Česká zemědělská univerzita v Praze

Technická fakulta

Spolehlivost biometrického systému skenu krevního řečiště ruky při záměrné falzifikaci biometrických údajů

Diplomová práce

Vedoucí práce: Ing. Veronika Hartová, Ph.D.

Autor práce: Bc. Viktorija Miščenko

Praha 2022

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Viktorija Miščenko

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Spolehlivost biometrického systému skenu krevního řečiště ruky při záměrné falzifikaci biometrických údajů

Název anglicky

Reliability of the biometric system of scanning the bloodstream of the hand in the case of intentional falsification of biometric data

---

Cíle práce: Diplomová práce je tematicky zaměřena na problematiku biometrických identifikačních systémů. Hlavním cílem práce bude určit spolehlivost biometrického systému při úmyslné falzifikaci biometrických údajů.

Metodika: Diplomová práce se bude věnovat spolehlivosti biometrického systému identifikace osob na základě skenu krevního řečiště ruky při záměrné falzifikaci biometrických údajů, tedy při použití tzv. metody „spoofing“. Bude vytvořen falzifikát, na jehož základě bude probíhat testování tohoto biometrického systému.
Práce bude zpracována dle osnovy:
1 Úvod
2 Cíl práce
3 Metodika práce
4 Přehled řešené problematiky
5 Praktická část práce
6 Zhodnocení výsledků a diskuse
7 Závěr
8 Seznam použitých zdrojů
9 Přílohy

Doporučený rozsah práce

30–60 str. včetně obrázků, tabulek a grafů

Klíčová slova

biometrie, krevní řečiště, falzifikace, spoofing, sensor

Doporučené zdroje informací

Hand-based biometrics: methods and technology. Editor Martin DRAHANSKÝ. London: The Institution of Engineering and Technology, 2018. IET book series in advanced biometrics. ISBN 978-1-78561-224-4.

LODROVÁ, Dana. Security of Biometric Systems. Beau Bassin, Mauritius: LAP LAMBERT Academic Publishing, 2017. ISBN 978-3-330-34325-2.

NIXON, Mark S. a S. Z. LI. Handbook of biometric anti-spoofing: trusted biometrics under spoofing attacks. Editor Sébastien MARCEL. London: Springer, [2014]. Advances in computer vision and pattern recognition. ISBN 978-1-4471-6523-1.

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

UHL, Andreas, Christian RATHGEB a Peter WILD. Iris Biometrics: From Segmentation to Template Security. New York: Springer Publishing Company, 2012 | 2013 ed. ISBN 978-1-4614-5570-7.

WECHSLER, Harry, GUO, Guodong, ed. Mobile Biometrics. Stevenage, United Kingdom: Institution of Engineering and Technology, 2017. ISBN 978-1-78561-095-0.

Předběžný termín obhajoby

2021/2022 LS – TF

Vedoucí práce

Ing. Veronika Hartová, Ph.D.

Garantující pracoviště

Katedra vozidel a pozemní dopravy

Elektronicky schváleno dne 28. 1. 2021

Ing. Martin Kotek, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 2. 2021

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 05. 11. 2021

Čestné prohlášení

*„Prohlašuji, že jsem diplomovou práci na téma: „**Spolehlivost biometrického systému skenu krevního řečiště ruky při záměrné falzifikaci biometrických údajů**“ vypracoval/a samostatně a použil/a jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.*

Jsem si vědom/a, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom/a, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom/a že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

V Praze dne 14.4.2022 Bc. Viktorija Miščenko .....

Poděkování

Mé poděkování patří Ing. Veronice Hartové, Ph.D. za odborné vedení práce, věcné připomínky, vstřícnost a lidský přístup při konzultacích a vypracování diplomové práce.

Abstrakt: Diplomová práce je zaměřena na testování spolehlivosti systémů identifikujících osoby pomocí krevního řečiště ruky při záměrné falzifikaci biometrických údajů neboli použití tzv. metody „spoofing“. Teoretická část je věnována definování a vysvětlení důležitých pojmů z oblasti identifikace osob, biometrie a bezpečnosti biometrických systémů. Dále se práce zabývá rozdělením a základním přehledem nejpoužívanějších biometrických metod identifikace osob. Také jsou zde uvedeny způsoby ochrany proti spoofingu a jejich praktické využití ve sféře zabezpečení přístupů k informacím. Poslední část je věnována popisu metody identifikace osob pomocí snímání krevního řečiště ruky, popis studií použití falzifikátu a technologie PalmSecure. Praktická část práce je věnována popisu měření spolehlivosti biometrického systému PalmSecure za použití metody „spoofing“ a zpracování a vyhodnocení výsledků tohoto měření. Metodika vytvoření falzifikátu a testování se odvíjí od výzkumu provedeného odborníkem na informační bezpečnost Julianem Albrechtem a etickým hackerem Janem Krisslerem, kteří za pomoci vyrobeného falzifikátu prolomili biometrický systém skenu krevního řečiště dlaně PalmSecure. Praktická část diplomové práce dále popisuje výrobu falzifikátu, průběh měření a otestování biometrického systému PalmSecure včetně zpracování výsledků měření. Otestovaný systém nemohl být na základě výsledků vyhodnocen, protože se v průběhu měření zjistilo nedokonalé provedení falzifikátu. Výsledkem této práce je zjištění, že v nelaboratorních podmínkách s použitím běžně dostupných nástrojů a materiálů je velice obtížné zhotovit falzifikát takové kvality, která je potřebná pro prolomení biometrického systému skenu krevního řečiště dlaně ruky.

Klíčová slova: biometrie; krevní řečiště; falzifikace; spoofing; sensor

Reliability of the biometric system of scanning the bloodstream of the hand in the case of intentional falsification of biometric data

Summary: The thesis is focused on testing the reliability of systems identifying persons using the vein pattern of the hand in the case of deliberate falsification of biometric data or using the so-called "spoofing" method. The theoretical part is devoted to defining and explaining important concepts in the field of personal identification, biometrics and security of biometric systems. Furthermore, the thesis deals with the parition and basic overview of the most used biometric methods of personal identification. Also, the methods of protection against spoofing and their practical use in the sphere of information access security are presented. The last section is devoted to the description of the method of identification of persons using the bloodstream scanning of the hand, the description of studies on the use of counterfeit and PalmSecure technology. The practical part of the thesis is devoted to the description of the measurement of the reliability of the PalmSecure biometric system using the "spoofing" method and the processing and evaluation of the results of this measurement. The methodology of creating the counterfeit and testing is based on research conducted by information security expert Julian Albrecht and ethical hacker Jan Krissler, whom used a manufactured counterfeit to crack the PalmSecure biometric system of palm vein scan. The practical part of the thesis further describes the production of the counterfeit, the course of measurement and testing of the PalmSecure biometric system, including the processing of the measurement results. The tested system could not be evaluated on the basis of the results, because the imperfect execution of the counterfeit was found during the measurement. As a result of this work, it was found that in non-laboratory conditions, using commonly available tools and materials, it is very difficult to produce a counterfeit of the quality required to break the biometric system of palm vein scan.

Key words: biometrics; palm vein; falsification; spoofing; sensor

Obsah

Seznam použitých zkratek

2D, 3D	Two Dimensional, Three Dimensional
AES	Advanced Encryption Standart
ANSI/NIST	American National Standard for Information Systems / National Institute of Standards and Technology
API	Application Program Interface
BMP	Bit Mapped Picture
CCD	Charge-Coupled Device
CLAHE	Contrast Limited Adaptive Histogram Equalization
CMOS	Complementary Metal-Oxide-Semiconductor
DDoS	Distributed Denial od Service
DPI	Dots Per Inch
DSRL	Digital Single-Lens Reflex camera
FRA	False Acceptance Rate
FRR	False Rejection Rate
ID	Identity Document
IR	Infrared Radiation (Infrared light)
IS	Information System
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
kB	kiloByte
LED	Light-Emitting Diode
NIR	Near-Infrared Radiation
NTSC	National Television Standards Committee
OSS	Open-Source Software
PC	Personal Computer

PDA	Personal Digital Assistant
PIN	Personal Identification Number
RGB	Red-Green-Blue (Color model)
ROI	Region of Interests
USB	Universal Serial Bus
UV	Ultra Violet
WDM	Windows Driver Model

1. Úvod

Moderní dostupné komunikační technologie umožňují přenos informací kamkoliv po světě ve velice krátkém čase. Ochrana strategických informací a informačních systémů je proto nedílnou součástí těchto procesů. Boj proti terorismu zvýšil požadavky na bezpečnost nejen informací, ale i osob a sledování jejich pohybu. Identifikace osob jako nástroj pro práci s informačními systémy a informacemi se proto stal každodenní součástí současného života. [1, 2]

Osobu lze identifikovat pomocí několika metod – vlastnictví, znalostí a biometrických charakteristik. Metoda vlastnictví je založena na principu, že daná osoba vlastní kartu, čip či jiný obdobný předmět, kterým prokazuje svoji identitu. Přestože velikou nevýhodou této metody je možnost ztráty či odcizení těchto předmětů, je stále hojně využívána v kombinaci s metodami znalostí a biometrických charakteristik. Metoda identifikace pomocí znalostí je jednou z nejrozšířenějších metod identifikace osob, ačkoliv není tou nejbezpečnější, neboť pro vyšší úroveň zabezpečení je potřeba použít komplexní hesla a PIN kódy, které jsou pro uživatele těžší na zapamatování. Nejbezpečnější metodou identifikace osob je použití biometrických charakteristik, které uživatel nemůže zapomenout, ztratit a nemohou být odcizeny. [1, 2]

Od svých počátků, kdy byla biometrie spojována především s policejně-soudními a bezpečnostními procesy, se dnes rozšířila i do civilní a komerční sféry. Rozvoj technologií umožnil prosazení biometrie do každodenního života lidí. Ochrana vstupů do objektů, cestování, platby a transakce, ochrana majetku a osobních údajů, telekomunikace a identifikace osob – to vše jsou oblasti, ve kterých se rozsah a použití biometrie zvyšuje čím dál tím více. [1]

Přestože použití biometrie přináší vysokou míru zabezpečení, vyskytují se i v biometrických systémech slabá místa, která se nesmí přehlédnout a je potřeba je zkoumat. U senzorů se jedná zejména o zneužití falešné biometriky. Obecně je používán termín „spoofing“, který označuje metodu vytvoření falzifikátu biometrických údajů, pomocí kterého je prolomen biometrický systém. Způsoby ochrany proti spoofingu jsou odvíjeny především od odolnosti dané biometrické charakteristiky vůči její falzifikaci. [1]

Biometrické charakteristiky se dělí na behaviorální neboli získané v průběhu života a anatomicko-fyziologické neboli vrozené. Mezi behaviorální se řadí charakteristiky hlasu, lokomoce, písma a podpisu. Mezi anatomicko-fyziologické patří charakteristiky tváře; charakteristiky oka jako jsou sítnice a duhovka; otisky prstů, dlaní a chodidel; geometrie ruky; topografie žil zápěstí; DNA a další. [1, 2]

Mezi jedny z nejbezpečnějších metod se řadí metoda identifikace osob pomocí skenu krevního řečiště ruky. Mezi výhody této metody patří bezkontaktnost a obecná vysoká přijatelnost uživateli. Krevní řečiště se nachází uvnitř ruky, proto je falzifikace těchto biometrických údajů obtížná, ale ne zcela nemožná. Proto je nezbytné provést experimenty, které mohou přinést zdokonalení této metody. [2]

2. Cíl práce

Cílem je otestovat spolehlivost systému identifikace osob pomocí skenu krevního řečiště dlaně při záměrné falzifikaci biometrických údajů neboli použití metody „spoofing“.

Teoretickým cílem práce je vysvětlit pojmy z oblasti identifikace osob a biometrie, seznámit s hlavními částmi biometrického systému a jeho slabých míst, provést rešerši a vypracovat přehled biometrických metod identifikace osob používaných v praxi a jejich ochrany proti spoofingu. Dílčím cílem je zpracovat problematiku identifikace osob na základě skenu krevního řečiště ruky a shrnout poznatky studie prolomení tohoto biometrického systému prezentované na bezpečnostní konferenci 35. Chaos Communication Congress (35C3) – Venenerkennung hacken.

Cílem praktické části diplomové práce je vypracovat přehled použitých nástrojů, jejich úprav a postupu vytvoření falzifikátu krevního řečiště ruky s popisem použitého materiálu, kterým bude otestován biometrický systém PalmSecure od firmy Fujitsu, Ltd. Dílčím cílem je analýza a prezentace výsledků měření. Dílčím cílem praktické části je zjistit, zda je možné prolomit tento biometrický systém v nelaboratorních podmínkách s běžně dostupnými nástroji a materiálem.

3. Metodika práce

Metodika řešené problematiky diplomové práce bude postavena na základě prostudování odborných informačních zdrojů. Literární rešerše se bude zabývat uvedením a vysvětlením důležitých pojmů z oblasti biometrie, jako jsou identifikace a verifikace, biometrický systém, popis jeho slabých míst a výpočty spolehlivosti biometrického systému, konkrétně pravděpodobnost chybného odmítnutí FRR a pravděpodobnost chybného přijetí FAR. Další část bude věnována popisu metody spoofingu a obecných způsobů ochrany. Dále se bude věnovat rozdělení a základnímu přehledu v praxi nejpoužívanějších biometrických metod identifikace osob, popisem jejich principů a ochrany proti zmanipulování senzoru pomocí falzifikace biometrických údajů. Poté bude provedeno vypracování problematiky identifikace osob pomocí skenu krevního řečiště ruky a také zpracování souhrnu již provedené studie použití metody spoofingu u technologie PalmSecure společnosti Fujitsu, Ltd. a Finger Vein Reader od společnosti Hitachi, Ltd.

V praktické části bude vypracován popis postupu přípravy falzifikátu biometrických údajů pro měření spolehlivosti biometrického systému identifikace osob pomocí skenu krevního řečiště ruky. Nejprve bude úkolem získání dat potřebných pro vytvoření falzifikátu. Prvním způsobem bude pořízení fotografií ruky a následná úprava snímků jak vyfocených, tak dříve uložených snímků biometrické šablony krevního řečiště z testovací aplikace systému PalmSecure. Dva výsledné obrazy (jeden ze snímku ruky, druhý z uloženého snímku testovací aplikace) budou použity pro výrobu falzifikátu krevního řečiště ruky, kterým bude následně otestován senzor skenu krevního řečiště ruky pomocí zmíněné testovací aplikace. Falzifikát bude vycházet z biometrických charakteristik autora diplomové práce (žena, věk 25 let). Samotné měření bude provedeno za obvyklých podmínek uvnitř budovy, přičemž testování proběhne v zatemněné místnosti bez přímého dopadajícího světla na senzor.

Dále budou zpracovány výsledky systematického měření provedeného na senzoru za pomoci falzifikátu. Výsledky měření budou zaznamenány do tabulky a z jejich průměru bude vypočítána hodnota FAR a porovnána s hodnotou uvedenou výrobcem.

4. Přehled řešené problematiky

Dnešní svět se z velké části již přenesl do světa internetu, a proto jsou data, informace a znalosti dnes považovány za velmi hodnotné komodity a požadavky na jejich zabezpečení stále rostou. Přenos dat, uložení dat a způsob jejich interpretace – to vše jsou oblasti, které jsou v souvislosti se zabezpečením, značně diskutovány a zkoumány. [1]

4.1. Základní pojmy v oblasti biometrie

Biometrie je vědní obor, který v posledních letech upoutává čím dál tím větší pozornost oblastní věnujících se bezpečnosti osob, informací a objektů. Spojuje zkoumání různých přístupů identifikace člověka, vývoje automatizovaných systémů identifikace a praktického využití těchto systémů. Pro výzkum v oboru biometrie je nutné pochopit terminologii a objasnit základní poznatky z oblasti zabezpečení informačních technologií. [1]

4.1.1. Identita osob – způsoby identifikace a verifikace

Identita neboli totožnost udává logický vztah mezi dvěma objekty, které mají všechny své charakteristické znaky stejné. Z tohoto logického vztahu vyplývá, že každý objekt je identický pouze sám se sebou. Pojem identita osoby v sobě skrývá kombinaci biologických, psychologických, filozofických, sociálních, vrozených i získaných vlastností člověka. Tato práce je věnována identitě osoby z hlediska biologických charakteristik. [1, 2]

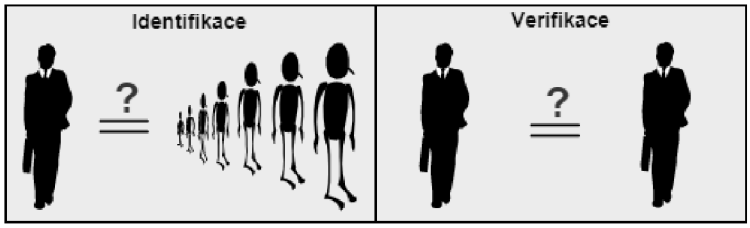
S procesem prokázáním identity jsou spojeny dva pojmy – identifikace a verifikace. Jsou to dva způsoby vyhodnocení identity objektu vůči jiným objektům. Hlavním rozdílem je cíl těchto procesů. Cílem identifikace je zjištění identity, cílem autentizace je prokázání identity (Obr. 1). [1]

Identifikace je proces stanovení, zda jsou porovnávané objekty identické. Toto porovnání je prováděno v poměru 1:N, tedy charakteristické vlastnosti dané osoby jsou porovnány s vlastnostmi všech osob zanesených v databázi. Tento proces je časově náročný, proto je tento způsob prověření identity většinou aplikován u méně náročných systémů s menší četností uživatelů daného systému. [1, 2]

Verifikace je proces vyhodnocení, zda je identita dané osoby shodná s identitou, kterou tato osoba stanoví. Je to tedy proces 1:1. Nejdříve je vybrán záznam v databázi, se kterým jsou

následně porovnány charakteristické vlastnosti osoby. Jestliže dojde ke shodě, je verifikace vyhodnocena kladně. Pojem verifikace bývá také označován jako „autentizace“. [1, 2]

Obr. 1 – Rozdíl mezi verifikací a identifikací



Zdroj: 2. DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. [Brno: M. Drahanský], 2011. ISBN 9788025489796.

Metody prokázání identity jsou rozděleny na tři kategorie:

Vlastnictví – tyto metody v sobě zahrnují identifikaci pomocí jména a příjmení, osobního dokladu, speciálních karet a čipů nebo biočipů. Nevýhodou těchto metod je proměnlivost, časová nestálost a vysoká četnost jmen, a také potenciální ztráta identifikačního prvku a poměrně jednoduchá falzifikace. [1, 2]

Znalosti – metody prokázání identity za použití znalostí využívají statická i dynamická hesla a PIN kódy. Nedostatkem těchto metod je přímá úměra bezpečnosti ku složitosti těchto hesel. Tyto metody jsou považovány za nejméně bezpečné, proto jsou většinou aplikovány v kombinaci s metodami identifikace na základě vlastnictví či biometrických charakteristik. [1]

Biometrické – využívají měřitelných vrozených a získaných biologických a fyziologických charakteristik člověka k prokázání jeho identity. Použití těchto charakteristik výrazně zvyšuje míru zabezpečení. [1, 2]

Často je též v souvislosti s identifikací osob spojován pojem „autorizace“, což je proces získání oprávnění k určitým operacím, který probíhá po provedení identifikačně-verifikačního procesu. [2]

4.1.2. Biometrie a biometrická charakteristika

Zcizení identity z hlediska identifikace osob je poměrně častým jevem. Použití biometrických metod identifikace osob zaručuje v tomto směru nejvyšší míru zabezpečení. [3]

Pojem biometrie v sobě nese vědní poznatky, výzkum a využití identifikace osob a objektů za pomoci automatizovaného rozpoznání vzorů biometrických charakteristik. Biometrická charakteristika je soubor markantů (znaků) biologické charakteristiky, který je

použit pro automatizované rozpoznání identity. Biometrické charakteristiky jsou univerzální, jedinečné, konstantní v čase, měřitelné, odolné a výkonné. Zpravidla jsou rozděleny do dvou kategorií – behaviorální a anatomicko-fyziologické. [1, 2]

Behaviorální metody využívají specifické dynamické rysy lidského chování. Řadí se mezi ně charakteristiky hlasu a řeči, mimiky obličeje, podpisu, chůze a dynamiky stisku kláves.

Anatomicko-fyziologické metody jsou oproti behaviorálním metodám neměnné a nezávislé na lidském chování, proto jsou častěji využívány. Používají vrozené charakteristiky, jako jsou například charakteristiky geometrie ruky, otisky prstů či krevního řečiště, charakteristiky obličeje, oční duhovky a sítnice. Mezi méně používané metody patří identifikace na základě DNA, pachu lidského těla a jeho rozměrů. [1, 2]

Mezi výhody použití biometrických charakteristik oproti jiným metodám identifikace osob, jako jsou vlastnictví či znalosti, patří:

- Uživatelský komfort – Biometrická charakteristika nemůže být zapomenuta či ztracena. Uživatel s sebou nemusí nosit např. kartu nebo čip v případě identifikace na základě vlastnictví či si pamatovat heslo nebo PIN.
- Vyšší bezpečnost – Uživatel může daný objekt ztratit (v případě vlastnictví). Heslo může být nechtěně prozrazeno. Biometrická charakteristika je v tomto případě nepřenositelná a její falzifikace je obtížná.
- Vyšší přesnost a rychlost při automatizované identifikaci.

Nevýhodou biometrických charakteristik je nemožnost jejich anulování, jako je to v případě hesel, čipů a karet. [1]

Při použití biometrických charakteristik pro identifikaci osob je důležité se zaměřit na výběr vhodně zvolené biometrické metody pro konkrétní aplikaci. Mezi hlavní parametry výběru se řadí náročnost prostředí, typ cílové skupiny a její velikost a míra zabezpečení. Poté jsou zvoleny potřebné vlastnosti biometrického systému a jejich míra (Tab. 1). [1]

Biometrická charakteristika je univerzální tehdy, když může být použita u většiny osob. Jedinečnost závisí na biometrické entropii neboli množství informace v konkrétní biometrické charakteristice. Ideální biometrická charakteristika by měla být konstantní v čase, jednoduše získatelná a výkonná. Její akceptovatelnost mezi uživateli by měla být vysoká a stejně tak

i odolnost proti falzifikaci. Posledním parametrem jsou náklady na zavedení a údržbu, které by měli být co nejmenší. [2, 4]

Tab. 1 – Porovnání vlastností nejpoužívanějších biometrických charakteristik

H - Vysoká M - Střední L - Nízká	Univerzalita	Jedinečnost	Konstantnost	Získatelnost	Výkonnost	Akceptace	Odolnost proti zfalšování	Náklady na pořízení
Obličej	H	L	M	H	L	H	L	L
Otisk prstu	M	H	H	M	H	M	H	L
Geometrie ruky	M	M	M	H	M	M	M	M
Žíly ruky	M	M	M	M	M	M	H	M
Duhovka oka	H	H	H	M	H	L	H	H
Sítnice oka	H	H	M	L	H	L	H	H
Podpis	L	L	L	H	L	H	L	L
Hlas	M	L	L	M	L	H	L	L

Zdroj: 2. DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. [Brno: M. Drahanský], 2011. ISBN 9788025489796. (upraveno)

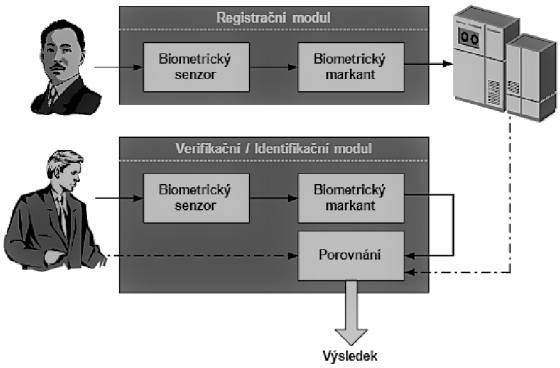
4.1.3. Biometrický systém

Obecný biometrický systém se skládá ze dvou modulů – verifikačně-identifikačního a registračního (Obr. 2). Registrační modul slouží pro zaznamenání a zápis biometrických markantů pomocí biometrického senzoru. Nejdříve je senzorem nasnímána biometrická charakteristika, ze které se poté extrahují markanty potřebné pro vytvoření referenční biometrické šablony, která je následně uložena do databáze. [2, 5]

Po registračním procesu následuje proces identifikačně-verifikační, kdy dochází k samotnému porovnání. Senzorem je nasnímána biometrická charakteristika, ze které se vyextrahují markanty a jsou porovnávány s referenční šablonou uloženou v databázi. [2, 5]

Většinou jsou tyto dva moduly obsaženy v jednom softwarovém balíčku a využívají jeden senzor. [2]

Obr. 2 – Schéma biometrického systému

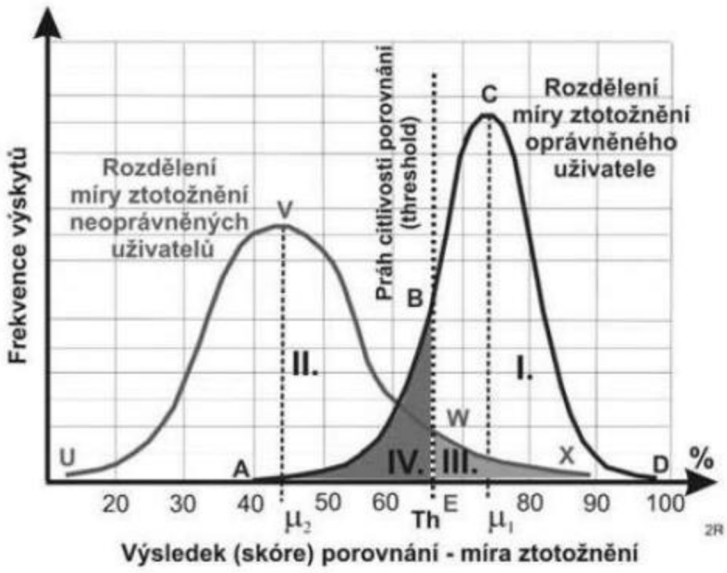


Zdroj: 2. DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. [Brno: M. Drahanský], 2011. ISBN 9788025489796.

Výsledek porovnání šablony s biometrickým vzorkem závisí na míře ztotožnění neboli tzv. skóre porovnání. Pro identifikačně-verifikační proces je nastaven určitý práh citlivosti tohoto skoré, čímž je rozhodování přímo ovlivněno. Práh citlivosti rozděluje tento proces na čtyři části (Obr. 3):

I. Korektní akceptace oprávněného uživatele
II. Korektní odmítnutí neoprávněného uživatele
III. Nekorektní přijetí neoprávněného uživatele
IV. Nekorektní odmítnutí oprávněného uživatele [1, 2]

Obr. 3 – Základní histogram rozdělení ztotožnění oprávněných a neoprávněných uživatelů



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

4.2. Spolehlivost a bezpečnost biometrických systémů

Kritéria výběru konkrétního biometrického systému do sebe zahrnují náklady na pořízení a provoz, uživatelskou přívětivost, specifika provozu a další parametry. Mezi nejdůležitější kritéria se řadí rychlost a spolehlivost identifikačně-verifikačního procesu. V praxi je u biometrických systémů často preferovaná spíše rychlost oproti bezpečnosti, avšak při aplikování těchto systémů je důležitý kompromis mezi těmito parametry. Spolehlivost biometrických systémů je měřena na základě pravděpodobnostních výpočtů situací, ke kterým během procesu rozpoznání může docházet. [1, 2]

4.2.1. Statistické základy pro měření spolehlivosti biometrického systému

Z matematického hlediska je identifikace definována jako porovnání množiny znaků X se všemi množinami znaků z celkového počtu množin N. Verifikace je definována jako porovnání množiny znaků X s konkrétní množinou znaků Y. Tato množina charakteristických znaků se nazývá biometrická entropie udávající množství informace obsažené v konkrétní biometrické charakteristice, které lze využít pro rozlišování osob. Čím vyšší je míra entropie, tím větší má daná biometrická charakteristika mezitřídní variabilitu, která udává různorodost jedinců mezi sebou. Takové systémy jsou robustnější také náročnější z hlediska automatizace procesu rozpoznání osob. U takových charakteristik totiž narůstá i vnitrotřídní variabilita neboli nestálost charakteristik během různých snímání, jako v případě identifikace pomocí charakteristik tváře, kdy daná osoba může měnit vzhled a mimiku. [2]

V ideální situaci by mezitřídní variabilita měla být co nejvyšší a vnitrotřídní variabilita by měla rovnat nebo blížit nulové hodnotě, nicméně v reálných aplikacích je tento ideální stav nedosažitelný. Proto je nutné analyzovat situace, kterým může v praxi docházet. [2]

Proces identifikace či verifikace osoby nabízí čtyři možné situace:

1) Osoba č. 1 je identifikována jako osoba č. 1 (požadovaný stav)
2) Osoba č. 1 je odmítnuta jako osoba č. 2 (chybný stav, nikoliv rizikový)
3) Osoba č. 1 je odmítnuta jako osoba č. 1 (chybný stav, nikoliv rizikový)
4) Osoba č. 1 je identifikována jako osoba č. 2 (chybný stav, rizikový)

Chybné stavy se v základě mohou rozdělit na dva typy:

a) Odmítnutí správného tvrzení.
b) Přijetí chybného tvrzení.

Tyto dvě chybná stanoviska negativně ovlivňují vyhodnocení identifikačně-verifikačního procesu. Každý biometrický systém je proto hodnocen na základě pravděpodobnosti výskytu tohoto chybného vyhodnocení. Mezi nejdůležitější faktory spolehlivosti patří pravděpodobnost chybného odmítnutí a pravděpodobnost chybného přijetí, které jsou vypočítány na základě statistických dat daného biometrického systému. [1, 2]

4.2.2. Měření spolehlivosti biometrického systému

Pravděpodobnost chybného odmítnutí neboli False Rejection Rate (FRR) udává procentuální chybovost daného biometrického systému v situaci, kdy dojde k chybnému negativnímu vyhodnocení správné identifikace dané osoby. Vypočítá se jako podíl počtu chybných odmítnutí k celkovému počtu porovnání. [1, 2, 4]

$$FRR = \frac{N_{FR}}{N_{EIA}} = \frac{N_{FR}}{N_{EVA}} = \frac{\text{počet chybných odmítnutí } (N_{FR})}{\text{počet pokusů oprávněných osob o identifikaci } (N_{EIA})/\text{verifikaci } (N_{EVA})}$$

Rce. 1 – False Rejection Rate

Pravděpodobnost chybného přijetí neboli False Acceptance Rate (FAR) udává procentuální chybovost daného biometrického systému v situaci, kdy dojde k chybnému pozitivnímu vyhodnocení identifikace osoby, která nemá právo na přístup. Vypočítá se jako počet chybných přijetí ku celkovému počtu porovnání. [1, 2, 4]

$$FAR = \frac{N_{FA}}{N_{IIA}} = \frac{N_{FA}}{N_{IVA}} = \frac{\text{počet chybných přijetí } (N_{FA})}{\text{počet pokusů neoprávněných osob o identifikaci } (N_{IIA})/\text{verifikaci } (N_{IVA})}$$

Rce. 2 – False Acceptance Rate

Z hlediska bezpečnosti biometrických systémů je hodnota FAR neboli míra chybného přijetí důležitým faktorem při výběru vhodného biometrického systému, neboť tato hodnota udává selhání odmítnutí možného útočníka. Dle normy ISO/IEC 15480 jsou definovány tři bezpečnostní skupiny biometrických systémů dle FAR [2]:

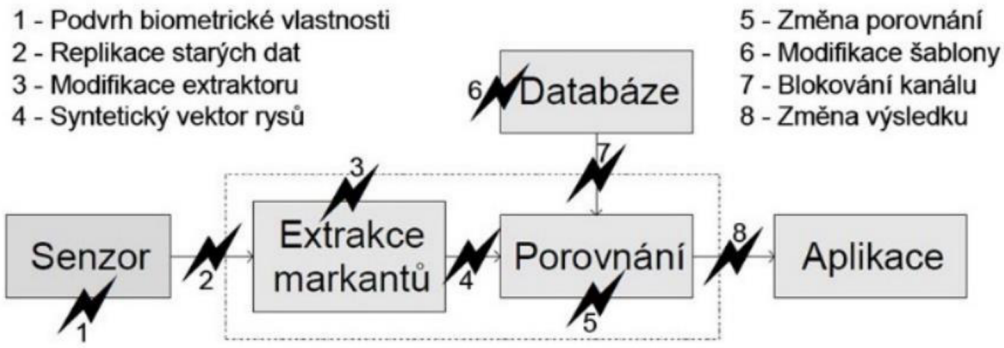
1. Základní FAR ≤ 10^{-2}
2. Střední FAR ≤ 10^{-4}
3. Vysoká FAR ≤ 10^{-6}

Mezi doplňující a přesnější koeficienty jsou řazeny: míra selhání registrace uživatele do systému (FTE – Failure To Enroll), míra selhání sejmutí biometrického vzorku (FTA – Failure to Acquire), míra chybné shody FMR (False Match Rate) a míra chybné neshody (FNMR – False Non-Match Rate). [4]

4.2.3. Slabá místa biometrického systému

Z hlediska zabezpečení informace a infrastruktury proti potenciálnímu napadení a zneužití dat je důležité eliminovat riziková místa a zamezit hrozbám pomocí bezpečnostních opatření. Pro určení spolehlivosti biometrického systému je potřeba obecně vymezit jeho zranitelná místa (Obr. 4), která mohou být potenciálně využita pro narušení procesu identifikace či verifikace. [2, 4]

Obr. 4 – Slabá místa biometrického systému



Zdroj: 2. DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. [Brno: M. Drahanský], 2011. ISBN 9788025489796.

1. Neoprávněné získání identity z hlediska senzoru může být realizováno několika způsoby. Přinucením či nátlakem na oprávněného uživatele. Popřením vlastní identity oprávněným uživatelem, který tvrdí, že jeho identita byla odcizena. Skrytým odcizením, paděláním či napodobením identity oprávněného uživatele tedy falzifikací biometrických dat předložených senzoru.
2. Mezi senzorem a extraktorem biometrických markantů lze využít opětovného odeslání dříve použitých biometrických dat.
3. Ovlivnění extraktoru markantů pomocí vygenerování množiny rysů a šablony.
4. Změna markantů během přenosu dat k porovnání.
5. Změna samotných výsledků porovnání.
6. Modifikace biometrické šablony v databázi, aby odpovídala předložených biometrickým údajům.
7. Útok na přenosový kanál mezi porovnávacím modulem a databází.
8. Změna finálního rozhodnutí.
9. Útok na samotnou aplikaci a zneužití administrátorských práv systému. [2, 6]

4.2.4. Spoofing a ochrana proti falzifikaci biometrických dat

Napadení biometrického systému může být provedeno třemi způsoby – narušení informační infrastruktury (hacking), sabotáž (DDoS útok) a bezprostřední útok na zařízení. Falzifikace biometrických údajů neboli metoda „spoofing“ je založena na přímém útoku na senzor při použití synteticky replikovaného artefaktu. Tato metoda neoprávněného získání identity je poměrně rozšířená a jednoduchá, proto je důležitá implementace ochranných prvků biometrických systémů. [1, 5, 7]

Způsoby ochrana proti spoofingu se obecně dělí na softwarově a hardwarově založené. Použití přídavného hardwaru přináší vyšší spolehlivost, zatímco použití speciálního softwaru vyžaduje nižší náklady. Kombinace obou přístupů přináší nejlepší řešení, pokud jde o bezpečnost. [6]

Softwarově založené systémy zpravidla využívají metodu multifaktorového ověření spojující identifikaci na základě biometrických vlastností a znalostní. Také jsou využívány speciální algoritmy pro extrakci různých charakteristických znaků a algoritmy porovnání eliminující úspěšné identifikace pomocí nekvalitního artefaktu. [6]

Hardwarově založená ochrana vychází zpravidla z aplikovaných senzorů, které mohou být unimodální a multimodální. Unimodální senzory snímají pouze jednu biometrickou charakteristiku, je proto nutné použít více takových senzorů nebo aplikovat například multifaktorové ověření identity. Multimodální senzory dokážou snímat více biometrických vlastností najednou či více charakteristických znaků u jedné biometrické charakteristiky, čímž poskytují vyšší míru ochrany a výrazně snižují úspěšnost útoků, neboť útočník musí získat dvě různé biometrické charakteristiky konkrétní osoby a úspěšně podvrhnout dvě různé technologie biometrických snímacích zařízení. [2, 5]

Doplňující znaky, které se dají využít jako ochrana proti falzifikaci biometrických údajů, mohou být visuálního (barva, tvar textura), fyzického (hustota, tuhost, elasticita), spektrálního (absorpce, odrazivost) a elektrického charakteru (permitivita, kapacitance). Tento způsob ochrany proti spoofingu je založen na tzv. detekci živosti, kdy se z velké části jedná o snímání tzv. nedobrovolných projevů, jako jsou krevní tlak, puls, pocení, pohyby zornic a další. [6]

4.2.5. Normy a obecné požadavky na senzory

Při rozšíření použití biometrie v identifikačně-verifikačních procesech bylo nezbytné zavedení norem umožňujících propojení jednotlivých složek biometrických systémů, jejichž dodržování umožnuje výměnu jednotlivých částí systému za provozu bez nutnosti znovunastavení systému. [2]

Kategorie norem jsou rozděleny podle tři základních vrstev biometrického systému: Normy, související s vrstvou API (aplikační programové rozhraní), umožňující vytvářet aplikace nezávislé na produktech od konkrétních výrobců a snadnější integraci vytvořené aplikace. Tyto normy byly vytvořeny organizacemi ISO a BioAPI Consortium. [1, 2]

Další vrstva se zaobírá formátem biometrické šablony a přenosem dat v ní uložených. Cílem standardizace formátu biometrické šablony je používání biometrického systému bez nutnosti znovu registrace uživatelů i v případě výměny části systému. ISO/IEC 19794 je norma, která definuje formát biometrických dat jako šablony i částečně zpracovaných dat. Další důležitou normou je Americký národní standard pro IS zabývající se formátem a přenosem dat otisků prstů, obličeje a dalších biometrických údajů (ANSI/NIST). Přestože jsou stanoveny tyto normy, sjednocení formátů biometrických šablon je velice zdlouhavý proces, neboť mnoho výrobců používá své vlastní formáty šablon a vytváří vlastní software, který mnohdy převyšuje zavedené standardy svou kvalitou. [1, 2]

Poslední vrstva je vrstva ovladače, jejíž standardizace umožňuje použití různých senzorů od rozličných výrobců bez nutnosti výměny celého systému. Společnost Microsoft zavedla normu WDM pro operační systém Windows, také se využívají normy NTSC či RS-170. [1, 2]

Kromě norem jsou také obecně vymezeny požadavky na senzory, mezi které se řadí:

- Vyhovující rozměry
- Přijatelná snímací plocha
- Dostatečné rozlišení
- Opakovatelnost dosažené kvality obrazu
- Uživatelská přívětivost
- Odolnost vůči mechanickému poškození
- Spolehlivost a ochrana vůči napodobení
- Dlouhá životnost [4]

4.3. Základní přehled nejběžnějších biometrických systémů a jejich ochrany proti spoofingu

Biometrické systémy jsou obecně děleny podle charakteru použité biometrické vlastnosti, které jsou dvojího typu – behaviorální charakteristiky vycházející z chování člověka, a anatomicko-fyziologické založené na vrozených vlastnostech. [1]

4.3.1. Behaviorální charakteristiky

Identifikace osob pomocí behaviorálních charakteristik souvisí s unikátním vzorem chováním dané osoby. Mezi nejrozšířenější metody patří identifikace pomocí charakteristik hlasu a řeči, chůze a podpisu. Mimoto jsou do této kategorie též řazeny metody identifikace pomocí mimiky obličeje a dynamiky stisku kláves, které jsou však méně rozšířené. [1]

4.3.1.1. Charakteristiky hlasu

Biometrický systém identifikace osob na základě charakteristik hlasu využívá analýzu zvukových vln v čase, kdy se zaznamenávají určité vlastnosti, jako jsou tón, výška a rychlost. Tyto biometrické systémy jsou rozděleny do tří kategorií – závislé na textu, nezávislé na textu a interaktivní. Systémy závislé na textu využívají stejnou sekvenci znaků (např. jedno slovo) pro každý pokus o identifikaci či verifikaci. Jsou nejméně spolehlivé a odolné vůči falzifikaci dat. Tyto systémy lze jednoduše obejít pomocí záznamu pořízeného na diktafon. Systémy nezávislé na textu jsou z hlediska automatizace poměrně obtížné, a proto jsou především využívány ve forenzních aplikacích. Interaktivní systémy fungují na principu výzva-odpověď, kdy systém náhodně vybere slovo, které musí uživatel vyslovit. Systém poté zpracuje hlasový signál, určí obsah řeči a následně ho porovná s uloženou šablonou. Účinnou ochranu proti spoofingu u identifikace osob pomocí hlasu přináší samotný princip interaktivního biometrického systému, kdy útočník nemůže přesně vědět, jaké slovo bude vyžadováno pro identifikaci. Tento princip má v základu zabudované testování živosti, proto potenciální útočník nemůže použít předem získanou nahrávku. Nejvíce používaným způsobem ochrany je integrace speciálních algoritmů na detekování falzifikátu pomocí matematické analýzy hlasového signálu. [1, 2, 6, 8]

4.3.1.2. Charakteristiky chůze

Identifikace osob pomocí chůze jedinečné pro každého jedince, je zaměřena na analýzu složitého vzoru lokomoce. Tato metoda je zejména využívaná při procesu verifikace osob a je

velice praktická z hlediska přirozenosti a přijatelností uživatelů, avšak je značně obtížná vzhledem k samotné automatizaci rozpoznání osob, ukládání dat a času potřebného pro výpočty. Chůze je analyzována dvěma způsoby – modelově orientovaným přístupem a analýzou pohybu siluety. Nejčastěji používanou metodou je záznam pohybu trajektorie určitých bodů na těle (většinou těžiště) vytvářející specifickou křivku podobnou sinusoidě, která je následně transformována do matematického modelu neboli biometrické šablony. Analýza pohybu siluety zaznamenává délky kontur siluety, které jsou zaneseny do grafu, čímž vytváří charakteristickou biometrickou šablonu. Identifikace osob na základě analýzy pohybu při chůzi je poměrně novou metodou v oblasti biometrie, proto ochrana proti spoofingu prozatím nebyla dostatečně prozkoumána. Avšak těmto útokům lze čelit účinnou metodou využití více kamer, které snímají osobu z více úhlů, čímž je možné zabránit útokům, kdy je přehrán video záznam před snímající kamerou. Dalším možným způsobem ochrany je detekce živosti pomocí použití akcelerometru, který má osoba připevněný na noze. [1, 4, 6, 8]

4.3.1.3. Charakteristiky podpisu

Identifikace osob na základě podpisu, spojená s dovedností písemného projevu a individuálním charakteristickým rukopisem člověka, je velice intuitivní, nenáročná a dobře akceptovatelná metoda. Tyto biometrické systémy jsou podle použitých technologií rozděleny na off-line systémy a on-line systémy. Off-line systémy, využívané především ve forenzní aplikaci, jsou založené na statistických vlastnostech podpisu, kdy je podpis digitalizován pomocí kamery nebo skeneru, zanesen do souřadnicové soustavy a porovnán pomocí algoritmů s údaji v databázi. On-line systémy využívají jak statické, tak i dynamické vlastnosti podpisu, jako jsou čas, tlak, zrychlení a trajektorie, zaznamenávané pomocí tabletu nebo PDA záznamníku. Všeobecně jsou tři možné způsoby falzifikace podpisu – náhodná shoda s podpisem jiné osoby v databázi; snaha o shodu nezaměřená na konkrétní osobu a cílené napodobení týkající se konkrétní osoby. Ochrana proti spoofingu pomocí detekce živosti je u off-line systémů téměř nemožná, zatímco u on-line systémů je detekce živosti obsažena přímo v principu metody. Bohužel v případě, kdy potenciální útočník okouká statistické i dynamické charakteristiky, je určení falzifikace velmi obtížnou úlohou i u těchto systémů. Nepřímou metodou anti-spoofingu je využití této metody v kombinaci s jinou metodou identifikace. [1, 4]

4.3.2. Anatomicko-fyziologické charakteristiky

Identifikace osob pomocí anatomicko-fyziologických charakteristik je spojena s genetickými predispozicemi člověka, jejichž výhodou je neměnnost z hlediska času. Nejvíce individuálních biometrických charakteristik lze najít na rukou a tváři. Mezi nejrozšířenější metody identifikace pomocí anatomicko-fyziologických charakteristik patří charakteristiky tváře snímané pomocí 2D a 3D technologií, charakteristiky sítnice a duhovky lidského oka a charakteristiky ruky, jako jsou geometrie ruky, otisk prstu a struktura krevního řečiště ruky. Mezi méně rozšířené metody patří identifikace osob pomocí termogramu obličeje či ruky, dentálního obrazu, snímku nehtu, DNA a tvaru vnějšího ucha. [1, 2, 9]

4.3.2.1. Charakteristiky tváře

Rozpoznání osob pomocí charakteristik tváře je nejvíce vědecky zkoumaná oblast biometrie. Nárůst aplikování této metody v praxi je způsoben zejména vysokou akceptovatelností uživateli, nízkými náklady na pořízení potřebného zařízení a snadným bezkontaktním snímáním dat, což je ale zároveň velký handicap, neboť získání těchto biometrických dat je poměrně jednoduché i pro potenciálního útočníka. Analýza charakteristik tváře je prováděna na základě 2D snímku, 3D snímku a termosnímku. Postupy získávání těchto dat se opírají o tzv. strojové vidění[1], kdy je provedena detekce a lokalizace tváře na snímku, a poté jsou extrahovány biometrické markanty. Metoda rozpoznání pomocí 2D snímku tváře využívá geometrických charakteristik výrazných bodů v obličeji (vzdálenost středu očí, šířka a výška nosu, tvar rtů apod.). Robustnější řešení z hlediska falzifikace biometrických dat nabízí metoda 3D snímku poskytující více informací zpracovávaných pomocí geometrického modelu. Identifikace osob pomocí termosnímku, disponuje vysokou mírou spolehlivosti na úkor vysokých nákladů. [1, 4, 8]

Útoky na biometrické systémy rozpoznání tváře jsou hojně diskutovány z důvodu nárustu počtu způsobů potenciálních útoků na tento druh systémů. 2D snímek lze obelstít například fotografií v měřítku 1:1 nebo maskováním pomocí líčidel, 3D snímek lze obejít použitím speciální celohlavové masky nebo v extrémních případech absolvováním plastické operace. Bylo provedeno nespočet studií zaměřených na prolomení biometrických metody identifikace pomocí charakteristik tváře, ze kterých pak vycházel výzkum inovativních způsobů ochrany proti spoofingu. Účinnou ochranou je detekce živosti prostřednictvím pohybu ať už

[1] Odvětví získávání a analýzy informací zachycených pomocí výpočetní techniky.

spontánního či na principu výzvy uživatele o provedení určitého pokynu (pohyb rtů, rotace hlavy, mrknutí nebo změna výrazu obličeje). Tento způsob ochrany lze oklamat videozáznamem, čemuž lze předejít použitím více nezávislých kamer společně s analýzou odrazivosti, textury a gradientní struktury charakteristických rysů tváře pomocí matematických algoritmů. [6, 10, 11]

4.3.2.2. Charakteristiky oka

Metody identifikace osob pomocí individuálních rysů lidského oka se řadí mezi biometrické systémy s nejvyšší mírou přesnosti, spolehlivosti a odolnosti vůči útokům. Biometrické charakteristiky oční duhovky a sítnice v sobě nesou veliký počet informací, které jsou v průběhu života neměnné, a proto mohou být aplikovány v systémech s velkým množstvím uživatelů. [1, 2, 8]

Oční duhovka je sval reagující na světlo smrštěním a roztahováním oční pupily, jehož barva, ovlivněná množstvím melaninu, a textura jsou dány genetickými predispozicemi. Biometrická metoda rozpoznání osob na základě matematické analýzy rozličných vzorů oční duhovky (rýhy, prstence, hřebeny, pihy atd.) využívá monochromatické CCD kamery citlivé na NIR světlo o vlnových délkách mezi 700 až 900 nm, která nezpůsobuje poškození oka a diskomfort v průběhu skenování. Systémy identifikace osob prostřednictvím duhovky jsou považovány za jedny z nejpřesnějších a nejspolehlivějších přístupových systémů využívaných na letištích (USA, Velká Británie, Kanada), ve věznicích i jaderných elektrárnách. [1, 2, 8, 12]

Sítnice je vrstva citlivá na světlo nacházející se na zadní straně oční bulvy, kterou zásobuje krví síť cév vystupujících ze zrakového nervu. Identifikace osob pomocí charakteristik sítnice vychází z principu snímání struktury cév, jejíž pravděpodobnost shody u dvou různých lidí je $1{:}10^{78}$. Zařízení používaná pro tuto metodu identifikace osob vycházejí z lékařských optických přístrojů (retinoskop). Pro snímání je použito infračervené LED diody vysílající paprsek světla na sítnici, odražené světlo pak vytváří charakteristický snímek zachycený pomocí CCD kamery. Z vytvořeného snímku je extrahována prstencová oblast, jejíž kontrastní rozdíly jsou následně zpracovány do binárního čísla o čtyřiceti bitech. [1, 2, 4]

Falzifikace biometrických údajů duhovky a sítnice není snadné, ale také není zcela nemožné. Metodu identifikace pomocí duhovky lze obelstít použitím texturovaných kontaktních čoček nebo uměle vytvořené oční bulvy. Nejčastěji používaným falzifikátem je černobílá fotografie oka vytištěná na papíře pomocí běžné inkoustové tiskárny. Jako ochrany

proti spoofingu je u tohoto biometrického systému využíváno detekce živosti vlivem fyziologických projevů. Mezi metody detekce těchto projevů patří: detekce mrkání pomáhající rozeznat skutečnou duhovku od falzifikátu díky své vizuální výraznosti; detekce přítomnost krve v cévkách bělma snímaná NIR světlem; detekce pupilárního reflexu při záměrné změně intenzity světla, kdy zornice reaguje smrštěním a roztahováním v rozmezí 250 až 400 ms; a měření změny poměru mezi průměrem zornice a duhovky při tzv. neklidu zornic (hippus), což je stav rytmické kontrakce a dilatace zornice při konstantní intenzitě světla. [1, 2, 6]

Biometrická metoda skenu sítnice je jednou z nejnovějších metod identifikace osob, proto metody ochrany proti spoofingu nebyly dosud dostatečně prozkoumány. I přesto je velice těžké tento biometrický systém oklamat, neboť oproti snímku duhovky je velice náročné získat obraz charakteristik sítnice pro účely oklamání biometrického systému, protože nejsou viditelné bez použití speciální techniky. Nicméně u aplikací, kde je vyžadováno skutečně robustní zabezpečení, jsou k tomuto systému přidány techniky detekce živosti prostřednictvím pohybu oka nebo metody podmíněné detekce mrknutí na principu výzva-odpověď. [1, 2, 6]

4.3.2.3. Geometrie ruky

Metoda identifikace osob na základě geometrie ruky je založena na snímání individuálních charakteristik, jako jsou; rozměry a tvar kontur ruky (silueta); délka a šířka dlaně, prstů a kloubů; vyvýšeniny a záhyby apod. Tato metoda je přívětivá zejména pro svou rychlost, jednoduchost, vysokou akceptovatelnost mezi uživateli a nízké náklady na pořízení a provoz. Její obrovskou výhodou je také malá velikost referenční šablony, která v porovnání s jinými metodami identifikace zabírá pouhých devět bitů. Vzhledem ke své robustnosti je preferovanou metodou zabezpečení přístupů do objektů a docházkových systémů především v průmyslovém odvětví, kde je možné se setkat se zašpiněním ruky uživatele nepředstavujícím překážku pro tento systém identifikace. Při samotném procesu identifikace uživatel umísťuje ruku na specifickou horizontální plochu s vysokou odrazivostí a speciálními distančními kolíky sloužící pro správné a při každém měření stejné umístění ruky a prstů. Následně je CCD kamerou s rozlišením cca 100–200 DPI pořízen snímek ve stupních šedi, ze kterého jsou extrahovány charakteristické rysy. Tato zařízení jsou dvojího typu – s přímou optickou cestou, kdy je kamera umístěna přímo nad ruku uživatele, a nepřímou optickou cestou využívající soustavy zrcadel odrážejících scénu přímo do kamery. [1, 2, 8, 9]

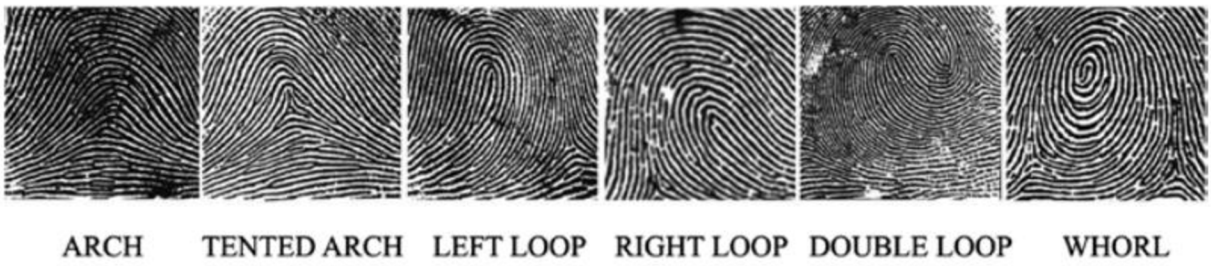
Základní myšlenka ochrany proti spoofingu u této metody rozpoznání osob vychází ze samotného principu zařízení využívaného pouze pro verifikační proces, kdy se uživatel

společně s biometrickou charakteristikou prokazuje též PIN kódem, čipem nebo ID kartou, do kterých lze uložit samotnou referenční šablonu bez nutnosti napojení na databázi. Další možností ochrany je použití této metody v kombinaci s jinou biometrickou metodou identifikace, jako je otisk dlaně či otestování živosti pomocí skenu krevního řečiště ruky. Testování živosti u této metody identifikace může být také zprostředkováno snímáním podmíněného tlaku prstů na distanční kolíky. Pro zvýšení spolehlivosti je také používáno postranní zrcadlo pro snímání tloušťky ruky, nicméně většina na trhu dostupné aparatury využívá pouze 2D charakteristik. [2, 6, 8, 9]

4.3.2.4. Otisk prstu

Identifikace osob pomocí otisku prstu je nejvíce používaná a probádaná metoda na světě vycházející z daktyloskopie[2] aplikované v policejně-soudní identifikaci. Tato biometrická metoda je založena na snímání charakteristických během života neměnných markantů tvořených jedinečnou strukturou papilárních linií, jejichž výška činí v průměru 0,1 – 0,4 mm a šířka 0,2 – 0,5 mm a v průběhu života je neměnná. Z globálního hlediska jsou otisky prstů děleny do pěti základních tříd – oblouk, klenutý oblouk, spirála, levá smyčka, pravá smyčka a dvojitá smyčka. (Obr. 5). Primárními markanty využívanými v bezpečnostních biometrických systémech jsou – delta (místo, kde se papilární linie rozbíhají do tří směrů), jádro (střed otisku prstu), potní póry ad. (Obr. 6). [1, 2, 9]

Obr. 5 – Třídy otisků prstů (zleva – oblouk, klenutý oblouk, levá smyčka, pravá smyčka, dvojitá smyčka, spirála)



Zdroj: 8. DASGUPTA, Dipankar, Arunava ROY a Abhijit NAG. Advances in User Authentication. Springer International Publishing, 2017. Infosys Science Foundation Series. ISBN 978-3-319-58806-3.

Na trhu existuje velké množství technologií snímání otisku prstu, která se dělí do třech kategorií na základě získání snímku – skenování inkoustového otisku, statické snímání a snímání šablonováním. V komerčně-bezpečnostní sféře je využíváno statického snímání a snímání šablonováním. [2, 4]

[2] Věda o otiscích prstů

Obr. 6 – Markanty otisku prstu

Zdroj: 13. DRAHANSKÝ, Martin. Biometrické systémy: Studijní opora. Vysoké učení technické v Brně, Brno, 2006.

S rozšířením použití metody identifikace osob pomocí otisku prstů se rozšířilo i povědomí o slabých místech těchto biometrických systémů. V průběhu let bylo provedeno nespočet výzkumů týkajících se senzorů otisku prstu a jejich ochrana proti spoofingu je nadmíru diskutovaným tématem z důvodu poměrné jednoduchého získání a padělání těchto biometrických údajů (např. sejmutí otisku ze skleněné plochy atp.). Existuje veliký počet technologií snímání, přičemž každá technologie je založena na jiném principu a přináší různé možnosti ochrany. [6, 8, 14]

Optické senzory detekují živost prstu pomocí změny barvy kůže od růžové k bílé při tlaku prstu na senzor. Většinou je tato vlastnost snímána v kombinaci se spektroskopickými charakteristikami kůže založenými na různé absorpci a odrazivosti jednotlivých vrstev kůže na základě jejich chemického složení. Na podobném principu fungují ultrazvukové senzory, kdy ultrazvukové vlny pronikají až pod povrch kůže a odrážejí se zpět k snímači, přičemž vlny odražené ze živého prstu nejsou charakteristické pro ultrazvukové vlny odražené od umělého prstu. Dalším charakteristickým znakem lidské kůže je pocení, které může být detekováno pomocí kapacitních senzorů snímajících vysoký rozdíl dielektrické konstanty potu a suché kůže. Také je často využíváno detekce živosti na základě detekce pulsu a oxidace krve pomocí pulzního oxymetru. [2, 5, 15]

4.4. Identifikace osob pomocí skenu krevního řečiště ruky

Biometrická metoda identifikace osob pomocí skenu krevního řečiště ruky je založena na snímání jedinečné stromové struktury cév daného jedince. Jedná se o jednu z nejnovějších metod identifikace osob, která přináší vysokou míru spolehlivosti a odolnosti vůči falšování biometrických údajů. Mimo jiné je tato metoda dobře akceptovatelná uživateli z důvodu bezkontaktního a neinvazivního přístupu. [1, 2]

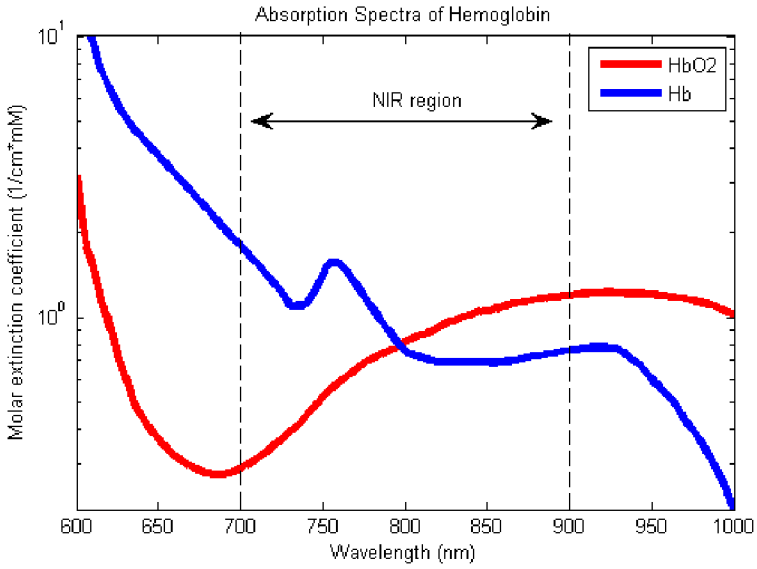
Sktrukturu cév tvoří tepny, přenášející okysličenou krev, a žíly, přenášející odkysličenou krev. Formování struktury probíhá již v prenatálním období, je u každé osoby unikátní (včetně jednovaječných dvojčat) a od dovršení dospělosti časově stálá, avšak vlivy stárnutí u této biometrické metody dosud nebyly dostatečně prozkoumány. Jedinečnost této biometrické charakteristiky poskytuje vysokou biometrickou entropii, čímž je umožněno tuto metodu identifikace aplikovat u systémů s až 18 tisíci uživatelů. Pokud jde o ovlivnění výsledku identifikace, onemocnění kůže či její zašpinění má na tento proces minimální vliv, avšak větší zranění narušující strukturu cév (zlomenina, chirurgický zákrok atp.) negativně ovlivňuje identifikačně-verifikační proces. [1, 2, 4]

4.4.1. Princip snímání obrazu krevního řečiště

Snímání obrazu krevního řečiště je založeno na principu pořízení černobílého snímku stromové struktury žil. Jelikož se cévy nacházejí uvnitř lidského těla, ve spektru viditelného světla je pořízení snímku struktury cév velice obtížné, proto je potřebné dodatečné nasvícení při snímání. K tomu je využíváno infračerveného zdroje světla citlivého na vyzařované teplo, který na základě různé absorpce záření cév oproti okolní tkáně vykreslí plošný obraz rozložení cév. Okysličené a odkysličené molekuly hemoglobinu v krvi absorbují záření elektromagnetického spektra o vlnové délce v rozmezí 650 až 950 nm odpovídající oblasti NIR světla (700–1400 nm). Odkysličený hemoglobin nejlépe pohlcuje IR světlo o vlnové délce cca 760 nm, zatímco okysličený hemoglobin nejvíce absorbuje záření o vlnové délce mezi 900–950 nm (Obr. 7). U systémů identifikace osob pomocí skenu krevního řečiště ruky je většinou využíváno zdroje světla vlnové délky 850 nm, které lépe proniká kůží. [1, 2, 9]

Obraz struktury cév je následně zachycen pomocí monochromatické CCD kamery citlivé na vlnové délky 1100 nm (v rozmezí NIR). Samotný proces nasnímání je kratší než 0,5 sekund a jeho výstupem je snímek v 16 stupních šedi. Výhodou použití CCD kamer jsou nízké pořizovací náklady a jednoduchost zpracování. [1, 2, 4]

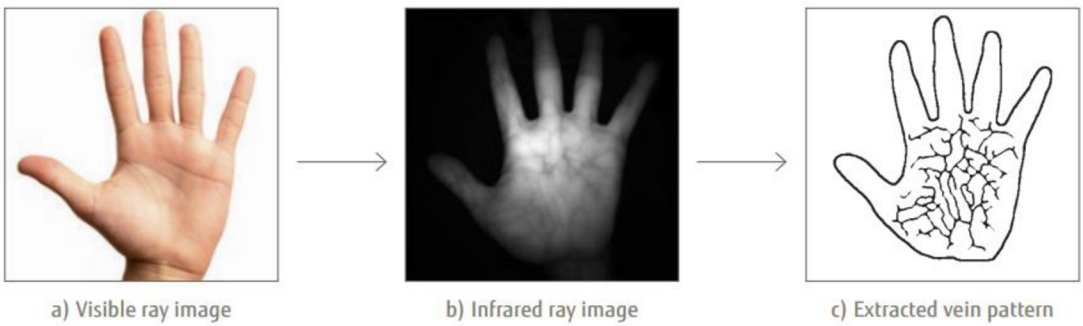
Obr. 7 – Spektrum absorpce světla hemoglobinu



Zdroj: 16. PARKER, Frank S. Near-Infrared Spectroscopy. Applications of Infrared Spectroscopy in Biochemistry, Biology, and Medicine. Boston, MA: Springer US, 1971, 1971, 25-40. ISBN 978-1-4684-1874-3. Dostupné z: doi:10.1007/978-1-4684-1872-9_2

Po pořízení snímku dochází k jeho segmentaci na oblasti zájmu (ROI) a eliminaci pozadí, kdy se extrahují kontury, a získává se geometrické rozmístění krevního řečiště. Následně je snímek oblasti zájmu upraven pomocí redukce šumu a vyhlazení hrubých přechodů. Dalším krokem je lokální prahování, kdy dochází k oddělení struktury žil od okolního prostředí. K tomu je využíváno různých segmentačních metod – segmentace porovnáním, segmentace oblastí, hranová segmentace ad. Poté následuje postprocessing, kdy jsou provedeny finální úpravy včetně odstranění šumu a je vytvořena černobílá biometrická šablona o velikosti přibližně 250 B. Samotný proces extrakce rysů a vytvoření biometrické šablony trvá přibližně 1–2 sekundy. (Obr. 8) [2, 4]

Obr. 8 – Proces extrahování referenční šablony krevního řečiště dlaně



Zdroj: 17. FUJITSU LTD. Fujitsu PalmSecure: The solution for user-friendly and reliable authentication – more secure than the competition. [online]. [cit. 2022-02-04]

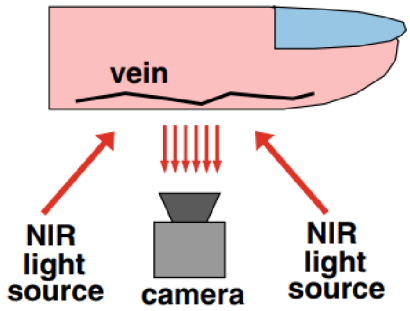
4.4.2. Metody snímání obrazu krevního řečiště

Metody snímání obrazu krevního řečiště se dělí na základě umístění snímacích prvků – CCD kamery a zdroje NIR záření. Jejich vzájemná poloha umožňuje tři různé metody: reflexivní, transmisivní a s použitím bočního světla. [18]

4.4.2.1. Reflexivní metoda

Reflexivní metoda snímání obrazu krevního řečiště využívá senzorů, které obsahují zároveň kameru i zdroj IR světla. Princip spočívá v záznamu rozdílů odraženého NIR světla přímo do kamery (Obr. 8). Cévy absorbující IR světlo se na výsledném snímku jeví tmavší než jejich okolí. Tento kontrast však u této metody nedosahuje příliš velikých hodnot, neboť je světlo odraženo také od povrchu prstu, proto je identifikačně-verifikační proces o něco zdlouhavější, nicméně stále se pohybuje v rozmezí přijatelné časové délky. Výhodou této metody jsou kompaktní rozměry senzoru a jednodušší manipulace ze strany uživatelů. [18]

Obr. 9 – Reflexivní metoda snímání krevního řečiště prstu

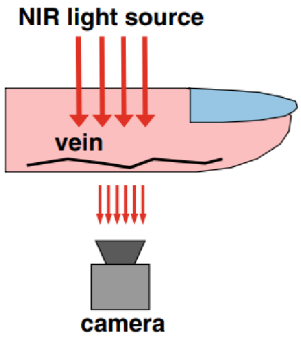


Zdroj: 18. UHL, Andreas et al. Handbook of Vascular Biometrics [online]. Cham: Springer, 2020;2019. ISBN 3030277313; 9783030277314; 3030277305; 9783030277307.

4.4.2.2. Transmisivní metoda

Transmisivní metoda je založena na principu prosvícení ruky skrz, kde se na druhé straně nachází snímací kamera. Tato metoda poskytuje vysoce kontrastní obraz stromového uspořádání cév, protože není snímáno odražené světlo (Obr. 9). Nevýhodou této metody je menší akceptovatelnost uživateli oproti reflexivní metodě z důvodu, že uživatel vkládá ruku či prst do zařízení tak, že není vidět, což může způsobovat obavy ze strany. Další potíží jsou větší rozměry celého zařízení, proto je tato metoda většinou využívána pouze pro sken krevního řečiště prstu. [18]

Obr. 10 – Transmisivní metoda snímání krevního řečiště prstu

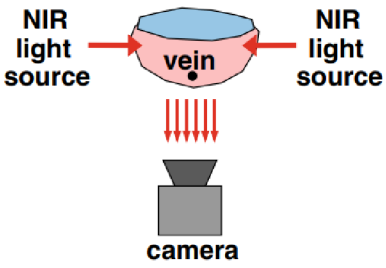


Zdroj: 18. UHL, Andreas et al. Handbook of Vascular Biometrics [online]. Cham: Springer, 2020;2019. ISBN 3030277313; 9783030277314; 3030277305; 9783030277307.

4.4.2.3. Metoda s použitím bočního světla

Třetím typem osvětlení je metoda snímání za pomoci bočního světla umožňující použití „otevřeného“ senzoru jako v případě reflexivní metody, čímž se zamezí uživatelskému diskomfortu. Této metody snímání se též využívá především u skenu krevního řečiště prstu z důvodu menší plochy snímání. Zdroje NIR světla mohou být umístěny buď z obou stran prstu, nebo pouze z jedné strany. Bočním světlem je docíleno jeho rozptýlení, čímž kamera může zachytit vysoce kontrastní obraz. Nevýhodou je přeexponování kontur prstu, které snižují velikost oblasti zájmu snímku. [18]

Obr. 11 – Metoda snímání krevního řečiště prstu s použitím bočního světla



Zdroj: 18. UHL, Andreas et al. Handbook of Vascular Biometrics [online]. Cham: Springer, 2020;2019. ISBN 3030277313; 9783030277314; 3030277305; 9783030277307.

4.4.3. Rozdělení na základě snímané části ruky

Identifikace osob na základě skenu krevního řečiště je na základě výběru snímané části ruky dělena na – sken krevního řečiště prstu, sken krevního řečiště hřbetu ruky a sken krevního řečiště celé dlaně. Každý přístup má své výhody a nevýhody, které je nutno zohlednit při aplikování těchto metod v praxi. [1, 2]

4.4.3.1. Identifikace osob na základě skenu krevního řečiště prstu

Identifikace osob na základě skenu krevního řečiště prstu je nejjednodušší biometrickou metodou v této oblasti. Avšak, oproti metodám zmíněným níže, tato metoda poskytuje mnohem méně biometrických dat (snímaná oblast cca 900 mm^2), čímž také klesá biometrická entropie. U biometrických systémů s menším počtem uživatelů se úroveň spolehlivosti a bezpečnosti této metody dá zvýšit implementací senzoru otisku prstu nepředstavující značné snížení kompaktnosti daného zařízení. [2, 18, 19]

4.4.3.2. Identifikace osob na základě skenu krevního řečiště hřbetu ruky

Méně využívanou metodou je identifikace na základě skenu krevního řečiště hřbetu ruky, kdy jsou snímány cévy rozmístěné na horní části ruky. Oproti snímku krevního řečiště prstu poskytuje větší množství biometrických informací, ale menší pohodlí pro uživatele z důvodu sevření pěsti kvůli zvýraznění cév. [18]

4.4.3.3. Identifikace osob na základě skenu krevního řečiště dlaně

Nejrozšířenější metodou je snímání krevního řečiště dlaně přinášející možnost extrakce většího množství biometrických údajů. Přibližná velikost snímané oblasti se pohybuje kolem 7 200 mm^2, což je 8 krát více než snímaná oblast krevního řečiště prstu. Míra uživatelské akceptovatelnosti je vysoká z důvodu pohodlnosti a rychlosti této biometrické metody. Jedná se také o nejbezpečnější přístup identifikace osob pomocí skenu krevního řečiště, poněvadž oproti prstu je krevní řečiště dlaně tvořeno větším počtem silnějších cév. [2, 18, 19]

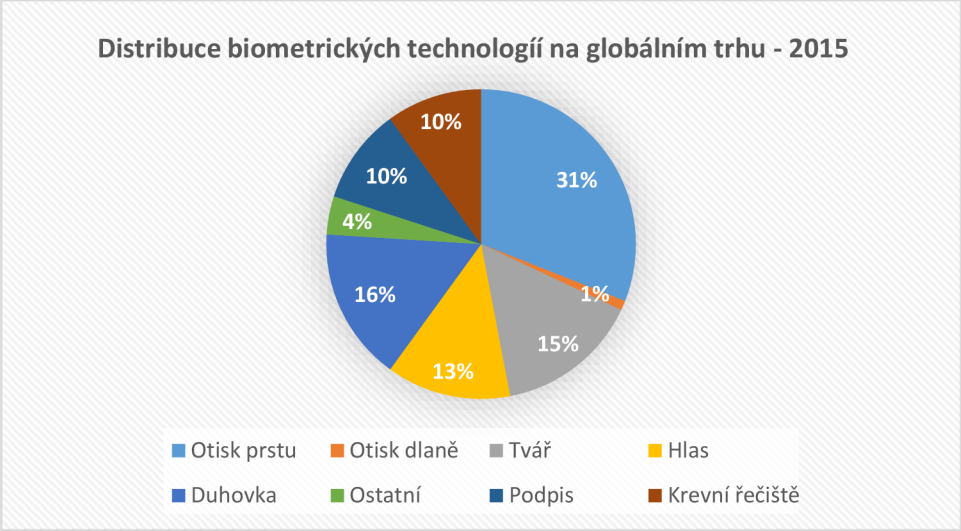
4.4.4. Ochrana proti spoofingu

Ochrana biometrických systémů skenu krevního řečiště proti spoofingu je založena především na testování živosti subjektu, které spočívá v samotném principu metody. Přestože krevní řečiště není viditelné pouhým okem, je možné získat tyto biometrické údaje pomocí speciálně upravené kamery. Pro zvýšení bezpečnosti těchto systémů identifikace je proto využíváno doplňujících snímačů – termokamera, snímač proudění krve, otisk prstu, které následně extrahují komplementární biometrické charakteristiky. Dalším ověřeným způsobem ochrany je využití multifaktorového ověření v kombinaci s metodou identifikace pomocí znalostí či vlastnictví. [2]

4.4.5. Využití metody v praxi

V posledních letech si biometrické systémy skenu krevního řečiště posílily své postavení na globálním trhu systémů identifikace osob (Obr. 12). Avšak oproti jiným biometrickým metodám, výrobců zabývající se biometrickými systémy a jejich distribucí na trhu není příliš mnoho. Lídry na tomto trhu jsou zejména japonské společnosti Hitachi, Ltd. a Fujitsu, Ltd. [9]

Obr. 12 – Distribuce biometrických technologií na globálním trhu (statistiky z roku 2015)



Zdroj: 20. UNAR, J. A.; SENG, Woo Chaw; ABBASI, Almas. A review of biometric technology along with trends and prospects. Pattern recognition, 2014, 47.8: 2673-2688. [upraveno]

Hitachi Industry & Control Solutions, Ltd. nabízí skener krevního řečiště prstu „M2-FV Finger Vein Reader“ (Obr. 20) a uvádí FRR s hodnotou 0,01 % a FAR s hodnotou 0.0001 % (výsledky měření při ověřování 1:1; přesnost vypočtená v souladu s metodami normy ISO/IEC 19795-1 – Testování a hodnocení výkonnosti biometrik). Výhodou tohoto biometrického systému je malá velikost a vysoká přesnost. [9, 21, 22]

Obr. 13 – Sensor skenu krevního řečiště prstu od výrobce Hitachi, Ltd.

Zdroj: 21. PCT-KCUA011: "H1E-USB series" USB authentication device. Hitachi Industry Control Solutions, Ltd. [online]. [cit. 2022-02-20].

Společnost Fujitsu, Ltd. poskytuje bezkontaktní řešení technologie PalmSecure snímající krevní řečiště dlaně. Za určitých podmínek měření se vyznačuje vysokou přesností – FAR 0,00008 % a FRR 0,01 %. Samotný senzor obsahuje všechny potřebné prvky – zdroj IR světla, snímající kameru, detektor umístění dlaně a jednotku předzpracování obrazových údajů. K tomuto senzoru je též nabízeno široké spektrum příslušenství (Obr. 14). Tento biometrický systém je nabízen včetně softwaru usnadňujícího implementaci této technologie v praxi. Velikost biometrické šablony se pohybuje v rozmezí 1–3 kB. [19, 22, 23]

Technologie PalmSecure je dnes využívaná ve veřejném sektoru, školství, zdravotnictví, a finančním sektoru. Tento biometrický systém byl v roce 2018 nasazen na 14 vnitrostátních letištích v Koreji, dále také u bankomatů japonské banky Tokyo-Mitsubishi UFJ, turecké banky T.C. Ziraat Bankasi, ruské banky Sberbank ad. [19, 24]

Obr. 14 – Senzor PalmSecure F-Pro a volitelné příslušenství

Zdroj: 25. Biometric Authentication PalmSecure® F-Pro PalmSecure® Products Fujitsu PalmSecure F-Pro Suite [online]. [cit. 2022-03-07].

Dalšími výrobci řešení identifikace osob na základě skenu krevního řečiště jsou Mofiria Corporation (dceřiná společnost Sony), BioSec Group Ltd., BioEnable Technologies ad. [19]

4.4.6. 35. Chaos Communication Congress (35C3)

Odborník na počítačovou bezpečnost Julian Albrecht společně s počítačovým vědcem a etickým hackerem[3] Janem Krisslerem provedli výzkum týkající se prolomení biometrických systémů identifikace osob pomocí skenu krevního řečiště pomocí metody spoofing. V prosinci

[3] Specialista na počítačovou bezpečnost zaměřující se na testování informační infrastruktury.

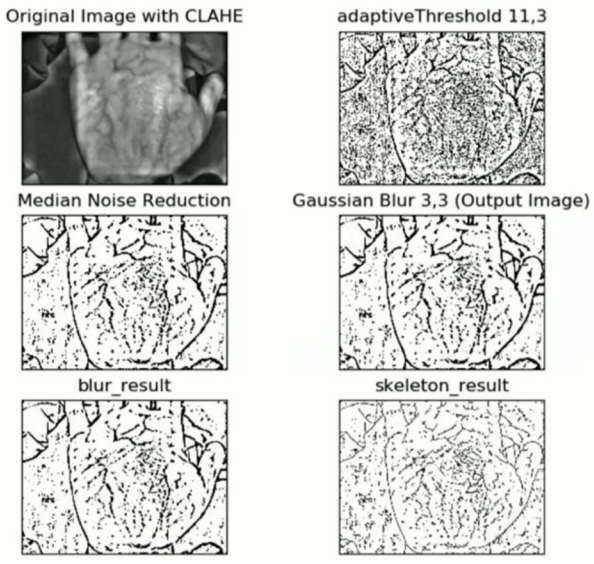
roku 2018 prezentovali a demonstrovali výsledky svého výzkumu na každoroční bezpečnostní konferenci 35. Chaos Communication Congress (35C3). [26, 27]

Pomocí vytvořené atrapy ruky vyrobené z vosku a snímku ze speciálně upravené DSRL kamery se vědcům podařilo obelstít skener krevního řečiště prstu společnosti Hitachi Ltd, a skener krevního řečiště dlaně společnosti Fujitsu, Ltd. [26, 27]

Nejdříve s J. Albrecht a J. Krissler věnovali získání obrazu žil pomocí upravené digitální zrcadlovky Nikon D500 včetně několika objektivů, na které byl odstraněn IR filtr z CMOS snímače. Fotografie pořizovali ze vzdálenosti 5 metrů, což by pro potenciálního útočníka byla ideální vzdálenost pro nenápadné pořízení snímku subjektu. Dalším možným způsobem, jak získat fotografii ruky subjektu je umístění přídavného modulu IR kamery pro Raspberry Pi do tryskových vysoušečů rukou nebo například do UV lampy na nehty. Během výzkumu vytvořili více než 2500 fotografií rukou a prstů, ze kterých následně vybrali nejoptimálnější vzorek pro maximální efektivitu testování. Fotografii upravili pomocí scriptu, který obsahoval následující kroky:

1. Zvýšení lokálního kontrastu pomocí pluginu CLAHE
2. Adaptivní prahování
3. Redukce šumu průměrováním
4. Použití filtru Gaussovského rozostření
5. Skeletizace

Obr. 15 – Postup úprav snímku a použití filtrů



Zdroj: 26.Venenerkennung hacken: Vom Fall der letzten Bastion biometrischer Systeme. Https://media.ccc.de/ [online]. [cit. 2022-03-20].

Výslednou biometrickou šablonu vytiskli v poměru 1:1. Následně byla pomocí formy vymodelována falzifikát ruka a prst z včelího vosku, na které byla přiložena papírová šablona pokrytá další vrstvou červeného včelího vosku. S těmito vzorky se podařilo za určitých podmínek testování obelstít oba senzory. Přestože se biometrické systémy skenu krevního řečiště řadí mezi pokročilé bezpečnostní systémy, byla tímto výzkumem prokázána zranitelnost těchto systémů použitím poměrně jednoduchého způsobu metod spoofingu a levným materiálem. Celý výzkum trval přibližně měsíc. [26, 27]

Závěry tohoto výzkumu byly prezentovány společnostem Fujitsu, Ltd. a Hitachi, Ltd., které projevily zájem o prozkoumání výsledků a spolupráci na vylepšení svých technologií. [26]

5. Praktická část práce

Praktická část diplomové práce je věnována otestování spolehlivosti a odolnosti biometrického systému skenu krevního řečiště ruky technologie PalmSecure vyvinuté společností Fujitsu, Ltd. vůči metodě „spoofing“.

5.1. Podmínky měření

Samotné měření a pořízení snímků pro vytvoření biometrické šablony probíhalo na konci prvního čtvrtletí roku 2022 uvnitř budovy o průměrné teplotě 21°C, relativní vlhkosti vzduchu v rozmezí od 40 % až 50 % a průměrného atmosférického tlaku o hodnotě 980 hPa.

Světelné podmínky pořízení snímků levé dlaně ruky byly upravovány podle potřeb zvýraznění kontrastů snímané plochy. Snímky byly pořízeny za svitu denního světla bez přímého slunečního záření, za svitu bílého i žlutého světla s vyšší intenzitou a též bílého protisvětla.

Testování byl podroben senzor technologie PalmSecure připojený přes USB kabel k počítači. Měření probíhalo v místnosti pouze za přísvitu LED zářivky, přičemž senzor byl umístěn ve stínu dřevěné zástěny nepropouštějící světlo. Během měřením bylo cílem provedení testování v tmavém prostředí bez přímého osvětlení senzoru.

Celého procesu testování biometrického systému skenu krevního řečiště ruky popsaného v praktické části se účastnil pouze autor této diplomové práce (žena, věk 25 let). Falzifikát byl vytvořen na základě biometrických charakteristik této osoby.

Celkový čistý čas testování trval přibližně dvě hodiny. Výroba falzifikátu trvala zhruba 5 hodin.

5.2. Použité nástroje

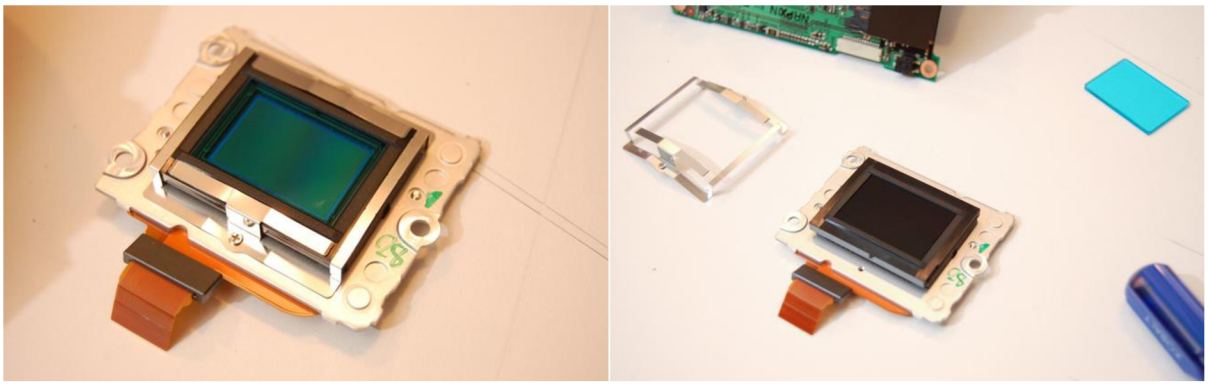
Při zpracování praktické části diplomové práce bylo použito následujících přístrojů, nástrojů a materiálů:

5.2.1. Nástroje pro pořízení snímku

Pro pořízení snímků ruky, které byly následně upraveny pro vytvoření biometrické šablony, byla použita digitální jednooká zrcadlovka Nikon D40x s obrazovým snímačem

formátu DX s maximálním rozlišením 3872 × 2592 pixelů. Tato digitální zrcadlovka speciálně upravena tak, aby propouštěla nejen viditelné světlo, ale i infračervené spektrum. Této úpravy bylo docíleno odebráním IR filtru (Obr. 16) nacházejícího se na snímacím čipu fotoaparátu. [28, 29]

Obr. 16 – Vlevo neupravený snímač, vpravo je IR filtr tyrkysového zbarvení odstraněn ze snímače



Zdroj: 29. Nikon D40 Infrared Conversion, Tutorial [online]. 2008 [cit. 2022-03-22].

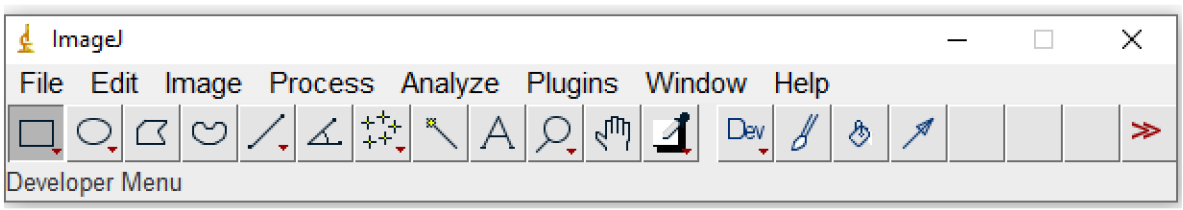
Během focení bylo použito dvou objektivů:

- Zoomový objektiv AF-S DX NIKKOR 18–105mm f/3.5–5.6G ED VR [31]
- Zoomový objektiv Tamron SP 70–300 mm F/4–5.6 Di VC USD [32]

5.2.2. Program pro úprava snímku

Pro úpravu získaných snímků a snímků z testovací aplikace byl použit OSS program ImageJ založený na bázi objektově orientovaného programovacího jazyka Java. Pomocí ImageJ lze zpracovávat, upravovat a analyzovat obrazy a snímky (Obr. 17). Mimo jiné umožňuje použití mnoha pluginů vytvořených samotnými uživateli. Tento nástroj podporuje mnoho obrazových formátů, provádí statistická měření obrazu, geometrické transformace, podporuje standardní funkce zpracování obrazu aj. Společně s ImageJ byl použit plugin umožňující aplikovat metodu CLAHE neboli metodu zvýšení lokálního kontrastu. [32]

Obr. 17 – Interface programu ImageJ



Zdroj: Obrázek z archivu autora

5.2.3. Použitý materiál pro výrobu falzifikátu

Falzifikát byl vytvořen pomocí následujících materiálů:

Pro vytvoření formy na odlití vzorku bylo použito 250 gramů dvousložkové silikonové pasty a 13 gramů katalyzátoru (výrobce Korálky.cz) k výrobě forem pro odlévání z pryskyřice, sádry či vosku (Obr. 18). Výhodou tohoto materiálu je jednoduchost použití a tepelná odolnost. [33]

Obr. 18 – Silikonová pasta a katalyzátor k výrobě forem

Zdroj: 33. Koralky.cz: Silikonová pasta k výrobě forem 250g [online]. [cit. 2022-04-01].

Materiál pro vytvoření falzifikátu byl vybrán na základě podobnosti lidské tkáně a včelího vosku [27]. Pro vytvoření odlitku vzorků levé a pravé ruky byl vybrán pravý včelí vosk, který lze zpracovávat po rozehřátí, od dodavatele včelařských potřeb VCEST.CZ (Obr. 19). [34]

Obr. 19 – Pravý včelí vosk (500 gramů)

Zdroj: 34. VCEST.CZ: Pravý včelí vosk 500g [online]. [cit. 2022-04-01].

Aby vytištěný snímek biometrické šablony nebyl příliš výrazný kvůli bíle barvě použitého papíru, byla použita tenká vrstva přírodního včelího vosku s červeným pigmentem od dodavatele výtvarných potřeb ARTMIE.cz (Obr. 20). [35]

Obr. 20 – Plát přírodního červeného včelího vosku

Zdroj: 35. ARTMIE: Přírodní včelí vosk – red *[online]. [cit. 2022-04-01].*

Pro vytištění vytvořené biometrické šablony bylo použito recyklovaného kancelářského papíru o velikosti A4 a gramáže 80 gramů. Pro tisk bylo použito laserové tiskárny Konica Minolta bizhub C258.

5.2.4. PalmSecure a testovací aplikace

Pro měření bylo použito patentované technologie PalmSecure od firmy Fujitsu, Ltd. Tato technologie identifikace osob na základě skenu krevního řečiště dlaně v sobě zahrnuje jak hardwarové řešení v podobě senzoru a příslušenství (ergonomické pomůcky, doplňkové periferie), tak i softwarového řešení v podobě ovladačů pro senzory, aplikace Workplace Protect pro zařízení firmy Fujitsu, Ltd. [19, 36, 37]

Systém PalmSecure je sestaven z iluminační, detekční a kamerové jednotky, které jsou umístěny v senzoru, který využívá rozhraní USB. Software v sobě zahrnuje porovnávací jednotku a databázi referenčních šablon, které jsou tvořeny číselným výsledkem matematické transformace obrazu, je tedy složité obnovit originální snímek z těchto dat. Biometrická šablona je vytvářena přímo „ v senzoru“, a poté je zašifrována standardizovaným šifrovacím algoritmem AES. Výsledná biometrická šablona je následně uložena do databáze. Výhodou je malá velikost šablony pohybující se v rozmezí 1–3 kB. [19, 36, 37]

Identifikačně-verifikační proces probíhá na základě prvotního pořízení biometrické šablony, vyžadující vytvoření tří snímků krevního řečiště, ze kterých je zprůměrována výsledná biometrická šablona. Při prokazování identity uživatel umisťuje dlaň nad senzor ve výšce 5–8 cm, který následně prosvítí daň pomocí NIR záření a kamera v senzoru zaznamená odražené světlo. [19, 36, 37]

Výrobce uvádí časový průběh verifikačního procesu v průměru 0,8 sekund a proces identifikace přibližně 1–2 sekundy. Pravděpodobnost chybného přijetí neoprávněného uživatele (FAR) odpovídá hodnotě 0,00008 % a pravděpodobnost chybného odmítnutí odpovídá hodnotě 0,01 %, čímž technologie PalmSecure nabízí vyšší úroveň zabezpečení oproti jiným biometrickým metodám identifikace osob (Tab. 2). [19, 36]

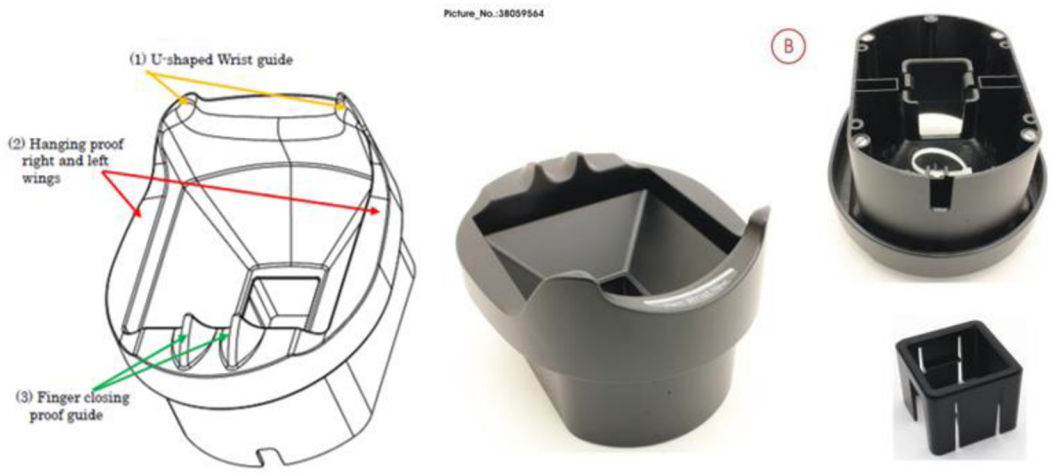
Tab. 2 – Porovnání hodnot FAR a FRR různých metod biometrické identifikace osob

Autentizační metoda	FAR (%) =	If FRR (%) =
Rozpoznání tváře	~ 1.3	~ 2.6
Hlasové vzorky	~ 0.01	~ 0.3
Otisk prstu	~ 0.001	~ 0.1
Cévy v prstu	~ 0.0001	~ 0.01
Duhovka/Sítnice	~ 0.0001	~ 0.01
Krevní řečiště v dlani	< 0.00008	~ 0.01

Zdroj: 19. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. PalmSecure a Palm Vein Sensory [online]. leden 2020; [cit. 2022-02-05]. Osobní komunikace.

Pro účely testování bylo použito speciálního ergonomického vodítka U-Guide (Obr. 21) pro správné umístění dlaně a prstů nad senzorem, které během testování umožnilo zachovat vždy stejné podmínky pro snímání subjektu i falzifikátu. [38]

Obr. 21 – Ergonomické vodítko U-Guide



Zdroj: 19. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. PalmSecure a Palm Vein Sensory [online]. leden 2020; [cit. 2022-02-05]. Osobní komunikace.

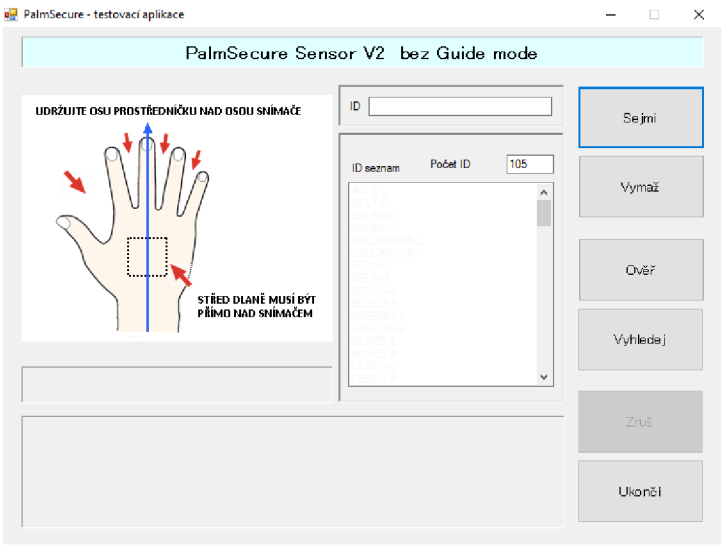
Při testování byl použit senzor F-Pro SDK (Obr. 22) umístěný ve speciálním otvoru ergonomického vodítka. Pro připojení senzoru k PC bylo použito standardního kabelu USB 2.0/Micro USB. [39]

Obr. 22 – Senzor F-Pro SDK

Zdroj: 39. FUJITSU Biometric Authentication PalmSecure® F-Pro PalmSecure® Products Fujitsu PalmSecure F-Pro Suite [online]. [cit. 2020-02-04].

Pro otestování odolnosti biometrického systému PalmSecure vůči spoofingu byla použita testovací aplikace (Obr. 23) vyvinutá pracovníky Fujitsu Technology Solutions s.r.o., která umožňuje rychlou a jednoduchou práci se senzorem F-Pro a ergonomickým vodítkem U-Guide (aplikaci lze využívat též bez ergonomického vodítka). Aplikace umožňuje vytvoření biometrické šablony přiřazené ke zvolenému ID (volba „Sejmi“) a také případně i smazání vytvořených šablon (volba „Vymaž“). Aplikace poskytuje možnost identifikace osoby (volba „Vyhledej“) a verifikace osoby (volba „Ověř“), přičemž v průběhu těchto procesů napomáhá uživateli správně umístit dlaň nad senzor a nabízí živý pohled na snímaný obraz. [19]

Obr. 23 – Interface testovací aplikace



Zdroj: 19. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. PalmSecure a Palm Vein Sensory [online]. leden 2020; [cit. 2022-02-05]. Osobní komunikace.

5.3. Postup získávání dat pro výrobu falzifikátu

Před samotným otestováním senzoru technologie PalmSecure bylo nutné vytvořit falzifikát biometrických údajů, na jejich základě byla následně otestována spolehlivost daného

biometrického systému vůči metodě „spoofing“. Prvním krokem vytvoření falzifikátu bylo získání biometrických údajů, které byly extrahovány ze dvou typů snímků – snímek z testovací aplikace a snímek pořízený speciálně upraveným fotoaparátem. Dalším krokem byla úprava snímků a vytvoření biometrické šablony. Dále byl vytvořen falzifikát z výše zmíněného materiálu (kap. 5.2.3.) a v kombinaci s biometrickou šablonou byl otestován biometrický systém skenu krevního řečiště dlaně. Získaná data byla zapisována do tabulek prezentovaných v kapitole 6.

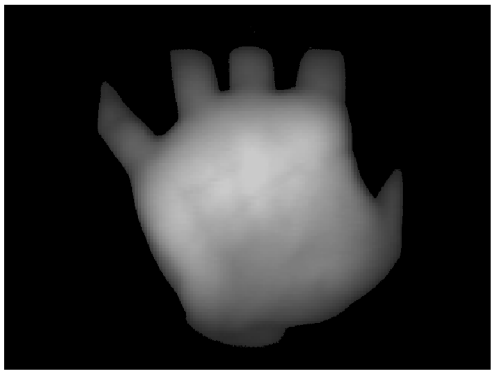
5.3.1. Vytvoření biometrické šablony

Biometrická šablona při použití technologie PalmSecure je vytvářena přímo „v senzoru“, a poté je zašifrována standardizovaným šifrovacím algoritmem AES. Výsledná biometrická šablona je následně uložena do interního uložiště. Výhodou je malá velikost šablony pohybující se v rozmezí 1–3 kB.

Pro vytvoření falzifikátu bylo použito dvou biometrických šablon:

1) Biometrická šablona získaná z testovací aplikace – Testovací aplikace automaticky ukládá snímky pořízené během identifikačně-verifikačního do interního uložiště ve formátu BMP. Snímek (Obr. 24), který byl pořízen hned po vytvoření biometrické šablony v systému, byl následně upraven pro extrahování potřebných charakteristik.

Obr. 24 – BMP snímek z testovací aplikace



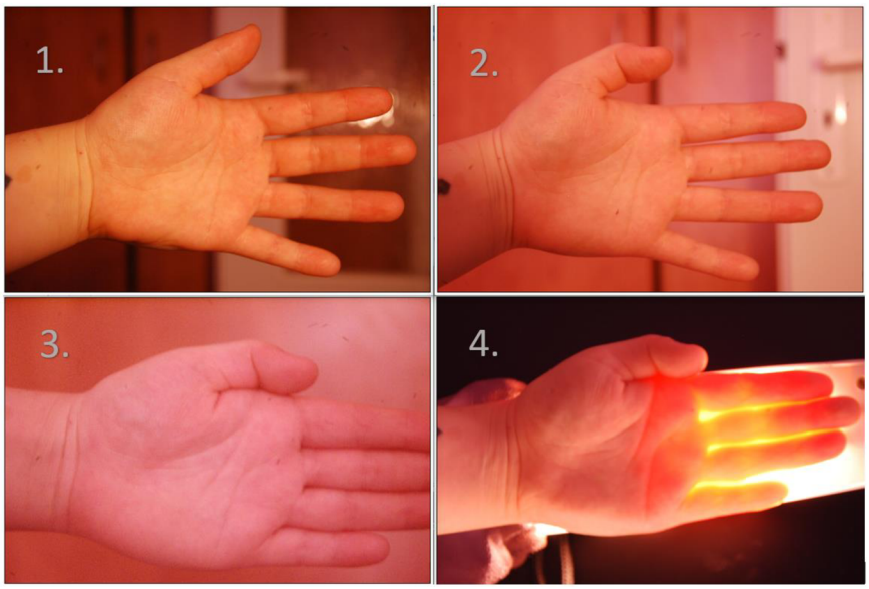
Zdroj: Obrázek z archivu autora

2) Druhá biometrická šablona byla vytvořena na základě snímku pořízeného pomocí speciálně upravené zrcadlovky (kap. 5.2.1).

5.3.2. Pořízení snímků pro výrobu falzifikátu

Pro výrobu falzifikátu bylo pořízeno cca 50 fotografií levé dlaně ruky za různých světelných podmínek a nastavení fotoaparátu.

Obr. 25 – Pořízené fotografie pro výrobu falzifikátu



Zdroj: Obrázek z archivu autora

Ze všech snímků byly následně vybrány čtyři nejostřejší snímky (Obr. 25) vyfocené za různých světelných podmínek ve formátu JPEG s parametry uvedenými v Tab. 3.

Tab. 3 – Parametry pořízených snímků

Snímek č.	*1*	*2*	*3*	*4*
Rozměry (px)	3872 x 2592	3873 x 2592	3874 x 2592	3875 x 2592
Závěrka clony	f/5	f/5	f/5.6	f/5
Délka expozice	1/15 sec.	1/13 sec.	1/13 sec.	0.62 sec.
ISO	ISO-800	ISO-800	ISO-400	ISO-100
Ohnisková vzdálenost	42 mm	42 mm	70 mm	50 mm
Režim expozimetru	Maticové měření	Maticové měření	Maticové měření	Maticové měření
Vyvážení bílé	Automaticky	Automaticky	Automaticky	Automaticky
Světelné podmínky	Nasvícení žlutým světlem	Nasvícení bílým světlem	Denní světlo (bez přímého sln. záření)	Bíle protisvětlo

Zdroj: Tabulka z archivu autora

5.3.3. Postprocessing snímků

Ze získaných snímků byly extrahovány prvky odpovídající biometrické šabloně. Snímky byly v průběhu postprocessingu upraveny za pomoci následujících nástrojů programu ImageJ:

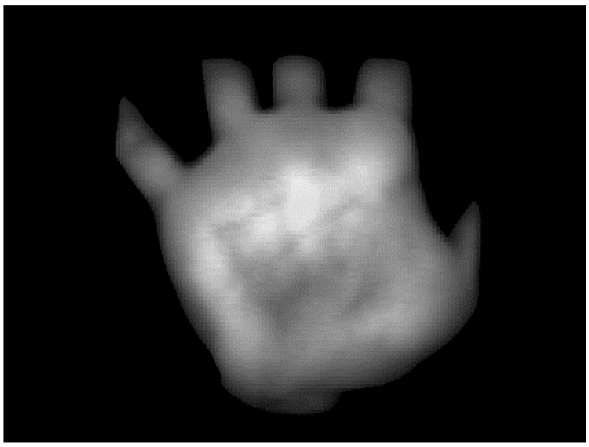
A. Každý ze čtyř snímků získaných pomocí speciálně upravené kamery byl **rozdělen na jednotlivé RGB kanály** do jednotlivých snímků (Obr. 26) – červený, zelený a modrý. Pro následující úpravy byly použity pouze snímky zeleného a modrého kanálu z důvodu zvýšeného kontrastu.

Obr. 26 – Rozdělení jednoho snímku na jednotlivé barevné kanály (zleva – červený, zelený, modrý)

Zdroj: Obrázek z archivu autora

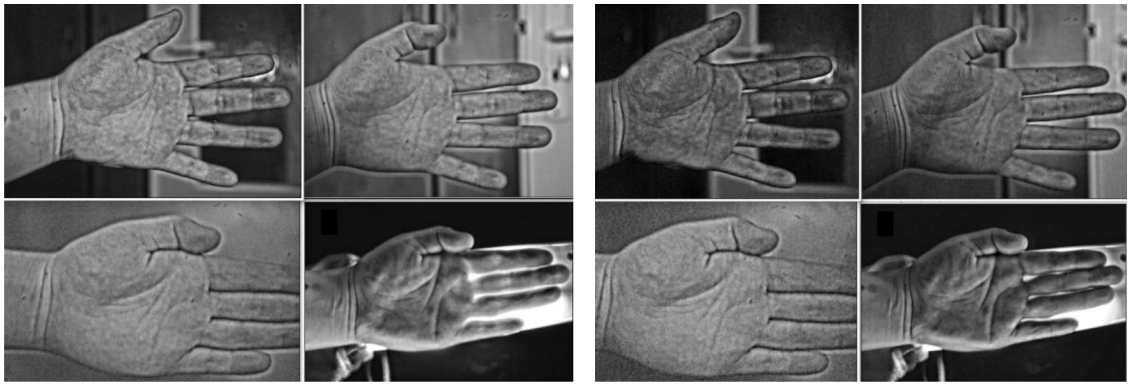
B. V druhém kroku bylo k dispozici 9 snímků, z čehož jeden snímek byl získán z testovací aplikace (Obr. 27) a celkem 8 snímků z pořízených fotografií (4 snímky modrého kanálu a 4 snímky zeleného kanálu). Na všech devět snímků byl aplikován **filtr CLAHE** [40] zvyšující lokální kontrast, při jehož použití bylo zapotřebí zadat tři specifické parametry ovlivňující výsledek transformace:
   - Velikost bloků udávající velikost oblasti kolem daného pixelu, pro kterou je histogram vyrovnáván. Zvolená hodnota musí být větší než velikost nejmenšího prvku, který musí být zachován = **127** (automatická předvolba)
   - Počet segmentových oblastí vyrovnání histogramu = **256** (automatická předvolba)
   - Maximální sklon omezující skokové zvýšení kontrastu. Čím vyšší je hodnota sklonu, tím větší je lokální kontrast = **3.00** (automatická předvolba)

Obr. 27 – Aplikování filtru CLAHE (snímek z testovací aplikace)



Zdroj: Obrázek z archivu autora

Obr. 28 – Porovnání aplikace filtru CLAHE na snímky různých barevných kanálů (vlevo zelené, vpravo modré)

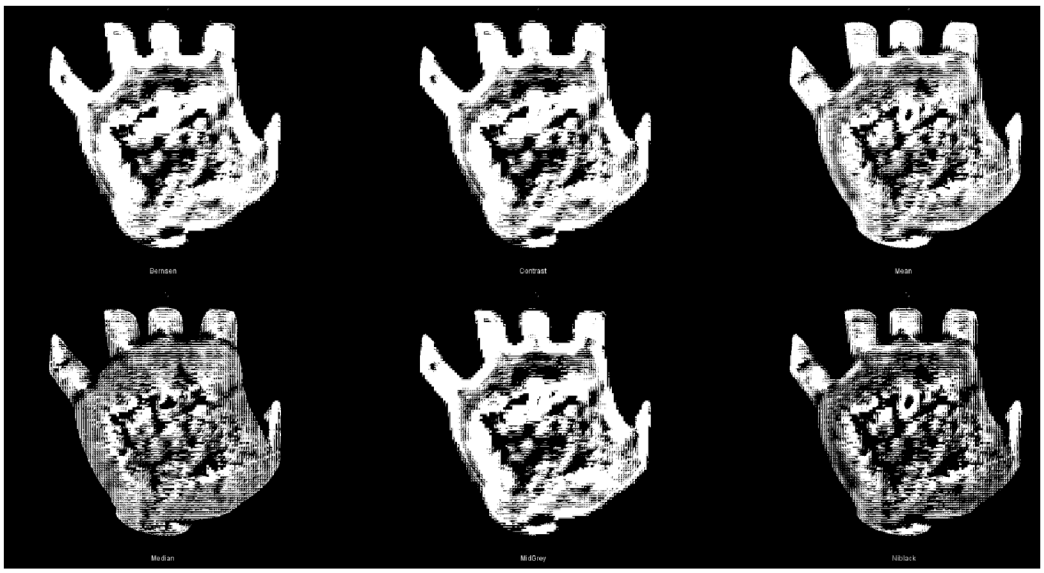


Zdroj: Obrázek z archivu autora

Pro následující úpravy byly použity snímky modrého kanálu z důvodu vyššího kontrastu (Obr. 28 – čtyři snímky vpravo).

C. Zbylých pět snímků bylo následně upraveno pomocí filtru **automatického lokálního prahování** metodami zobrazenými na Obr. 29 – zleva: Bernsen, Contrast, Mean, Median, MidGray a Niblack.

Obr. 29 – Příklady použití různých metod automatického lokálního prahování

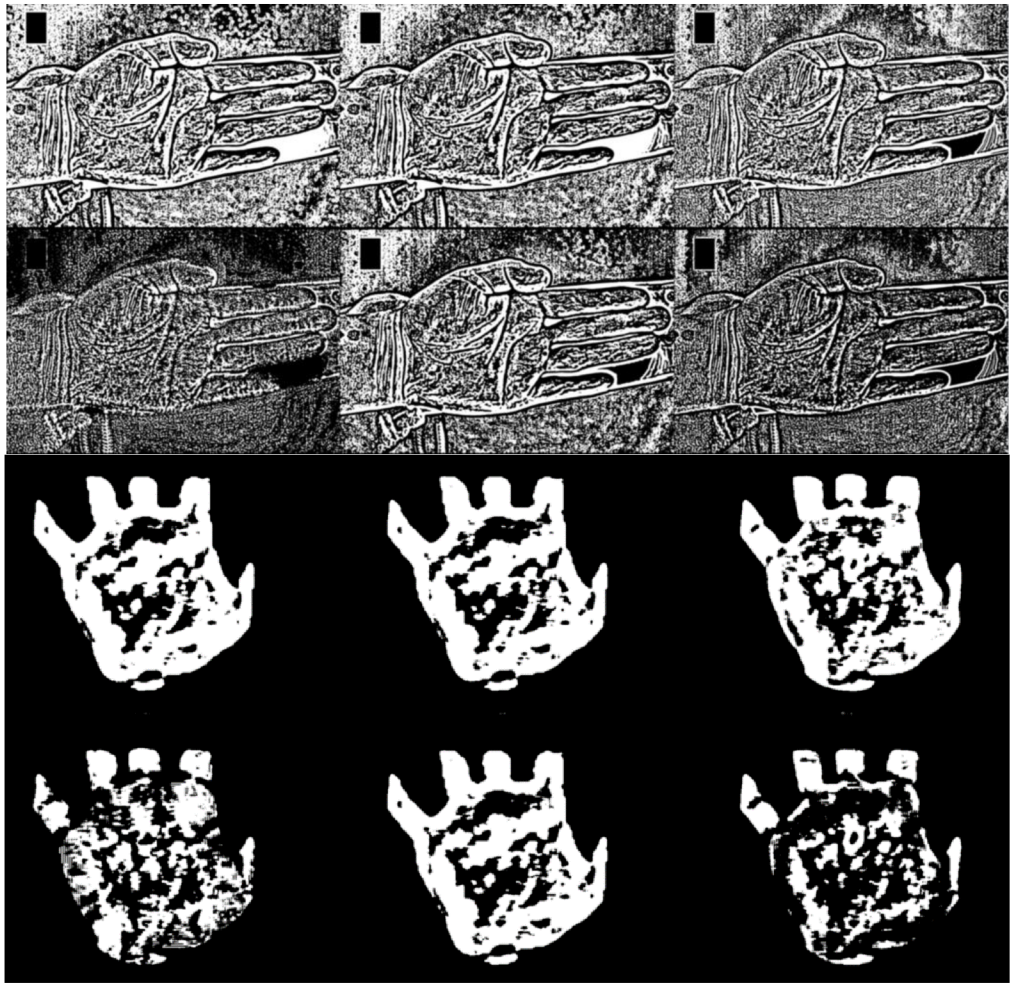


Zdroj: Obrázek z archivu autora

D. Dále byl u snímků redukován šum pomocí průměrování (**Median Filter**) s rádiusem 3.0 pixelů.

E. Na všechny snímky byl dále aplikován filtru **Gaussovského rozostření** s rádiusem 3.0 pixelů u snímků pořízených fotoaparátem a s rádiusem 1.0 u snímku z testovací aplikace. Příklad výsledných snímků je zobrazen na Obr. 30.

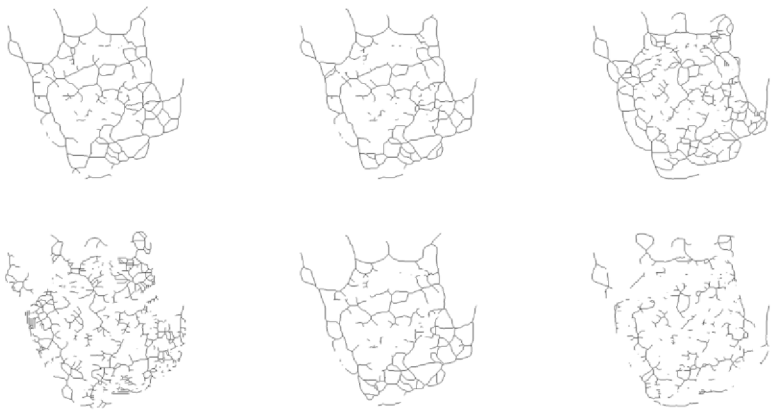
Obr. 30 – Rozdíl výsledných snímků po redukci šumu průměrováním a použití Gaussovského rozostření



Zdroj: Obrázek z archivu autora

F. Na výsledný snímek z testovací aplikace byla aplikována **skeletizace**, čímž se dosáhlo požadované úpravy snímku (Obr. 31).

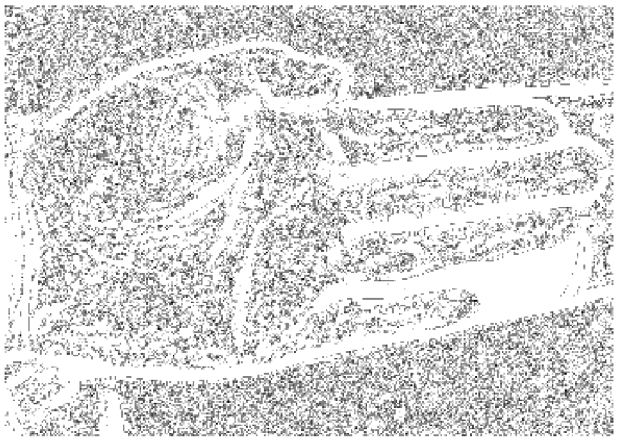
Obr. 31 – Výsledný snímek (z testovací aplikace) po procesu skeletizace



Zdroj: Obrázek z archivu autora

Skeletizace byla použita pouze u snímku z testovací aplikace. Ostatní snímky byly převedeny do binární podoby, neboť snímky pořízené fotoaparátem obsahují mnoho informací, které při procesu skeletizace vytvořily velmi jemné vzorkování (Obr. 32), které pro účely testování nebylo možné použít.

Obr. 32 – Skeletizace snímku pořízeného fotoaparátem



Zdroj: Obrázek z archivu autora

Pro účely otestování biometrického systému skenu krevního řečiště dlaně bylo použito snímků uvedených v příloze č. 1.

5.3.4. Výroba falzifikátu

Při výrobě falzifikátu bylo použito silikonové formy, která byla zpracována následujícím způsobem: 250 gramů silikonové pasty (výrobce Korálky.cz) bylo smícháno s 13 gramy katalyzátoru a následně byla hmota přelita do nádoby, kde byly umístěny dvě latexové rukavice naplněné vodou (Obr. 33). Proces vytvrzení silikonové hmoty trval 24 hodin, proto nebylo možné využít lidské ruky jako potřebného tvaru pro vytvoření silikonové formy.

Obr. 33 – Postup výroby silikonové formy

Zdroj: Obrázek z archivu autora

Po ztvrdnutí formy byly latexové rukavice vyjmuty a následně byl ve vodní lázni rozpuštěn červený včelí vosk, kterým byla odlita několik milimetrů tenká vrstva. Po ztuhnutí vosku byly vzorky odlitků levé a pravé ruky vyjmuty z formy a stejným postupem byly vytvořeny další dva odlitky z přírodního včelího vosku bez barevného pigmentu o tloušťce cca 1 cm (Obr. 34).

Obr. 34 – Hotová silikonová forma a vytvořené odlitky

Zdroj: Obrázek z archivu autora

Vytvořené biometrické šablony byly po vytištění jednotlivě vloženy mezi odlitky potištěnou stranou na červenou vrstvu odlitku.

5.4. Metodika měření

Před samotným testováním byla ověřena shodnost vytvořené biometrické šablony uložené v interním uložišti PC (viz kapitola 5.3.1) s dlaní živého subjektu pomocí procesu identifikace i verifikace v testovací aplikaci. Celkem byla v systému zanesena pouze jedna biometrická šablona, konkrétně levá dlaň subjektu. Při testování senzoru byl každý snímek jednotlivě vložen mezi odlitky a falzifikát byl následně položen na ergonomické vodítko. Poté byl pomocí testovací aplikace proveden proces identifikace (1:N), avšak vzhledem k přítomnosti pouze jednoho záznamu v databázi biometrických šablon lze považovat identifikaci i verifikaci za totožné procesy.

Každý ze třiceti upravených snímků byl na základě identifikačního procesu prověřen dvakrát. Teoretické výsledné hodnoty mohly nabývat dvou stavů – „ověřeno“ (úspěšné prolomení biometrického systému pomocí falzifikátu) a „neověřeno“ (tento stav byl výsledkem tří jednotlivých nezdařených ověření za sebou během jednoho procesu identifikace). Výsledky vyhodnocení identifikace byly zaznamenány do tabulky. Celkem proběhlo 60 samostatných měření (každý ze třiceti snímků dvakrát podroben identifikačnímu procesu).

Vzhledem k výsledkům měření, bylo dodatečně provedeno doplňujících 30 měření (každý snímek jednou podroben identifikaci) na základě nově vytvořené biometrické šablony v systému, která byla pořízena z „biometrických“ údajů falzifikátu (byl použit obrázek č. 7, viz příloha č. 1). Tato měření sloužila pro prověření tvrzení, zda je biometrický systém PalmSecure opravdu odolný vůči falzifikaci biometrických dat, nebo byly výsledky ovlivněny potenciální nedokonalostí vytvořeného falzifikátu.

6. Výsledky a diskuse

Výsledky měření spolehlivosti biometrického systému skenu krevního řečiště dlaně při záměrné falzifikaci biometrických údajů nevyvrátily ani nepotvrdily tezi diplomové práce. Výsledky jsou neprůkazné z důvodu nesprávně vytvořeného falzifikátu, který nebyl dostatečně kvalitní na to, aby s ním byl tento biometrický systém prolomen.

V Tab. 4 jsou prezentovány výsledky měření. Během první části bylo provedeno 60 jednotlivých měření shodnosti falzifikátu a třiceti upravených snímků s biometrickou šablonou vytvořenou na základě biometrických údajů autora, přičemž ani jeden z pokusů nebyl vyhodnocen pozitivně. Z tohoto důvodu bylo provedeno dalších 30 měření, jejichž účelem bylo zjistit shodnost falzifikátu a snímků s biometrickou šablonou vytvořenou na základě falzifikátu s použitím snímku č. 7 (viz příloha č. 1). Tato kontrolní měření potvrdila, že vytvořený falzifikát nesplňuje kvalitativní podmínky potřebné pro úspěšné prolomení systému.

Příčiny neúspěšného vytvoření falzifikátu mohly být následující:

- Vyfocené fotografie dlaně ruky neobsahovaly dostatek informací pro následné vypracování šablony. Lepšího výsledku by se dalo dosáhnout použitím přídavného infračerveného filtru nasazeného na objektiv fotoaparátu nebo úpravou snímače fotoaparátu tak, aby zachycoval pouze světlo v infračerveném spektru. Pro zvýraznění žil dlaně ruky by též mohla být použita infračervená lampa.
- Snímek dlaně z testovací aplikace nebyl dostatečně kvalitní na to, aby po jeho úpravě byla struktura žil dostatečně výrazná. V tomto případě by bylo vhodné použít snímek pořízený fotoaparátem (viz předchozí bod).
- Úpravy snímků pomocí programu ImageJ se mohly lišit od úprav provedených během studie J. Krisslera a J. Albrechta. Nastavené parametry daných filtrů a úprav mohly být mírně odlišné, čímž byly nekorektně extrahovány rysy a výsledný snímek se mohl parametrálně lišit od snímku potřebného pro úspěšné prolomení biometrického systému.
- Upravené snímky mohly být vytištěny v nesprávném měřítku. Neprůkaznost výsledků mohla být též ovlivněna nedostatečnou kvalitou tisku nebo nevyhovujících tiskových médií.

- Tloušťka a struktura povrchu voskového falzifikátu mohla způsobit negativní vliv na průběh měření.
- Průběh měření mohl být negativně ovlivněn nevyhovujícími světelnými podmínkami.

Závěry vycházející z měření ukázaly, že vytvoření falzifikátu v nelaboratorních podmínkách s běžně dostupnými nástroji a materiály není jednoduché a je potřeba více prostředků pro zvýšení kvality falzifikátu v průběhu výroby. Hodnoty pravděpodobnosti chybného přijetí (FAR) nemohly být na základě výsledků vypočítány.

Tab. 4 – Výsledky měření

Číslo snímku (legenda viz příloha č. 1)	Ověřeno (biometrická šablona subjektu)	Ověřeno (biometrická šablona falzifikátu)	FAR
Obrázek 1 – T-M3-G1-S-BR	0/2	0/1	0,00 %
Obrázek 2 – T-M3-G1-S-CO	0/2	0/1	0,00 %
Obrázek 3 – T-M3-G1-S-MA	0/2	0/1	0,00 %
Obrázek 4 – T-M3-G1-S-MD	0/2	0/1	0,00 %
Obrázek 5 – T-M3-G1-S-MG	0/2	0/1	0,00 %
Obrázek 6 – T-M3-G1-S-NB	0/2	0/1	0,00 %
Obrázek 7 – F-M3-G3-BR (1)	0/2	1/1	0,00 %
Obrázek 8 – F-M3-G3-MD (1)	0/2	1/1	0,00 %
Obrázek 9 – F-M3-G3-BR (2)	0/2	1/1	0,00 %
Obrázek 10 – F-M3-G3-MD (2)	0/2	1/1	0,00 %
Obrázek 11 – F-M3-G3-BR (3)	0/2	1/1	0,00 %
Obrázek 12 – F-M3-G3-CO (1)	0/2	1/1	0,00 %
Obrázek 13 – F-M3-G3-MG (1)	0/2	1/1	0,00 %
Obrázek 14 – F-M3-G3-CO (2)	0/2	1/1	0,00 %
Obrázek 15 – F-M3-G3-MG (2)	0/2	1/1	0,00 %
Obrázek 16 – F-M3-G3-CO (3)	0/2	1/1	0,00 %
Obrázek 17 – F-M3-G3-MA (1)	0/2	1/1	0,00 %
Obrázek 18 – F-M3-G3-NB (1)	0/2	1/1	0,00 %
Obrázek 19 – F-M3-G3-MA (2)	0/2	1/1	0,00 %
Obrázek 20 – F-M3-G3-NB (2)	0/2	1/1	0,00 %
Obrázek 21 – F-M3-G3-MA (3)	0/2	0/1	0,00 %
Obrázek 22 – F-M3-G3-MD (3)	0/2	0/1	0,00 %
Obrázek 23 – F-M3-G3-BR (4)	0/2	1/1	0,00 %
Obrázek 24 – F-M3-G3-MD (4)	0/2	1/1	0,00 %
Obrázek 25 – F-M3-G3-MG (3)	0/2	1/1	0,00 %
Obrázek 26 – F-M3-G3-CO (4)	0/2	1/1	0,00 %
Obrázek 27 – F-M3-G3-MG (4)	0/2	1/1	0,00 %
Obrázek 28 – F-M3-G3-NB (3)	0/2	1/1	0,00 %
Obrázek 29 – F-M3-G3-MA (4)	0/2	1/1	0,00 %
Obrázek 30 – F-M3-G3-NB (4)	0/2	1/1	0,00 %

Zdroj: Vytvořeno autorem

7. Závěr

V teoretické části diplomové práce byly formulovány nejdůležitější pojmy z vědního oboru biometrie zabývajícího se měřitelnými individuálními anatomicko-fyziologickými a behaviorálními znaky člověka. Na začátku byly definovány pojmy související s identitou osob a jejího ověřování – konkrétně byl popsán rozdíl mezi identifikací a verifikací osob, dále způsoby ověření identity na základě znalostí, vlastnictví a biometrických charakteristik, a také byly vysvětleny definice pojmů biometrie, biometrické charakteristiky a biometrického systému. Následně byly představeny základní moduly a schéma obecného biometrického systému včetně možných výsledků rozhodnutí identifikačně-verifikačních procesů na základě prahu citlivosti daného biometrického systému.

Dalším důležitým bodem byl popis statistických základů hodnocení spolehlivosti a bezpečnosti biometrických systémů zahrnující dva nejdůležitější měřitelné parametry – pravděpodobnost chybného odmítnutí oprávněného uživatele (FRR) a pravděpodobnost chybného přijetí neoprávněného uživatele (FAR). V této části práce byly vysvětleny výpočty těchto hodnot, na jejichž základě jsou biometrické systémy řazeny do určitých bezpečnostních kategorií.

Pro hodnocení a zvyšování bezpečnosti bylo též důležité obeznámit čtenáře se slabými místy biometrického systému, která mohou být využita potenciálními útočníky pro narušení systému. Klíčovými kroky jsou analýza možných metod prolomení biometrických systémů a eliminace případných rizik a hrozeb. Jedním z možných a často používaných způsobů prolomení biometrických systémů je falzifikace biometrických údajů neboli metoda „spoofing“. Z důvodu stále se zvyšující míry implementace biometrických systémů identifikace a přibývajících hrozeb byly zavedeny obecné bezpečnostní požadavky a normy, které ale také usnadnily použití různorodých senzorů a softwarů bez nutnosti opakované konfigurace z důvodu zavedených standardů.

V následujících kapitolách byly představeny nejrozšířenější biometrické metody identifikace osob na základě behaviorálních charakteristik (charakteristiky hlasu, podpisu a chůze) a anatomicko-fyziologických charakteristik (charakteristiky tváře, oka, geometrie ruky a otisku prstu). U každé z těchto metod identifikace byly popsány základní principy technologií a možností ochrany proti spoofingu.

Poslední kapitola teoretické části poskytla popis identifikace osob na základě skenu krevního řečiště, kde byl vysvětlen princip snímání a extrakce rysů stromové struktury krevního řečiště ruky a také popis zařízení potřebného pro tyto procesy. Dále bylo představeno základní rozdělení metod snímání krevního řečiště (reflexivní metoda, transmisivní metoda a metoda bočního světla) a rozdělení těchto biometrických systému z hlediska snímané oblasti na systémy skenu krevního řečiště hřbetu ruky, krevního řečiště prstu a krevního řečiště dlaně ruky. V neposlední řadě byly popsány základní bezpečnostní parametry tohoto biometrického systému, způsoby ochrany vůči spoofingu a využití této metody identifikace osob v praxi.

V poslední kapitole byly rovněž prezentovány výsledky výzkumu odborníka na počítačovou bezpečnost Juliana Albrechta a etického hackera Jana Krisslera, kteří se v roce 2018 zabývali prolomením biometrického systému skenu krevního řečiště dlaně a prstu. Výzkum spočíval ve vytvoření falzifikátu, kterým byl úspěšně prolomen patentovaný biometrický systém PalmSecure of firmy Fujitsu, Ltd. a skener krevního řečiště prstu společnosti Hitachi, Ltd. Výsledky svého výzkumu prezentovali na každoroční bezpečnostní konferenci 35. Chaos Communication Congress (35C3).

Praktická část diplomové práce byla věnována popisu a vyhodnocení výsledků měření spolehlivosti systému identifikace osob na základě krevního řečiště dlaně při úmyslné falzifikaci biometrických údajů. Cílem praktické části bylo vypracování přehledu použitých nástrojů, materiálů a postupů vytvoření falzifikátu biometrických údajů krevního řečiště dlaně. Cílem měření bylo otestování odolnosti biometrického systému PalmSecure vůči metodě „spoofing“ vycházející z poznatků výše zmíněného výzkumu vědců J. Krisslera a J. Albrechta. Od výsledků měření bylo očekáváno, že se budou podobat výsledkům zmíněné studie.

Biometrický systém skenu krevního řečiště technologie PalmSecure je patentovaný systém identifikace osob vyráběný společností Fujitsu, Ltd., který nabízí hardwarové i softwarové řešení v jednom. Tento biometrický systém je velice rychlý, jednoduchý a spolehlivý z hlediska zabezpečení. Za účelem ověření spolehlivosti tohoto systému za použití metody „spoofing“ byl otestován externí senzor V2 s USB rozhraním s ergonomickým vodítkem V2 U-Guide umožňující zachovat vždy stejné umístění ruky nad senzorem. Při měření byla použita speciální testovací aplikace vyvinutá pracovníky Fujitsu Technology Solutions s.r.o., umožňující rychlou a jednoduchou práci se senzorem a uloženými biometrickými šablonami.

Falzifikát byl vyroben na základě poznatků výše zmíněné studie. Nejdříve bylo nutné získat snímky, které byly následně upraveny pro extrakci potřebných biometrických rysů. První snímek byl získán z testovací aplikace technologie PalmSecure, která automaticky ukládá snímek ve formátu BMP do interního uložiště počítače. Následně byly pomocí speciálně upravené DSRL kamery, které byl ze snímače odebrán IR filtr, pořízeny snímky dlaně ruky. Z padesáti fotografií byly vybrány 4 nejostřejší snímky. Všech pět snímků (1 z testovací aplikace a 4 fotografie) byly upraveny v programu ImageJ za použití následujících filtrů a úprav: Barevné fotografie byly rozděleny na jednotlivé RGB kanály (pro úpravu použity zelený a modrý kanál). V druhém kroku se upravilo 9 snímků pomocí filtru CLAHE zvyšující lokální kontrast. Z důvodu vyššího kontrastu byly použity jenom snímky modrého kanálu. Na zbylých pět snímků byl aplikován filtr automatického lokálního prahování šesti různých metod (Bernsen, Contrast, Mean, Median, MidGray a Niblack), dále byl redukován šum pomocí průměrování a použito Gaussovské rozostření. Pro úpravu snímku z testovací aplikace bylo navíc použito procesu skeletizace. Celkem bylo vytvořeno 30 upravených snímků za účelem otestování biometrického systému skenu krevního řečiště.

Pro výrobu falzifikátu bylo nejdříve nutné vytvořit silikonovou formu ruky. Po smíchání silikonové pasty a katalyzátoru byla hmota přelita do nádoby se dvěma latexovými rukavicemi naplněnými vodou. Po vytvrzení silikonové formy po 24 hodinách byly latexové rukavice s vodou odstraněny a do formy byla odlita několik milimetrů tenká vrstva rozpuštěného včelího vosku červené barvy. Po vychladnutí a vyjmutí vrstvy byl vytvořen druhý odlitek o tloušťce jednoho centimetru ze včelího vosku bez barevného pigmentu. Materiál pro vytvoření falzifikátu byl vybrán na základě podobnosti lidské tkáně a včelího vosku, červená barva byla zvolena z důvodu zvýraznění rysů biometrické šablony při měření. Všech 30 upravených snímků bylo vytištěno v poměru 1:1 na recyklovaný kancelářský papír pomocí laserové tiskárny. Šablony byly vystřihnuty a v průběhu testování jednotlivě vkládány mezi vrstvy včelího vosku. Falzifikát byl vytvořen na základě biometrických charakteristik autora diplomové práce.

Měření probíhalo uvnitř budovy za běžných atmosférických podmínek (21°C, 980 hPa). Během pořízení fotografií byly světelné podmínky různě upravovány pro zvýšení kontrastu výsledné fotografie. Měření probíhalo v zatemněné místnosti za přísvitu bílého světla z LED zářivky.

Před samotným měřením bylo nutné vytvořit a uložit do testovací aplikace záznam s biometrickou šablonou subjektu, se kterou se poté porovnával falzifikát. Během měření byl každý ze třiceti upravených snímků jednotlivě vkládán mezi vrstvy včelího vosku, falzifikát se položil na ergonomické vodítko U-Guide a dvakrát otestován pomocí procesu identifikace. Výsledky celkem 60 měření byly zapsány do tabulky.

Během měření spolehlivosti biometrického systému skenu krevního řečiště dlaně nebyl žádný pokus identifikace úspěšně ověřen, proto nemohly být ani vypočítány hodnoty FAR. Na základě výsledků měření bylo provedeno doplňujících 30 měření z důvodu ověření neprůkaznosti výsledků. Před samotným doplňujícím testováním byl vytvořen nový záznam s biometrickou šablonou z „biometrických" charakteristik falzifikátu při použití jednoho z upravených snímků. Tato měření potvrdila tezi, že vytvořený falzifikát nesplňuje kvalitativní podmínky pro úspěšné prolomení biometrického systému skenu krevního řečiště.

Cíl vytvoření falzifikátu nemohl být potencionálně splněn následkem: nedostatečné kvality pořízených fotografií a snímku z testovací aplikace; nekorektních úprav snímku v programu ImageJ; vytištění snímků neodpovídajícím potřebnému měřítku a kvalitě; použití nevyhovujících tiskových médií; nedostatečně precizně upraveného falzifikátu z včelího vosku nebo negativně ovlivněných podmínek v průběhu měření.

Závěry vycházející z měření potvrdily, že vytvoření falzifikátu dostatečné kvality pomocí běžně dostupných nástrojů a materiálů v nelaboratorních podmínkách není lehce proveditelné. Doporučením pro další měření je použití přídavného zařízení, jako je například infračervený filtr nasazený na objektiv fotoaparátu. Pro zvýraznění krevního řečiště je též možné použít infračervené lampy.

8. Seznam použitých zdrojů

1. RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.
2. DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie.* [Brno: M. Drahanský], 2011. ISBN 9788025489796.
3. ГАФНЕР, Василий Викторович, СПИВАК, А. М., ed. *Информационная безопасность*. Ростов-на-Дону: Феникс, 2010г. ISBN 978-5-222-17389-3.
4. ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi. Studijní text.* Ostrava: VŠB TU Ostrava, 2008. [cit. 2021-10-11] Dostupné také z: http://www.rucnepsanypodpis.cz/PDF/biometricke_metody.pdf
5. LODROVÁ, Dana. *Security of Biometric Systems*. Beau Bassin, Mauritius: LAP LAMBERT Academic Publishing, 2017. ISBN 978-3-330-34325-2.
6. NIXON, Mark S. a S. Z. LI. *Handbook of biometric anti-spoofing: trusted biometrics under spoofing attacks*. Editor Sébastien MARCEL. London: Springer, 2014. Advances in computer vision and pattern recognition. ISBN 978-1-4471-6523-1.
7. WECHSLER, Harry, GUO, Guodong, ed. *Mobile Biometrics*. Stevenage, United Kingdom: Institution of Engineering and Technology, 2017. ISBN 978-1-78561-095-0.
8. DASGUPTA, Dipankar, Arunava ROY a Abhijit NAG. *Advances in User Authentication*. Springer International Publishing, 2017. Infosys Science Foundation Series. ISBN 978-3-319-58806-3.
9. *Hand-based biometrics: methods and technology*. Editor Martin DRAHANSKÝ. London: The Institution of Engineering and Technology, 2018. IET book series in advanced biometrics. ISBN 978-1-78561-224-4.
10. *Age factors in biometric processing*. Editor Michael FAIRHURST. London, UK: The institution of engineering and technology, 2014. ISBN 978-1-84919-502-7.
11. MAATTA, Jukka, Abdenour HADID a Matti PIETIKAINEN. Face spoofing detection from single images using micro-texture analysis. In: *2011 International Joint Conference on Biometrics (IJCB)* [online]. IEEE, 2011, 2011, s. 1-7 [cit. 2021-11-16]. ISBN 978-1-4577-1359-0. Dostupné z: doi:10.1109/IJCB.2011.6117510

12. UHL, Andreas, Christian RATHGEB a Peter WILD. *Iris Biometrics: From Segmentation to Template Security*. New York: Springer Publishing Company, 2012 | 2013 ed. ISBN 978-1-4614-5570-7.
13. DRAHANSKÝ, Martin. *Biometrické systémy: Studijní opora*. Vysoké učení technické v Brně, Brno, 2006.
14. SUNDARAN, Sreejit, Joycy K. ANTONY a K VIPIN. Biometrie liveness authentication detection. In: *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* [online]. IEEE, 2017, 2017, s. 1-3 [cit. 2021-11-16]. ISBN 978-1-5090-3294-5. Dostupné z: doi:10.1109/ICIIECS.2017.8276098
15. DRAHANSKÝ, Martin. *Fingerprint recognition technology: related topics: skin disease, image quality and liveness detection*. Saarbrücken: LAP Lambert Academic Publishing, c2011. ISBN 978-3-8443-3007-6.
16. PARKER, Frank S. Near-Infrared Spectroscopy. *Applications of Infrared Spectroscopy in Biochemistry, Biology, and Medicine*. Boston, MA: Springer US, 1971, 1971, 25-40. ISBN 978-1-4684-1874-3. Dostupné z: doi:10.1007/978-1-4684-1872-9_2
17. FUJITSU LTD. *Fujitsu PalmSecure: The solution for user-friendly and reliable authentication – more secure than the competition*. [online]. [cit. 2022-02-04] Dostupné z: https://www.fujitsu.com/my/imagesgig5/PalmSecure%20Global%20Solution%20Catalogue.pdf
18. UHL, Andreas et al. *Handbook of Vascular Biometrics* [online].Cham: Springer, 2020;2019. ISBN 3030277313; 9783030277314; 3030277305; 9783030277307. [cit. 2022-1-15] Dostupné z: https://ris.utwente.nl/ws/files/161155615/10.1007_978_3_030_27731_4.pdf
19. FUJITSU TECHNOLOGY SOLUTIONS, Technická podpora, Obchodní oddělení. *PalmSecure a Palm Vein Sensory* [online]. leden 2020; [cit. 2022-02-05]. Osobní komunikace.
20. UNAR, J. A.; SENG, Woo Chaw; ABBASI, Almas. A review of biometric technology along with trends and prospects. *Pattern recognition*, 2014, 47.8: 2673-2688.
21. PCT-KCUA011: "H1E-USB series" USB authentication device. *Hitachi Industry Control Solutions, Ltd.* [online]. [cit. 2022-02-20]. Dostupné z:

https://info.hitachi-ics.co.jp/eng/products/e_fvein/h1eusb.html

22. BOURGET, Denis a Denis Jean-Claude SIEW. Biometric authentication system and method: WO2012083456A1. Zapsáno 21.12.2011. [online] [cit. 2022-03-05]. Dostupné z: Https://patents.google.com/patent/WO2012083456A1/
23. HAMA, Soichi, Mitsuaki FUKUDA a Takahiro AOKI. FUJITSU LTD. Authentication apparatus: US20100085151A1. Zapsáno 22. 09. 2009. [online] [cit. 2022-03-15]. Dostupné také z: https://patents.google.com/patent/US20100085151A1/
24. *Fujitsu's PalmSecure Deployed in World's First Palm Vein Authentication System at Korean Airports* [online]. [cit. 2022-03-15]. Dostupné z: https://www.fujitsu.com/global/about/resources/news/press-releases/2019/0327-01.html
25. *Biometric Authentication PalmSecure® F-Pro PalmSecure® Products Fujitsu PalmSecure F-Pro Suite* [online]. [cit. 2022-03-07]. Dostupné z: https://www.fujitsu.com/us/Images/Fujitsu_DS-F-Pro_103017.pdf
26. Venenerkennung hacken: Vom Fall der letzten Bastion biometrischer Systeme. Https://media.ccc.de/ [online]. [cit. 2022-03-20]. Dostupné z: https://media.ccc.de/v/35c3-9545-venenerkennung_hacken
27. KRISSLER, Jan a J. ALBRECHT. Venenerkennung hacken: Vom Fall der letzten Bastion biometrischer Systeme. *Proceedings of the 35th Chaos Communication Congress*. Leipzig, 2018.
28. *Technická specifikace – D40X Camera* [online]. 2008 [cit. 2022-03-22]. Dostupné z: https://www.nikon.cz/cs_CZ/product/discontinued/digital-cameras/2009/camera-body-d40x#tech_specs
29. *Nikon D40 Infrared Conversion, Tutorial* [online]. 2008 [cit. 2022-03-22]. Dostupné z: https://www.dpreview.com/forums/post/29011053
30. *Technická specifikace – AF-S DX NIKKOR 18-105mm f/3.5-5.6G ED VR* [online]. 2008 [cit. 2022-03-22]. Dostupné z: https://www.nikon.cz/cs_CZ/product/nikkor-lenses/auto-focus-lenses/dx/zoom/af-s-dx-nikkor-18-105mm-f-3-5-5-6g-ed-vr#tech_specs
31. *Technická specifikace – Tamron SP 70-300 mm F/4-5.6 Di VC USD: https://tamron.cdngc.net/inst/pdf/a005inst_1504_cz.pdf* [online]. 2008 [cit. 2022-03-22]. Dostupné z: https://tamron.cdngc.net/inst/pdf/a005inst_1504_cz.pdf

32. *ImageJ: Image Processing and Analysis in Java* [online]. [cit. 2022-03-22]. Dostupné z: https://imagej.nih.gov/ij/
33. *Koralky.cz: Silikonová pasta k výrobě forem 250g* [online]. [cit. 2022-04-01]. Dostupné z: https://www.koralky.cz/silikonova-pasta-k-vyrobe-forem-250g
34. *VCEST.CZ: Pravý včelí vosk 500g* [online]. [cit. 2022-04-01]. Dostupné z: https://www.vcest.cz/pravy-vceli-vosk-500g_z889/
35. *ARTMIE: Přírodní včelí vosk – red* [online]. [cit. 2022-04-01]. Dostupné z: https://www.malirske-platno.cz/prirodni-vceli-vosk-red-CCH73206
36. *Datasheet Fujitsu PalmSecure Contactless Biometrics Authentication* [online]. [cit. 2022-02-04]. Dostupné z: https://www.fujitsu.com/global/Images/PalmSecure_Datasheet.pdf
37. *PalmSecure A new level of Biometric Technology Solutions* [online]. [cit. 2020-02-04]. Dostupné z: https://www.fujitsu.com/pt/Images/Palm_Secure_tcm72-630557.pdf
38. *Datasheet Příslušenství FUJITSU PalmSecure U Guide: Zabezpečení přístupu* [online]. [cit. 2022-03-07]. Dostupné z: https://sp.ts.fujitsu.com/dmsp/Publications/public/ds-PalmSecure-U-Guide-cz.pdf
39. FUJITSU Biometric Authentication PalmSecure® F-Pro PalmSecure® Products Fujitsu PalmSecure F-Pro Suite [online]. [cit. 2020-02-04]. Dostupné z: https://www.fujitsu.com/us/Images/Fujitsu_DS-F-Pro_103017.pdf
40. CLAHE (Contrast Limited Adaptive Histogram Equalization). *Imagej.nih.gov* [online]. [cit. 2022-03-22]. Dostupné z: https://imagej.nih.gov/ij/plugins/clahe/index.html

8.1. Seznam obrázků

8.2. Seznam tabulek

8.3. Seznam rovnic

9. Seznam příloh

Příloha č. 1

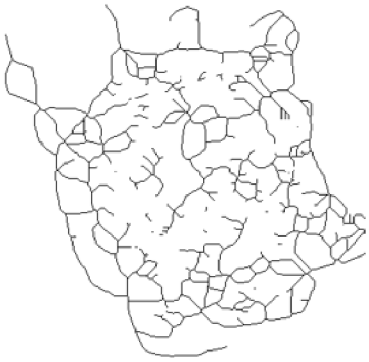
Upravené snímky použité pro otestování biometrického systému krevního řečiště dlaně při záměrné falzifikaci biometrických údajů

LEGENDA K NÁZVŮM OBRÁZKŮ

T	Snímek z testovací aplikace
F	Snímek pořízený fotoaparátem
M3	Medián (rádius 3.0 Mpx)
G1	Gaussovské rozostření (rádius 1.0 Mpx)
G3	Gaussovské rozostření (rádius 3.0 Mpx)
S	Skeletizace
BR	Lokální prahování – Metoda Bernsen
CO	Lokální prahování – Metoda Contrast
MA	Lokální prahování – Metoda Mean
MD	Lokální prahování – Metoda Median
MG	Lokální prahování – Metoda MidGray
NB	Lokální prahování – Metoda Niblack

Obrázek 1 – T-M3-G1-S-BR

Obrázek 3 – T-M3-G1-S-MA



Obrázek 5 – T-M3-G1-S-MG

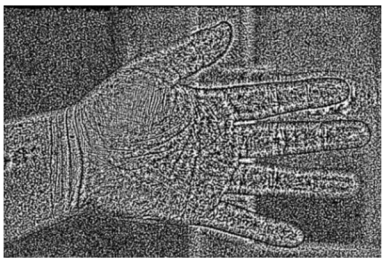
Obrázek 2 – T-M3-G1-S-CO

Obrázek 4 – T-M3-G1-S-MD

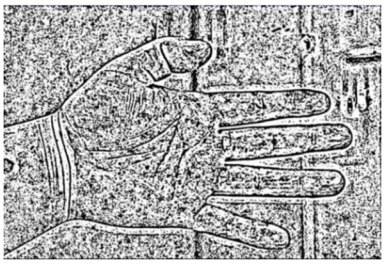
Obrázek 6 – T-M3-G1-S-NB

Obrázek 7 – F-M3-G3-BR (1)

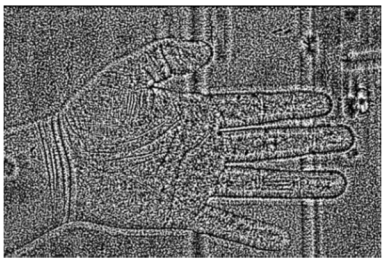
Obrázek 8 – F-M3-G3-MD (1)



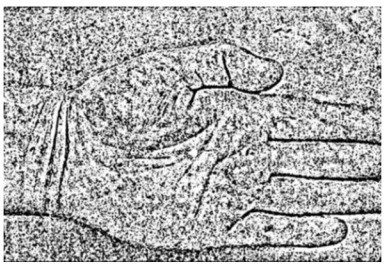
Obrázek 9 – F-M3-G3-BR (2)



Obrázek 10 – F-M3-G3-MD (2)

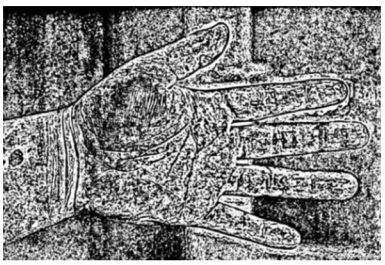


Obrázek 11 – F-M3-G3-BR (3)

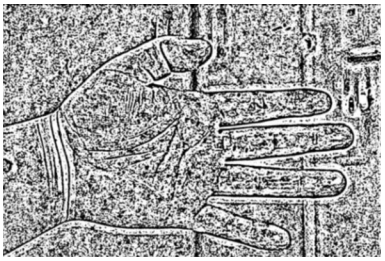


Obrázek 12 – F-M3-G3-CO (1)

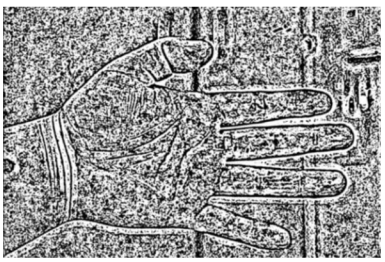
Obrázek 13 – F-M3-G3-MG (1)



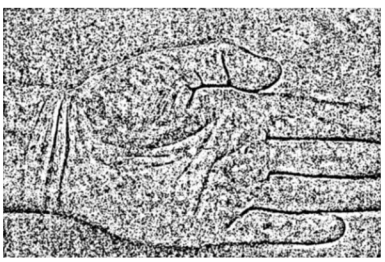
Obrázek 14 – F-M3-G3-CO (2)



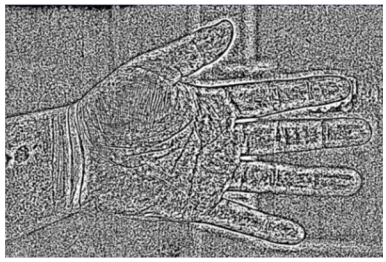
Obrázek 15 – F-M3-G3-MG (2)



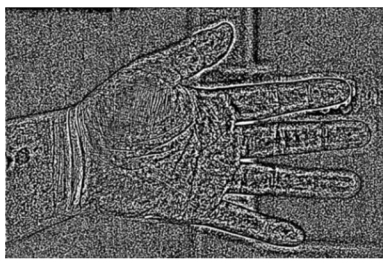
Obrázek 16 – F-M3-G3-CO (3)



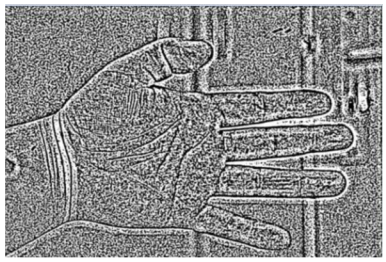
Obrázek 17 – F-M3-G3-MA (1)



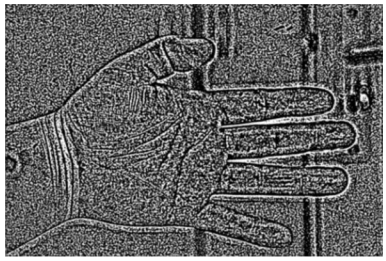
Obrázek 18 – F-M3-G3-NB (1)



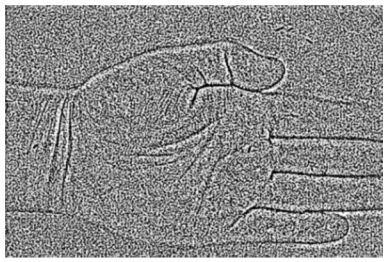
Obrázek 19 – F-M3-G3-MA (2)



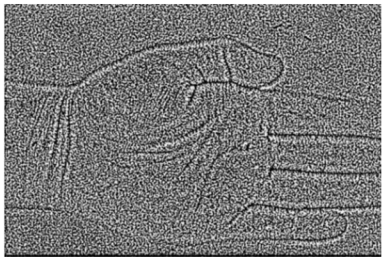
Obrázek 20 – F-M3-G3-NB (2)



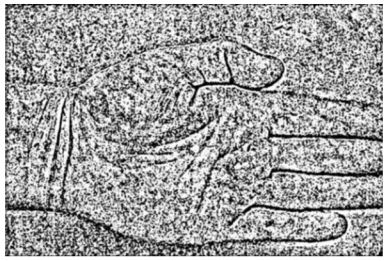
Obrázek 21 – F-M3-G3-MA (3)



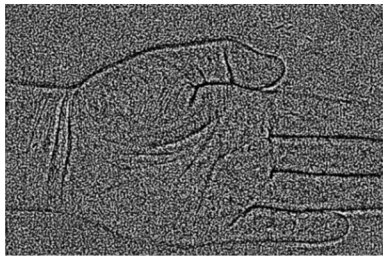
Obrázek 22 – F-M3-G3-MD (3)



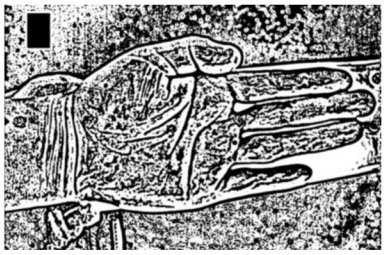
Obrázek 25 – F-M3-G3-MG (3)



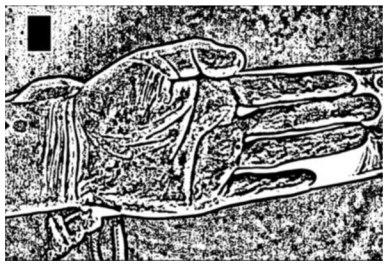
Obrázek 28 – F-M3-G3-NB (3)



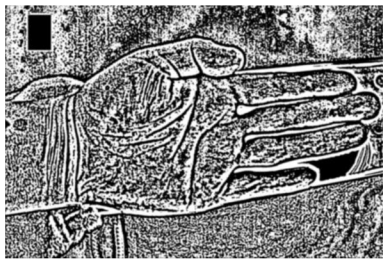
Obrázek 23 – F-M3-G3-BR (4)



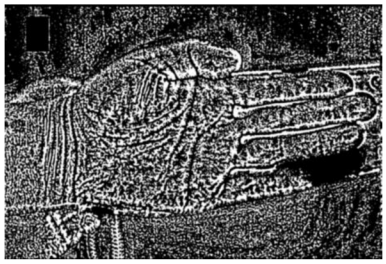
Obrázek 26 – F-M3-G3-CO (4)



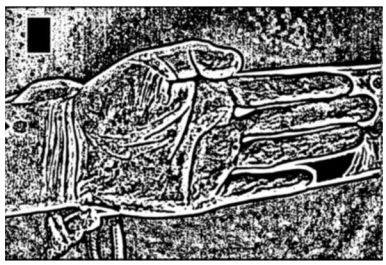
Obrázek 29 – F-M3-G3-MA (4)



Obrázek 24 – F-M3-G3-MD (4)



Obrázek 27 – F-M3-G3-MG (4)



Obrázek 30 – F-M3-G3-NB (4)