nižšou jasnosťou do obrázka syntetického odtlačku prsta. Implementovaný je mód náhodného generovania priehľadných oblastí, aj generovania na základe užívateľského vstupu zadaného pomocou myši tým, že do syntetického odtlačku prsta sú vykreslené elipsy reprezentujúce nepriehľadné časti falzifikátu. Elipsy sa môžu prekrývať a ich časť môže ležať mimo oblasti odtlačku prsta.

Zadanie vstupných údajov sprostredkuje metóda `enterThickerLayers`, ktorá je volaná po zvolení módu pre generovanie oblastí s nižšou jasnosťou. Jadrom metódy je výpočet veľkostí osí elipsy a uhla jej otočenia v závislosti na pohybe myšou po zadaní stredu elipsy. Stred elipsy je určený ľavým klikom myši, následným pohybom do strán je určená dlhšia os elipsy a uhol jej otočenia. Na základe dlhšej osi je vypočítaná kratšia os ako  $\frac{3}{4}$  jej dĺžky. Po



odkliknutí ľavého tlačidla myši je základná reprezentácia elipsy predstavujúcej nepriehladnú oblasť uložená do vektora `thickerLayersBase`.

Metóda `createThickerLayersMask` pracuje s vektorom `thickerLayersBase` a podľa uložených reprezentácií elíps vytvára čierno-bielu masku daných oblastí, pričom biela farba reprezentuje hrubšie, nepriehladné oblasti, čierna farba tenšie, priehladné oblasti, v ktorých má byť vygenerované poškodenie.



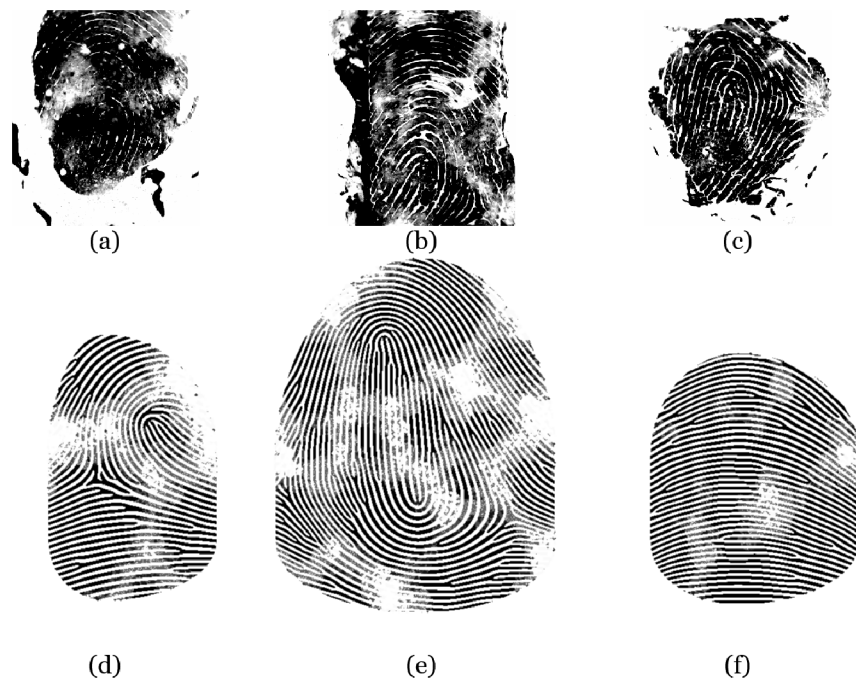
Obrázok 6.4: Proces generovania oblastí s nižšou jasnosťou zadaných užívateľom: (a) – elipsy zadané užívateľom, (b) – oblasti s odlišným stupňom generovaného poškodenia odlišené odtieňmi modrej farby, (c) – výsledný obrázok, (d) – maska oblastí s hrubšou vrstvou materiálu na začiatku generovania poškodenia, (e) – viacnásobne rozšírená maska oblastí s hrubšími vrstvami materiálu s poškodenými okrajmi na konci generovania poškodenia, (f) – anotácia vygenerovaného poškodenia.

Následne je volaná metóda `generateLowerClarity`, ktorá generuje grafickú reprezentáciu nižšej jasnosti. Poškodenie je generované podľa postupu opísanom v kapitole 5.3.2. Opakované vygenerovanie tmavého alebo svetlého šumu v podobe náhodne umiestnených malých kruhov umožňuje metóda `generateNoise`. Jej parametre určujú požadovaný odtieň šumu, polomer generovaných útvarov a pravdepodobnosť, s ktorou sú vygenerované

pri priechode pixelmi určenými prienikom masky oblasti odtlačku prsta, papilárnych línií a stupňa oblasti s nižšou jasnosťou, pre ktorú je práve generované poškodenie. Podobne pracuje metóda `lowerIntensity`, ktorá zosvetľuje odtieň na požadovanú hodnotu a generuje náhodné biele pixely pre simuláciu grafického vzhľadu obrázka s daným prejavom falzifikátov po snímaní skenerom.

Zároveň je periodicky volaná metóda `recomputeThickerAreas`, ktorá pripočíta k polomeru jednotlivých elíps uložených vo vektore `thickerLayersBase` hodnotu zadanú parametrom, čím sa hrubšie oblasti rozšíria a je umožnené v rôznych vzdialenostiach od okraja tenších oblastí po ich stred generovať rôzny druh poškodenia. Táto metóda zároveň obsahuje volanie `createThickerLayersMask`, čím je po prepočte polomerov vytvorená nová maska. Okrem toho je po každom prepočte a v úvode generovania poškodenia volaná metóda `damageEllipse`, v rámci ktorej sú po kontúrach masky vygenerované kruhové útvary s polomerom v rozsahu [1; 10] pre porušenie okraja elíps a dosiahnutie realistickejšieho vzhľadu falzifikátu s nedokonalými hranicami oblastí s hrubšou vrstvou materiálu.

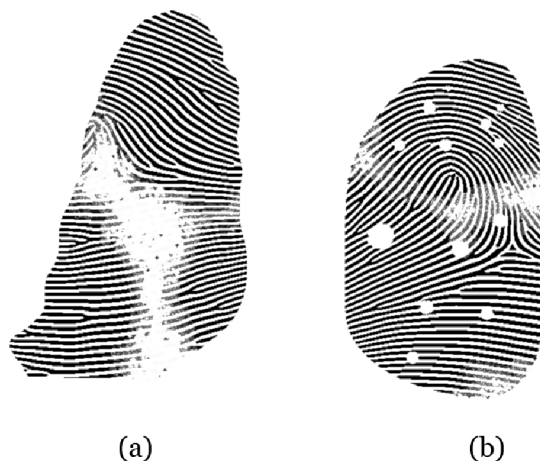
Na obrázku 6.4 je znázornený proces generovania oblastí s nižšou jasnosťou zadaných užívateľom, ktorý začína zadaním umiestnenia hrubších oblastí materiálu prostredníctvom elíps (a). Následne je vygenerovaná maska týchto oblastí (d), ktorá je počas výpočtu rozširovaná a zakaždým sú poškodené okraje elíps pre dosiahnutie realistickejšieho vzhľadu, výsledná maska po skončení výpočtu je znázornená na obrázku (c). Na obrázku (b) sú odtieňmi modrej odlišené oblasti s rôznym stupňom generovaného poškodenia vzniknuté postupným rozširovaním masky a korešpondujúce s finálnym vygenerovaným poškodením, ktoré je znázornené na obrázku (c). Pre lepšiu predstavu je na obrázku (f) zobrazená anotácia poškodenia.



Obrázok 6.5: Skutočné falzifikáty snímané skenerom odtlačkov prstov – (a) – (c). Obrázky pochádzajú z databázy výskumnej skupiny STRaDe. Syntetické odtlačky prstov s vygenerovanými oblasťami s nižšou jasnosťou – (d) – (f).

Na obrázku 6.5 sú uvedené výsledky implementácie v porovnaní s obrázkami skutočných falzifikátov. Skutočné falzifikáty sú uvedené na obrázkoch (a), (b), (c), na obrázkoch (d), (e), (f) sú uvedené syntetické obrázky odtlačkov prstov s vygenerovanými oblasťami papilárnych línií s nižšou jasnosťou.

Na obrázku 6.6 sú uvedené ukážky kombinácií implementovaného prejavu s prejavmi už implementovanými v pôvodnej aplikácii pre generovanie prejavov falzifikátov. Na obrázku (a) je uvedená kombinácia oblastí s nižšou jasnosťou papilárnych línií a neprirodzeného tvaru falzifikátu, na obrázku (b) je kombinácia so vzduchovými bublinami.



Obrázok 6.6: Kombinácia oblastí s nižšou jasnosťou s ďalšími prejavmi falzifikátov: (a) s neprirodzeným celkovým tvarom odtlačku prsta, (b) so vzduchovými bublinami. Oba obrázky obsahujú aj ďalší znak falzifikátov, a to náhle ukončenie papilárnych línií.

### 6.3.1 Náhodné generovanie

Trieda `LowerClarity` implementuje aj náhodné generovanie oblastí s nižšou jasnosťou. Pri náhodnom generovaní tohto prejavu bolo potrebné vyriešiť otázku počtu generovaných elíps. V aplikácii bolo zvolené riešenie, že užívateľ zadá pomer medzi plochou pokrytou nepriehľadnými oblasťami s hrubšou vrstvou materiálu a celkovou plochou odtlačku prsta. Na výber sú štyri možnosti, 50 %, 60 %, 70 % a 80 %, ktoré vyzerajú vizuálne akceptovateľne a porovnateľne s obrázkami vyskytujúcimi sa v databáze falzifikátov. Počet generovaných elíps teda nie je dopredu náhodne vygenerovaný, elipsy sú generované postupne jedna po druhej a generovanie končí, keď sa dosiahne požadovaný pomer. Na obrázku 6.7 je znázornené porovnanie vygenerovaných oblastí s nižšou jasnosťou papilárnych línií pri zvolení každého z možných pomerov medzi oblasťami.

Ďalšie otázky pri náhodnom generovaní súviseli s voľbou stredov elíps. Bolo rozhodnuté, že dôjde k diskretizácii a po inicializácii triedy sa vypočítajú vhodné kandidáti na stredy elíps tak, že ich budú tvoriť body tvoriace mriežku s rozstupom 10 pixelov. V súvislosti s kandidátnymi bodmi na stredy elíps sa vyskytli dva problémy:

1. či majú byť stredy elíps generované aj mimo plochy odtlačku, alebo len v rámci neho,
2. či majú byť stredy elíps generované aj v bodoch ležiacich pod už vygenerovanými elipsami.



Obrázok 6.7: Náhodné generovanie oblastí s nižšou jasnosťou s rôzne zvoleným pomerom medzi plochou oblastí s hrubšou vrstvou materiálu a celkovou plochou odtlačku prsta.

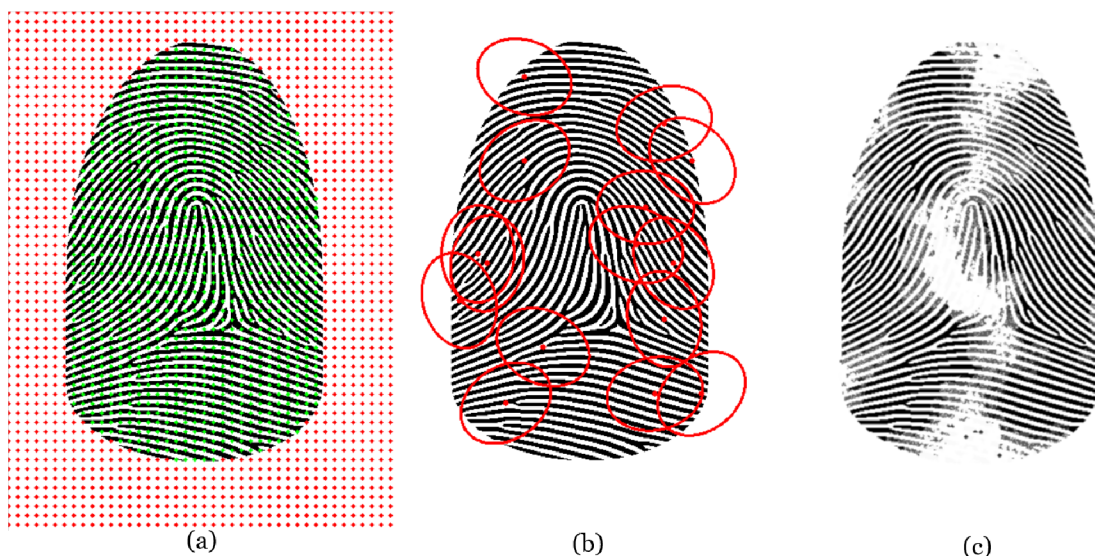
Druhý problém súvisel s tým, že pri úplne náhodnom generovaní vzniká veľa elíps, ktoré sa takmer celkom prekrývajú a sú veľmi podobné. Riešením tohto problému je po každej vygenerovanej elipse vylúčiť kandidátne body, ktoré daná elipsa prekrýva.

Vyskúšané boli všetky štyri kombinácie riešenia prvého aj druhého problému a všetky produkovali vizuálne nerozlíšiteľné obrázky. Výsledná kombinácia bola preto určená na základe výsledkov testovania rýchlosti generovania pre všetky kombinácie riešenia. Testovanie zahŕňalo 40 spustení generovania pre každú kombináciu možných riešení uvedených problémov, čo predstavovalo 10 spustení pre každý zvolený pomer medzi oblasťami. Ako reprezentujúci čas behu generovania bol vždy vybraný maximálny čas dosiahnutý v každej kategórii a tie boli na záver medzi sebou porovnávané.

Počas testovania bolo zistené, že je rýchlejšie prepočítať kandidátne body po vygenerovaní každej elipsy a vylúčiť z nich body prekryté už vygenerovanými elipsami, ako generovať podobné elipsy, ktoré plochu hrubších oblastí zvyšujú len minimálne. Rovnako bolo rýchlejšim riešením zvoliť kandidátne body len v rámci plochy odtlačku. Najmä v obrázkoch, v ktorých je plocha odtlačku malá, bolo generovaných príliš veľa elíps úplne mimo plochy odtlačku, čo spomaľovalo výpočet. V aplikácii ostali ponechané konštanty triedy *LowerClarity* určujúce spôsob výberu stredov elíps, a je preto v prípade potreby možné zmeniť hodnotu týchto konštánt, a tým aj spôsob generovania.

Poslednou otázkou, už nesúvisiacou so stredmi elíps, bol spôsob generovania ich polomeru. Zvolená bola možnosť, že polomer sa vypočíta ako  $\frac{1}{8}$  zo šírky vstupného obrázka, nie plochy odtlačku, pretože jej šírka sa najmä po vygenerovaní neprirodeného celkového tvaru nedá aproximovať vierohodným spôsobom.

Na obrázku 6.8 (a) sú vizuálne znázornené kandidátne body na stredy elíps tvoriace mriežku s rozstupmi 10 pixelov, červenou farbou sú zvýraznené body mimo plochy odtlačku prsta, ktoré do výsledných kandidátov zahrnuté nie sú, zelenou farbou sú zvýraznené body, ktoré do kandidátnych bodov zahrnuté sú. Obrázok reflektuje stav pred vygenerovaním prvej elipsy. Na obrázku 6.8 (b) sú znázornené vygenerované elipsy aj s ich stredmi a polermi. Je možné vidieť, že žiadne dve elipsy sa úplne neprekrývajú, čo je zapríčinené zvolením riešenia druhého vyššie uvedeného problému. Na obrázku 6.8 (c) je výsledný vzniknutý obrázok s poškodením vytvoreným mimo oblastí vygenerovaných elíps.



Obrázok 6.8: Proces náhodného generovania oblastí s nižšou jasnosťou: (a) – diskretizácia pre výber kandidátnych bodov na stredy elíps, zelenou farbou sú znázornené body vo vnútri odtlačku, z ktorých budú náhodne vybrané stredy elíps, červenou sú znázornené body odtlačku patriace do mriežky, ale ležiace mimo plochy odtlačku, ktoré nebudú patriť medzi výsledné kandidátne body, (b) – náhodne vygenerované elipsy s ich stredmi, (c) – výsledné vygenerované poškodenie.

## 6.4 Trieda Defect

Trieda `Defect` obsahuje metódy pre generovanie rôznych typov prasklín do syntetického odtlačku prsta. Na základe výsledkov analýzy, ktorá je opísaná v kapitole 5.4, boli implementované tri rôzne typy praskliny, ktoré sú bližšie opísané v nasledujúcich podkapitolách. V závere podkapitoly sú podrobnejšie opísané niektoré skutočnosti zo spôsobu implementácie náhodného generovania praskliny.

### 6.4.1 Rovná prasklina

Prvým typom generovanej praskliny je rovná prasklina. V obrázkoch falzifikátov síce prasklina nemá úplne rovný priebeh, obsahuje rôzne výbežky a nerovnomernú šírku, ale spomedzi všetkých ostatných prasklín najviac pripomína rovnú čiaru, preto je v práci označovaná ako rovná prasklina, prípadne *straight crack*.

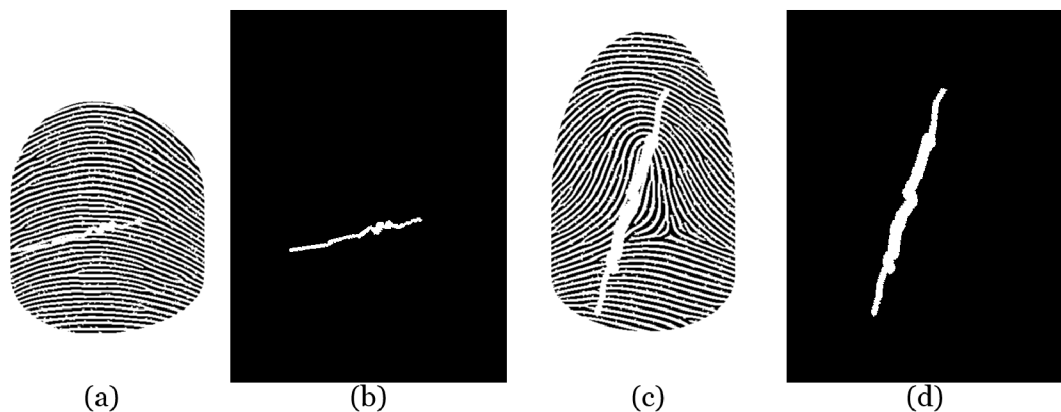
Pri generovaní tohto typu praskliny je nutné vypočítať body ležiace na úsečke medzi jej koncovými bodmi, ktorými je určená. V triede `Defect` je implementovaná dátová štruktúra `Line`, ktorá na základe dvoch zadaných koncových bodov praskliny vypočíta a uloží parametre priamky nimi určenej. Podľa všeobecne známej rovnice priamky z analytickej geometrie  $y = ax + b$  sú zistené parametre  $a, b$ , dĺžka úsečky, dimenzia, v ktorej úsečka rastie pomalšie ( $x$  alebo  $y$ ), a či bol užívateľom zadaný ako prvý bod, ktorý má v tejto dimenzii nižšiu, alebo vyššiu súradnicu. Tieto informácie sú potrebné najmä pre určenie všetkých bodov ležiacich na danej úsečke, kedy sa postupuje v smere pomalšieho rastu, aby bolo zachytených čo najviac bodov ležiacich na priamke, ale napríklad aj počas vykreslenia zužujúcich sa okrajov, kedy je nutné poznať, ktorý koncový bod bol užívateľom zadaný ako

prvý, resp. ktorý koncový bod bol vygenerovaný a uložený do vektora `controlPoints` ako prvý.

Na základe známych parametrov priamky (v aplikácii pri zadaní koncových bodov úsečky) sú v metóde `computePointsOnLine` vypočítané body ležiace na úsečke, s ktorými sa ďalej pracuje. Celkové generovanie rovnej praskliny obsluhuje metóda `renderStraightCrack`, ktorá podľa dĺžky úsečky určí počet bodov, ktoré budú posunuté o náhodný počet pixelov v oboch smeroch. Počet týchto bodov je určený vzťahom  $\text{lineLength} / 15$ , kde `lineLength` je dĺžka úsečky, a každý z týchto bodov je posunutý o náhodný počet pixelov z rozsahu  $[-5; 5]$  pixelov v smere  $x$  a o iný náhodný počet pixelov z uvedeného intervalu v smere  $y$ . Posunuté body sú uložené do vektora `adjustedPoints`. Do obrázka s čiernym pozadím je bielou farbou prostredníctvom metódy `polyLines` z knižnice `OpenCV` vykreslená čiara prechádzajúca danými bodmi, so šírkou zadanou užívateľom.

Následne je náhodne určený počet sekcií, 1 alebo 2, ktoré sú v praskline vykreslené s dvojnásobnou šírkou. Podľa počtu sekcií sa z posunutých bodov `adjustedPoints` náhodne vyberú 2 alebo štyri body, ktoré určujú začiatok a koniec hrubších sekcií. Ak vygenerované body nie sú rovnaké, časť praskliny medzi nimi sa vykreslí s dvojnásobnou šírkou vzhľadom ku šírke zadanej užívateľom. Uvedenými úpravami sa dosiahne realistickejší priebeh praskliny, ktorý v skutočných falzifikátoch po snímaní skenerom nie je úplne rovný, ako aj nerovnosť v šírke, ktorá sa v daných prasklinách tiež vyskytuje.

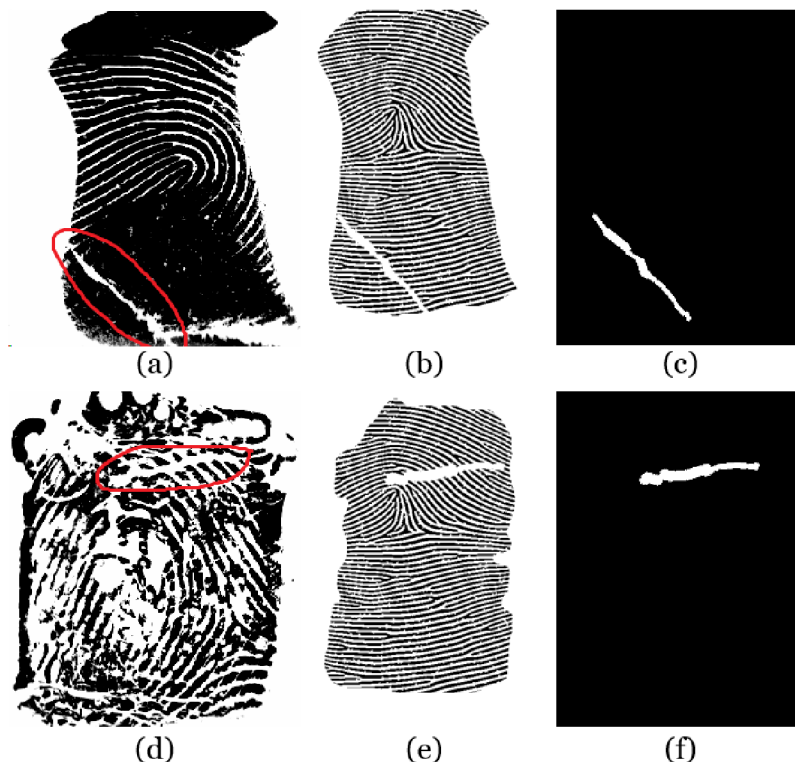
Po vygenerovaní finálneho priebehu a šírky praskliny sú jej okraje poškodené metódou `damageCrackEdgesWithCircles`, ktorá dostane na vstupe čierno-biely obrázok vygenerovanej praskliny, nájde jej kontúry a s určitou pravdepodobnosťou pri prechádzaní bodov kontúr vygeneruje malý čierny kruh s polomerom 2, čo zapríčiní mierne poškodenie okrajov praskliny. Následne je ešte prasklina vyhladená oknom s veľkosťou  $2 \times 2$ , čo umožňuje metóda `blur` knižnice `OpenCV` a pixely, ktoré nie sú vo výslednej reprezentácii praskliny čierne, sú skopírované do syntetického odtlačku prsta. Výsledné rovné praskliny s rôznou šírkou vygenerované do syntetických odtlačkov prstov sú znázornené na obrázku 6.9 (a) a (c), ich anotácie sú pre lepšiu viditeľnosť prasklín zobrazené na obrázku 6.9 (b) a (d).



Obrázok 6.9: Generovanie rovnej praskliny: (a), (c) – rovné praskliny s rôznou šírkou vygenerované do syntetických odtlačkov prstov, (b), (d) – anotácie vytvorených prasklín.

Na obrázku 6.10 sú znázornené obrázky z databázy falzifikátov obsahujúce rovnú prasklinu. Jedná sa o falzifikáty z materiálu Kato (a) a vosk (d) a sú zobrazené v porovnaní s obrázkami syntetických odtlačkov prstov vygenerovanými v aplikácii, (b) a (e). Pre lepšiu

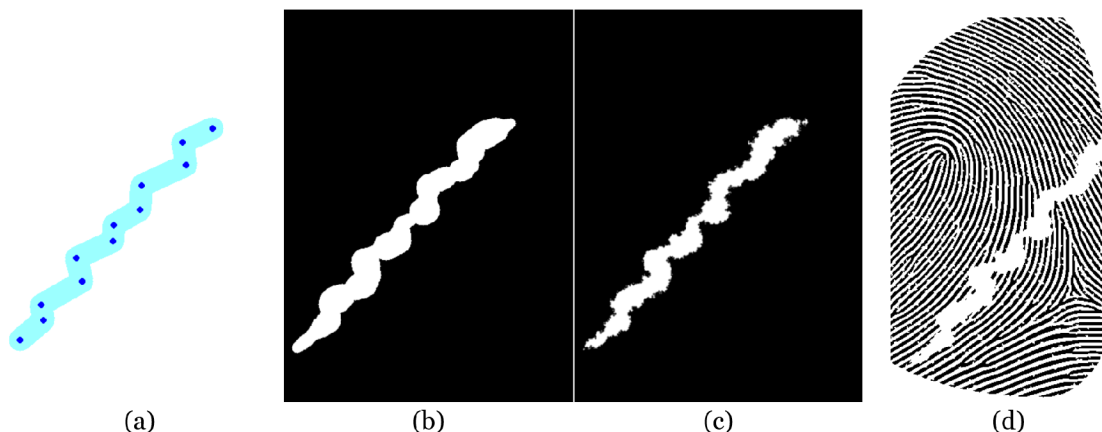
názornosť sú zobrazené aj anotácie vygenerovaných prasklín na čiernom pozadí, (c) a (f). Praskliny boli vytvorené v móde generovania podmieneného užívateľom. Syntetické odtlačky boli úmyselne aj orezané do neprirodzeného celkového tvaru. V prípade syntetického odtlačku na obrázku (b) bola použitá maska konkrétne vytvorená z falzifikátu z obrázka (a).



Obrázok 6.10: Obrázky falzifikátov obsahujúce rovné praskliny, (a) a (d), v ktorých sú uvažované praskliny vyznačené červenou farbou. Na obrázkoch (b) a (e) sú pre porovnanie rovné praskliny vygenerované do syntetických odtlačkov prstov, v ktorých bol navyše vygenerovaný aj ďalší prejav falzifikátov, neprirodzený celkový tvar. Na obrázku sú znázornené aj anotácie vygenerovaných prasklín (c) a (f).

#### 6.4.2 Zúbkovitá prasklina

Druhým typom generovanej praskliny je zúbkovitá prasklina, ktorá je v práci nazývaná aj *zigzag crack*. Zúbkovitý tvar je dosiahnutý tým, že prasklina je rozdelená do viacerých segmentov. Počet segmentov je určený náhodne z intervalu  $[\text{lineLength}/60; \text{lineLength}/30]$ . Opäť sú vypočítané body ležiace na úsečke medzi počiatočným a koncovým bodom praskliny a podľa počtu segmentov sú určité body z nich vybrané ako riadiace body segmentov tak, aby mal každý segment približne rovnakú dĺžku. Riadiace body segmentov sú následne posunuté v smere  $x$  aj  $y$  tak, aby bola porušená táto pravidelnosť. Posunutie je opäť určené náhodne, pričom intervaly minimálneho a maximálneho posunutia sú určené rôzne, v závislosti od šírky praskliny. Čím širšia prasklina, tým väčšie možné posunutie a naopak. Prasklina rozdelená do segmentov spolu s naznačenými riadiacimi bodmi segmentov je znázornená na obrázku 6.11 (a).



Obrázok 6.11: Generovanie zúbkovitej praskliny: (a) – prasklina rozdelená do viacerých segmentov, s posunutými riadiacimi bodmi segmentov, (b) – prasklina vygenerovaná na čiernom pozadí s variabilnou šírkou a zužujúcimi sa koncami, (c) – prasklina s poškodenými okrajmi, (d) – finálny vzhľad praskliny vygenerovanej do syntetického odtlačku prsta.

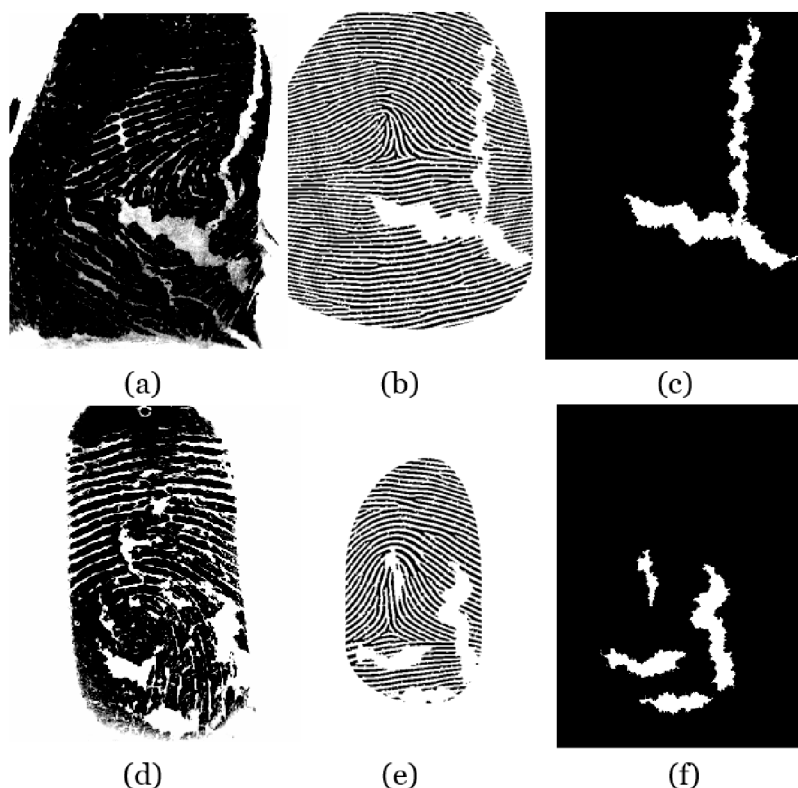
Po vygenerovaní riadiacich bodov segmentov je každý segment vykresľovaný ako niekoľko úsečiek vzniknutých medzi každou dvojicou jeho vypočítaných bodov, vždy s inou šírkou, ktorá je náhodne vybraná z intervalu určeného šírkou praskliny zadanou užívateľom. Týmto je dosiahnutý efekt častého zužovania a rozširovania praskliny pozorovaný na obrázkoch zúbkovitej praskliny z databázy falzifikátov. Následne je volaná metóda `extendEdge`, ktorá má na vstupe koncový segment praskliny, dve dĺžky, o ktoré má byť segment postupne predĺžený a dve znižujúce sa šírky, s ktorými majú byť vykreslené predĺžené časti. Metóda je volaná pre oba konce praskliny a vygeneruje efekt zúženia praskliny na jej koncoch. Šírky predĺžených častí sú určené ako  $0,5 \cdot crackWidth$  a  $0,4 \cdot crackWidth$ , kde `crackWidth` je základná šírka praskliny zadaná užívateľom. Na obrázku 6.11 (b) sú zobrazené vykreslené segmenty praskliny s variabilnou šírkou a zúženými okrajmi.

Postupné generovanie praskliny s rôznou šírkou zapríčiňuje, že prasklina sa nepravidelne zužuje a rozširuje, avšak jej okraje sú v dôsledku toho oblé a nevyzerajú realisticky v porovnaní s obrázkami prasklín z databázy falzifikátov. Na záver je vygenerované rozsiahlejšie poškodenie okrajov praskliny, niekoľkokrát je volaná metóda `damageCrackEdgesWithSquares`, ktorá vytvorí seriózne poškodenie okrajov pravdepodobnostným vygenerovaním malých štvorcíkov po kontúrach praskliny. Následne je tento efekt zjemnený volaním metódy `damageCrackEdgesWithCircles`, ktorá vygeneruje po novovzniknutých kontúrach malé kruhy, čím čiastočne zjemní efekt poškodenia okrajov a dosiahne realistickejší vzhľad. Počet volaní daných metód je ovplyvnený šírkou praskliny, pri väčšej šírke sú volané viackrát. Následne je prasklina ešte vyhladená oknom s veľkosťou  $2 \times 2$ . Prasklina s poškodenými okrajmi na čiernom pozadí je zobrazená na obrázku 6.11 (c), skopírovaná do syntetického odtlačku prsta je znázornená na obrázku 6.11 (d).

Na obrázku 6.12 sú znázornené obrázky z databázy falzifikátov, obsahujúce zúbkovitú prasklinu (a) a (d), v porovnaní s obrázkami syntetických odtlačkov prstov vygenerovanými v aplikácii (b) a (e). Pre lepšiu názornosť sú zobrazené aj anotácie vygenerovaných prasklín na čiernom pozadí (c) a (f). Praskliny boli vytvorené postupným generovaním jednotlivých prasklín do rovnakého odtlačku, v móde generovania podmieneného užívateľom. Úmyselne boli vytvorené tak, aby umiestnením, dĺžkou a šírkou pripomínali praskliny na obrázkoch



falzifikátov z databázy. Pri implementácii prasklín a ich rozdelení na tri typy bol kladený veľký dôraz na realistický vzhľad a podobnosť s prasklinami nachádzajúcimi sa v obrázkoch reálnych falzifikátov v databáze.



Obrázok 6.12: Obrázky falzifikátov obsahujúce praskliny so zúbkovitým tvarom (a) a (d), v porovnaní s prasklinami vygenerovanými do syntetických odtlačkov prstov (b) a (e). Na obrázku sú znázornené aj anotácie vygenerovaných prasklín (c) a (f).

### 6.4.3 Oblúkovitá prasklina

Tretím typom generovanej praskliny je oblúkovitá prasklina, v práci nazývaná aj *arcuate crack*. Pri tejto praskline je nutné zadať okrem dvoch koncových bodov aj jeden riadiaci bod, vďaka ktorému môžu byť pomocou Bézierovej krivky druhého stupňa vypočítané body ležiace na parabole, čím je napodobnený oblúkovitý priebeh praskliny.

Béziérová krivka  $n$ -tého stupňa je určená  $n + 1$  riadiacimi bodmi a vzťahom

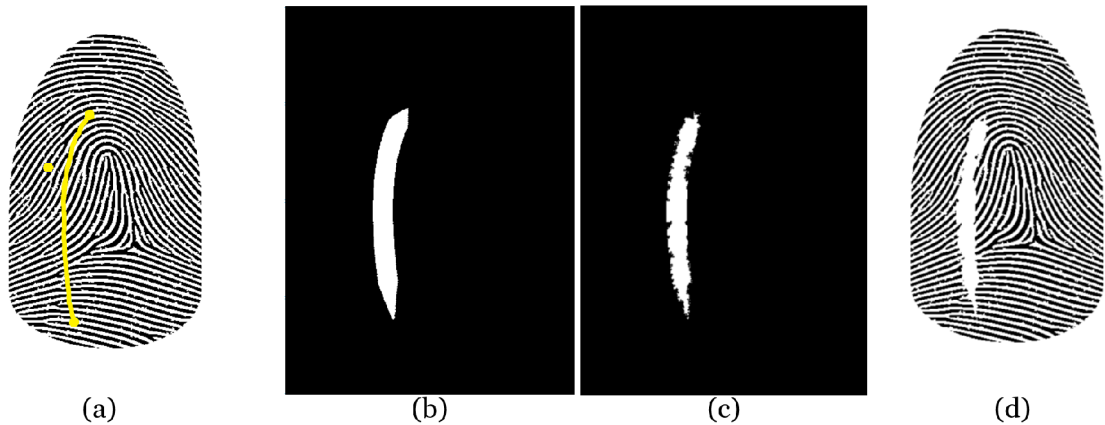
$$Q(t) = \sum_{i=0}^n p_i \cdot B_{i,n}(t), \quad t \in [0, 1], \quad (6.1)$$

kde  $B_{i,n}(t)$  sú Bernsteinove polynómy a sú určené ako [58]:

$$\begin{aligned} B_{0,3}(t) &= t^2 - 2t + 1 \\ B_{1,3}(t) &= -2t^2 + 2t \\ B_{2,3}(t) &= t^2 \end{aligned} \quad (6.2)$$

Bézierová krivka druhého stupňa je kvadratická, v podstate sa jedná o parabolu zadanú tromi bodmi. Dva body predstavujú koncové body paraboly, tretí bod určuje jej priebeh. S použitím toho princípu krivka prechádza koncovými bodmi, neprechádza však tretím riadiacim bodom, je aproximačná. [58]

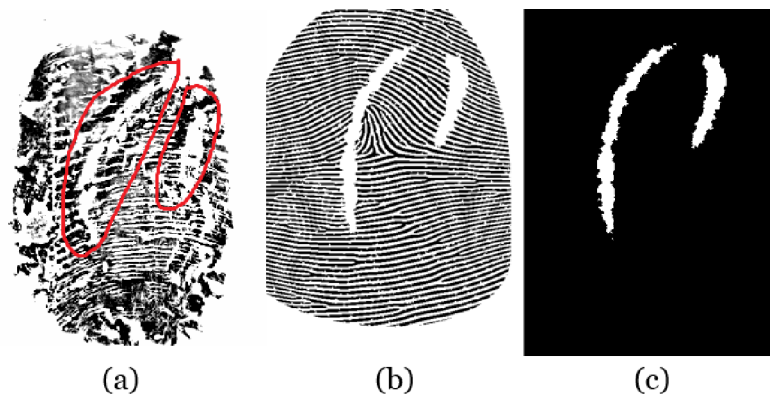
Metóda `computePointsOnParabola` realizuje výpočet bodov ležiacich na parabole uvedeným spôsobom s využitím Bernesteinových polynómov a s krokom 0,01 pri postupnom zvyšovaní  $t$ . Na obrázku 6.13 (a) sú znázornené vypočítané body ležiace na parabole medzi zadanými koncovými bodmi spolu s tretím riadiacim bodom, ktorý leží mimo paraboly. Celkovo generovanie oblúkovitej praskliny realizuje metóda `renderArcCrack`. Po výpočte bodov ležiacich na parabole je prasklina vykreslená do obrázka s čiernym pozadím tak, že jej šírka na začiatku/konci postupne rastie/znižuje sa, v centrálnych častiach dosahuje hodnotu získanú od užívateľa. Postupné zvyšovanie či znižovanie šírky praskliny je ovplyvnené základnou šírkou praskliny zadanou užívateľom. Na obrázku 6.13 (b) je zobrazená základná reprezentácia praskliny vykreslená so zužujúcimi sa okrajmi na čiernom pozadí.



Obrázok 6.13: Generovanie oblúkovitej praskliny: (a) – body ležiace na parabole zobrazené spolu s tretím riadiacim bodom, ktorý leží mimo paraboly, (b) – prasklina so zužujúcimi sa okrajmi vygenerovaná na čiernom pozadí, (c) – prasklina s poškodenými okrajmi, (d) – finálny vzhľad praskliny vygenerovanej do syntetického odtlačku prsta.

Na záver sú okraje praskliny porušené s využitím metódy `damageCrackEdgesWithSquares`, ktorá síce generuje malé štvorčky, volaná je však v tomto prípade len raz, preto okraje oblúkovitej praskliny nie sú až také porušené, ako je to v prípade zúbkovitej praskliny. Na obrázku 6.13 (c) je zobrazená oblúkovitá prasklina s poškodenými okrajmi na čiernom pozadí, na obrázku 6.13 (d) je prasklina skopírovaná do syntetického odtlačku prsta.

Na obrázku 6.14 je znázornený obrázok z databázy falzifikátov obsahujúci oblúkovité praskliny vyznačené červenou farbou (a), v porovnaní s obrázkom syntetického odtlačku prsta vygenerovaného v aplikácii (b). Pre lepšiu názornosť je zobrazená aj anotácia vygenerovaných prasklín na čiernom pozadí (c). Praskliny boli vytvorené postupným generovaním jednotlivých prasklín do rovnakého odtlačku, v móde generovania podmieneného užívateľom.



Obrázok 6.14: Obrázok falzifikátu obsahujúceho praskliny s oblúkovitým tvarom (a), v porovnaní s prasklinami vygenerovanými do syntetického odtlačku prsta (b). Na obrázku je znázornená aj anotácia vygenerovaných prasklín (c).

#### 6.4.4 Náhodné generovanie

Pri náhodnom generovaní praskliny užívateľ volí šírku a typ praskliny, náhodne sú vybrané jej riadiace body. Výber bodov pritom nie je úplne náhodný, kvôli zachovaniu realistického vzhľadu prasklín podlieha niekoľkým pravidlám. Je potrebné uviesť, že náhodné generovanie riadiacich bodov praskliny sa líši pre rôzne typy prasklín, pre rovnú a zúbkovitú prasklinu prebieha rovnakým spôsobom, pri oblúkovitej je nutný dodatočný výpočet pre určenie tretieho riadiaceho bodu.

Pri všetkých typoch prasklín je najskôr vykonaná diskretizácia. Zo všetkých bodov vstupného obrázka sú vybrané len tie, ktoré ležia vo vnútri odtlačku prsta a tvoria na ňom mriežku s rozstupmi 5 pixelov. Nájdenie týchto bodov realizuje metóda `findControlPointsCandidates`, ktorá na vstupe dostane masku plochy odtlačku prsta a vráti vektor vhodných kandidátnych bodov spĺňajúcich uvedené podmienky.

Celý proces náhodného generovania praskliny realizuje metóda `generateCrack`. Po nájdení kandidátnych bodov je z nich náhodne vybraný jeden bod určujúci koncový bod praskliny. Plocha odtlačku prsta je následne pomocou metódy `enlargeFingerprintArea` zväčšená v každom smere o určitý počet pixelov. Konkrétny počet je daný ako  $\frac{1}{6}$  najväčšej šírky plochy odtlačku prsta. Najväčšia šírka plochy odtlačku je zistená v rámci metódy `findBorders`, ktorá tiež pracuje s maskou plochy odtlačku. Vo zväčšenej oblasti odtlačku prsta je opäť urobená diskretizácia a z nových kandidátnych bodov je vybraný druhý riadiaci bod praskliny. Výber môže byť zopakovaný viackrát, druhý bod musí totiž spĺňať podmienku, že vzdialenosť medzi ním a prvým vybraným bodom musí byť väčšia ako  $\frac{1}{6}$  najväčšej šírky odtlačku, aby sa nestalo, že celá prasklina leží mimo plochy odtlačku prsta vo zväčšenej ploche, a tým pádom je vo výslednom obrázku neviditeľná. Zväčšená plocha odtlačku a dva náhodne vybrané koncové body praskliny z oboch plôch odtlačku vytvárajúce úsečku sú graficky znázornené na obrázku 6.15 (a). Týmto náhodné generovanie koncových bodov pre rovnú a zúbkovitú prasklinu končí a prasklina je vykreslená do vstupného obrázka.

Pri oblúkovitom type praskliny je ešte nutné vygenerovať tretí riadiaci bod, ktorý určuje zakrivenie paraboly. Aby výsledná prasklina vyzerala realisticky, je nutné zredukovať plochu, v rámci ktorej môže byť vygenerovaný tretí riadiaci bod pri znalosti dvoch vy-

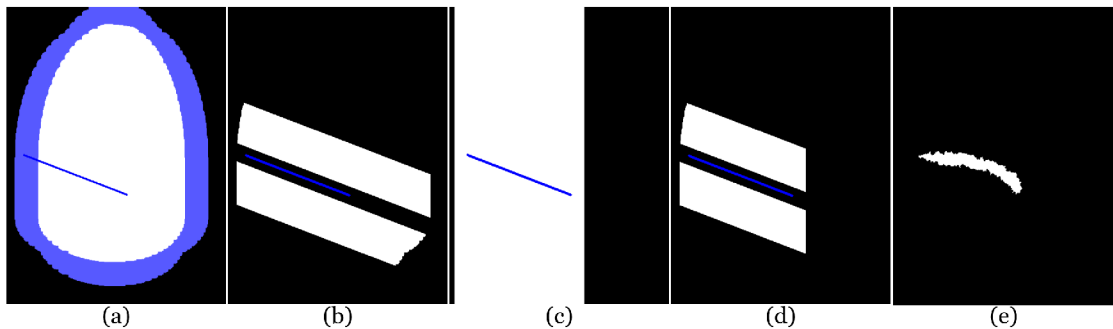
generovaných koncových bodov. Najskôr je použitý všeobecne známy vzorec z analytickej geometrie, určujúci vzdialenosť bodu od priamky:

$$|Mp| = \frac{|am_1 + bm_2 + c|}{\sqrt{a^2 + b^2}}, \quad (6.3)$$

kde  $p$  je priamka určená všeobecnou rovnicou priamky v rovine  $p: ax + by + c = 0$  a  $M$  je bod v rovine,  $M = [m_1; m_2]$ .

Na základe tohto vzorca je vytvorená maska plochy okolo priamky, obsahujúca body vo vzdialenosti od priamky, ktorá je menšia ako  $\frac{1}{3}$  najväčšej šírky odtlačku. Okrem toho je z tejto masky vylúčená plocha zahŕňajúca body veľmi blízke ku priamke určujúcej prasklinu, nakoľko ak by bol vybraný bod z blízkeho okolia, nebolo by viditeľné zakrivenie paraboly a prasklina by sa javila ako rovná. Výpočet tejto masky realizuje metóda `recomputeMaskForArc` a graficky je znázornená na obrázku 6.15 (b). Biela plocha predstavuje miesta, v ktorých môže byť vygenerovaný tretí bod určujúci tvar oblúkovitej praskliny po prvej úprave masky.

Pre dosiahnutie skutočne realistického vzhľadu praskliny je nutné ohraničiť plochu pre generovanie tretieho bodu aj v určitej vzdialenosti od koncov praskliny. Je to dosiahnuté jednoduchým spôsobom, okraje úsečky určenej dvomi koncovými bodmi praskliny sú posunuté v smere  $x$  alebo  $y$ , podľa smeru pomalšieho rastu úsečky. Tieto body určujú priamky kolmé na os  $x$  alebo  $y$ , ohraničujúce plochu za koncami úsečky, za ktorou nie je možné vygenerovať tretí riadiaci bod. Výpočet tejto masky realizuje metóda `recomputeMaskForArcRect` a graficky je znázornená na obrázku 6.15 (c). Biela plocha predstavuje miesta, v ktorých môže byť vygenerovaný tretí bod určujúci tvar oblúkovitej praskliny v rámci druhej úpravy masky. Tretí riadiaci bod paraboly je potom náhodne vybraný z bodov ležiacich v prieniku týchto dvoch vytvorených masiek, ktorý je znázornený na obrázku 6.15 (d). Finálna oblúkovitá prasklina vytvorená na základe náhodne vybraných riadiacich bodov podľa opísaného postupu je znázornená na obrázku 6.15 (e).



Obrázok 6.15: Náhodné generovanie riadiacich bodov oblúkovitej praskliny: (a) – rozšírená maska s dvomi náhodne vygenerovanými bodmi určujúcimi koncové body praskliny, (b) – prvá redukcia oblasti pre vygenerovanie tretieho riadiaceho bodu pozdĺž priebehu priamky určenej koncovými bodmi praskliny, (c) – druhá redukcia oblasti za koncovými bodmi praskliny, (d) – finálna maska oblasti pre vygenerovanie tretieho kontrolného bodu oblúkovitej praskliny a (e) – výsledná vygenerovaná prasklina.

## Kapitola 7

# Testovanie

V tejto kapitole je opísané testovanie a vyhodnotenie dosiahnutých výsledkov pri generovaní syntetických odtlačkov prstov s prejavmi falzifikátov prostredníctvom vytvorenej aplikácie. Vygenerovaných bolo niekoľko dátových setov a odtlačky v nich boli vyhodnotené pomocou nástroja FiQiVi pre určenie kvality odtlačku a VeriFinger pre zistenie skóre podobnosti pri identifikácii odtlačku. V nasledujúcich podkapitolách sú podrobnejšie opísané vytvorené dátové sety, použité nástroje a vyhodnotenie výsledkov testovania.

### 7.1 Vytvorené dátové sety

V rámci testovania dosiahnutých výsledkov bolo vytvorených 10 dátových setov, z ktorých každý obsahuje 250 obrázkov syntetických odtlačkov prstov vo formáte BMP s rozlíšením 500 PPI<sup>1</sup>, kvôli požiadavkám nástroja VeriFinger. Dátové sety boli vytvorené pomocou automatizovaných skriptov vytvorených v aplikácii SikuliX, obrázky základných syntetických odtlačkov prstov boli vytvorené v generátore SFinGe, prejavy falzifikátov boli vygenerované v rozšírenej aplikácii SpoofGenerator a ich rozlíšenie bolo upravené v aplikácii IrfanView.

Dátový set č. 1 obsahuje 250 referenčných syntetických odtlačkov prstov vytvorených generátorom SFinGe bez akýchkoľvek vygenerovaných prejavov falzifikátov. V snahe o zachovanie možnosti porovnať dosiahnuté výsledky s výsledkami testovania pôvodnej aplikácie a priebeh vyhodnotenia čo najviac prispôbiť predchádzajúcemu vyhodnoteniu, bol použitý rovnaký dátový set ako pri hodnotení originálnej aplikácie vytvorenej v rámci [1]. Generátor SFinGe vytvára odtlačky piatich rôznych prstov a na výber je päť tried, do ktorých odtlačok môže patriť – ľavá slučka, pravá slučka, oblúk, klenutý oblúk alebo špirála. Vo vytvorených 250 syntetických odtlačkoch v dátovom sete č. 1 sú rovnomerne zastúpené všetky druhy prstov aj triedy odtlačkov prstov [1].

V ostatných dátových setoch bol do referenčných syntetických odtlačkov prstov vždy vygenerovaný minimálne jeden prejav falzifikátov. Pri generovaní bol použitý aj parameter `-d`, ktorý spôsobuje poškodenie dokonalých papilárnych línií v syntetickom odtlačku. Toto poškodenie bolo generované z dôvodu kompatibility pri vyhodnotení generovania prejavov implementovaných v [1], kedy bolo poškodenie dokonalých papilárnych línií vytvorené automaticky pri každom spustení aplikácie.

Dátové sety č. 2 - 4 obsahujú zaradom obrázky odtlačkov prstov s vygenerovanou rovnou prasklinou, zubkovitou prasklinou a oblúkovitou prasklinou. V každom dátovom sete boli rôzne hrúbky praskliny v rámci konkrétneho typu praskliny generované rovnomerne tak,

---

<sup>1</sup>Points Per Inch, miera kvality obrázku

aby každá hrúbka bola vygenerovaná do približne rovnakého počtu syntetických odtlačkov prstov.

Dátové sety č. 5 - 8 obsahujú obrázky odtlačkov prstov s vygenerovanými oblasťami s nižšou jasnosťou, pričom každý dátový set obsahuje odtlačky s iným pomerom medzi oblasťami s hrubšou vrstvou materiálu a celou plochou odtlačku, a sice 50 %, 60 %, 70 % a 80 %.

Dátový set č. 9 obsahuje obrázky odtlačkov prstov so súčasne vygenerovanou prasklinou aj oblasťami s nižšou jasnosťou papilárných línií. V databáze, v ktorej bola robená analýza, sa falzifikáty s oboma prejavmi súčasne síce nevyskytovali, ale teoreticky je takáto kombinácia prejavov možná napríklad vo falzifikátoch vytvorených z rôznych druhov lepidla. V tomto prípade boli vlastnosti prejavov generované náhodne, čiže nebol kladený dôraz na to, aby boli všetky kombinácie vlastností prasklín a oblastí s nižšou jasnosťou zastúpené rovnomerne.

Dátový set č. 10 obsahuje obrázky odtlačkov prstov orezané do neprirodeného celkového tvaru. Pôvodná aplikácia obsahovala 40 masiek vytvorených podľa neprirodených tvarov skutočných falzifikátov. V rámci rozšírenia aplikácie bol pridaný špeciálny mód umožňujúci vytvorenie novej masky na orezanie z ľubovoľného vstupného obrázka falzifikátu a jej pripojenie medzi používané masky. Týmto spôsobom bolo spomedzi obrázkov falzifikátov z databázy, v ktorej prebiehala aj analýza implementovaných prejavov, vytvorených 10 nových masiek tvarov falzifikátov z obrázkov falzifikátov, ktoré mali iný tvar ako už vytvorené masky v originálnej aplikácii. Pred výberom finálnych 10 nových masiek bolo masiek vytvorených viac, ale množstvo z nich malo tvar veľmi podobný s už existujúcimi maskami, a preto boli zo spracovania vylúčené.

Zoznam všetkých vytvorených dátových setov spolu s vygenerovanými prejavmi falzifikátov je prehľadne zobrazený v tabuľke 7.1.

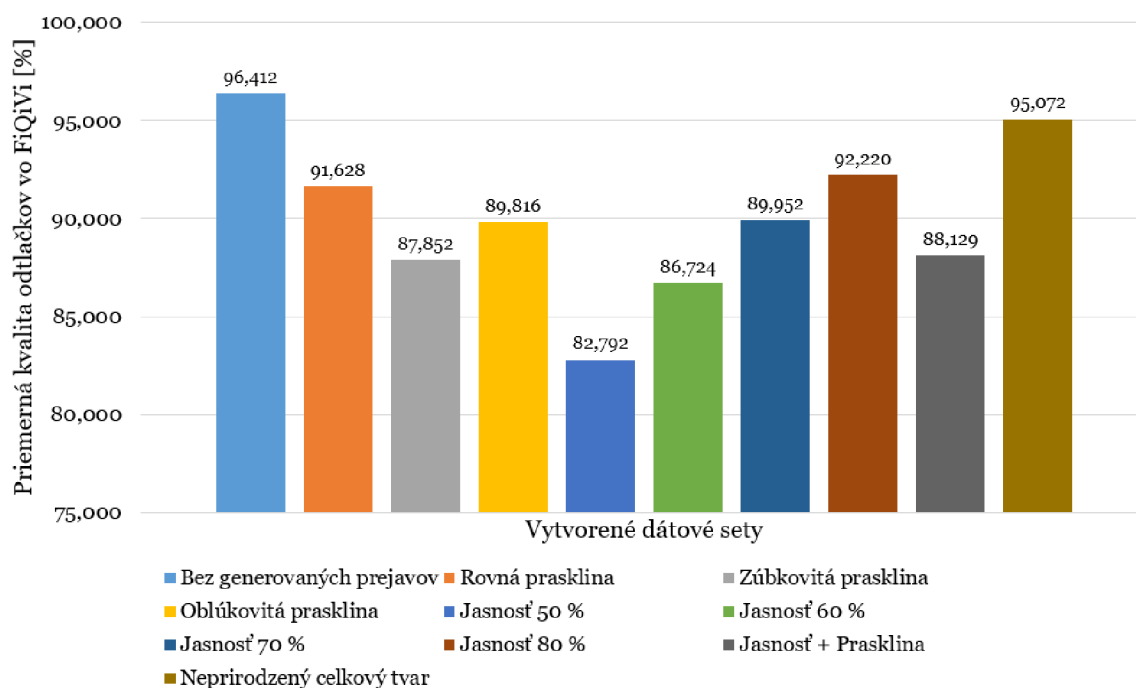
Tabuľka 7.1: Prehľad vytvorených dátových setov s vygenerovanými prejavmi falzifikátov.

Dátový set číslo	Vygenerované prejavy falzifikátov
1	-
2	Rovná prasklina
3	Zúbkovitá prasklina
4	Oblúkovitá prasklina
5	Nižšia jasnosť s pomerom 50 %
6	Nižšia jasnosť s pomerom 60 %
7	Nižšia jasnosť s pomerom 70 %
8	Nižšia jasnosť s pomerom 80 %
9	Nižšia jasnosť + prasklina
10	Neprirodzený celkový tvar

## 7.2 Vyhodnotenie testovania nástrojom FiQiVi

Prvou z dvoch metrík zvolených pre vyhodnotenie testovania je metóda, ktorú navrhol pán Oravec vo svojej diplomovej práci [59]. Software implementujúci túto metódu bol následne rozšírený v rámci diplomovej práce pána Dejerala a pomenovaný FiQiVi [60]. Vo FiQiVi je obrázok odtlačku rozdelený na menšie oblasti, v ktorých je samostatne posudzovaná kvalita odtlačku. Kvalita je posudzovaná na základe viacerých kritérií, medzi ktoré patria naprí-

klad pomer veľkostí papilárnych línií a medzier medzi nimi, kontinualita papilárnych línií, rozdiel orientácií medzi posudzovanou oblasťou a okolitými časťami odtlačku, výraznosť papilárnych línií voči pozadiu a inými. Kvalita je v každej oblasti vyhodnotená samostatne a následne je z čiastkových kvalít v percentách určená celková kvalita odtlačku.



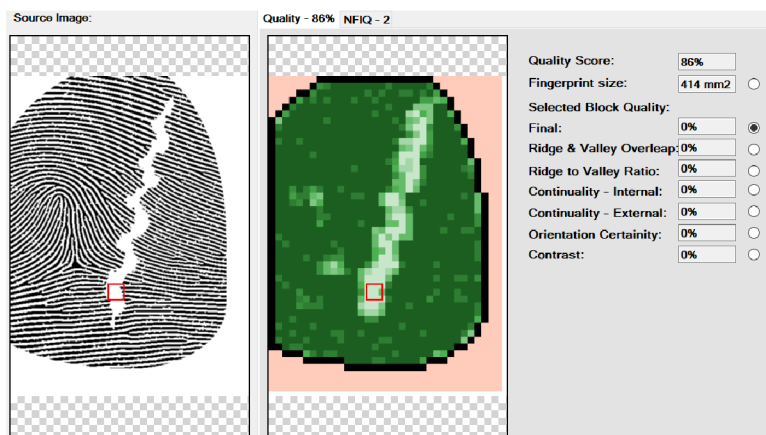
Obrázok 7.1: Grafické znázornenie priemerných kvalít odtlačkov v dátových setoch vytvorených v tejto práci získaných nástrojom FiQVi.

Na grafe zobrazenom na obrázku 7.1 sú v percentách uvedené priemery kvalít obrázkov odtlačkov prstov v jednotlivých dátových setoch zistených pomocou nástroja FiQVi. Dátový set č. 1 bez vygenerovaných prejavov dosiahol najvyššiu kvalitu 96,412 %, čo je v súlade s očakávaniami, keďže sa jednalo o dokonalé reprezentácie syntetických odtlačkov prstov bez dodatočných úprav.

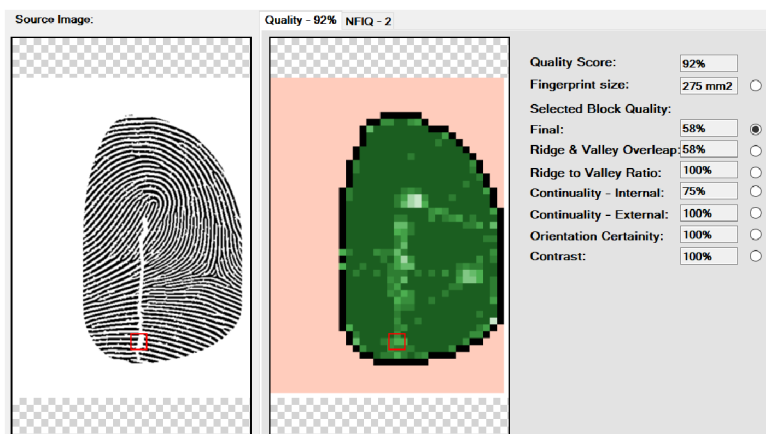
V dátových setoch obsahujúcich prasklinu kvalita klesla najmenej pri generovaní rovnej praskliny, v porovnaní s pôvodným dátovým setom klesla približne len o 4,784 %. Šírka rovnej praskliny aj pri maximálne novej generovanej šírke nie je veľmi veľká, tým pádom nezasahuje do veľkého množstva oblastí odtlačku a kvalitu v nich porušuje len minimálne. Zúbkovitá prasklina spôsobila pokles v kvalite až o 8,560 %, čo je najviac spomedzi rôznych typov prasklín. Je to spôsobené tým, že jej šírka je podstatne väčšia ako šírka rovnej praskliny, obvod jej okrajov je kvôli zúbkovitému priebehu najväčší zo všetkých typov praskliny a porušenie okrajov je taktiež najmasívnejšie, čo dokopy spôsobuje relatívne vysoký pokles kvality vo veľkom počte oblastí v rámci odtlačku, do ktorých zasahuje prasklina alebo jej okraje. Oblúkovitá prasklina spôsobila pokles o 6,596 %, čo je takmer v strede medzi dvomi ostatnými typmi prasklín a vyplýva to aj z vlastností oblúkovitej praskliny ako šírka a poškodenie okrajov, ktoré môžeme tiež považovať za akýsi stred medzi ostatnými typmi.

Na obrázku 7.2 je možné vidieť výrez z okna aplikácie FiQVi, na ktorom je zobrazené určovanie kvality odtlačku prsta obsahujúceho zúbkovitú prasklinu. Vľavo je vstupný

obrázok odtlačku prsta, červený štvorček označuje oblasť, ktorej hodnoty kvality jednotlivých kritérií sú zobrazené vpravo. V strede je farebná mapa vypočítanej kvality oblastí v rámci odtlačku, bledo oranžová farba predstavuje okolie odtlačku, čierna farba hranice odtlačku a odtiene zelenej predstavujú rôzne úrovne kvality, najkvalitnejšie časti dosahujú najtmavšiu zelenú farbu [59]. Na základe toho je možné vidieť, že aj keď štvorček zahŕňa aj časť odtlačku mimo praskliny, všetky hodnoty kvality okrem celkovej, počítanej pre celý odtlačok, majú hodnotu 0 %. Pre porovnanie je na obrázku 7.3 zobrazené určovanie kvality aj pre odtlačok s rovnou prasklinou. Oblasť určovania kvality je nastavená na najhrubšiu časť rovnej praskliny, a aj napriek tomu dosahuje kvalita v niektorých kritériách hodnotu 100 %. Obrázky ilustrujú proces určovania kvality v nástroji FiQVi ako aj zdôvodnenie rozdielneho porušenia kvality pri generovaní rôznych typov prasklín.



Obrázok 7.2: Určovanie kvality obrázka odtlačku prsta s vygenerovanou zúbkovitou prasklinou. Vo vstupnom obrázku je červeným štvorčekom naznačená oblasť určovania kvality. Vpravo sú uvedené hodnoty jednotlivých posudzovaných kritérií.



Obrázok 7.3: Určovanie kvality obrázka odtlačku prsta s vygenerovanou rovnou prasklinou. Vo vstupnom obrázku je červeným štvorčekom naznačená oblasť určovania kvality. Vpravo sú uvedené hodnoty jednotlivých posudzovaných kritérií.



V dátových setoch obsahujúcich oblasti s nižšou jasnosťou papilárnych línií klesla kvalita najmenej v dátovom sete s nastaveným pomerom medzi oblasťami s hrubšou vrstvou materiálu a celkovou plochou odtlačku na 80 %, čo znamená, že oblasti s nižšou jasnosťou sa vyskytovali približne len na 20 % plochy odtlačku a ich vzhľad vytváralo väčšinou len zosvetlenie odtieňa, nie generovanie veľkých bielych oblastí, ako je to pri nastavení vyšších pomerov, kde sú oblasti s generovaným poškodením väčšie. Výsledok testovania je v súlade s očakávaniami, v tomto dátovom sete kvalita klesla o 4,195 %. V ostatných dátových setoch, so znižujúcim sa pomerom, a tým pádom zvyšujúcou sa plochou s vygenerovaným poškodením, klesla priemerná kvalita postupne o 6,460 %, 9,688 % a 13,620 %.

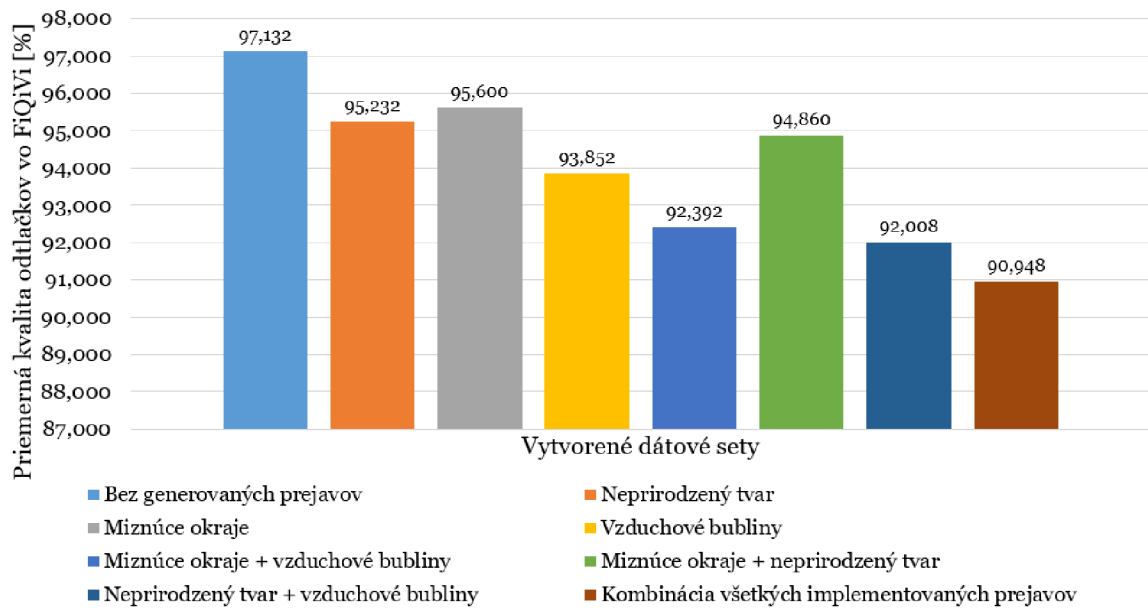
V rámci dátového setu č. 10, obsahujúceho odtlačky prstov orezané do nepravidelného celkového tvaru, klesla kvalita najmenej zo všetkých dátových setov, len o 1,340 %. Je to spôsobené tým, že pri generovaní nepravidelného celkového tvaru je obrázok odtlačku len orezaný, žiadne ďalšie poškodenie v rámci jeho plochy už nie je generované. FiQiVi okrem výslednej kvality uvádza aj hodnoty iných metrík, vďaka ktorým je možné lepšie vyhodnotiť tento konkrétny prejav. Jedná sa o počet markantov a percentuálnu veľkosť odtlačku v rámci celého obrázka.

Priemerné počty markantov v originálnych a upravených odtlačkoch prstov, ako aj priemerná percentuálna plocha odtlačkov, sú uvedené v tabuľke 7.2. Počet markantov po vygenerovaní prejavu neprirodený celkový tvar klesol takmer o 70 %, plocha odtlačku vzhľadom na veľkosť celého obrázka klesla približne o 65 %. Po posúdení hodnôt týchto metrík je možné konštatovať, že vygenerovanie neprirodeného celkového tvaru spôsobilo znehodnotenie odtlačku, aj keď sa to na celkovej kvalite až tak neprejavilo. V porovnaní s údajmi z vyhodnotenia testovania pôvodnej aplikácie uvedenými v [1] bol pokles v kvalite po rozšírení nižší, v danom vyhodnotení kvalita klesla o 1,9 %. Je preto možné usudzovať, že rozšírením o nové masky sa sada masiek vhodných na generovanie rozšírila práve o také masky, ktoré spôsobujú len malý pokles v celkovej kvalite odtlačku. Údaje o počte markantov a percentuálnej ploche odtlačkov pred a po vygenerovaní nepravidelného celkového tvaru v rámci testovania pôvodnej aplikácie nie sú k dispozícii, preto porovnanie s pôvodným riešením v tejto oblasti nemôže byť vykonané.

Tabuľka 7.2: Hodnoty dodatočných metrík vyčíslených v nástroji FiQiVi pre pôvodné odtlačky a odtlačky s vygenerovaným prejavom nepravidelný celkový tvar.

	Pôvodné odtlačky	Neprirodzený celkový tvar
<b>Priemerný počet markantov</b>	1144,61	784,36
<b>Priemerná relatívna plocha odtlačku [%]</b>	51,48	33,20

Na obrázku 7.4 sú uvedené priemerné kvality obrázkov odtlačkov prstov dosiahnuté počas testovania pôvodnej aplikácie. Hodnoty nemôžu byť porovnané s hodnotami dosiahnutými v testovaní rozšírenej aplikácie absolútne, pretože aj priemerná kvalita obrázkov v dátovom sete bez generovaných prejavov bola vyčíslená inak. Orientačne je však možné konštatovať, že v pôvodnej aplikácii priemerná kvalita v žiadnom vygenerovanom dátovom sete neklesla pod 90 %, celkovo bol najväčší rozdiel v priemernej kvalite 6,184 %, medzi dátovým setom s referenčnými odtlačkami a dátovým setom obsahujúcim kombinácie všetkých vygenerovaných prejavov falzifikátov implementovaných v pôvodnej aplikácii. V rámci testovania rozšírenej aplikácie priemerná kvalita klesla najviac na 82,792 %, čo je rozdiel až 13,620 % od priemernej kvality referenčného dátového setu. Tento rozdiel bol dosiahnutý v dátovom sete s vygenerovanými oblasťami s nižšou jasnosťou pokrývajúcej polovicu



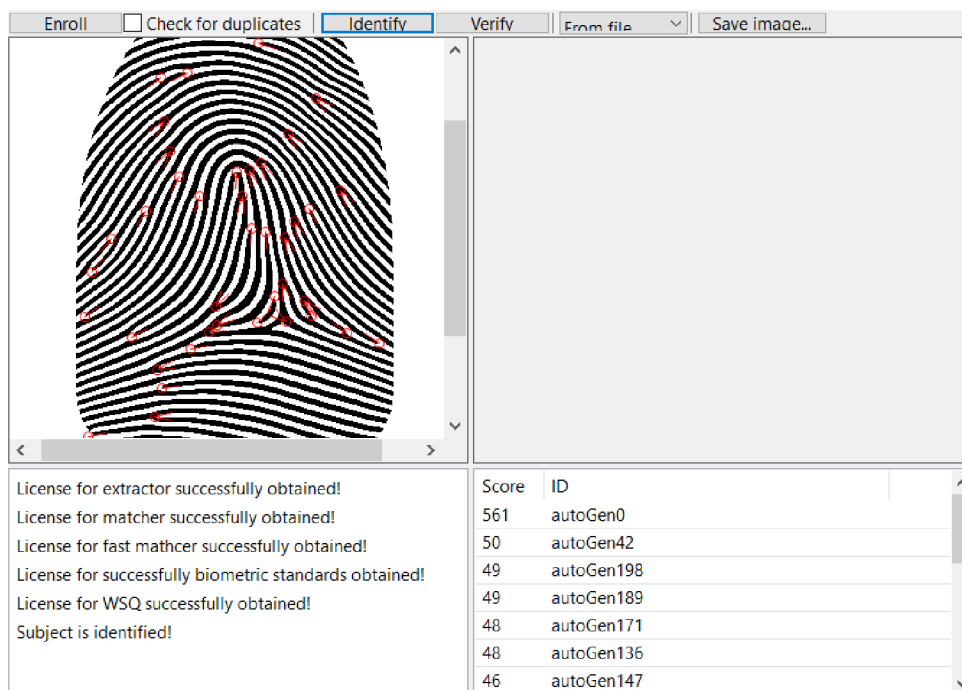
Obrázok 7.4: Grafické znázornenie priemerných kvalít odtlačkov v dátových setoch vytvorených počas testovania originálnej aplikácie v [1]. Graf bol vytvorený na základe údajov uvedených v [1].

plochu odtlačku. Aj keď referenčné dátové sety neboli ohodnotené v oboch testovaniach rovnako, rozdiel medzi ich priemernými kvalitami tvoril len 0,72 %, čo nie je signifikantné číslo a orientačné porovnanie medzi testovaniami je možné vykonať.

### 7.3 Vyhodnotenie testovania nástrojom VeriFinger

VeriFinger je technológia používaná pre identifikáciu odtlačkov prstov [61]. Okrem samotnej identifikácie či verifikácie umožňuje zistiť skóre vyjadrujúce mieru zhody medzi dvomi odtlačkami, ktoré môže byť použité pre vyhodnotenie testovania vytvorených dátových setov. Pred vyhodnotením odtlačkov s vygenerovanými prejavmi falzifikátov je najskôr nutné zistiť skóre medzi rovnakými obrázkami originálneho odtlačku prsta, ktoré sa líši pre každý odtlačok a vyjadruje úplnú zhodu. Toto skóre je následne považované za referenčné skóre každého odtlačku, vďaka ktorému je možné určiť aj normovanú hodnotu skóre odtlačku po vygenerovaní prejavov falzifikátov. Vplyvom vygenerovaných zmien by absolútna aj normovaná hodnota skóre mala mať nižšiu hodnotu ako referenčné skóre zistené pri porovnaní dvoch rovnakých odtlačkov prstov bez úprav.

Na obrázku 7.5 je znázornený priebeh identifikácie odtlačku prsta bez vygenerovaných prejavov falzifikátov. Vľavo je zväčšený vstupný obrázok s naznačenými markantmi, vpravo dole je zoznam podobných odtlačkov s uvedeným skóre podobnosti. V tomto prípade je najväčšie skóre 561 a je to referenčná hodnota považovaná za úplnú zhodu pri počítaní normovaného skóre po vygenerovaní prejavov falzifikátov do tohto konkrétneho syntetického odtlačku.



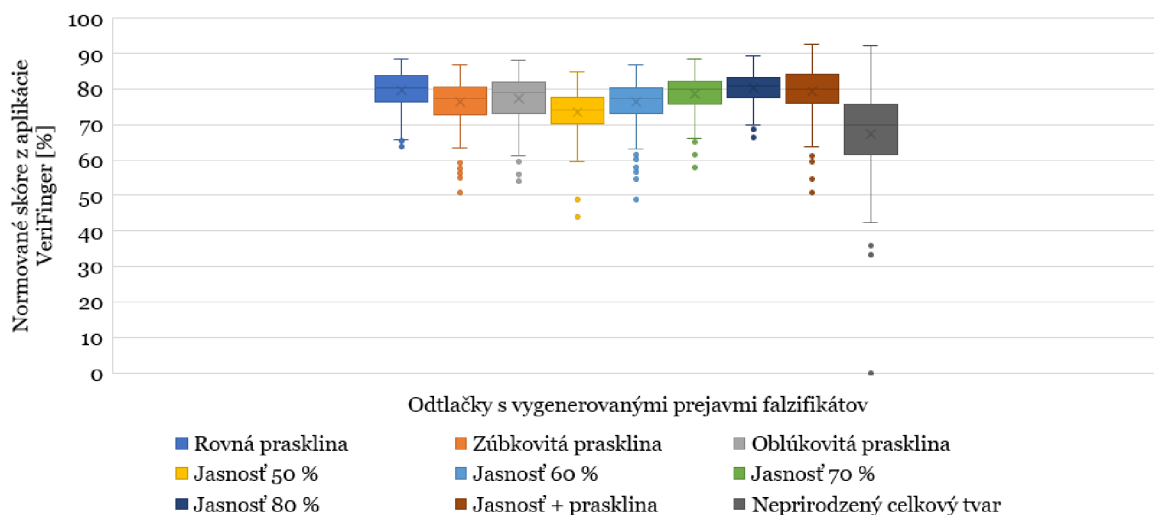
Obrázok 7.5: Identifikácia obrázka odtlačku prsta bez vygenerovaných poškodení v nástroji VeriFinger. Vľavo je zväčšený obrázok vstupného odtlačku, červenými značkami sú naznačené markanty použité pri identifikácii. Vpravo dole je zoznam nájdených podobných odtlačkov z databázy s uvedeným skóre podobnosti.

Tabuľka 7.3: Výsledky štatistického spracovania skóre získaného v nástroji VeriFinger.

Set	Prejav falz.	Priemer	Normovaný priemer	Maximum	Minimum
1	-	584,60	100,00 %	100,00 %	100,00 %
2	Rovná prasklina	464,87	79,63 %	88,51 %	63,74 %
3	Zúbkovitá prasklina	446,30	76,41 %	86,74 %	50,95 %
4	Oblúkovitá prasklina	452,63	77,50 %	88,00 %	54,10 %
5	Jasnosť 50 %	429,71	73,66 %	84,85 %	44,15 %
6	Jasnosť 60 %	445,95	76,41 %	86,73 %	48,96 %
7	Jasnosť 70 %	459,68	78,75 %	88,29 %	57,88 %
8	Jasnosť 80 %	469,13	80,33 %	89,51 %	66,50 %
9	Jasnosť + prasklina	463,17	79,33 %	92,61 %	50,90 %
10	Tvar	401,18	67,47 %	92,31 %	0,00 %

Výsledky štatistického spracovania údajov z vyhodnotenia dátových setov v nástroji VeriFinger sú uvedené v tabuľke 7.3. V tabuľke je uvedené priemerné, absolútne, aj normované skóre z vyhodnotenia každého vytvoreného dátového setu. Pre úplnosť je uvedená aj absolútna a normovaná hodnota referenčného skóre získaného pri vyhodnotení dátového setu č. 1 bez vygenerovaných prejavov falzifikátov. Okrem priemerných hodnôt sú v tabuľke uvedené aj maximálne a minimálne hodnoty skóre, v týchto prípadoch sa jedná o hodnoty v rámci normovaného skóre, aby mohli byť lepšie porovnateľné medzi dátovými setmi navzájom. V dátovom sete č. 10 obsahujúcom syntetické odtlačky prstov s vygenerovaným

prejavom neprirodzený celkový tvar je hodnota minimálneho skóre 0 %. Je to z dôvodu, že vplyvom orezania sa niektoré odtlačky prstov nepodarilo identifikovať, konkrétne sa jednalo o 5 odtlačkov z celkového počtu 250, čo predstavuje 2 %. Identifikácia prebiehala s FAR<sup>1</sup> nastaveným na hodnotu 0,0001. Pri daných 5 odtlačkoch bola identifikácia vykonaná opakovane, s postupne znižovanou hodnotou FAR až na 0,1, avšak odtlačky sa ani týmto spôsobom nepodarilo identifikovať.



Obrázok 7.6: Grafické znázornenie hodnôt normovaného skóre z nástroja VeriFinger pre odtlačky vo vytvorených dátových setoch s rôznymi vygenerovanými prejavmi falzifikátov.

Variácie v normovanom skóre medzi jednotlivými množinami odtlačkov sú pre lepšiu predstavu graficky znázornené na grafe na obrázku 7.6. V škatulovom grafe sú štvoruholníkmi vyznačené najčastejšie rozsahy hodnôt normovaného skóre v jednotlivých dátových setoch. Krížikom je vyznačený medián, ktorý by mal približne korešpondovať aj s priemernou hodnotou normovaného skóre uvedenou v tabuľke 7.3. Čiary vychádzajúce zo štvoruholníkov zobrazujú maximálne a minimálne hodnoty v rámci jednotlivých dátových setov, bodkami sú znázornené odľahlé hodnoty vzhľadom na vypočítané parametre pravdepodobnostného rozloženia hodnôt. Pri dátovom sete obsahujúcom neprirodzený celkový tvar je v danom rozložení hodnota skóre 0 %, symbolizujúca neidentifikované odtlačky prstov, považovaná za odľahlú hodnotu, zatiaľ čo v čistom štatistickom spracovaní hodnôt v tabuľke 7.3 bola určená ako minimálna hodnota nájdená medzi hodnotami v rámci dátového setu, nakoľko sa pri danom spracovaní nepracovalo s rozložením pravdepodobnosti.

Z grafu je možné vidieť, že hodnota skóre klesla najviac pri generovaní neprirodzeného celkového tvaru, čo je v rozpore so zisteniami v kapitole 7.2, ale je to logicky správny výsledok, nakoľko orezanie odtlačku do neprirodzeného celkového tvaru zásadným spôsobom nenarušuje kvalitu odtlačku, ale odstraňuje z odtlačku markanty, ktoré sú použité pre identifikáciu v rámci nástroja VeriFinger, a tým spôsobuje najväčší pokles v skóre spomedzi všetkých generovaných prejavov falzifikátov.

Vygenerovanie rôznych typov prasklín a oblastí s nižšou jasnosťou s rôznou hodnotou pomeru, či kombinácia generovania oblastí s nižšou jasnosťou a praskliny, obsiahnuté v dáto-

<sup>1</sup>False Acceptance Rate – chybová miera používaná pri určovaní parametrov biometrického systému, percento prípadov identifikácie, v ktorých sú neoprávnené osoby nesprávne akceptované

Tabuľka 7.4: Výsledky štatistického spracovania skóre získaného v nástroji VeriFinger počas testovania originálnej aplikácie vytvorenej v [1]. Tabuľka bola vytvorená na základe údajov uvedených v [1].

Set	Generovaný prejav	Priemer	Normovaný priemer	Maximum	Minimum
1	-	1119,00	100,00 %	100,00 %	100,00 %
2	Bubliny	841,87	75,19 %	90,15 %	36,92 %
3	Tvar	660,83	59,18 %	88,83 %	25,04 %
4	Okraje	841,28	75,18 %	91,03 %	57,89 %
5	Okraje + bubliny	771,43	68,89 %	87,04 %	45,13 %
6	Okraje + tvar	632,16	56,53 %	83,94 %	25,59 %
7	Tvar + bubliny	606,46	54,27 %	83,12 %	19,75 %
8	Kombinácia všetkých	566,79	50,64 %	76,36 %	20,73 %

vých setoch č. 2 - 9, viedlo k veľmi podobnému zníženiu skóre. Medzi týmito dátovými setmi nie sú prítomné žiadne mimoriadne rozdiely v celkovom poklese skóre oproti referenčnému.

Ako bolo preukázané aj vo vyhodnotení testovania kvality odtlačkov v kapitole 7.2, zvyšujúci sa pomer nepriehľadných oblastí s hrubšími vrstvami materiálu k celkovej ploche odtlačku spôsobuje zvyšovanie skóre, keďže je so zvyšovaním tohto pomeru generované miernejšie poškodenie. V rámci rôznych typov prasklín je výsledok opäť rovnaký, najmenej skóre ubudlo pri generovaní rovnej praskliny, najviac pri generovaní zúbkovitej praskliny a oblúkovitá sa nachádza niekde medzi nimi.

V tabuľke 7.4 sú pre porovnanie uvedené údaje získané počas testovania pôvodnej aplikácie v nástroji VeriFinger. Význam hodnôt je rovnaký ako v tabuľke 7.3 obsahujúcej hodnoty z testovania rozšírenej aplikácie. Pri testovaní rozšírenej aplikácie bola použitá novšia verzia aplikácie VeriFinger, rovnako ako aj obrázky s hodnotou  $PPI = 500$ , pričom pri testovaní originálnej aplikácie boli použité obrázky s hodnotou  $PPI = 72$ , nakoľko v danej verzii aplikácie ešte nebola požadovaná minimálna hodnota 500. Tieto skutočnosti zapríčinili veľký rozdiel medzi priemernou absolútnou hodnotou skóre v referenčných dátových setoch, ktorá bola v pôvodnom testovaní 1119 a v testovaní rozšírenej aplikácie klesla na 584,6. V rámci normovaných hodnôt však je možné originálnu aplikáciu s rozšírenou aspoň orientačne porovnať.

V rozšírenej aplikácii spôsobilo najväčší pokles skóre generovanie neprirodzeného celkového tvaru, ostatné prejavy nespôsobili pokles skóre pod 73 % z pôvodnej hodnoty. V originálnej aplikácii generovanie samostatných prejavov vzduchových bublín a postupne miznúcich okrajov papilárnych línií spôsobilo v oboch prípadoch pokles skóre približne na hodnotu 75 % z pôvodnej hodnoty. Pri generovaní samostatných prejavov falzifikátov okrem neprirodzeného tvaru sa teda jedná aj v prípade prasklín a oblastí s nižšou jasnosťou o porovnateľné hodnoty s pôvodnou aplikáciou. Generovanie neprirodzeného celkového tvaru v rozšírenej aplikácii spôsobilo pokles skóre na 67,47 % z pôvodnej hodnoty, v originálnej aplikácii na 59,18 % z pôvodnej hodnoty. Rozdiel potvrdzuje závery uvedené v kapitole 7.2, že pridané masky na orezanie nespôsobujú až také drastické orezanie odtlačku, ako priemerne spôsobovala sada pôvodných masiek vytvorených v pôvodnej aplikácii.

Generovanie kombinácie dvoch prejavov falzifikátov v pôvodnej aplikácii spôsobilo pokles hodnoty skóre na 68,89 %, 56,53 % a 54,27 %, čo sú opäť vyššie hodnoty ako 79,33 % pri generovaní kombinácie oblastí s nižšou jasnosťou a praskliny v rozšírenej aplikácii. Je nutné poznamenať, že v prípade, kedy oblasti s nižšou jasnosťou prekrývajú podstatnú časť

odtlačku prsta, pri náhodnom generovaní sa často stáva, že prasklina je úplne prekrytá priehľadnou oblasťou s nižšou jasnosťou, alebo je viditeľná len malá časť praskliny, čo spôsobuje, že táto kombinácia ani nemôže spôsobiť taký podstatný pokles ako kombinácie generovania neprirodzeného celkového tvaru s iným prejavom, keď samotný neprirodzený celkový tvar spôsobuje najväčší pokles spomedzi implementovaných prejavov falzifikátov.

# Kapitola 8

## Záver

Cieľom práce bolo rozšíriť aplikáciu pre generovanie prejavov falzifikátov o možnosť generovania nových prejavov falzifikátov spolu s anotáciami vytvorených poškodení. Dosiahnuté výsledky bolo potrebné vhodným spôsobom otestovať, porovnať s pôvodným riešením a spolu s teoretickým základom a postupom práce zhrnúť v texte práce.

Formálne zadanie práce obsahuje päť bodov. Tieto body zahŕňajú preštudovanie relevantnej literatúry, zoznámenie sa s artefaktmi falzifikátov odtlačkov prstov, návrh vylepšenia aktuálneho modelu spolu s algoritmami pre generovanie minimálne dvoch prejavov falzifikátov tak, aby riešenie umožňovalo anotáciu vykonaného poškodenia a jej export, implementáciu a vyhodnotenie navrhnutého riešenia.

Na základe štúdia literatúry bola vytvorená teoretická časť práce. Následne bola vykonaná analýza prejavov falzifikátov z databázy obrázkov falzifikátov odtlačkov prstov výskumnej skupiny STRaDe. Na základe prvotnej analýzy boli zvolené dva artefakty odtlačkov prstov vyskytujúce sa v databáze, a to výskyt oblastí papilárnych línií s nižšou jasnosťou a projekcia defektov v materiáli do obrázka odtlačku prsta, konkrétne bola zvolená prasklina. Tým bol splnený prvý bod zadania.

Nasledovala pokročilejšia analýza zameraná na zvolené prejavy, na základe ktorej boli navrhnuté algoritmy pre ich generovanie do obrázkov syntetických odtlačkov prstov. Navrhnuté algoritmy spolu s výsledkami analýzy boli taktiež uvedené v texte práce. Zvolené bolo riešenie umožňujúce vytvorenie anotácií nielen nových vybraných prejavov, ale aj pôvodných, implementovaných v originálnej aplikácii. Tým bol splnený aj druhý bod zadania.

Navrhnuté algoritmy boli implementované v jazyku C++ s využitím metód knižnice OpenCV. Do aplikácie boli pridané možnosti náhodného aj podmieneného generovania troch rôznych typov prasklín a oblastí s nižšou jasnosťou papilárnych línií. Celkové prepínanie medzi módmami generovania prejavov bolo zjednotené, čo vyžadovalo pridanie možnosti náhodného generovania postupne miznúcich okrajov papilárnych línií, ktoré v pôvodnej verzii aplikácie chýbalo. Pre jednoduchšie nastavenie parametrov generovaných prejavov bolo vytvorené jednoduché grafické užívateľské rozhranie. V rozšírenej verzii aplikácie môže byť na základe nastavenia parametrov pri spustení voliteľne generované poškodenie dokonalejšej reprezentácie papilárnych línií, ktoré bolo v pôvodnom riešení automaticky generované pri každom spustení. Rovnako je pomocou parametrov ovládané generovanie anotácií vytvorených poškodení odtlačku. V prípade, že majú byť vytvorené anotácie, sú vygenerované čiernobiele obrázky predstavujúce mapy vykonaných poškodení pre každé uložené poškodenie samostatne, ako aj spolu v dodatočnej anotácii všetkých vykonaných poškodení. Posledným vylepšením aplikácie je rozšírenie jedného z pôvodných implementovaných prejavov falzifikátov, neprirodzeného celkového tvaru. Pridaná bola možnosť vytvorenia masky

neprirodzeného celkového tvaru falzifikátu pre akýkoľvek vstupný obrázok s falzifikátom. Implementáciou dvoch nových prejavov falzifikátov bol splnený tretí bod zadania. Ako bolo uvedené, v rámci rozšírenia zadania boli okrem dvoch nových prejavov implementované viaceré vylepšenia pôvodnej aplikácie.

Po skončení implementácie bolo vytvorených 10 dátových setov, každý s 250 obrázkami samostatných syntetických odtlačkov prstov alebo syntetických odtlačkov prstov s 1 – 2 vygenerovanými prejavmi falzifikátov. Dátové sety boli ohodnotené prostredníctvom nástroja FiQiVi pre určenie kvality odtlačku prsta a pomocou skóre získaného v nástroji VeriFinger pri identifikácii odtlačkov prstov. Rozšírené riešenie spôsobilo celkovo väčšie porušenie kvality odtlačku prsta ako pôvodné riešenie. V prípade vyhodnotenia skóre podobnosti dosiahlo generovanie samostatných nových prejavov okrem neprirodzeného celkového tvaru porovnateľné výsledky ako pôvodné riešenie. Neprirodzený celkový tvar pri určení kvality aj skóre podobnosti odtlačky viac poškodil v pôvodnom riešení, z čoho vyplýva, že v tejto práci boli pridané masky, ktoré spôsobili menšie poškodenie, ako samostatné pôvodné masky zahrnuté v originálnom riešení. Výsledky testovania a porovnanie s pôvodným riešením boli taktiež opísané v texte práce, čím bol splnený aj štvrtý bod zadania.

Posledným bodom zadania bolo zhrnutie dosiahnutých výsledkov, ktoré už bolo uvedené v predchádzajúcom texte, v praktickej časti textu práce, ako aj v tejto záverečnej kapitole. Druhou časťou posledného bodu zadania bolo uvedenie ďalších možných rozšírení vytvoreného riešenia. Prácu by bolo možné doplniť o implementáciu ďalších prejavov falzifikátov, ktoré by mohli byť vybrané napríklad na základe celkovej analýzy databáz falzifikátov, ktorá bola uskutočnená v rámci tejto práce a jej výsledky sú uvedené v textovej časti. Zaujímavým rozšírením práce by mohlo byť zameranie sa na rôzne materiály použité pri výrobe falzifikátov a generovanie prejavov falzifikátov na základe znalostí fyzikálnych vlastností materiálu, na čo sa čiastočne bral ohľad už aj v rámci tejto práce, najmä pri posudzovaní rôznych typov prasklín vyskytujúcich sa v rôznych materiáloch falzifikátov.



# Literatúra

- [1] VRÁBLOVÁ, Z. *Generování projevu falzifikátu do syntetických otisků prstů z generátoru SFinGe*. Brno, CZ, 2019. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: <https://www.fit.vut.cz/study/thesis/21537/>.
- [2] DRAHANSKÝ, M., ORSÁG, F. a DOLEŽEL, M. *Biometric*. 1. vyd. Brno: Computer Press a. s., 2011. ISBN 978-80-254-8979-6.
- [3] ISO/IEC. *International Standard ISO/IEC 2382-37 Information technology – Vocabulary – Part 37: Biometrics*. 1. vyd. Switzerland, 2012.
- [4] BOLLE, R. M., CONNELL, J. H., PANKARTI, S. et al. *Guide to Biometrics*. 1. vyd. New York: Springer, 2004. ISBN 978-1-4419-2305-9.
- [5] FLORENCIO, D. a HERLEY, C. *A Large-Scale Study of Web Password Habits*. 6th International World Wide Web Conference, 2007. DOI: 10.1145/1242572.1242661.
- [6] PRABHAKAR, S., PANHANTI, S. a JAIN, A. K. *Biometric Recognition: Security and Privacy Concerns*. Security & Privacy, IEEE, 2003. DOI: 10.1109/MSECP.2003.1193209.
- [7] JAIN, A. K., ROSS, A. A., a NANDAKUMAR, K. *Introduction to Biometrics*. New York: Springer, 2011. ISBN 978-0-387-77325-4.
- [8] MALTONI, D., MAIO, D., JAIN, A. K. et al. *Handbook of Fingerprint Recognition*. New York: Springer, 2003. ISBN 0-387-95431-7.
- [9] WERTHEIM, K. *Embryology, Physiology, and Morphology of Friction Ridge Skin*. In: *Fingerprint Sourcebook-Chapter*. USA: National Institute of Justice, 2011, kap. 3.
- [10] KANICH, O. *Fingerprint Damage Simulation: A simulation of fingerprint distortion, damaged sensor, pressure and moisture*. Saarbrücken: LAP LAMBERT Academic Publishing, 2014. ISBN 978-3-659-63942-5.
- [11] KANICH, O. *Research in Fingerprint Damage Simulations*. Brno, CZ, 2019. Disertační práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: <https://www.fit.vut.cz/study/phd-thesis/832/>.
- [12] DRAHANSKÝ, M. *Hand-based biometrics: methods and technology*. London: The Institution of Engineering and Technology, 2018. ISBN 978-1-78561-224-4.

- [13] DRAHANSKÝ, M. *Fingerprint Recognition Technology – Related Topics: Skin Diseases, Image Quality and Liveness Detection*. Saarbrücken: LAP LAMBERT Academic Publishing, 2011. ISBN 978-3-844-33007-6.
- [14] STRAUS, J. *Kriminalistická technika*. 1. vyd. Plzeň: Aleš Čeněk s.r.o., 2012. ISBN 978-80-7380-409-1.
- [15] RAK, R., MATYÁŠ, V. a ŘÍHA, Z. *Biometrie a identita člověka ve forezních a komerčních aplikacích*. Praha: Grada, 2008. ISBN 978-80-247-2365-5.
- [16] KOMARINSKI, P. *Automated Fingerprint Identification Systems (AFIS)*. USA: Elsevier Academic Press, 2005. ISBN 0-12-418351-4.
- [17] DRAHANSKÝ, M. a KANICH, O. *Rozpoznávání podle otisků prstů* [online]. FIT VUT v Brně, 2020 [cit. 2020-11-28]. Dostupné z: <https://www.fit.vutbr.cz/study/courses/BIO/private/>.
- [18] JAIN, A. K., FLYNN, P. a A.ROSS, A. *Handbook of Biometrics*. USA: Springer, 2008. ISBN 978-0-387-71040-2.
- [19] JAIN, A., BOLLE, R. a PANKANTI, S. *Biometrics: Personal Identification in Networked Society*. USA: Springer, 2006. ISBN 978-0387-28539-9.
- [20] JAIN, A. K. a FENG, J. *Latent Fingerprint Matching*. Transactions on pattern analysis and machine intelligence, IEEE, 2011. DOI: 10.1109/TPAMI.2010.59.
- [21] FISHER, B. A. J., TILSTONE, W. J. a WOYOTOWICZ, C. *Introduction to Criminalistics: The Foundation of Forensic Science*. USA: Elsevier, 2009. ISBN 978-0-12-088591-6.
- [22] RATHA, N. a BOLLE, R. *Automatic Fingerprint Recognition Systems*. USA: Springer, 2004. ISBN 0-387-95593-3.
- [23] KHANYILE, N. P., TAPAMO, J. R. a DUBE, E. *A Comparative Study of Fingerprint Thinning Algorithms*. Information Security South Africa Conference 2011, Johannesburg, South Africa, 2011.
- [24] ITO, K., NAKAJIMA, H., KOBAYASHI, K. et al. *A Fingerprint Matching Algorithm Using Phase-Only Correlation*. IEICE Trans. Fundamentals, 2004.
- [25] JAIN, A. K. *CSE 891 – Selected Topics: Biometrics* [online]. 2004 [cit. 2020-12-03]. Dostupné z: <https://is.muni.cz/el/1433/jaro2013/PV204/um/03bio/NonminutiaeRepresentations.pdf>.
- [26] MARCEL, S., NIXON, M. S. a LI, S. Z. *Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*. London: Springer, 2014. ISBN 978-1-4471-6523-1.
- [27] WERTHEIM, P. A. *The Murder of Sir Harry Oakes*. Fingerprint Whorld, The Internation Journal of The Fingerprint Society, 2000. ISSN 0951-1288.
- [28] DER MEULEN, L. J. van. *False Fingerprints – A New Aspect* [online]. Journal of Criminal Law and Criminology, Article 15, 1955 [cit. 2020-12-06]. Dostupné z: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=4355&context=jclc>.

- [29] BENNER, K. a LICHTBLAU, E. *U. S. Says It Has Unlocked iPhone Without Apple* [online]. 2016 [cit. 2020-12-06]. Dostupné z: <https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?hpw=&rref=technology&action=click&pgtype=Homepage&module=inline&region=bottom-well&WT.nav=bottom-well>.
- [30] RATHA, N. K., CONNELL, J. a BOLLE, R. *An Analysis of Minutiae Matching Strength*. LNCS, 2001. DOI: 10.1007/3-540-45344-X\_32.
- [31] MATSUMOTO, T., MATSUMOTO, H., YAMADA, K. et al. *Impact of Artificial „Gummy“ Fingers on Fingerprint Systems*. Electronic imaging 2002, International society for optics and photonics, 2002. DOI: 10.1117/12.462719.
- [32] AFP. *Woman fools Japan's airport security fingerprint system* [online]. 2009 [cit. 2020-12-06]. Dostupné z: <https://www.traveller.com.au/woman-fools-japans-airport-security-fingerprint-system-78rv>.
- [33] BBC. *Doctor' used silicone fingers' to sign in for colleagues* [online]. 2013 [cit. 2020-12-06]. Dostupné z: <https://www.bbc.com/news/world-latin-america-21756709>.
- [34] BVDA. *DFO: 1,8-diazafluoren-9-one* [online]. BVDA International BV [cit. 2021-01-09]. Dostupné z: <https://www.bvda.com/en/dfo>.
- [35] ESPINOZA, M., CHAMPOD, C. a MARGOT, P. *Vulnerabilities of fingerprint reader to fake fingerprints attacks*. Forensic Science International, 2010. DOI: 10.1016/j.forsciint.2010.05.002.
- [36] SPURNÝ, J., DOLEŽEL, M., KANICH, O. et al. *New materials for spoofing touch-based fingerprint scanners*. IEEE: Proceedings of Interntional Conference on Computer Application Technologies, 2015. DOI: 10.1109/CCATS.2015.57.
- [37] HARPER, W. W. *Fingerprint Forgery – Transferred Latent Fingerprints*. Journal of Criminal Law and Criminology, Article 7, 1937 [cit. 2021-01-10]. Dostupné z: <https://scholarlycommons.law.northwestern.edu/jcllc/vol28/iss4/7>.
- [38] STRADE. *Security Technology Research and Development: Výzkumná skupina na Fakultě informačních technologií, Vysokého učení technického v Brně* [online]. 2020 [cit. 2020-12-08]. Dostupné z: <https://strade.fit.vutbr.cz/cs/>.
- [39] DRAHANSKÝ, M., NÖTZEL, R. a FUNK, W. *Liveness Detection based on Fine Movements of the Fingertip Surface*. United States Military Academy, West Point, NY: IEEE, Workshop on Information Assurance, 2006. ISBN 978-1424-40130-7.
- [40] DRAHANSKÝ, M. a LODROVÁ, D. *Liveness Detection for Biometric Systems Based on Papillary Lines*. Busan, Korea: IEEE, Proceedings of Information Security and Assurance, 2008. DOI: 10.1109/ISA.2008.58.
- [41] ROWE, R. K. *A Multispectral Sensor for Fingerprint Spoof Detection* [online]. 2005 [cit. 2020-12-15]. Dostupné z: <https://www.fierceelectronics.com/embedded/a-multispectral-sensor-for-fingerprint-spoof-detection>.

- [42] LEE, C. D. *Finger-Prints Can Be Forged*. Journal of Criminal Law and Criminology, Article 16, 1934 [cit. 2020-12-16]. Dostupné z: <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=2507&context=jclc>.
- [43] CUMMINS, H. *Counterfeit Finger-Prints*. Journal of Criminal Law and Criminology, Article 15, 1934 [cit. 2020-12-16]. Dostupné z: <https://scholarlycommons.law.northwestern.edu/jclc/vol25/iss4/15/>.
- [44] CAPELLI, R., MAIO, D. a MALTONI, D. *Synthetic Fingerprint-Database Generation*. Quebec City: IEEE, 2002. DOI: 10.1109/ICPR.2002.1048096.
- [45] YANUSHKEVICH, S. N. *Synthetic Biometrics: A Survey*. The 2006 IEEE International Joint Conference on Neural Network Proceedings, IEEE, 2006. DOI: 10.1109/IJCNN.2006.246749.
- [46] CAPELLI, R. *SFinGe: Synthetic Fingerprint Generator*. University of Bologna, Italy: BioLab - Biometric Systems Lab, 2006 [cit. 2020-12-16]. Dostupné z: [https://www.researchgate.net/publication/226083265\\_Synthetic\\_Fingerprint\\_Generation](https://www.researchgate.net/publication/226083265_Synthetic_Fingerprint_Generation).
- [47] LEDDA, A. *Mathematical Morphology in Image Processing*. Universiteit Gent, 2007. ISBN 978-90-8578-127-1.
- [48] FAJMON, B., HLAVIČKOVÁ, I., NOVÁK, M. et al. *Numerická matematika a pravděpodobnost*. Ústav matematiky FEKT VUT v Brně, 2014.
- [49] ANSARI, A. H. *Generation and Storage of Large Synthetic Fingerprint Database*. Bangalore, India, 2011. Master's thesis. Department of Computer Science, Indian Institute of Science.
- [50] CHALOUPKA, R. *Generátor otisků prstů*. Brno, CZ, 2007. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: <https://www.fit.vut.cz/study/thesis/2480/>.
- [51] KANICH, O. a DRAHANSKÝ, M. *Simulation of synthetic fingerprint generation using Petri nets*. IET Biometrics, Institution of Engineering and Technology, 2017. DOI: 10.1049/iet-bmt.2016.0041. ISSN 2047-4938.
- [52] REISIG, W. *Petri Nets: Modeling Techniques, Analysis Methods, Case Studies*. Springer-Verlag, 2013. ISBN 978-3-642-33277-7.
- [53] IISC. *Anguli: Synthetic Fingerprint Generator* [online]. Indian Institute of Science [cit. 2020-12-21]. Dostupné z: <https://dsl.cds.iisc.ac.in/projects/Anguli/>.
- [54] MUHAMMAD, A. *A Computationally Efficient Framework for Large-scale Distributed Fingerprint Matching*. Witwatersrand, Johannesburg, 2017. Master's thesis. School of Computer Science and Applied Mathematics, University of the Witwatersrand. Dostupné z: [http://wiredspace.wits.ac.za/bitstream/handle/10539/23747/finalSubmission\\_447235.pdf?sequence=1&isAllowed=y](http://wiredspace.wits.ac.za/bitstream/handle/10539/23747/finalSubmission_447235.pdf?sequence=1&isAllowed=y).
- [55] RIAZI, M. S., CHAVOSHIAN, S. M. a KOUSHANFAR, F. *SYnFi: Automatic Synthetic Fingerprint Generation*. 2020. DOI: arXiv:2002.08900.

- [56] KANICH, O. a DRAHANSKÝ, M. *Use of Creative Materials for Fingerprint Spoofs*. IEEE Conference Publications IEEE Xplore, 2018 International Workshop on Biometrics and Forensics (IWBF), 2018. DOI: 10.1109/IWBF.2018.8401565.
- [57] BEVILACQUA, F. *Cvui* [online]. 2018 [cit. 2021-04-21]. Dostupné z: <https://www.bvda.com/en/dfo>.
- [58] FELKEL, P. *Křivky a plochy I*. Katedra počítačové grafiky a interakce, ČVUT FEL, Praha, 2016 [cit. 2021-04-20]. Dostupné z: [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwIj8vuEsY3wAhVF\\_qQKHeTrAr0QFjAGegQIBRAD&url=https%3A%2F%2Fwww.fel.cvut.cz%2Ffold%2F\\_media%2Fcourses%2Fb0b39pgr%2F10-krivky.pdf&usg=A0vVaw3XfQ2-AJlqve2q5i7B89sn](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwIj8vuEsY3wAhVF_qQKHeTrAr0QFjAGegQIBRAD&url=https%3A%2F%2Fwww.fel.cvut.cz%2Ffold%2F_media%2Fcourses%2Fb0b39pgr%2F10-krivky.pdf&usg=A0vVaw3XfQ2-AJlqve2q5i7B89sn).
- [59] ORAVEC, T. *Metodika měření kvality otisků prstu*. Brno, CZ, 2018. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: <https://www.fit.vut.cz/study/thesis/20656/>.
- [60] DEJMAL, D. *Analýza systémů pro měření kvality otisku prstů*. Brno, CZ, 2019. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: <https://www.fit.vut.cz/study/thesis/19344/>.
- [61] NEUROTECHNOLOGY. *VeriFinger SDK* [online]. 2021 [cit. 2021-04-26]. Dostupné z: <https://www.neurotechnology.com/verifinger.html>.