TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

Využití biometrie v praxi

Bakalářská práce

Studijní program: B6209 – Systémové inženýrství a informatika
Studijní obor: 6209R021 – Manažerská informatika

Autor práce: **Jakub Vlnatý**
Vedoucí práce: Ing. David Kubát, Ph.D., Ing.Paed.IGIP

Liberec 2018

TECHNICKÁ UNIVERZITA V LIBERCI
Ekonomická fakulta

Akademický rok 2017 / 2018

Zadání bakalářské práce

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jakub Vlnatý**
Osobní číslo:	E15000284
Studijní program:	B6209 Systémové inženýrství a informatika
Studijní obor:	B6209R021 – Manažerská informatika
Zadávající katedra:	katedra informatiky
Vedoucí práce:	Ing. David Kubát, Ph.D., ING.PAED.IGIP
Konzultant práce:	Ing. Vlastislav Cháb ŠKODA AUTO a. s., IT Business analytik IT bezpečnosti
Název práce:	**Využití biometrie v praxi**

Zásady pro vypracování:

1. Biometrické metody identifikace a jejich využití.
2. Důvěryhodnost identifikace otisků prstů.
3. Vyhodnocení testování.
4. Dotazníkové šetření.
5. Analýza výsledků a doporučení pro praxi.

Seznam odborné literatury:

MITRA, Sinjini a Mikhail GOFMAN. 2017. *Biometrics in a tada driven world: trends, technologies, and challenges.* Boca Raton: CRC PRess. ISBN 9781498737647.

HOUCK, Max M. 2016. *Forensic fingerprints.* San Diego: Academic Press. ISBN 0128005734.

SMEJKAL, Vladimír a Karel RAIS. 2013. *Řízení rizik ve firmách a jiných organizacích.* 4. vyd. Praha: GRADA Publishing. ISBN 978-80-247-4644-9.

RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. 2008. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích.* Praha: GRADA Publishing. ISBN 978-80-247-2365-5.

PROQUEST. 2017. *Databáze článků ProQuest* [online]. Ann Arbor, MI, USA: ProQuest. [cit. 2017-09-28]. Dostupné z: http://knihovna.tul.cz/

Rozsah práce:	30 normostran
Forma zpracování:	tištěná / elektronická
Datum zadání práce:	31. října 2017
Datum odevzdání práce:	31. srpna 2019

Technická univerzita v Liberci
Ekonomická fakulta

L.S.

prof. Ing. Miroslav Žižka, Ph.D.
děkan Ekonomické fakulty

doc. Ing. Klára Antlová, Ph.D.
vedoucí katedry

V Liberci dne 31. října 2017

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím mé bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum:

Podpis:

Poděkování

Rád bych poděkoval mému vedoucímu práce, panu Ing. Davidu Kubátovi, Ph.D, ING.PAED.IGIP, za jeho odborné rady a vedení při tvorbě bakalářské práce.

Rád bych také poděkoval celému oddělení FIG ve společnosti ŠKODA AUTO a.s., jmenovitě panu Vlastislavu Chábovi, Ing. Danielu Čepovi a Bc. Filipovi Štěrbovi za poskytnuté informace, cennou podporu a spolupráci.

Anotace

Cílem této bakalářské práce s názvem Využití biometrie v praxi je ukázat, jak jednoduché je zfalšovat otisk prstu cizí osoby. Bakalářská práce je rozdělena do části praktické, kde si představíme základy biometrie a biometrické metody. V druhé částí podrobíme falešný otisk prstu testům na mobilních zařízeních. Také zjistíme názor veřejnosti na biometrické metody a dodržování bezpečnosti. V závěru si analyzované výsledky zhodnotíme a pokusíme se odhadnout možnosti budoucího vývoje.

Klíčová slova

Biometrie, identifikace, otisk prstu, falšování, FAR, FRR

Annotation

The purpose of this bachelor´s thesis, The Use of Biometrics in Practice, is to show how simple it is to falsify the fingerprint of a stranger. The bachelor thesis is divided into a practical part, where we introduce the basics of biometrics and biometric methods. In the second part, we are subjected to a false fingerprint test on mobile devices. We will also discover public opinion on biometric methods and how precatious they are with passwords. In the end, we will evaluate the analyzed results and try to estimate the possibilities for future development

Key words

Biometrics, identification, fingerprint, falsification, FAR, FRR

Obsah

Seznam obrázků

Seznam grafů

Seznam tabulek

Vymezení pojmů

CAD	Computer aided design – 2D a 3D počítačové projektování
DOD	Ministerstvo obrany Spojených států amerických
FAR	False acceptance rate
FBI	Federální úřad pro vyšetřování
FERET	The Facial Recognition Technology
FRR	False recognition rate
FRVT	Face Recognition Vendor Test
NSTC	National Software Testing Conference
IAFIS	Integrated Automated Fingerprint Identification Systém
ICAO	Mezinárodní organizace pro civilní letectví
INCIST	International Commmittee for Information Technology Standards
NSTC	National Software Testing Conference

Úvod

Žijeme v době, kdy se biometrie stává součástí našeho každodenního života. Dnes jsou o každém z nás někde uchovávána data, ať už se jedná o stav bankovního účtu nebo informace osobního zaměření. Dat je čím dál více, proto je velmi důležité jejich zabezpečení. S postupným rozvojem digitalizace začíná být využívání biometrických systémů pro komerční účely naprosto běžnou věcí. Každý z nás je schopný si vytvořit bezpečné heslo, ale jak přístroj zjistí, jedná-li se skutečně o oprávněného uživatele, pokud je heslo odcizeno nebo prolomeno? S touto problematikou nám do určité míry může pomoci právě biometrie. Biometrie si zakládá na skutečnosti unikátnosti každého z nás. Každý člověk má jiný otisk prstu, DNA, duhovku a další biometrické údaje. Bohužel se však i tyto údaje se dají odcizit. Biometrie člověka zůstává po celý život téměř neměnná, proto odcizení těchto údajů může způsobit mnohonásobně větší škody než pouhé odcizení hesla, které je obměnitelné.

Cílem této práce je seznámení s biometrickými metodami a následné hlubší zaměření na nejpoužívanější technologii, otisk prstu. V dalším kroku se pokusíme vyrobit falešný otisk prstu, nejprve jednodušší metodou a následně složitější, a otestovat několik telefonů z hlediska bezpečnosti. Zanalyzujeme si povědomí lidí o biometrických metodách a jejich přesvědčení o bezpečnosti a vyhodnotíme si, jak námi testované mobilní telefony obstály v testech.

1. Biometrické metody identifikace a jejich využití

V poslední době se slovo identifikace stává velmi moderním termínem, který může nabývat mnoha různých významů. V minulosti byl tento pojem spojován s bezpečnostními a vojenskými aplikacemi. Z vědeckého hlediska byla identifikace spojována převážně s forenzními vědami a kriminalistikou.

1.1 Identifikace člověka

Lidstvo se s touto problematikou potýká již po staletí. Zmínky o různých pokusech identifikace pochází již ze starověkého Egypta. Jednalo se o měření těla, zaznamenávání mateřských znamének, jizev a jiných tělesných deformací. Touto metodou se ve starověkém Egyptě kontrolovala pracovní docházka pracovníků, aby jim na základě toho byla vyplacena správná mzda. Časem vznikla větší potřeba lépe identifikovat člověka. Jednalo se například o přístup k financím, datům, cestování do zahraničí nebo identifikaci při policejním vyšetřování. Jak uvádí kniha Biometrie a identita člověka: tak *identita osoby je definována jako „nezbytná podmínka bytí každé konkrétní osoby“.* (Rak Roman, 2008, str. 37)

1.1.1 Identifikace tokenem

Token má mnoho forem/podob, převážně s vícestupňovým zabezpečením. Pod vícestupňovým zabezpečením si můžeme představit kombinaci použití karty a zároveň otisku prstu, nelze se identifikovat pouze pomocí jednoho z těchto prvků. Tokeny jsou k dostání zejména od organizací, rychlé příklady tokenů jsou zaměstnanecké karty (firmy), pas, občanský průkaz, řidičský průkaz (úřady), kreditní karty (banky). (Gofman, 2017)w

1.2 Historie biometrie

Pojem „biometrie“ pochází z řeckého slova bio (život) a metric (porovnávat). Automatické biometrické systémy jsou dostupné pouze posledních pár desítek

let. Mnoho těchto automatizovaných technik je založeno na nápadech, které byly vymyšleny stovky nebo dokonce tisíce let zpátky.

Jedním z nejstarších a základních příkladů charakterizování člověka je jeho obličej. Už od počátku věků civilizace používaly lidský obličej na identifikování známých a neznámých jedinců. Tato jednoduchá činnost se stávala čím dál více komplikovanou v důsledku neustálého zvyšování populace a také cestování, díky kterému se mnoho nových jedinců dostávalo do dříve malých komunit. Koncept rozpoznávání člověka člověkem je možné také zpozorovat v behaviorální biometrii, jako je rozpoznávání chůze a hlasu. Jednotlivci používají tyto vlastnosti poněkud nevědomě, aby rozpoznali známé osoby na denní bázi.

Jiné charakterizování člověka bylo používáno napříč historií civilizací, uvedeme si některé jako příklady:

- V jeskyni, jejíž věk je odhadován minimálně 31 000 let, jsou stěny ozdobeny malbami, o kterých se předpokládá, že byly vytvořeny prehistorickým člověkem. Kolem těchto maleb můžeme nalézt několik otisků dlaně. Tyto otisky dlaně jsou považovány za jakýsi druh podpisu majitele.
- Záznamů o používání otisku prstu jako prostředku identifikace osob. Tyto záznamy se datují až k roku 500 před naším letopočtem. Byly to Babylonské obchodní záznamy, které byly zaznamenávány do jílových desek spolu s otiskem prstu.
- Joao de Barros, španělský průzkumník a spisovatel, napsal o raných čínských obchodnících, kteří používali otisk prstu na uzavření obchodních transakcí. Čínští rodiče používali otisk prstu i na rozlišování jednoho dítěte od druhého.
- V Egyptských dějinách je záznam o obchodnících rozlišovaných podle jejich „obchodních knížek“, které obsahovaly záznamy o jejich transakcích, aby bylo možné rozlišení mezi důvěryhodnými obchodníky a novými obchodníky na trhu.

V době industriální revoluce, která měla za následek rapidní růst měst a rozvoj efektivního farmaření, se začala rozvíjet potřeba více identifikovat lidi. Obchodníci a jiné autority byly postaveny před neustále se zvyšující mobilnější populaci, nemohli tak nadále spoléhat jen na své osobní zkušenosti a místní znalosti. Soudy v této době začaly kodifikovat pojmy spravedlnosti, které s námi přetrvávají až dodnes. Soudní systémy

začaly trestat mírněji pachatele, kteří neměli žádný trestní záznam a tvrději pachatele, kteří záznam již měli. Tím vznikla potřeba vytvoření systému, který bude zaznamenávat přestupky společně s identitou pachatele. První ze dvou přístupů byl Bertillonův systém měření různých rozměrů těla, který vznikl ve Francii. Tato měření byla vepsána do karet tříděné podle výšky, délka ramene nebo jakéhokoliv jiného parametru. Tento vědní obor se nazývá antropometrie.

Druhým, odlišným přístupem bylo formální používání otisku prstu policejními odděleními. Tento proces vznikl v Jižní Americe, Asii a Evropě. Koncem 18. století byla vyvinuta metoda na zaznamenávání otisku prstů, která umožňovala zpřesnění nebo rozšíření záznamů o určitém člověku, podobně jako Bertillonova metoda. Byla však založena na více individuální metrice – otisky prstů a záhyby prstů. První robustní systém na zaznamenávání otisku prstu vznikl v Indii, Azizulem Haqueem pro Edwarda Henryho, inspektora a generála policie v Bengálu. Tento systém se nazýval Henryho systém. Jeho určité variace jsou používány dodnes.

Skutečné biometrické systémy začaly vznikat v pozdní půlce 20. století, důsledkem vzniku počítačových systémů. Toto vznikající pole zaznamenalo největší skok v technologii v 90 letech 20. století a začalo se používat v každodenním světě po roce 2000. (Mayhew, 2012)

1.2.1 Časová osa biometrie

- **1858** - Zaznamenání prvního systému na zachycení obrazu ruky.
- **1870** - Alphons Bertillon vyvinul antropometrii, což je metoda na identifikování jedinců pomocí detailních záznamů jejich rozměrů těla, fyzického popisu a fotografií.
- **1892** - Francis Galton napsal detailní studii otisku prstu, ve které presentuje nový systém používající všech deset prstů. Charakteristiky, které Galton použil, se používají dodnes.
- **1896** - Henry vyvinul svůj klasifikační systém pro otisky prstů.
- **1903** - Státní věznice v New Yorku začínají používat otisky prstů.

- **1903** - Bertillonův systém se zhroutil. Dva muži, kteří byli později identifikováni jako identická dvojčata, byli oba posláni do nápravného zařízení v USA. Jejich těla měla stejné rozměry a identifikační prvky, které používal Bertillonův systém. Později byl tento příběh několikrát napaden jako falešný. Příběh byl však stále používán jako argument, že je Bertillonův systém neschopný rozeznat mezi jednovaječnými dvojčaty.
- **1936** - Předložení konceptu na používání oční duhovky jako formy identifikace.
- **1960** - Rozpoznávání obličeje se stává polo-automatickým.
- **1960** - První model akustické řečové produkce: Gunnar Fant, švédský profesor publikoval model popisující psychologické komponenty mluvené řeči. Jeho poznatky byly založeny na analýze rentgenových paprsků jedinců vytvářející určitý zvuk.
- **1963** - Hughes publikoval výzkum o automatizování otisků prstů.
- **1965** - Začíná výzkum na automatické rozpoznávání podpisu.
- **1969** - FBI se snaží, aby bylo rozpoznávání otisku prstu automatické.
- **1970** - Rozpoznávání obličeje podniká další kroky k automatizaci.
- **1970** - Behaviorální komponenty řeči jsou poprvé vymodelovány.
- **1974** - První komerční systém na ruční geometrii je dostupný.
- **1975** - FBI financuje vývoj senzorů a extrahováni miniatur.
- **1976** - První prototyp systému na rozeznání hlasu.
- **1977** - Vydání patentů na dynamické rozpoznávání podpisu a zaznamenání dynamické charakteristiky jedincova podpisu.
- **1985** - Návrh konceptu o jedinečnosti oka.
- **1985** - Vydání patentu na identifikaci pomocí ruky.
- **1986** - Publikování standardu pro výměnu otisků prstu.
- **1986** - Vydání patentu o použití duhovky pro identifikaci.
- **1988** - Použití prvního polo-automatického systému na rozpoznávání obličeje.
- **1991** - Detekce obličeje je průkopníkem a umožňuje rozpoznávání obličeje v reálném čase.
- **1992** – Založení Biometrického konsorcia v rámci vlády USA: Agentura národní bezpečnosti zahájila formování Biometrického konsorcia a pořádala její první poradu

v říjnu roku 1992. Konsorcium bylo pronajaté v roce 1995 radou bezpečností politiky. Tato rada byla v roce 2001 zrušena. Účast v konsorciu byla původně limitována jen na vládní agentury, členové soukromých firem a akademické obce byli limitování kapacitou pro návštěvníky. Konsorcium brzy na to expandovalo. Tyto komunity byly přirazeny do stálých účastníků, tím se rozvinulo mnoho pracovních skupin. Skupiny pracovaly na novém, či již běžícím standardním vývoji, testování, interní operativnosti a spolupracovaly s vládou. S velkým rozvojem biometrických aktivit začátkem 21. století, byly integrovány aktivity těchto pracovních skupin do jiných organizací (jako jsou INCITS, ISO a NSTC), z důvodu expandovaní a zrychlení jejich aktivit a dopadu. Konsorcium samo o sobě zůstává aktivní jako klíčové spojení a diskuzní fórum mezi vládou, průmyslem a komerční sférou.

- **1993** – Zahájení Programu na rozpoznávání obličeje (FERET).
- **1994** – Patentování prvního algoritmu na rozpoznávání duhovky.
- **1994** – Integrovaný automatický systém na rozpoznávání otisku prstu (IAFIS).
- **1994** - Testování systému na otisk ruky.
- **1994** - Implementace INSPASS. INSPASS (The Immigration and Naturalization Service Passenger Accelerated Service System) byla biometrická implementace, která umožnila cestovatelům obejít imigrační fronty ve vybraných letištích skrz USA do té doby, než byl v roce 2004 zrušen.
- **1995** - Prototyp na rozpoznávání duhovky je dostupný jako komerční produkt.
- **1996** – Použití ruční geometrie na Olympijských hrách. První velké veřejné použití ruční geometrie se stalo na olympijských hrách v Atlantě.
- **1996** - NIST (National Institute of Standards and Technology) pořádá každoroční zhodnocení hlasového rozpoznávání.
- **1997** – Zveřejnění prvního komerčního biometrického standardu.
- **1998** - FBI spouští COOIS (databáze forensní DNA): Combined DNA Index System digitálně ukládá, hledá a načítá markery DNA pro účely soudního práva. Sekvenování je laboratorní proces trvající mezi 40 minutami a několika hodinami.
- **1999** - Studie na kompatibilitu biometrie a strojů na dokumenty pro cestování je zahájena.
- **1999** - Hlavní komponenty IAFIS od FBI se stávají funkčními. IAFIS, systém FBI na rozpoznávání všech 10 prstů, začal fungovat.

- **2000** - První globální test na rozpoznávání obličeje (FRVT – Face Recognition Vendor Test 2000)
- **2000** - První výzkum popisující použití žilního řečiště na identifikaci osob.
- **2000** - Univerzita West Virginia zakládá biometrii jako studijní program.
- **2001** – Použití rozpoznávání obličeje při Super Bowlu v Tampě na Floridě. Systém na rozpoznávání obličeje byl implementován na Super Bowl v lednu roku 2001 na Floridě. Důvodem byla potřeba identifikace osob vstupujících na stadion.
- **2002** - ISO/IEC standardy pro využití biometrie: The International Organization for Standardization (ISO) zavedla ISO/IEC na podporu standardizace biometrických technologií. Rozvíjejí se standardy na podporu interoperability a výměnu dat mezi aplikacemi a systémy.
- **2002** – Založení Technická komise M1 pro biometrii. Tato technická komise se zodpovídá INCITSu (InterNational Committee on Information Technology Standards), akreditované organizaci, což usnadňuje vývoj standardů mezi akreditovanými organizacemi.
- **2003** - Vláda USA začíná koordinovat biometrické aktivity.
- **2003** - ICAO si propůjčuje nákresy na integrování biometrie do strojově čitelných cestovních dokumentů.
- **2004** - Spuštění programu US-VISIT. The United States Visitor and Immigrant Status Indication Technology je základním stavebním kamenem pro budoucí víza, vstupní a výstupní strategii.
- **2004** - DOD implementuje ABIS. The Automated Biometric Identification System je systém implementován DoD (Department of Defense) s cílem zlepšit schopnost vlády USA sledovat a identifikovat hrozby pro národní bezpečnost.
- **2004** - Prezident USA požaduje státní identifikační průkazy pro všechny federální zaměstnance a dodavatele.
- **2004** – Spuštění První automatizovaná databáze otisku dlaně v USA.
- **2004** - Velka výzva na rozpoznávání obličejů. FRGC (The Face Recognition Grand Challenge) je akce sponzorovaná vládou USA na vývoj algoritmů pro zlepšení identifikace určitých částí obličeje.
- **2005** - Patent USA na rozpoznávání duhovky vypršel.

- **2005** - Na biometrické konferenci je oznámena „duhovka v pohybu“. Systém, který dokáže sejmout obraz duhovky osob procházející vstupní bránou.
- **2008** - Vláda USA začíná koordinovat použití biometrické databáze.
- **2010** - USA začínájí používat biometrii na identifikaci teroristů. Otisky prstů z důkazů shromážděných na předpokládaném místě pro plánování 11. září byly pozitivně přiřazeny k osobě zadržené ve věznici Guantánamo.
- **2011 –** Použití Biometrické identifikace na identifikaci těla Osama bin Ladena. CIA použila technologii rozpoznávání na identifikování pozůstatků Osama Bin Ládina. Společně s technologií DNA došlo k identifikaci s 95% jistotou.
- **2013** - Apple zabudovává čtečku otisku prstů do chytrých telefonů pro běžné zákazníky. Touch ID je funkce na rozpoznávání otisků prstů navržená a vydaná společností Apple Inc., která byla k dispozici na iPhonu 5S, 6, 6 Plus, iPad Air 2, iPad Mini 3. Touch ID je integrováno do iOS, což umožňuje svým uživatelům odemknout své zařízení a také nakupovat v různých obchodech digitálních médií Apple (iTunes Store, App Store, iBookstore). Dále také umožňuje ověřovat Apple Pay online nebo v jiných aplikacích. Při ohlášení této funkce společnost Apple uvedla, že informace o otiscích prstů jsou ukládány lokálně na bezpečném místě, než aby byly vzdáleně uloženy na serverech Apple, nebo iCloud, což je pro externí přístup velmi obtížné. (Mayhew, 2012)

1.3 FAR a FRR

1.3.1 FAR

„The false acceptance rate“ neboli FAR poměřuje pravděpodobnost biometrického zabezpečení, že povolí přístup osobě, která povolení nemá. FAR je většinou stanoveno poměrem mezi špatnými přístupy a počtem žádostí o identifikaci.

$$FAR = \frac{Celkový\ počet\ chybných\ přijmutí}{Celkový\ počet\ pokusů\ oprávněných\ osob}$$

V komerční sféře ochraňující jakýkoliv osobní majetek je FAR nežádoucí. Pokud se na tuto problematiku podíváme z pohledu kriminalistiky, tak FAR vyjadřuje míru odsouzení nesprávných osob. FAR se zaměřuje na bezpečnost systémů, čím menší FAR, tím je systém bezpečnější. FAR také úzce souvisí s prostředky a znalostmi pachatele, který se snaží systém překonat. (Bayometric, 2018)

1.3.2 FRR

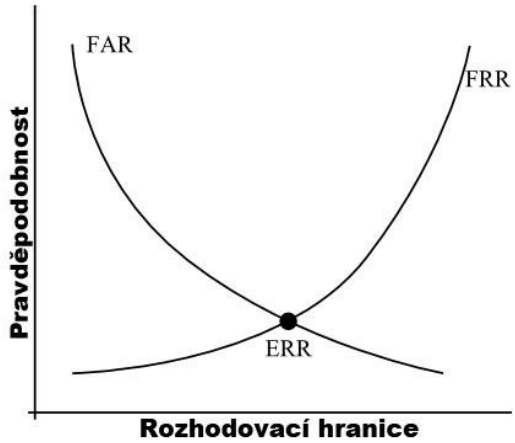
„The false rejection rate“ neboli FRR je poměr pravděpodobnosti, kdy biometrické zabezpečení špatně odmítne přístup autorizované osobě. FRR je většinou stanoveno poměrem mezi špatným rozpoznáním uživatele a počtem žádostí o identifikaci.

$$FRR = \frac{Celkový\ počet\ chybných\ odmítnutí}{Celkový\ počet\ pokusů\ oprávněných\ osob}$$

Čím menší FRR vypočítáme, tím menší je šance aby, oprávněný uživatel měl odmítnutý přístup do systému. Pokud bude mít nějaký biometrický prvek FRR vysoké, stává se nepoužitelným pro komerční účely, jelikož spousta uživatelů požaduje pohodlnost a tato skutečnost by je spíše frustrovala. Pokud se naopak podíváme na systémy používané v kriminalistice mají FRR vyšší. Potřebují, aby jejich systém byl naprosto bezchybný a nedocházelo k situacím, kdy systém není schopen identifikovat pachatele. (Bayometric, 2018)

1.3.3 **FAR-FRR**

Vezmeme-li FAR a FRR dohromady a převedeme je do komerční sféry, tak bychom chtěli biometrickou ochranu spojenou s aplikací, která má obě veličiny rovné nule. Obě veličiny můžeme přirovnat ke křivkám, které jdou proti sobě. Pokud si budeme přát nulové FAR, musíme ho vykompenzovat vysokou hodnotou FRR a pak bude přístup do systémů složitější a naopak.



Obrázek 1: Autentizační hranice
Zdroj - (Biometric Line, 2018)

Z obrázku grafu je patrné, že pokud chceme dosáhnout nulové hodnoty FAR, tedy eliminovat jevy neoprávněných přístupů do systému, pak zároveň musíme vzít v potaz jevy vzniklé vysokým FRR. Takto nastavený systém bude velice „přísný“ a shoda šablony se

vzorem bude muset být dokonalá. Bohužel v mnoha případech je téměř nemožné udělat dokonalou shodu se šablonou, proto bude docházet k mnoha pokusům o autentizaci.

Máme zde také nový prvek, ERR (Equal Error Rate). Jeho funkcí je poukázání na rovnost obou zmíněných křivek pravděpodobnosti. (Rak Roman, 2008)

1.3.4 Identifikace a verifikace

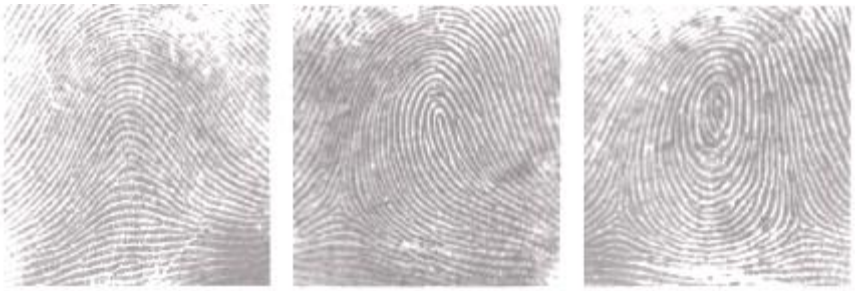
Biometrický systém na rozpoznávání může běžet na 2 různé módy. Identifikace nebo verifikace. Identifikace je proces, kdy se snažíme zjistit identitu osoby zkoumáním biometrického vzorce vypočítaného pomocí biometrických vlastností osoby.

Při procesu identifikace je systém testován se vzorci velkého počtu osob. Pro každou osobu je vypočítána biometrická šablona. Vzorec bude identifikován a přiřazen ke každé známé šabloně, která se buď velice přibližuje nebo je naprostou shodou mezi vzorem a šablonou. Systém poté přiřadí vzor k osobě s nejvíce podobnou biometrickou šablonou. Aby falešné otisky nebo otisky, které nejsou v systému, nebyly identifikovány tak jednoduše, je nutné, aby podobnost dosahovala určité úrovně. Pokud úroveň podobnosti není dosažena, vzor je odmítnut.

Při verifikaci je identita uživatele identifikována např. pomocí karty. Vzor této osoby se pak porovnává pouze s osobní šablonou té osoby. Podobně jako u identifikace, kontroluje se určitá úroveň podobnosti, aby byl umožněn přístup. (Gofman, 2017)

1.4 Otisk prstů

Otisk prstu je určitý vzor záhybů na povrchu prstu. Konečné body prstu a body přechodů se nazývají markanty (speciální útvary na otisku prstu, které tvoří papilární linie). Všeobecně uznávaným předpokladem je unikátnost detailního vzorce každého prstu. (Houck, 2016)



Obrázek 2: Otisky prstu
Zdroj: (Houck, 2016, str. 20)

1.4.1 Proč používat otisk prstu

Otisk prstu je považován za nejlepší a nejrychlejší metodu pro biometrickou identifikaci. Jeho použití je relativně bezpečné, je unikátní pro každou osobu a po dobu života se nemění. Implementace do systému na rozeznávání otisků prstů je levná, jednoduchá a dost přesná na to, aby ochrana byla uspokojivá.

Rozpoznávání pomocí otisku prstů je široce rozšířeno a používáno, jak ve forenzní, ale i civilní oblasti. Pokud tuto metodu porovnáváme s ostatními biometrickými prvky, otisk prstů se osvědčil jako technika s největším podílem na trhu. Vysloužila si to především díky své rychlosti a nízké spotřebě energie v porovnání ostatními metodami.

1.4.2 **Snímací technologie**

Snímací technologie je technikou, která se používá pro snímání otisků prstů využívané zejména v komerční sféře. Technika snímání a její možnosti se dají rozdělit do dvou kategorií:

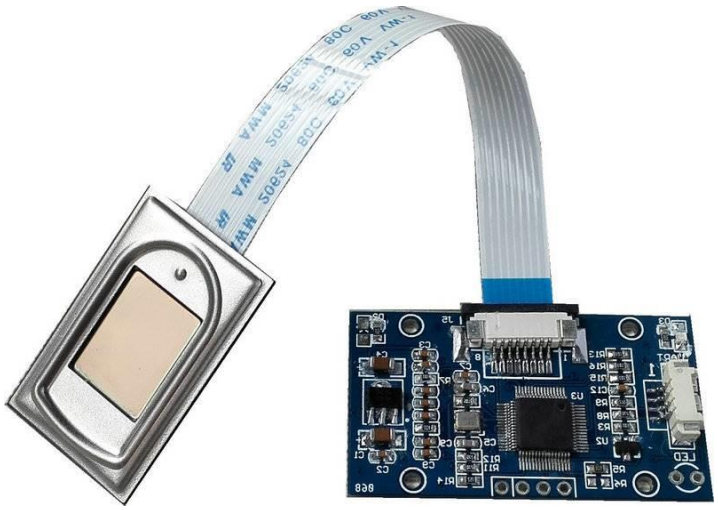
1. Kontaktní,
2. Bezkontaktní.

Nejvíce používanou technologií je kontaktní, nicméně v poslední době se dostává do popředí i technologie bezkontaktní, zejména kvůli hygienickým důvodům.

Optické snímače jsou založeny na nasnímání otisku prstu, který se přiloží na průhledný povrch, pod kterým je ukrytý senzor na snímání. Poté vrstva fosforu ozáří veškerý prostor, námi přiloženého otisku prstu. Odražené světlo poté proniká luminoforní úrovní k CCD maticovému detektoru. Paprsky tohoto snímače zaznamenávají pouze papilární linie, nikoliv prohlubně, tím vzniká vysoce kvalitní otisk prstu. Kvalitu považujeme za jednu z výhod, stejně jako neovlivnitelnost okolního prostředí. Mezi nevýhody patří nekvalitní snímaní otisku prstu, pokud jsou papilární linie znečištěny. Zároveň jsou optické snímače větších rozměrů, proto jsou nepoužitelné v přenosných zařízeních. Další nevýhodou je možnost zachycení stopy předchozího otisku současně vytvářeným otiskem. Typ tohoto snímače se řadí mezi bezkontaktní.

Obrázek 3: Optický snímač
Zdroj - (INJES Technology Co.,Ltd, 2017)

Kapacitní snímače jsou založeny na využití rozdílu kapacity mezi deskou snímače a povrchem prstu. Velkou roli zde hraje rozdíl mezi odporem papilárních linií a prohlubní. Snímač tvoří dvě desky. Jednou je deska kapacitoru, druhá deska představuje jednotlivá místa pro prst. Otisk se poté z pixelů získává v digitální formě. Pro načtení obrazu se prst přiloží na citlivou plochu, která je osazena velkým množstvím elektrod a ty poté převedou kapacitně otisk prstu na digitální obraz.



Obrázek 4: Kapacitní snímač
Zdroj - (Grow Tech Store, 2018)

Mezi výhody patří malý rozměr, vysoká kvalita a zároveň jednoduchý princip funkčnosti. Velkou nevýhodou je doba životnosti snímače.

Jelikož vlivem statické elektřiny dochází ke zničení snímače je nutné snímače měnit v rozmezí 3 let.

Elektroluminiscenční biometrické snímače jsou založeny na využívání speciální vrstvy reagující na tlak, který je způsobený luminiscenčním efektem. Aby přístroj správně fungoval, je nutné zajištění přístupu ke světlu. Funguje zde tzv. eliminující vrstva filtrující světlo z míst, kde na ni tlačí papilární linie. Zpracování otisku prstu je zajištěno pomocí fotodiod a výstup je v digitální podobě. Terminál má miniaturní rozměry, které nabízejí velice dobrý poměr poskytovaného rozlišení v poměru k pořizovací ceně. Terminál dovede rozeznat otisk při srovnatelné kvalitě, extrémně suché otisky nejsou také překážkou. Figurují

zde však nevýhody v konstrukčním řešení, otisky mají menší odolnost proti mechanickému poškození a jsou náchylné na znečištění vodou či prachem.

Teplotní biometrické snímače jsou vybaveny malým citlivým čipem. Čip snímá rozdíl teplot mezi jednotlivými papilárními liniemi a prostor mezi nimi. Abychom dostali obraz otisku prstu, je nutné přejíždět prstem přes citlivou plochu. Na výstupu získáme obraz otisku ve formě digitálních pásů, ty se následně skládají do výsledného obrazu otisku. U teplotní biometrie převažují nevýhody značně nad výhodami. Nevýhodami jsou nízká kvalita snímků, díky které vzniká problém pro zpracování markant, dále otisk prstu snímaný pohybem, neboť je pokaždé sejmuta jiná část prstu. Z těchto snímků je velmi obtížné vytvořit databázi otisků. Metoda použití teplotních snímačů je také nevhodná v přístupových systémech kvůli jeho špatné kvalitě obrazu.

Radiofrekvenční biometrické snímače spočívají v připojení generátoru střídavého signálu na 2 rovnoběžné desky, jedna deska je plocha snímače a druhá plocha je pro otisk prstu. Vlnová délka je mnohem delší než délka desek. Složka elektrického pole je bez pole magnetického. Pokud tedy na jedné z desek bude náš otisk prstu, tvar pole bude změněn a bude kopírovat tvar papilárních linií (výběžky a prohlubně prstu). Vodivého prostředí mezi prstem a plochou docílíme pomocí vodivé plochy kolem každého snímače. Suché prsty v tomto případě nepředstavují překážku, jelikož pracujeme s živou tkání těsně pod povrchem pokožky. Zvlnění pole je způsobeno přiložením otisku prstu, které poté dopadá na senzory s rozdílnou velikostí signálu. Výběžky mají větší signál, prohlubně signál nižší. Senzory měří rozdílnou permitivitu mezi výběžky a prohlubněmi. Tato technologie je odolná vůči nečistotám, je přizpůsobivá stavu kůže (vysušená pokožka nebo lehce poškozená kůže). Pořizujeme několik snímků, které se optimalizují do té doby, dokud není snímek přesně přijat nebo odmítnut. (Line, 2012)

1.4.3 Využití otisku prstu

Vezmeme-li biometrii jako celek, její jedinečnost a stálost, jí umožňuje pronikat stále do více vrstev ve společnosti. Využití začíná u kriminálních služeb, pokračujících přes bankovní sféru do komerčních systémů.

1.4.4 Bezpečnost uložení otisku prstu

Stále dochází k případům uniknutí nebo ukradení otisku prstu. Například v roce 2015 na konferenci Black Hat Security výzkumníci Tao Wei a Yulong Zhang odhalili chyby v systému Android. Zneužitím těchto chyb bylo možné odcizit uložené otisky z telefonu, který ani nemáte v ruce. Tento útok byl označen jako „fingerprint sensor spying attack“. Firmy se snaží co nejlépe zašifrovat odebrané otisky od uživatelů a tím pádem zabránit jejich odcizení. (PROQUEST, 2015)

1.5 Geometrie ruky

Ruční geometrie je další oblastí biometrických systémů. Zahrnuje ruku a prsty, ale nezískává z nich otisky. Uživatel položí ruku na povrch snímače, který má umístěné vodící tyče pro správné umístění rukou. Tyto tyče jsou mezi prsty před zahájením čtecího procesu. Nicméně, geometrie prstů používá pouze 3 nebo 4 prsty. Prostorové geometrické měření rukou a prstů se provádí tak, že spodní úroveň dlaně je jedinečným znakem každého jednotlivce. Tento systém má nižší míru přesnosti než jiné biometrické systémy, avšak má velmi nízkou falešnou míru odmítnutí. Mnoho uživatelů považuje tento systém za snadnější a tím pro uživatele přijatelnější. Tato technologie se úspěšně používá v různých oblastech pro fyzickou kontrolu přístupu, například systém pro docházku zaměstnanců letiště v San Francisku obsahující zhruba 3000 přihlášených uživatelů najednou. Tuto biometrii můžeme aplikovat jak v malých, tak velkých obchodních kancelářích. Přestože používáme ruční geometrii již v mnoha oblastech, tato technologie se nepovažuje za zcela vhodnou pro identifikační aplikace. Její stupeň rozlišení uživatelů není ještě na přijatelné úrovni. Slabé stránky zahrnují například stopy po bižuterii. Otlačený prst od prstýnku může způsobit potíže při shromažďování šablon. Další slabou stránkou je velikost šablony, zřídka ji můžeme použít ve všech vestavěných systémech. Neustálý posun vývoje by mohl pomoci znovuzavedení této technologie. (Gofman, 2017)

Obrázek 5: Snímač geometrie ruky
Zdroj - (Synerion, 2014)

1.6 Oční duhovka

Jedinečnost duhovky je všeobecně dobře známa. Oční duhovka je nejpřesnější biometrickou šablonou pro ověření. Z tohoto důvodu se více průmyslových odvětví zaměřilo na vývoj kvalitních produktů pro kontrolu duhovky a ověřování její totožnosti. Kromě reakce duhovky na světlo, není duhovka ovlivněna žádnými jinými environmentálními a okolními faktory. Považujeme ji za jeden z neměnných orgánů. Vzory duhovky jsou vytvořeny v naprosté náhodnosti a mají stabilní náhodnou strukturu. Žádné dva vzory duhovky se navzájem neshodují, dokonce i pravé a levé oko jedné osoby je jiné. Pro účel skenování můžeme použít digitální fotoaparát disponující zařízením s vázanými náboji (CCD), které využívá blízké infračervené světlo a viditelné světlo pro zachycení vysokého kontrastu s výrazně jasným obrazem duhovky. Duhovka se změní na černou barvu, aby kamera mohla určit a rozlišit duhovku od zorničky. Jakmile se fotoaparát zaměří na duhovku, najde střed zorničky, okraj zorničky, okraj duhovky, oční víčka a řasy. Poté se vše zkonvertuje na digitální data a použije jako šablona. Tyto šablony poskytují až 200 referenčních bodů pro porovnání ověření. (Gofman, 2017)

Tuto formu biometrie již v současnosti běžně používáme. Bankomaty ATM, fyzický přístup na letiště, velkoobchody, některé hotely aplikovali skenování duhovky do autentizaci osob. Nejen průmyslová odvětví se stále častěji zabývají přijetím těchto systémů.

Bohužel, žádný systém nemůže být naprosto bezchybný, rozpoznávání duhovky má následující slabiny:

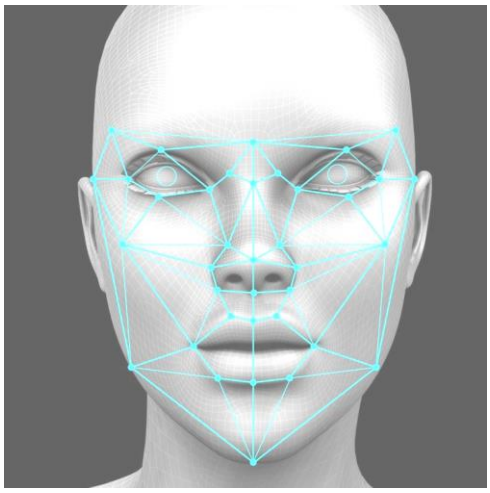
1. Detailní a ostrý obraz můžeme použít k obejití skeneru.
2. Kód duhovky může být zpětně zrekonstruován na vytvoření šablon.
3. Nastavení skenovacích zařízení je drahé.
4. Jasné světlo snižuje kvalitu obrazu.
5. Skenování může být zakryto řasami, čočkami nebo odrazy.

Jako příklad uvádíme výzkumného pracovníka pana Galballyho, který dokázal vytvořit duhovku, jež prolomila 80 % komerčně dostupných rozpoznávacích systémů na duhovku. Letiště v Birminghamu a Manchesteru přestala používat systém na rozpoznání duhovky, protože ověření není až tak rychlé, důsledkem byla ztráta 9 miliónů liber.

1.7 Rozpoznávání obličeje

O rozšíření této technologie se v roce 2011 postarala sociální síť Facebook, která implementovala rozpoznávání podle obličeje na svých 900 milionů uživatelů. Na základě objemnosti těchto dat se algoritmy tohoto systému zjednodušily. Ve světě se tato technologie používá nejvíce k bezpečnostním účelům, napomáhá k vyhledávání hledaných osob nebo nebezpečných jedinců či skupin. Se stále rostoucím počtem moderních kamer s vysokým rozlišením je možné rozpoznat obličej i na velké vzdálenosti. Jsme také schopni rozpoznat neúplný obličej, či z části začerněný. Pokud vezmeme rozpoznávání obličeje jako celek, můžeme mluvit o metodách či jejich kombinacích, nejznámějšími jsou 2D a 3D rozpoznávání. Základní 2D geometrie změří vzdálenost mezi nosem, ústy, očima a jinými rysy. Došlo se k závěru, že tato technologie neověřuje identitu osob dostatečně, tím navázala na tuto technologii 2D geometrie i 2D statistika, ve kterých dochází ke komplnějším výpočtům. Využije tvorby abstraktního obličeje, který je následně porovnán s kontrolovaným. 2,5D kombinace dokáže přidat k předchozím metodám ještě prostorový

efekt, jenž zvládne eliminovat některé pokusy o obelstění systému přiloženou fotografií. Nejvíce vyvinutou metodou je 3D rozpoznávání. Pomocí laserových snímačů zaznamená obličej a není závislá na okolním prostředí nebo poloze. Pokud chceme dosáhnout vysoké úrovně bezpečnosti, doporučujeme používat tento systém v kombinaci s jinou metodou, jako je snímání duhovky, tepelná obraz tváře a jiné. (Gofman, 2017)



Obrázek 6: Scan obličeje
Zdroj - (Tech This Out News, 2018)

1.8 Žilní řečiště

Metoda žilního řečiště používá záření blízké infračerveným paprskům, které dokáží zachytit obraz žilního řečiště. Nabízí ohromnou míru přesnosti, která je 0,01% FRR a méně než 0,00008% FAR. Tato technologie je již od roku 2004 využívána mnoha bankami v Japonsku pro identifikaci a ověřování. Vzor žilního řečiště je jedinečný pro každého jednotlivce, včetně dvojčat. Neexistuje téměř žádná šance krádeže jakéhokoliv vzoru, vzhledem k tomu, že žíly je možné získat pouze dvěma způsoby fotografování žil. Odraz a přenos. Podle společnosti Fujitsu: „Metoda reflexe osvětluje dlaň a fotografuje světlo, které se odrazilo od dlaně, zatímco metoda přenosu fotografuje světlo, které prochází přímo pod rukou. Oba tyto typy zachycují blízké infračervené světlo, využívané pro identifikaci.“ Navzdory minimální chybovosti vykazuje rozpoznávání žil také určité vady, jako je zrnění v zachyceném obraze

způsobené kalibrací fotoaparátu, vlhkostí, tepelným zářením těla, teplotou těla, žílami blízkými k povrchu kůže a jiné. (Gofman, 2017)

Obrázek 7: Scan žilního řečiště
Zdroj - (Cui, 2018)

1.9 Dynamická biometrie

Dynamika psaní vyjádřená psaním na klávesnici, je oblast biometrie, kde systém zkoumá jednotlivce pomocí jeho psaní. Systém je velice podobný dynamickému podpisu, testuje rychlost a tlak aplikovaný uživatelem při vytahování určitých klíčů, čas strávený uživatelem při psaní určitého slova či hesla a čas mezi zadáváním určitých kláves. Tato technologie může být úspěšně použita pro ověřování totožnosti a poskytování přístupu uživatelům. I když považujeme tuto technologii za biometrickou, její rozlišovací způsobilost je stále předmětem zdokonalování. Slabou stránkou je software se záznamem stisků kláves, který tak můžeme použít k obejití bezpečnostního systému.

1.10 DNA

Pokud vezmeme DNA (deoxyribonukleovou kyselinu) jako celek, tak 99,9% mají všichni lidé shodné. Právě ta jedna zbývající setina je pro nás důležitá. Uvádí se, že dva nepříbuzní

lidé mají v DNA až deset miliónů rozlišností, to neznamená, že počet možností je právě deset miliónů. Mohou nabývat různých hodnot, z toho tedy vyplývá, že ve skutečnosti je jich o mnoho více. Jakákoliv buňka s jádrem tvoří vzorek. Například jedna bílá krvinka, která obsahuje krev nebo sliny nebo kořínek vlasů, jelikož samotný vlas nemá buňky s jádrem. Můžeme použít i buňky bez jader, ale musí být z kostí nebo zubů.

Tato metoda je velice spolehlivá, zároveň však velice nákladná a náročná na provedení. Pokud bychom chtěli tuto metodu použít v průmyslovém prostředí, musíme vzít v potaz navýšení nákladů na realizaci kvůli časové náročnosti.

Kritici této metody také upozorňují na relativně snadné získávání stop z vlasů a slin. Z DNA lze také zjistit mnohem více informací, náchylnost k nemocem, dědičné dispozice a podobně. Tyto informace jsou pro potřeby biometrie nežádoucí. Musíme také počítat s transplantacemi orgánů, které také ovlivňují výsledky DNA. Negativita zde bohužel značně převažují nad pozitivy, výsledkem je nepoužitelnost v komerčním prostředí. (Rak Roman, 2008)

1.11 Mozkové vlny

Základní mozkové vlny mohou být pozměněny pomocí konzumace drog a jiných látek. Avšak signálem používaným k rozpoznávání v biometrii jsou základní mozkové vlny, které není možné pozměnit jakýmkoliv způsobem. Tato technologie je dobře použitelná pro tělesně postižené, například v případě amputace ruky nebo jiných anomálií. Jak uvádí Gunkleman, „Mozkové vlny se rozpínají do určitých vzorů. Kdybychom byli schopni identifikovat alespoň jeden vzor, který je unikátní, neměnící a monotónní, pak bychom měli biometrickou ochranu dominantní nad všemi ostatními.“ Bohužel stále ještě existuje obrovská neprozkoumaná oblast výzkumu, proto nemohou být mozkové vlny používány jako biometrická ochrana. Metoda však stále zůstává jednou z možností biometrické autentizace v budoucnosti. Protokoly a algoritmy na rozpoznávání jsou stále ve fázi vývoje a nejsou uspokojivě otestovány, abychom byli schopni mluvit o prokázaných výhodách a nevýhodách této metody.

1.12 Rozpoznávání tělesných pachů

Každý z nás jistě ví, že psi jsou používání k identifikaci osob na základě jejího tělesného pachu. Digitalizace všech věcí se však rapidně posouvá dopředu a sensory vyvinuté Universitou v Cambridge jsou schopny zachytit a analyzovat čichové vůně lidského těla z nepotících se částí těla jako je ruka, které jsou potom extrahovány biometrickým systémem a použity jako šablona a autentizační prostředky. Rozpoznávání tělesných pachů je jedním z mála biometrických prvků, které nebyly naplno prozkoumány. Rozdělení jejich definitivních kladů a záporů stále čeká na potvrzení od výzkumných pracovníků.

1.13 Rozpoznávání uší

Francouzská společnost ART Techniques vyvinula „Optophone“, který je velikostně srovnatelný s telefonem. Skládá se ze dvou hlavních komponentů, světelného zdroje a kamer. Každý člověk má svůj unikátní vzor uší, strukturu kostí, velikost a podobně. Na rozdíl od mnoha biometrických systémů, kdy je nutný přímý kontakt, tato technologie ho nevyžaduje. Je to možné díky detektoru Optophone.

Vzhledem k tomu, že existuje řada detailních vlastností, které jsou již přítomny v uších jednotlivců, mohou být zjištěné ušní vzory shromažďovány a porovnávány s biometrickými šablonami. Celkový proces je podobný procesu u systémů otisků prstů a funguje na bázi identifikace funkčních bodů. Tento biometrický systém založený na uchu je velmi slibný v různých aplikacích, zejména v situaci, kdy jednotlivec má vážný stupeň popálení na obličeji a na rukou. V této situaci může být ušní vzor užitečný k identifikaci osoby. V neposlední řadě mohou být ušní vzory použity společně s dalšími biometrickými modalitami, aby byla zajištěna přesnost ověřování. (Gofman, 2017)

1.13.1 Obrázek ucha

Tato metoda zahrnuje porovnávání obrazů uší. Metoda se vyznačuje velkou chybovostí, pokud první bod není správně přiřazen, celá procedura selže. V roce 1999 byla navrhnuta nová metoda porovnávání, která zahrnuje získání celého ucha, vrásek a podobně.

1.13.2 Ušní znaky

Znaky můžeme získat z videí, fotografií, přitisknutím ucha na materiál, na kterém je možno otisknout ušní znaky, například sklo. Tato metoda je považována za nespolehlivou, proto není používána.

1.13.3 Tepelný obraz ucha

Záměrem této metody je minimalizovat chybovost způsobenou vlasy na uchu. Termální obraz používáme k ulehčení rozpoznávání masek. Různé barvy jsou používány pro různé části ucha. Lidské ucho bohužel stárne a gravitace může způsobit roztažení ucha, což způsobuje nepřesnou identifikaci.

2. Důvěryhodnost identifikace otisků prstů

Tato část se zabývá bezpečností biometrické metody – otisk prstu. Zaměřil jsem se na tuto biometrickou metodu, protože je nejpoužívanější na světě. Kvůli tomuto faktu si zaslouží největší pozornost a také kritiku.

V úvodní části se zaměřím na potřebné materiály k vytvoření falešných otisků prstu, následnou výrobu a výsledný výrobek. Rozebereme si dvě metody, které se setkaly s nejvyšší úspěšností.

2.1 Metoda I

Zde si popíšeme, jak vytvořit otisk prstu, pokud máme k dispozici prst fyzicky.

2.1.1 Potřebné materiály

Abychom vůbec mohli začít, budeme potřebovat osobu, která nám otisk poskytne, nebo použít vlastní otisk na testování. Nejlépe osvědčenou metodou, která byla zároveň nejjednodušší, bylo použití tavné pistole na formu otisku a vytvoření odlitku pomocí lepidla Herkules.

Následující tabulka sleduje cenu potřebných materiálů k výrobě. Celková cena je 399 Kč.

Tabulka 1: Cena potřebných materiálů metody I

Název	**Cena (Kč)**	**Množství**
Tavná pistole	200,-	1 ks
Herkules	27,-	30 g
Náplň do tavné pistole	169,-	1 kg

2.1.2 **Výroba**

Nejprve musíme udělat formu na otisk prstu, ten dostaneme pomocí tavné pistole. Roztavené lepidlo naneseme například na papír či plastovou fólii. Musíme počkat alespoň 2-3 minuty před otisknutím prstu, kvůli teplotě lepidla. Pozor, pokud počkáme až moc dlouho, lepidlo ztvrdne a otisk již nebude kvalitní. Přitiskneme požadovaný prst a ponecháme ho v lepidle alespoň 10 sekund. Doporučuji udělat alespoň 5 těchto odlitků, protože se občas některý nepovede.

Než se pustíme do dalšího kroku, kterým je odlitek otisku, je nutné počkat na zaschnutí lepidla. 15 minut je dostatečná doba. Následně lehce potřete otisk lepidlem Herkules, je důležité, aby vrstva nebyla příliš tlustá. Zároveň s otiskem jednejme velice opatrně, velmi snadno lze roztrhnout. Tenká vrstva lepidla umožňuje obejít kontrolu živosti některých čtecích zařízení. Lepidlo Herkules necháme zaschnout, dokud není vidět žádná bílá část lepidla. Čas potřebný pro zaschnutí bude mezi 4 až 8 hodinami.

2.1.3 **Výsledný výrobek**

S výsledným otiskem je nutné zacházet opatrně, aby nedošlo k jeho narušení nebo roztržení. Z tohoto důvodu připravujeme více forem.

2.2 Metoda II

Tato metoda je mnohem složitější než metoda I. Jedná se metodu, kdy vytváříme otisk prstu pomocí fotografie prstu určité osoby.

2.2.1 Potřebné materiály

Tento otisk je možné provést dvěma způsoby. Jednodušší verzí je použití mobilního telefonu, přiložit ho k prstu požadované osoby. Tento test jsem provedl s fotoaparátem rozlišením 13 megapixelů v mobilu, ale samozřejmě lze provést za použití drahého objektivu a fotoaparátu. Pokud budeme mít k dispozici i velmi drahý objektiv (pořizovací ceny se pohybují od 50.000,-), můžeme tuto fotku pořídit i bez vědomí fotografované osoby.

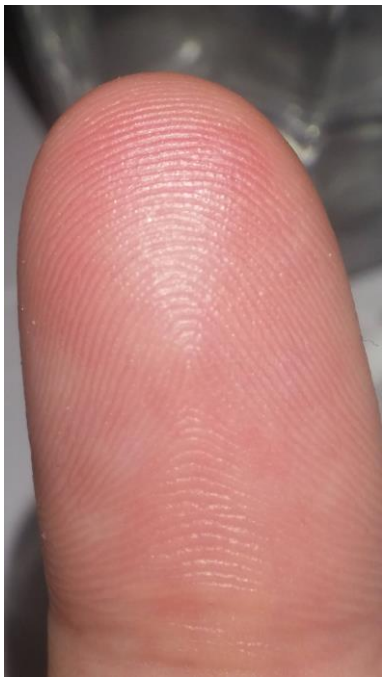
Tabulka 2: Cena potřebných materiálů metody II

Název	**Cena (Kč)**	**Množství**
Fotoaparát Canon 7D	39 490,-	1 ks
Objektiv Sigma 105mm f/2,8 makro	12 000,-	1 ks
Fotopolymerová tiskárna (Formlabs Form 2)	102 838,-	1 ks
Náplň do tiskárny (ABS plast)	363,-	0,5kg
Herkules	27,-	30g
Software (CAD + Photoshop)	8 267,-	-
Celkem	**168 985,-**	-

2.2.2 **Výroba**

Pokud budeme otisk vyrábět pouze pomocí mobilního telefonu, náklady jsou mnohem nižší. Podmínkou je pořízení fotky prstu ze vzdálenosti cca 30 cm a za dobrých světelných podmínek. Pokud budeme preferovat jednodušší práci s otiskem, zvolíme fotoaparát s objektivem na makro fotografie.

Obrázek 8: Fotografie otisku fotoaparátem
Zdroj – Vlastní tvorba



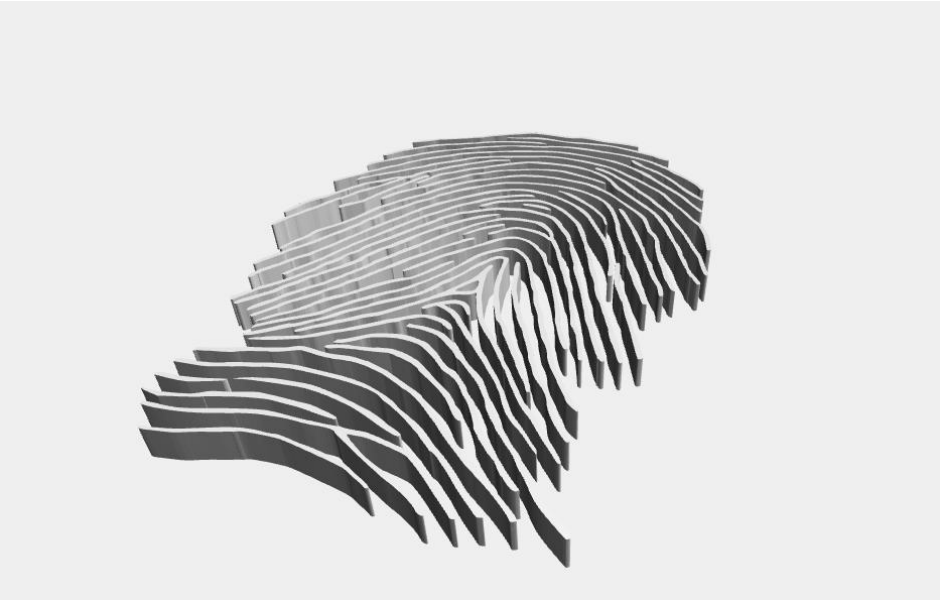
Obrázek 9: Fotografie otisku mobilem
Zdroj – Vlastní tvorba

Obrázek 10: Vytvořený 2D model otisku
Zdroj – Vlastní tvorba

Po vyfocení této fotografie je nutné otisk přenést do počítače a následně jej pomocí softwaru upravit. Pří zpracování této práce byl použit software Zoner Photo Studio. Doporučuji použít

Photoshop, s možností vrstev, která v Zoneru chyběla, usnadní práci mnohonásobně. Nejprve otisk zrcadlově otočíme, následně pomocí přiblížení a malování čar opatrně začneme vyplňovat prohlubiny papilárních linií. Důvodem vyplňování je potřeba přenesení otisku z 2D modelu do 3D modelu vytažením. Tento 3D model následně vytiskneme fotopolymerovou tiskárnou. Chceme se dostat do tohoto konečného modelu.

Následný krok vyžaduje software program CAD, ve kterém námi vytvořený model importujeme a vytvoříme z něj 3D model, vizualizace výsledného 3D modelu je na obrázku číslo 11.



Obrázek 11: Vytvořený 3D model otisku
Zdroj – Vlastní tvorba

Poté model nahrajeme do fotopolymerové tiskárny a necháme ji pracovat.

2.2.3 **Výsledný výrobek**

Po dokončení výrobního procesu 3D tiskárny, zůstane 3D model otisku prstu, který vidíme na obrázku číslo 12. Nyní nám již postačí nanést tenkou vrstvu lepidla Herkules a vyčkat, dokud lepidlo nezaschne. Fáze zasychání lepidla trvá v rozsahu 4 až 8 hodin. Následně otisk opatrně sejmeme.

Obrázek 12: Vytisknutý model otisku

Zdroj – Vlastní tvorba

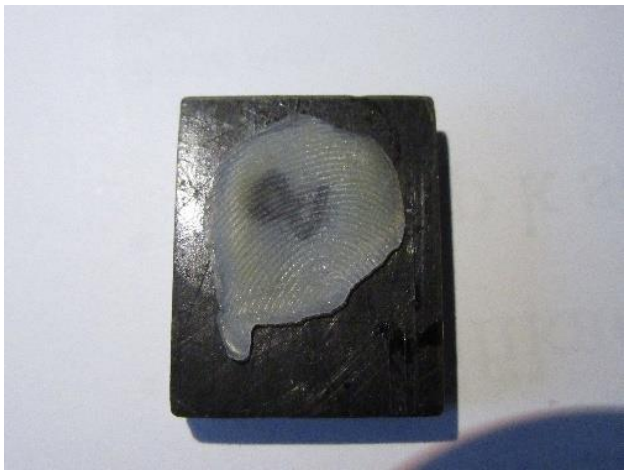
3. Vyhodnocení testování

V této kapitole si popíšeme otisky vytvořené pro průběh testování a zaznamenáme si výsledky. V následující kapitole této práce si všechny tyto výsledky zanalyzujeme, shrneme výhody a nevýhody všech mobilních zařízení.

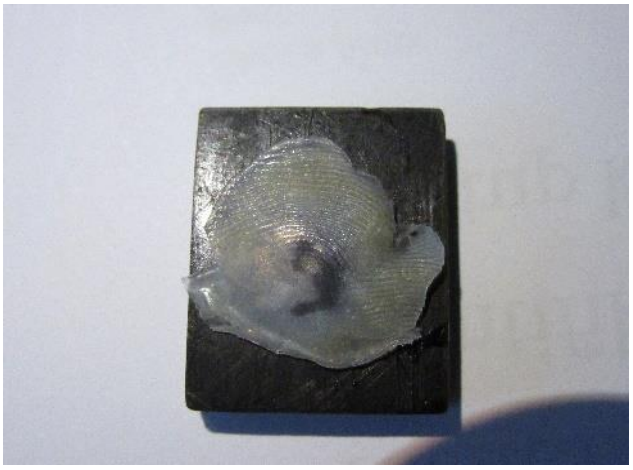
Každý telefon jsme podrobili testu, který se skládal ze 7 otisků vytvořených metodou I a dále 3 otisků vytvořených metodou II.

3.1 Metoda I

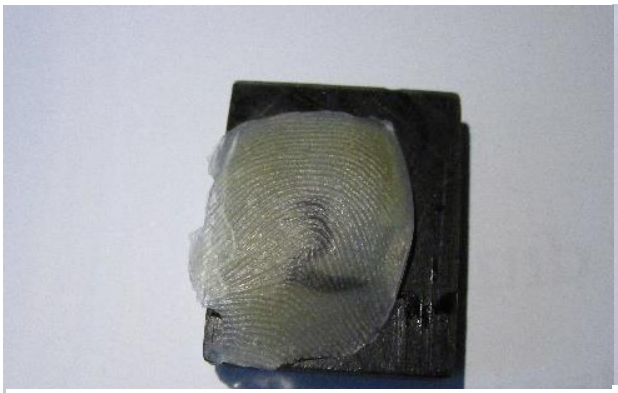
Podstatou metody I bylo prokázání možnosti přístupu do mobilního telefonu s ručně vyrobeným otiskem. Některé vyrobené otisky vykazovaly mírnou deformaci, díky které měly 0% úspěšnost. U další skupiny vyhotovených otisků byla hledána správná poloha přiložení otisku, avšak poté bylo dosaženo přístupu. Některé z otisků byly dokonce natolik povedené, že byl přístup získán na první pokus.



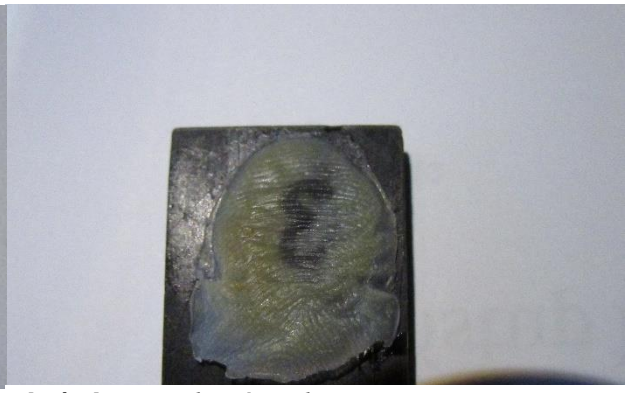
Obrázek 13: Flešný otisk 1
Zdroj – Vlastní tvorba



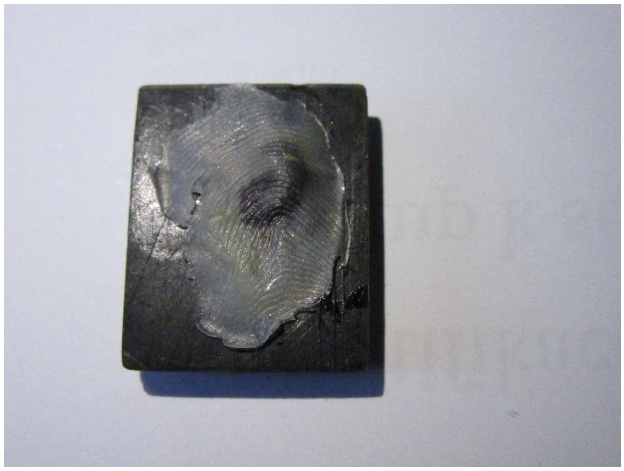
Obrázek 14: Falešný otisk 2
Zdroj – Vlastní tvorba



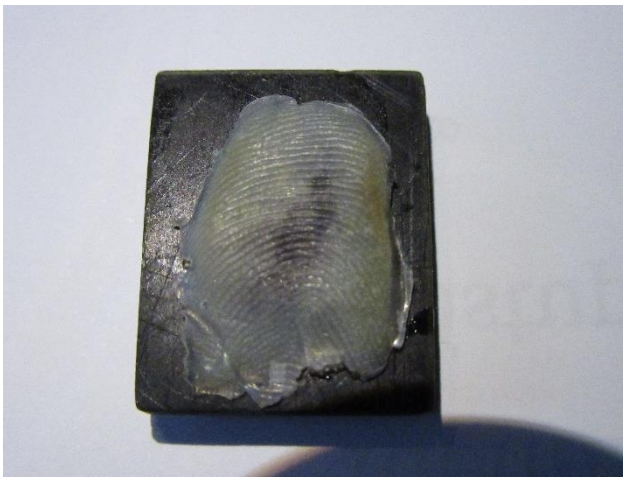
Obrázek 17: Falešný otisk 3
Zdroj – Vlastní tvorba



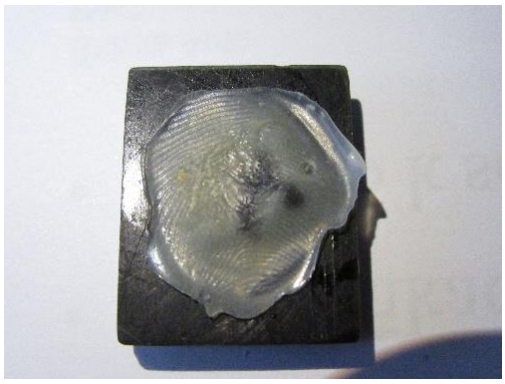
Obrázek 16: Falešný otisk 4
Zdroj – Vlastní tvorba



Obrázek 19: Falešný otisk 5
Zdroj – Vlastní tvorba



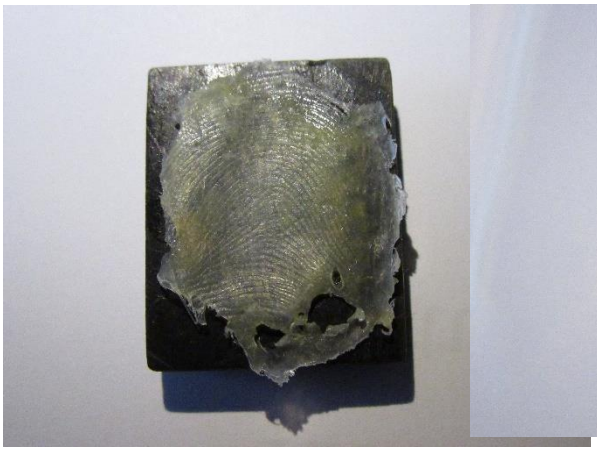
Obrázek 18: Falešný otisk 6
Zdroj – Vlastní tvorba



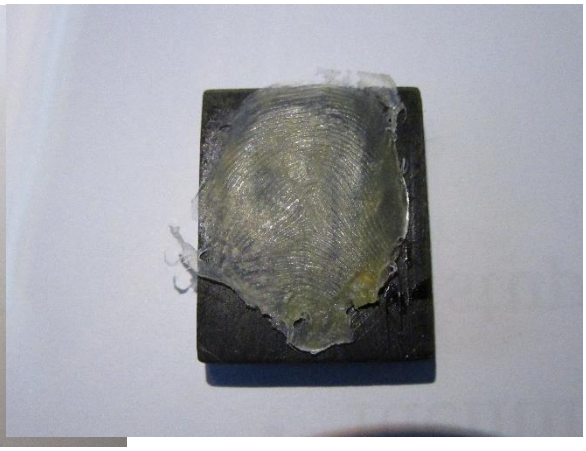
Obrázek 20: Falešný otisk 7
Zdroj – Vlastní tvorba

3.2 Metoda II.

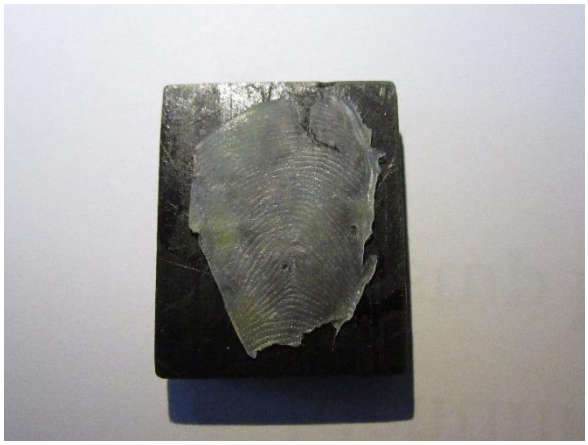
Metodou II byly vytvořeny 3 vzorky otisku prstu., metoda byla v porovnání s metodou I více náročnou. Bylo nutno vymezit delší časový úsek, než jsme dokázali vyladit vzorky na takovou úroveň, aby byly rozeznatelné pro naše testované mobilní telefony. Následné testování ukázalo, že pokud se vyladí všechny detaily, lze i s takto vytvořeným otiskem překonat zabezpečení mobilního telefonu.



Obrázek 21: Falešný otisk 2.1
Zdroj – Vlastní tvorba



Obrázek 22: Falešný otisk 2.2
Zdroj – Vlastní tvorba



Obrázek 23: Falešný otisk 2.3
Zdroj – Vlastní tvorba

3.3 Huawei P9 lite

Mobilní telefon Huawei P9 lite byl v procesu testování nejméně náročný na kvalitu otisků. Stačila pouze malá část otisku, aby byla potvrzena shoda s naskenovaným prstem, a došlo k povolení přístupu neautorizovanému uživateli.

Tabulka 3: Huawei - Test otisků: Metoda I

Metoda I			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	100	100%
2	100	45	45%
3	100	65	65%
4	100	0	0%
5	100	38	38%
6	100	30	30%
7	100	0	0%
Celkem	**700**	**278**	**39.7%**
Celkem bez 0.	**500**	**278**	**55,6%**

Tabulka 4: Huawei - Test otisků:Metoda II

Metoda II			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	94	94%
2	100	82	82%
3	100	76	76%
Celkem	**300**	**252**	**84%**

3.4 Iphone 6

Mobilní telefon Iphone 6 byl při testování metodou I odolnější. Důvodem byl fakt, že se jednalo o první iteraci těchto testů, a chtěli jsme provést porovnání na stejné úrovni. U metody II si Iphone 6 nevedl o nic lépe než model Huawei P9 lite. Důvodem byla vysoká kvalita vyrobených otisků.

Tabulka 5: Iphone - Test otisků: Metoda I

Metoda I			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	79	100%
2	100	38	38%
3	100	51	51%
4	100	0	0%
5	100	24	24%
6	100	25	25%
7	100	0	0%
Celkem	**700**	**217**	**31%**
Celkem bez 0.	**500**	**217**	**43,4%**

Tabulka 6: Iphone - Test otisků: Metoda II

Metoda II			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	88	88%
2	100	86	86%
3	100	62	62%
Celkem	**300**	**236**	**78,7%**

3.5 Samsung Galaxy J5

Mobilní telefon Samsung Galaxy J5 dopadl v testech nejlépe. Nutností byla kvalita otisku, zejména potřeba, aby otisk byl opravdu tenký a hlavně konzistentní po celé ploše. Pokud byl však otisk lehce porušený, nebo nepřesný na určitém místě, bylo velmi těžké najít vhodnou polohu otisku, aby byl telefonem otisk přijat.

Tabulka 7: Samsung - Test otisků: Metoda I

Metoda I			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	85	100%
2	100	32	45%
3	100	55	65%
4	100	0	0%
5	100	20	37,5%
6	100	15	30%
7	100	0	0%
Celkem	**700**	**207**	**29,57%**
Celkem bez 0.	**500**	**207**	**41,4%**

Tabulka 8: Samsung - Test otisků. Metoda II

Metoda II			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	90	90%
2	100	79	79%
3	100	52	52%
Celkem	**300**	**221**	**73,7%**

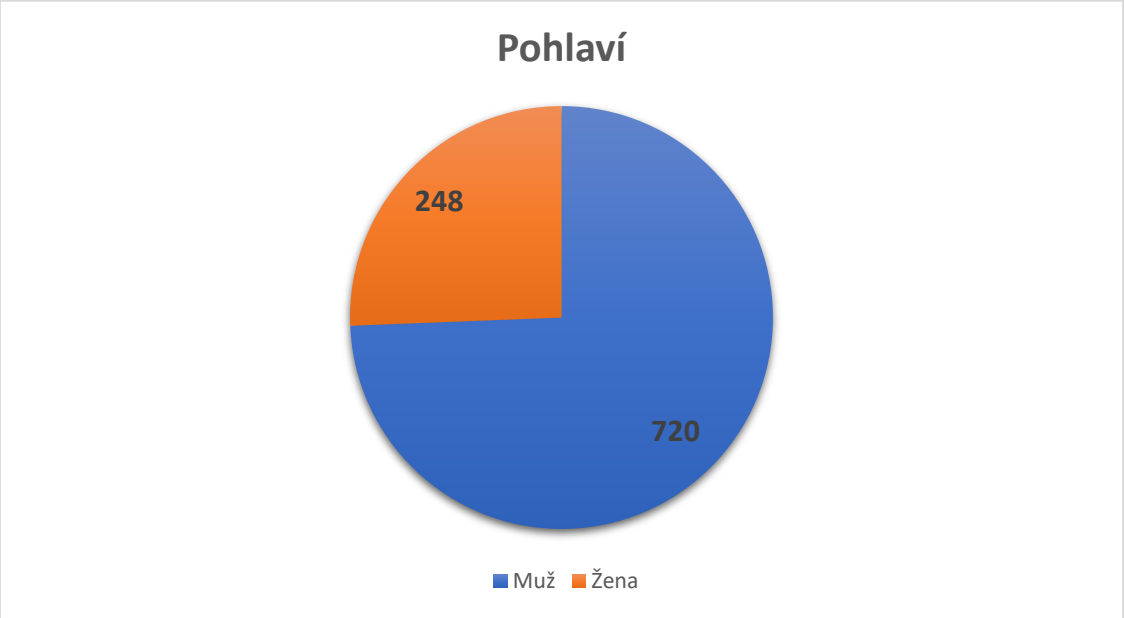
4. Dotazníkové šetření

Cílem mého dotazníkového šetření bylo zmapování povědomí respondentů o biometrických metodách, jejich názoru na tyto metody, zejména z pohledu bezpečnosti těchto metod. Dotazníkové šetření bylo možné vyplnit v časovém rozmezí 30-ti dnů, od 1. 3. 2018 do 31. 3. 2018. Dotazník byl distribuován online pomocí různých diskuzních fór zaměřených na podobná témata v rámci biometrie, dále pomocí sociální sítě Facebook.

Tento dotazník byl zaměřen na bezpečnost autentizace uživatelů pomocí biometrických metod a jejich pohled na tuto problematiku.

4.1 Charakteristika respondentů

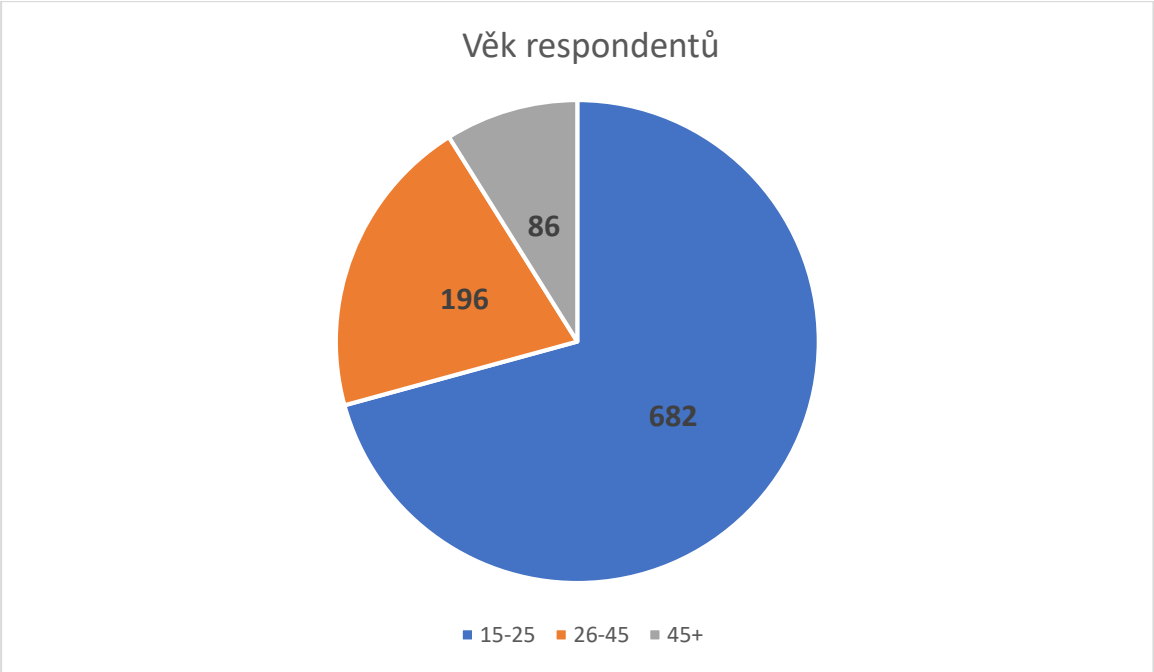
V této části se zabýváme charakteristikou našich respondentů, kteří se zúčastnili dotazníkového šetření. Zaměříme se na věk, pohlaví a počet respondentů, abychom zjistili, jak je tato skupina heterogenní.



Graf 1: Pohlaví respondentů

Zdroj – Vlastní analýza

Dotazníkového šetření se zúčastnilo celkem 968 respondentů, 720 respondentů mužského pohlaví a 248 respondentů ženského pohlaví.



Graf 2: Věk respondentů

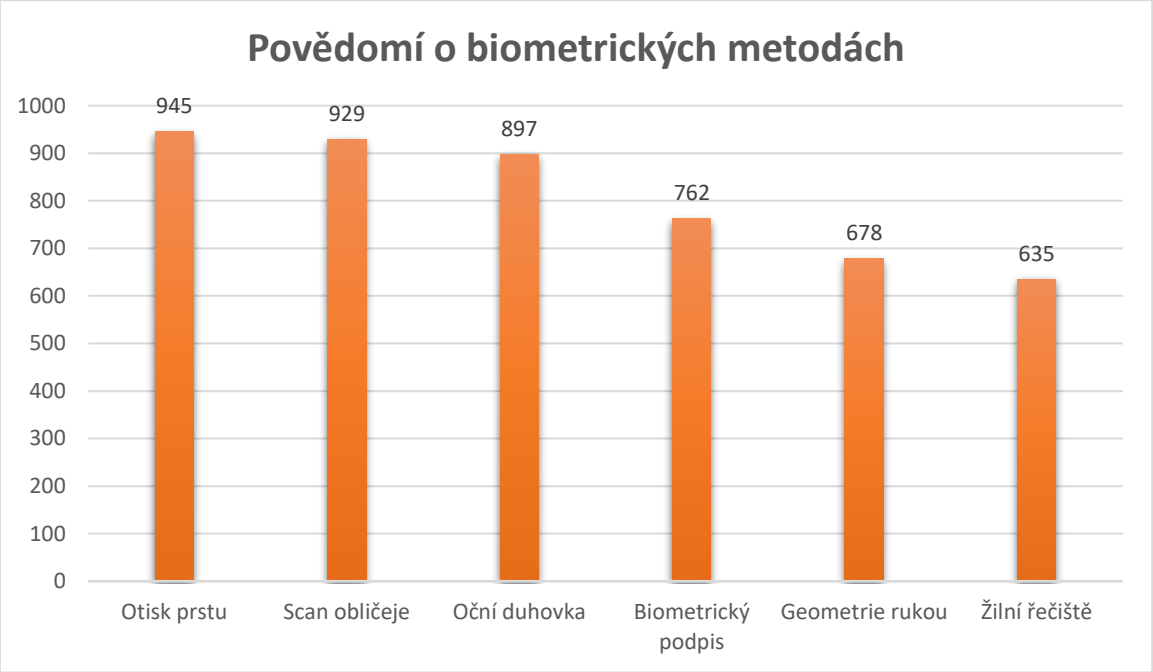
Zdroj – Vlastní analýza

Převážnou část respondentů v tomto dotazníkovém šetření tvoří zástupci mladší generace, zejména dotazovaní lidé prostřednictvím sociální sítě Facebook. Dotazovaní lidé ve věku nad 26 let a více odpovídali na různých internetových fórech.

V kategorii 15-25 let odpovídalo 682 osob, převážně z řad studentů. V kategorii 26-45 let odpovídalo 196 osob a v kategorii 45 let a více 86 osob.

4.2 Analýza povědomí o biometrických metodách

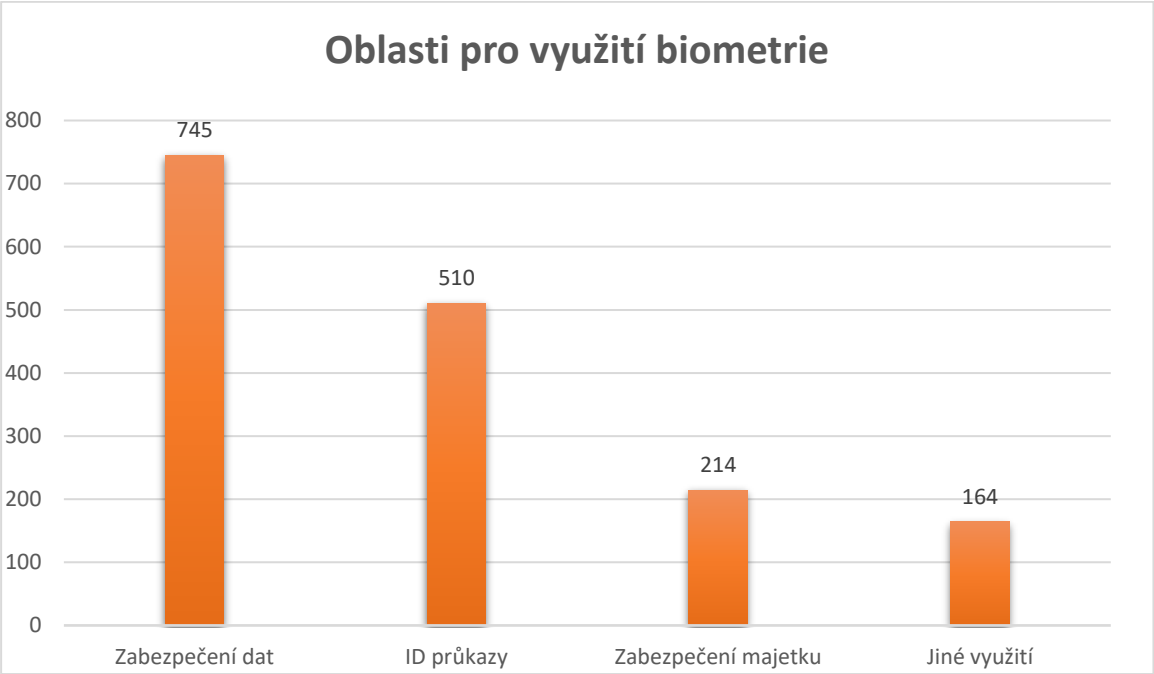
V této části se zabýváme prozkoumáním povědomí respondentů o určitých biometrických metodách.



Graf 3: Povědomí o biometrických metodách
Zdroj – Vlastní analýza

Pokud se podíváme na tento graf jako celek, můžeme s jistotou říci, že povědomí o biometrických metodách je v dnešní době na vysoké úrovni. Více specifické biometrické metody, žilní řečiště a biometrie ruky, však nejsou v současné době ještě známy všem respondentům.

Následující graf zobrazuje oblasti, kde by si naši dotázaní respondenti dokázali představit využití biometrie v každodenním životě.

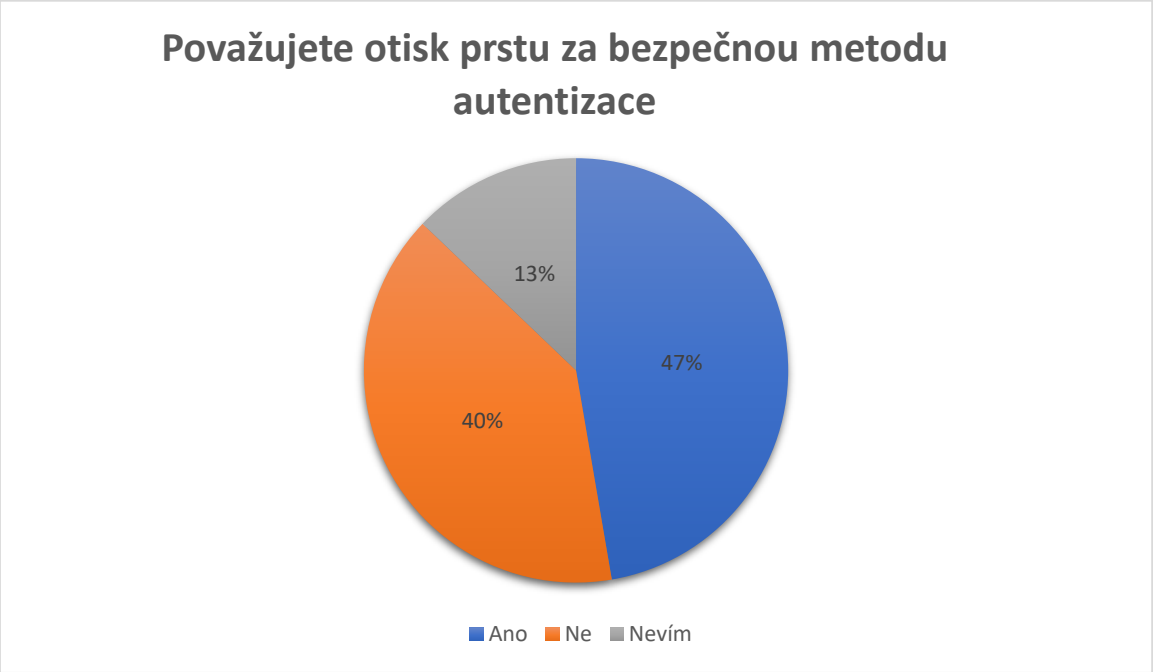


Graf 4: Oblasti pro využití biometrie
Zdroj – Vlastní analýza

Nejčetnější odpovědí respondentů bylo využití v oblasti zabezpečení dat. Jako druhou oblast využití označili respondenti ID průkazy, dále následovala oblast zabezpečení majetku. S jiným využitím, které nebylo v možnostech dotazníku blíže specifikováno, se ztotožnilo 164 lidí.

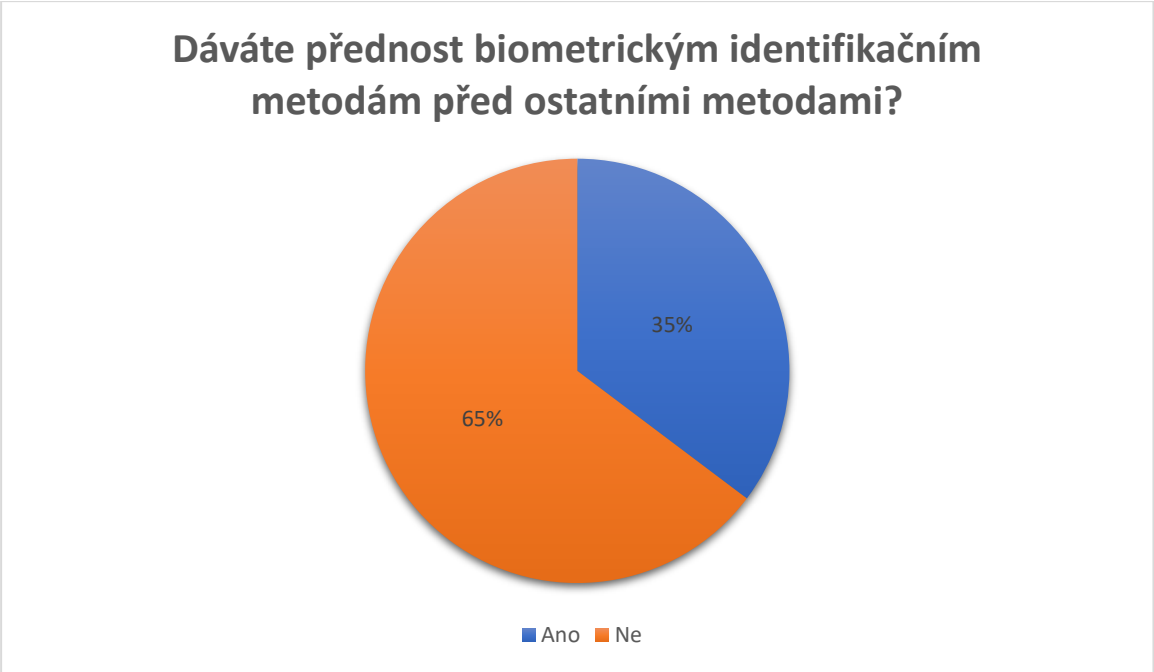
4.3 Bezpečnost a biometrie

Biometrie je zde reprezentována formou otisku prstu. Bezpečnost byla testována již v předcházejících kapitolách, na jejichž základě vyvstaly nové otázky: „Máme se bát všech kvalitních fotoaparátů na veřejných místech? Může mi být biometrie ukradena na ulici za bílého dne?“.



Graf 5: Bezpečnost metody otisk prstu
Zdroj – Vlastní analýza

Respondenti byli seznámeni s faktem prolomení bezpečnosti otisku, jak s falešným prstem odlitým z mého prstu, tak i vyfoceným otiskem prstu. I přes tuto skutečnost odpovědělo 47% respondentů kladně. Tito respondenti i nadále považují otisk prstu za bezpečnou metodu autentizace. Další skupina respondentů o velikosti 40% označila otisk prstu jako metodu autentizace, které nedůvěřují. Zbývajících 13% respondentů se nemohlo rozhodnout, zda je metoda autentizace otiskem prstu dostatečně bezpečná či nikoliv.



Graf 6: Biometrie oproti ostatním metodám

Zdroj – Vlastní analýza

Graf číslo 6 ukazuje, že 65% respondentů dává přednost identifikaci do svých zařízení formou použití přístupových bodů pomocí biometrie, namísto zapamatování si různých hesel. Pokud porovnáme výše uvedené s dříve provedenými studiemi, dozvíme se, že se stejná otázka v roce 2014 u 76% setkala s preferencí autentizace formou různých hesel. Naopak v dnešní době začínají být Touch ID a jiné čtečky požadovaným standardem.

Graf 7: Bezpečná hesla

Zdroj – Vlastní analýza

Bezpečná hesla jsou pro majitele, který je dodržuje, v nastavení chránícímu proti standardnímu riziku. Pravidla jsou různá, avšak báze používaná firmami je obdobná. V dnešní době je mnoho služeb poskytováno prostřednictvím internetu, kde je vyžadován jedinečný přístup, běžný uživatel si má ke službě vytvořit a zapamatovat unikátní heslo. V realitě bohužel mnohdy dochází k tvorbě identických hesel pro různé služby. Více než polovina respondentů se přiznala k nedodržování pravidel bezpečných hesel.

5. Analýza výsledků a doporučení pro praxi

5.1 Analýza výsledků

V této podkapitole si rozvedeme jednotlivé výsledky testovaných mobilních telefonů. Uvedeme si poznatky, které byly zaznamenány při vytváření otisků prstu, dále různé chyby a jak se jich vyvarovat. Následně si celou část zhodnotíme a podíváme se na možnosti budoucího vývoje.

Telefony byly otestovány 100 pokusy o přístup s každým otiskem, každý výsledek byl zaznamenáván do excelové tabulky a následně zpracován.

5.1.1 Huawei P9 lite

Práce s mobilním telefonem Huawei P9 lite byla v rámci testování otisků prstu nejjednodušší. Byl to model, na kterém jsme začínali testovat již naše první pokusy o otisky. Naším testem prošlo velmi mnoho méně kvalitních otisků. Z hlediska bezpečnosti je tento telefon, dle mého názoru, zcela nedostačující. Pokud je telefon uzamčen, počet pokusů na otevření telefonu je cca 30, s rozsvíceným displejem je tento počet omezen na 10. Toto číslo je stále z mého pohledu vysoké na to, jak malá část otisku stačí, aby došlo k odemknutí telefonu.

U otisků samotných nebyl problém, pokud byly tlustší, i více než 3mm, ale bylo nutné dodržet dostačující úroveň kvality. Z výsledků testování je zřejmé, že telefon je citlivý na pokládání otisku stejně, či velice podobně, jak je nasnímán.

Tabulka 9: Huawei - Analýza metody I

Metoda I			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	100	100%
2	100	45	45%
3	100	65	65%
4	100	0	0%
5	100	38	38%
6	100	30	30%
7	100	0	0%
Celkem	**700**	**278**	**39.7%**
Celkem bez 0.	**500**	**278**	**55,6%**

Otisky vytvořené metodou I v tomto případě dosahovaly téměř 40% úspěšnosti. Vyškrtneme-li otisky, které byly odmítnuty ve všech pokusech, potom tedy úspěšnost dosáhla dokonce 55,6%.

Tabulka 10: Huawei - Analýza metody II

Metoda II			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	94	94%
2	100	82	82%
3	100	76	76%
Celkem	**300**	**252**	**84%**

Metoda II byla v tomto případě mnohem úspěšnější, důvodem je zřejmě skutečnost výroby otisků více pokusy, dokud nebylo dasaženo dostatečné kvality.

5.1.2 **Iphone 6**

Mobilní telefon Iphone 6 dosáhl z pohledu bezpečnosti vyšší úrovně než telefon Huawei P9 lite. Pokusů o přístup máme před vyžadování PIN kódu celkem 5, pokud je telefon nepoužíván více než 24 hodin, je kód automaticky vyžadován. Pokud máme telefon zamknutý, na otisk nereaguje, pouze po zapnutí displeje. Sensor čtečky otisku není tak citlivý na pozici otisku, pokud je otisk naskenován do telefonu, tak je možné jej položit téměř pod jakýmkoliv úhlem, aby byl akceptován. Otisk musel být o hodně tenčí, v některých případech jej bylo potřeba lehce navlhčit. Takto jednoduše se dala obejít kontrola živosti. Z hlediska bezpečnosti tento telefon doporučuji více než telefon Huawei P9 lite.

Tabulka 11: Iphone - Analýza metody I

Metoda I			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	79	100%
2	100	38	38%
3	100	51	51%
4	100	0	0%
5	100	24	24%
6	100	25	25%
7	100	0	0%
Celkem	**700**	**217**	**31%**
Celkem bez 0.	**500**	**217**	**43,4%**

První metoda se setkala s úspěšností 31%, pokud vyškrtneme otisky s nulovou úspěšností, potom tedy 43,4%. V porovnání s mobilním telefonem Huawei P9 lite se jedná rozhodně o pokles úspěšnosti získání přístupu.

Tabulka 12: Iphone - Analýza metody II

Metoda II			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	88	88%
2	100	86	86%
3	100	62	62%
Celkem	**300**	**236**	**78,7%**

Při testování metodou II došlo také k poklesu úspěšnosti, celkem o 5,3%. Pokles však není tak značný jako u první metody. Nutno podotknout, že při testování těchto otisků došlo pouze ve dvou případech k uzamčení mobilního telefonu z 300 pokusů, kdy byl následně vyžadován PIN.

5.1.3 **Samsung Galaxy J5**

Z testovaných mobilních telefonů dopadl nejlépe Samsung Galaxy J5. Byl nejvíce citlivý na kvalitu otisků a také velmi citlivý na kontrolu živosti. V případě, kdy bylo čidlo jakkoliv mokré, vlhké, nebo ušpiněné, byl otisk odmítnut. Pokud se tedy snažíme obejít kontrolu živosti navlhčením otisku, je nutné odhadnout vlhkost, aby otisk za sebou nezanechával příliš velké stopy. Otisk bylo možné aplikovat pod téměř jakýmkoliv úhlem. Byl-li telefon vypnutý více než 24 hodin, byl požadován PIN kód. Počet pokusů na autentizaci je 10, tedy více pokusů než u telefonu iPhone 6. Co se týká citlivosti zařízení na pravost otisku, Samsung jednoznačně vyhrává.

Tabulka 13: Samsung - Analýza metody I

Metoda I			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	85	100%
2	100	32	45%
3	100	55	65%
4	100	0	0%
5	100	20	37,5%
6	100	15	30%
7	100	0	0%
Celkem	**700**	**207**	**29,57%**
Celkem bez 0.	**500**	**207**	**41,4%**

U Samsungu se metoda I setkala s nejnižší úspěšností. Některé otisky byly pro čtečku příliš silné, bylo tedy s nimi velmi obtížné získat přístup do telefonu. Bohužel i s těmito otisky se to však několikrát podařilo.

Tabulka 14: Samsung - Analýza metody II

Metoda II			
Číslo otisku	Počet pokusů o přístup	Počet úspěšných pokusů	Procentuální úspěšnost
1	100	90	90%
2	100	79	79%
3	100	52	52%
Celkem	**300**	**221**	**73,7%**

Metoda II zaznamenala u Samsungu 5% pokles úspěšnosti pokusů o přístup v porovnání s modelem iPhonu 6. Za upozornění stojí fakt, že pokud telefon napíše „šmouha na čtečce“ či podobné hlášení, nezapočítává se tento pokus do nesprávných pokusů o přístup. Tato skutečnost byla důvodem, proč se tento telefon ani jednou nedostal do stavu požadování zadání PIN kódu.

5.2 Celkové zhodnocení a možnost budoucího vývoje

5.2.1 Celkové zhodnocení

Z testovaných mobilních telefonů můžeme s jistotou označit model Samsung jako nejlepší. Avšak z hlediska bezpečnosti ani jeden telefon nepodal uspokojivé výsledky, falešný otisk byl přijat až příliš často. Nutno podotknout, že telefony byly testovány pouze s falešnými otisky, žádné modifikace softwaru nebyly provedeny.

5.2.2 Budoucí vývoj

Co se týče biometrie jako celku, můžeme v budoucnosti jistě očekávat zlepšování kvality všech čidel, snímačů, technologií šifrování a mnoho dalšího. Z jednoho úhlu pohledu je stále zvyšující se kvalita těchto zařízení včetně kamer indikátorem zvýšení bezpečí, avšak ubírá nám soukromí. Již dnes existuje mnoho různých systémů, které dokáží zmapovat pohyb osob. Patří mezi ně i termo kamery, které například dokáží určit, zda je radost z výhry opravdová, nebo předstíraná. Tyto termo kamery jsou z velké části využívány v kasinech. Budoucnost jistě přinese i další rozvoj těchto systémů k rozeznání behaviorální biometrie, rozvoj jejich kvality obrazu i snímání.

Také otisk prst se bude jistě vyvíjet, budeme se jistě více snažit eliminovat míru chybovosti přijmutí neznámého uživatele a míru chybovosti odmítnutí oprávněného uživatele. Avšak s postupně rozvíjející se technikou fotoaparátů, bude v budoucnu také o mnoho lehčí získat otisk cizí osoby bez jejího vědomí, a dále tím replikovat její biometrickou identitu.

Závěr

Se stále rozvíjejícími se technologiemi začíná každý z nás přicházet s biometrií do styku, někteří i každodenně na svých mobilních zařízeních. Biometrie je náš druh identifikace a odlišení se od ostatních, je jedinečná, stálá a pohodlná na používání. Bohužel mnoho osob v této době si neuvědomuje, že jejich biometrická data mohou být lehce odcizena a pokud jsou používána například na potvrzování plateb přes mobil, tak i lehce zneužita.

Hlavním cílem teoretické části bylo představení biometrie, její historie, její fungování a dále její rizika. Práce popisovala postupný vývoj biometrie od jejího počátku až k dnešním dnům. Práce je nejvíce zaměřena na otisk prstu a jeho bezpečnost v komerčním využití. Rozebrali jsme si různé metody snímání, druhy snímače a jejich využití. Popsali vybrané biometrické metody, které se již používají pro komerční účely, dále metody ve fázi vývoje.

Cílem praktické části práce bylo ukázat, že biometrie není až tak bezpečná, jak si mnozí myslíme. Podle výsledků testů můžeme tvrdit, že samostatný otisk prstu není dostatečnou formou biometrické ochrany pro velmi důvěrná data, bankovní účty a jiné. Následně jsme zjišťovali, prostřednictvím dotazníkového šetření, přehled jednotlivých kategorií osob o biometrických metodách a jejich přístup k bezpečnosti.

Za největší přínos této práce považuji praktickou ukázku obcházení bezpečnosti biometrických systémů za použití různých metod vyhotovení otisku prstu. Tato práce může posloužit jako návod pro budoucí specialisty v oblasti biometrie na otestování systémů v jejich organizacích.

Zdroje

MITRA, Sinjini a Mikhail GOFMAN. 2017. *Biometrics in a data driven world: trends, technologies, and challenges.* 1. vyd. Boca Raton: CRC Press, Taylor & Francis. ISBN 9781498737647

HOUCK, Max M. 2016. *Forensic fingerprints*. 1. vyd. San Diego, CA: Academic Press, imprint of Elsevier, Advanced forensic science series. ISBN 0128005734

SMEJKAL, Vladimír a Karel RAIS. 2013. *Řízení rizik ve firmách a jiných organizacích*. 4. Aktualizované a rozšířené vydání. Praha: Grada, Expert (Grada). ISBN 978-80-247-4644-9

RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. 2008. *Biometrie a identita člověka: ve forenzních a komerčních aplikacích*. 1. vyd. Praha: Grada. ISBN 978-80-247-2365-5.

PROQUEST. 2015. Databáze článků ProQuest [online]. *Android fingerprint readers may be easier to hack than Touch ID*. AOL Inc. [cit. 2015-08-05]. Dostupné z: http://www.engadget.com/2015/08/05/android-fingerprint-readers-may-be-easier-to-hack-than-touch-id/

BIOMETRIKY. *Biometric Line* [online]. 612 00 Brno: ABBAS, [2017] [cit. 2018-10-01]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/

BIOLOGIE. *Science world* [online]. 130 00 Praha 3: F solutions, 2008 [cit. 2018-10-01]. Dostupné z: https://www.scienceworld.cz/

BIOMETRIC update. *Explaining Biometrics* [online]. Toronto, ON, M5A 3C3: Biometrics Research Group, [2012] [cit. 2018-10-01]. Dostupné z: https://www.biometricupdate.com/201802/history-of-biometrics-2

BAYOMETRIC. *Bayometric* [online]. USA – Bayometric, 1743 Park Avenue,San Jose,CA 95126: Bayometric [cit. 2018-10-01]. Dostupné z: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/

Biometric Line [online]. Praha: ABBAS, as., 2013 [cit. 2018-11-22]. Dostupné z: http://www.biometricke-ctecky.cz/biometriky/otisk-prstu/

Crossmatch Portable Biometric Finger print Reader. In: *Injes* [online]. Čína, 2017 [cit. 2018-11-22]. Dostupné z: http://www.injes.com/crossmatch-portable-biometric-finger-print-reader-u-are-u-5300-with-digitalpersona-optical-fingerprint-sensor_p59.html

R303 Capacitive Fingerprint Reader [online]. 2013 [cit. 2018-11-22]. Dostupné z: https://www.aliexpress.com/item/R303-Capacitive-Fingerprint-Reader-Module-Sensor-Scanner/32620290283.html

Hand Geometry terminal. In: *Synerion Blog* [online]. Team Synerion, 2014 [cit. 2018-11-22]. Dostupné z: https://blog.synerion.com/biometric-time-clocks-what-are-they-what-can-they-do

Facial recognition. In: *Synerion Blog* [online]. USA: Tech this out, 2018 [cit. 2018-11-22]. Dostupné z: http://www.techthisoutnews.com/u-s-military-just-figures-facial-recognition-dark/facial-recognition-biometrics-vectors-1-e1509551990917/

A finger vein scanner. In: *MDPI* [online]. MDPI - Publisher of Open Access Journals, 2018 [cit. 2018-11-22]. Dostupné z: https://www.mdpi.com/2078-2489/9/9/213/htm#B28-information-09-00213