VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

ROZPOZNÁVÁNÍ ŽIVOSTI OTISKŮ PRSTŮ

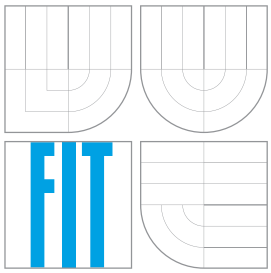
DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. DANA LODROVÁ

BRNO 2007

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

ROZPOZNÁVÁNÍ ŽIVOSTI OTISKŮ PRSTŮ

LIVENESS TESTING BY FINGERS

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. DANA LODROVÁ
AUTHOR

VEDOUCÍ PRÁCE — Ing. Dipl.-Ing. MARTIN DRAHANSKÝ, Ph.D.
SUPERVISOR

BRNO 2007

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav inteligentních systémů Akademický rok 2006/2007

Zadání diplomové práce

Řešitel	**Lodrová Dana, Bc.**
Obor	Inteligentní systémy
Téma	**Rozpoznávání živosti otisků prstů**
Kategorie	Bezpečnost

Pokyny:

1. Nastudujte literaturu, týkající se rozpoznávání otisků prstů se zaměřením na testování živosti prstů.
2. Popište podrobněji hardwarové metody testování živosti prstů.
3. Popište podrobněji softwarové metody testování živosti prstů.
4. Porovnejte jednotlivé metody a uveďte jejich výhody a nevýhody.
5. Implementujte jednu ze softwarových metod testování živosti prstů.
6. Zhodnoťte dosažené výsledky.

Literatura:

- Dle specifikace školitele.

Při obhajobě semestrální části diplomového projektu je požadováno:

- Body 1 až 3.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese
`http://www.fit.vutbr.cz/info/szz/`

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci ročníkového a semestrálního projektu (30 až 40% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním paměťovém médiu (disketa, CD-ROM), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí	**Drahanský Martin, Ing., Dipl.-Ing. , Ph.D.**, UITS FIT VUT
Datum zadání	28. února 2007
Datum odevzdání	22. května 2007

Licenční smlouva

Licenční smlouva je uložena v archivu Fakulty informačních technologií Vysokého učení technického v Brně.

Abstrakt

Cílem této práce je po nastudování literatury, týkající se rozpoznávání otisků prstů se zaměřením na testování živosti, podání podrobného přehledu hardwarových i softwarových metod testování a dále pak popsání mnou implementovaného řešení.
V rámci studia těchto metod bylo nutné v této práci objasnit strukturu biometrického systému a principy na kterých fungují v praxi používané senzory otisků prstů. Z uvedeného přehledu metod testování živosti je zde více místa věnováno metodě založené na pocení pokožky vyvinuté v laboratoři BioSAL a také spektroskopické metodě firmy Lumidigm.
Studium metod testování živosti mne inspirovalo k vytvoření nového typu senzoru pro snímání otisků prstů, který má v sobě zabudováno testování živosti na základě dvou charakteristických vlastností živé lidské tkáně. V rámci testování tohoto senzoru bylo zapotřebí v této práci uvést v současnosti známé metody oklamání senzorů. Z jejich rozboru vyplývá, že nově navržený senzor by měl být teoreticky odolný proti každé z nich.

Klíčová slova

Otisk prstu, daktyloskopie, testování živosti, biometrie, biometrický systém, senzor, vlastnosti lidského těla, pot, spektroskopie, umělý prst.

Abstract

This document deals with presentation of nowadays software and hardware methods used for fingerprint recognition with focus on liveness testing and thereafter it deals with description of my solution.
In order to describe results obtained from study of technical literature, we discuss important terminology of biometric systems at first and further main principles of fingerprint sensors used in practice are shown. From overviewed methods of liveness detection we underline one method based on perspiration (researched by BioSAL laboratory) and one spectroscopic method researched by Lumidigm Corporation.
The study of liveness testing methods inspired me to creation of new type fingerprint sensor which has built-in livennes testing method based on two characteristic properties of living human tisue. In order to test this sensor, we discuss nowadays sensor deception method. It follows from their analysis, that newly designed sensor should be theoretically resistant to each of them.

Keywords

Fingerprint, dactyloscopy, liveness testing, biometry, biometric system, sensor, properties of living body, perspiration, spectroscopy, artificial finger.

Citace

Dana Lodrová: Rozpoznávání živosti otisků prstů, diplomová práce, Brno, FIT VUT v Brně, 2007

Rozpoznávání živosti otisků prstů

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně pod vedením Ing., Dipl.-Ing. Martina Drahanského, Ph.D. a uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

.....
Dana Lodrová
22. května 2007

Poděkování

Tímto bych ráda poděkovala svému vedoucímu diplomové práce panu Ing., Dipl.-Ing. Martinovi Drahanskému, Ph.D. za cenné rady a odborné vedení.

Obsah

Kapitola 1

Úvod

V současnosti můžeme sledovat rostoucí touhu po bezpečnosti ve všech oblastech lidského života. Vyvíjejí se stále dokonalejší systémy pro identifikaci člověka, docházkovými systémy počínaje a přístupem k utajovaným datům konče. V této situaci se dostává do popředí biometrie. Pokud použijete k identifikaci čipovou kartu nebo jinou věc, můžete ji ztratit nebo vám ji někdo ukradne či zkopíruje. Heslo můžete zapomenout, poznačit si na papír ze kterého si jej někdo opíše, nebo jej někdo prostě získá útokem hrubou silou. Biometrickou vlastnost neztratíte, nezapomenete, je s vámi neustále.

V současnosti se používá mnoho biometrických systémů založených na rozpoznávání charakteristických anatomických rysů (obličej, duhovka, sítnice, atd.) a charakteristického chování (podpis, chůze, stisk kláves, atd.). Abychom mohli nějakou vlastnost lidského těla použít v biometrii musí splňovat mnoho požadavků [2]. Každá osoba by měla mít tuhle vlastnost (universalita) a přitom by se u každých dvou osob měla lišit (jedinečnost). V průběhu času by měla zůstat neměnná (konstantnost). Je velmi důležité, aby tato vlastnost byla snadno měřitelná (získatelnost) a přitom byl daný způsob měření pro většinu lidí akceptovatelný. Celý systém musí být co nejlevnější a přitom dostatečně bezpečný, aby nebylo snadné vytvořit falsifikát dané biometrické vlastnosti (bezpečnost). Těchto požadavků je mnoho a je téměř nemožné všem stoprocentně vyhovět. Je nutno dělat kompromisy mezi pohodlím uživatele, bezpečností a cenou systému. V současnosti, dle mého mínění, všem požadavkům nejlépe vyhovuje technologie otisku prstu, což ostatně potvrzuje i její čtyřiceti osmi procentní zastoupení na trhu biometrických řešení [2].

O vzory tvořené papilárními liniemi se lidé zajímali od nepaměti, důkazem toho jsou i některé z jeskynních maleb. Seriózněji se jimi však začali zabývat až v 18. století J. E. Purkyně, Thomas Bewick nebo Nehemiah Grew. Roku 1892 pak Francis Galton vydal knihu *Fingerprints* a o několik let později se mu podařilo prosadit daktyloskopii (nauka o papilárních liniích) do běžné policejní praxe Scotland Yardu. V tomto období byly formulovány také daktyloskopické zákony.

Papilární linie se formují během embryonálního vývoje. V dospělosti se obnovují dorůstáním kůže. Pokud je poškozena spodní vrstva, dle které kůže dorůstá, nedojde v tomto místě k opětovnému vytvoření papilárních linií. Dočasné poškození může být způsobeno mělčím zraněním nebo například bradavicemi. Po vyléčení se však původní papilární linie obnoví. Vzor tvořený liniemi zůstává tedy po celý život stejný a natolik unikátní, že se na světě nenachází žádní dva lidé, jejichž otisky prstů by byly stejné. Dokonce i jednovaječná dvojčata, která není možné např. dle fotografie rozeznat, mají snadno odlišitelné otisky prstů. Vzhledem k tomu, že vzory tvořené papilárními liniemi nejsou stoprocentně geneticky podmíněny, můžeme se také domnívat, že naklonovaný člověk by měl odlišné otisky prstů

než jeho předloha.

Samotné papilární linie jsou asi 0.1 až 0.4 mm vysoké a 0.2 až 0.5 mm široké [2]. Na jejich vrcholcích se nacházejí potní póry. Papilární linií nejsou jen nekonečné jednoduché čáry, ale obsahují i některé změny (ukončení nebo třeba rozdvojení linie), kterým říkáme markanty. Podle pozic a typů nalezených markantů pak rozlišujeme jednotlivé otisky prstů.

Jak je vidět, otisky prstů splňují většinu kritérií pro použití v biometrii. Otisky prstů jsou universální i jedinečné a v průběhu času se nemění. Vzhledem k tomu, že patří k nejdéle používaným biometrickým vlastnostem, existuje mnoho druhů senzorů pro jejich zaznamenání. Tyto senzory jsou vcelku levné a lidé je dobře přijímají, protože si na ně už zvykli. Poslední nediskutovanou vlastností je bezpečnost, tedy jak snadné je vyrobit napodobeninu této biometrické vlastnosti a úspěšně ji použít. Bohužel u mnoha současných senzorů nepatří bezpečnost mezi jejich nejsilnější stránky.

V minulosti došlo k mnoha úspěšným i neúspěšným pokusům obelstít senzory otisků prstů. Roku 2002 zkoumala Lisa Thalheimová (Německo) a její spolupracovníci možné způsoby ošálení biometrických senzorů, zejména senzorů pro snímání otisků prstů [9]. Výsledky byly velmi překvapivé, senzory bylo možno ošálit mnohem snadněji než se očekávalo a to s pomocí běžně dostupných věcí.

Výzkumem v této oblasti se také zabývá profesor Matsumoto (Yokohama National University) a kolektiv jeho spolupracovníků. Vymysleli metodu výroby umělých otisků z želatiny [8], která je hlavní složkou dobře známých "gumových medvídků". Takto vyrobený otisk snadno ošálil většinu kapacitních i optických senzorů. Navíc je možno ho ihned po použití zkonzumovat a zničit tak případný důkazní materiál.

Při běžném provozu dochází také k mnoha (mnohdy velmi laickým) pokusům obelstění senzoru. Jeden ukázkový případ popsala doktorka Valenciaová [5]: V Jižní Africe se k identifikaci osob pro vydávání penze používají otisky prstů. Jednou dovlekli dva mladí lidé na poštu starce. Tvrdili, že jejich strýc je příliš líný, že je mu na obtíž být vzhůru, aby si vyzvedl penzi. Poštovnímu úředníkovi to bylo podezřelé. Prohlásil, že pro vyzvednutí penze musí mít žadatel plnou kontrolu nad svým jednáním a chtěl zavolat vedoucího. Mladí lidé však utekli a nechali starce ležet na podlaze. Stařec byl totiž už mnoho hodin mrtvý.

Jediným řešením jak předcházet výše uvedeným situacím a jak zabránit ošálení senzoru je včlenění testování živosti do senzoru, ať již na hardwarové nebo softwarové úrovni. Je nezbytné testovat zda snímaný vzorek patří živé lidské bytosti, je uměle vyroben nebo byl z jiného lidského těla odejmut.

Testování živosti u otisků prstů je tématem této práce. Abychom mohli hlouběji porozumět metodám testování živosti, musíme nejprve pochopit funkce jednotlivých senzorů otisků prstů a také celého biometrického systému, na což se zaměřím v kapitole 2. V další kapitole se teoreticky věnuji možnostem testování živosti u otisků prstů založených na různých vlastnostech živé tkáně (ať již softwarových nebo hardwarových) a podrobněji rozebírám známější z nich. Čtvrtá kapitola je věnovaná návrhu nového senzoru pro snímání otisků prstů, který obsahuje i testování živosti, a programu pro demonstraci funkce tohoto senzoru. Poslední kapitola obsahuje informace o testování tohoto programu s návodem na výrobu umělých otisků prstů a dalších metod ošálení senzoru.

Kapitola 2

Technologie při práci s otisky prstů

2.1 Typy senzorů

Abychom mohli implementovat metody testování živosti pro konkrétní senzory otisků prstů, je nezbytné, abychom detailně porozuměli principu, na kterém jednotlivé typy senzorů fungují. Ne každá metoda testování živosti se totiž hodí pro každý typ senzoru.

Obecně by senzor měl být schopen pracovat i za extrémnějších podmínek prostředí (např. teplota, vzdušná vlhkost), zvládnout nasnímat mokré a suché prsty i prsty s nevýraznými papilárními liniemi. Pokud by totiž senzor nebyl často schopen nasnímat dostatečně kvalitní otisk pro následné porovnávání, lidé by si vytvořili cestičky jak snímání otisků obejít a celý systém by tak byl zbytečný. Senzor by také měl mít krátkou dobu snímání a zpracování otisku prstu, aby jej mohlo nárazově využít i velké množství lidí (např. příchod ranní směny do práce). A v ideálním případě by měl přímo obsahovat hardwarovou nebo umožňovat snadnou softwarovou implementaci testování živosti. Ale jak již bylo řečeno, je nutné dělat kompromisy mezi bezpečností, uživatelskou přívětivostí a cenou.

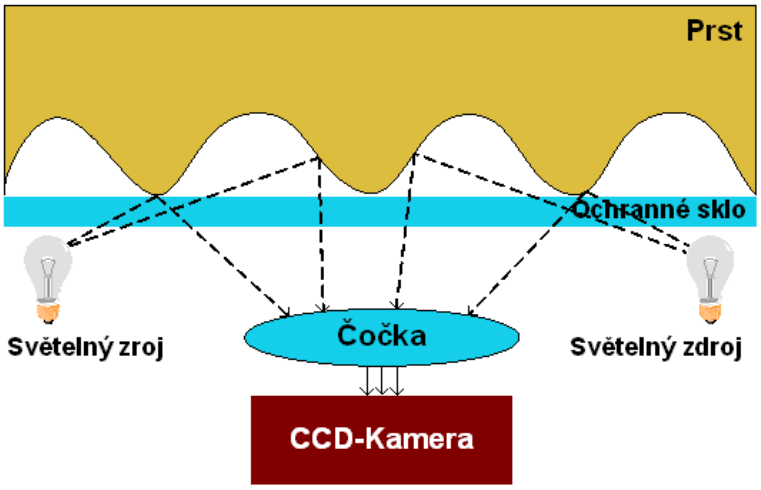
V zásadě máme sedm druhů senzorů snímajících otisky prstů [2, 7, 20]:

Ultrazvukový senzor je složen z ultrazvukového vysílače obsahujícího i přijímač, který opisuje kruhovou dráhu a snímá otisk prstu.

Výhodou ultrazvukových senzorů je skutečnost, že ultrazvukové vlny proniknou i pod svrchní vrstvu kůže. Díky tomuto principu senzoru tolik nevadí poškozený nebo zašpiněný prst a navíc to umožňuje implementaci algoritmu testování živosti. Amplituda a celkový charakter přijatých vln se totiž liší podle toho jedná-li se o umělý nebo živý prst. Navíc celý proces snímání může být bezdotykový, takže se zde nemusí řešit problémy s latentními otisky prstů zanechanými na ploše senzoru. Nevýhodou je složitější algoritmus získávání otisku prstu a samozřejmě také vyšší cena.

V současnosti tento typ senzoru není příliš rozšířen. Zabývá se jimi například polská společnost Optel, Ltd. [25], která tvrdí, že její senzory jsou schopny detekovat i úroveň stresu u snímané osoby, nebo americká společnost Ultra-Scan, Corp. používající technologii LUIS [28]. Tato informace by mohla být užitečná pro detekci, zda si člověk nechává sejmout otisk prstu dobrovolně nebo je k tomu donucen pod hrozbou násilí.

Optický senzor má vcelku jednoduchý princip. Prst je přiložen na skleněnou plochu senzoru, zespodu je pomocí LED (Light-Emitting Diode) diod nasvícen a poté obyčejná CCD (Charge-Coupled Device) nebo CMOS (Complementary Metal Oxide Semiconductor) kamera nasnímá obraz.



Obrázek 2.1: Princip optického senzoru [2].

Existují dva typy optických senzorů. První možností je použití LED diod emitujících světlo jen jedné vlnové délky. V tomto případě se jedná o vcelku levný, nicméně snadno oklamatelný senzor. Je možné jej ošálit nejen umělým prstem, ale i 2D vytištěným otiskem prstu. Navíc je potřeba čistit plochu senzoru kvůli zanechaným latentním otiskům prstů. Latentní otisk je v tomto případě obtížné použít pro oklamání senzoru. Po posypání libovolnou látkou jsou poprášené části (původně vrcholky) vnímány senzorem jako údolí a dochází tedy k revertování otisku prstu. Nicméně je stále možné zanechaný latentní otisk ze senzoru sejmout a na jeho základě udělat umělý otisk prstu nebo jen vytištěný otisk.

Optické senzory používající jen jednu vlnovou délku světla jsou velmi rozšířené a v současnosti je vyrábí například SecuGen Corporation [26], která deklaruje schopnost detekce 2D podvodů, nebo L-1 Identity Solutions, Inc. (dříve Identix, Inc.)[23].

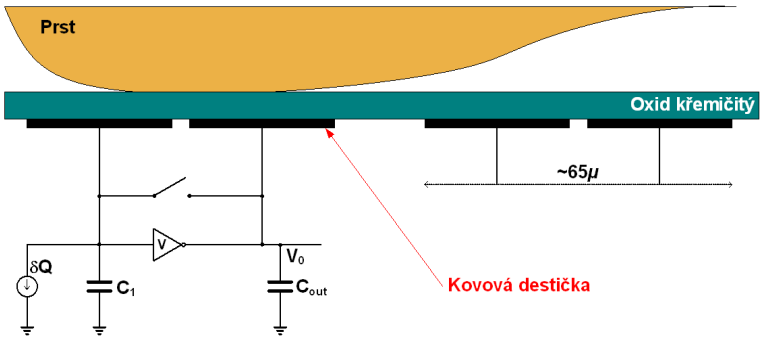
Druhým typem optického senzoru je tzv. multispektrální senzor, který obsahuje LED diody emitující světlo různých vlnových délek z viditelného spektra a také krátkovlnné infračervené záření. Tento princip narozdíl od předchozího umožňuje testování živosti a proto je blíže popsán v části 3.3. Senzory tohoto typu vyrábí Lumidigm, Inc. [24].

Elektrooptický senzor má složitější princip. Skládá se ze čtyř vrstev: izolační, černé koaxiální, fosforové a základní. Uživatel přiloží prst na izolační vrstvu. Jeho přítlakem dojde v místě papilárních linií ke kontaktu koaxiální vrstvy s fosforovou a následnému emitování světla. Světlo poté projde základní vrstvou a je zaznamenáno.

Výhodou elektrooptických senzorů je vyšší kvalita obrazu. Nejsou také oklamatelné latentními otisky prstů, ani jim nevadí suché, či mokré prsty. Nevýhodou je jejich vyšší citlivost na fyzické poškození a znečištění (např. prachem). Tyto senzory vyrábí například společnost Security First Corp. [27](dříve Ethentica), která si pro tento účel nechala patentovat technologii TactileSense, nebo DELSY (Dactyloscopic Electronic Systems), divize ruské společnosti Elsys Corp. [22].

Kapacitní senzor je složen z pole kovových destiček, jejichž rozměry jsou menší než je šířka papilární linie (menší než 0.2 mm). Na tomto poli se nachází souvislá vrstva

oxidu křemičitého fungující jako dielektrikum. Po přiložení prstu se z destiček stanou kondenzátory, jejichž výsledná kapacita odpovídá procentu překrytí destiček papilární linií.



Obrázek 2.2: Princip kapacitního senzoru [2].

Nevýhodou kapacitních senzorů je špatná práce se suchými prsty (příliš světlý obraz) nebo mokrými prsty (téměř černý obraz). Tyto senzory vyrábí například společnost Sony, firma Veridicom International [30] nebo americká společnost UPEK, Inc. [29].

Kapacitní senzory jsou velmi často používány, a proto nechybí v žádném srovnávacím testu senzorů. Bohužel na ploše senzoru často zůstávají latentní otisky prstů a senzor je náchylný k jejich reaktivaci. Podrobnosti o metodách, kterými je možno tento typ senzoru oklamat pak uvádím v části 5.1.

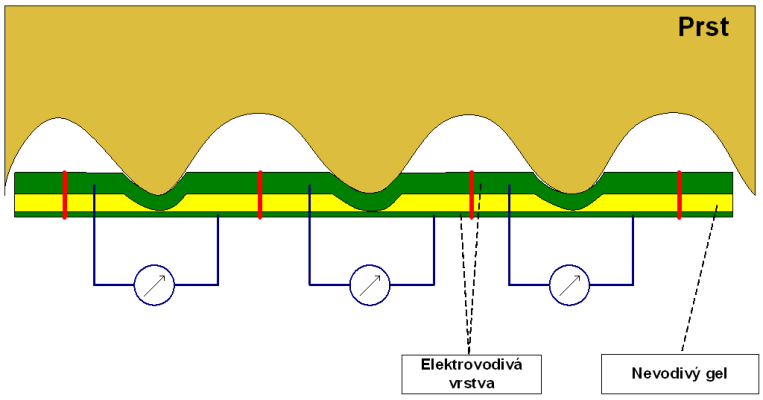
Firma Veridicom International i jiné se snažily vyřešit problém reaktivace latentních otisků prstů implementováním samočisticího mechanismu. Jednalo se v podstatě o ochranný kryt s miniaturní čisticí houbou, který by po každém sejmutí otisku očistil plochu senzoru od případně zanechaného latentního otisku. Bohužel spouštění krytu šlo zablokovat malým dřívkem nebo kouskem zápalky, aniž by senzor odmítl sejmout další otisk bez předchozího očištění plochy.

Ochranou proti reaktivaci latentních otisků prstů by mohlo být porovnání dvou po sobě jdoucích sejmutých otisků prstů. Pokud by se tyto otisky navzájem lišily méně než je nějaká předem stanovená mez, jednalo by se o reaktivaci latentního otisku a biometrický systém by takový otisk odmítl. Při realizaci tohoto řešení ale musíme někde uchovávat předchozí otisk prstu a mít nastavený práh podobnosti, což vytváří nová zranitelná místa biometrického systému.

Tlakový senzor je složen ze dvou elektrovodivých vrstev mezi nimiž je rozprostřen nevodivý gel. Papilární linie přiloženého prstu protlačí svrchní vodivou vrstvu přes nevodivý gel, čímž dojde v místech odpovídajících papilárním liniím ke kontaktu se spodní vodivou vrstvou.

Tento typ senzoru nemá oproti jiným problém se suchými nebo naopak mokrými prsty. Ve srovnání s ostatními mají tyto senzory velkou snímací plochu, sejmou celý otisk prstu, což vede k nižší hodnotě EER (Equal Error Rate) [2]. Výhodou je také nízká spotřeba energie. Nevýhodou je naopak jednobitový výstupní obraz (jen černá a bílá barva), který oproti obvyklému osmibitovému (256 úrovní šedé) poskytuje méně informací.

Tlakové senzory vyrábí například firma BMF Corporation [21].



Obrázek 2.3: Princip tlakového senzoru [2].

Termický senzor se skládá z pyroelektrické buňky zaznamenávající změny teploty a izolační vrstvy. Uživatel musí přetáhnout prst přes pyroelektrickou buňku, která zaznamenává rozdíl teploty mezi teplejšími papilárními liniemi a chladnějšími prohlubněmi.

Tato technologie nemá problémy se suchými či mokrými prsty a vzhledem k principu snímání není ani potřeba čistit senzor od případných zanechaných latentních otisků prstů. Nevýhodou je vyšší spotřeba energie, protože musí být zajištěno, aby nenastala tepelná rovnováha mezi senzorem a povrchem otisku prstu. Dle mého názoru je velkou nevýhodou i uživatelská nepřívětivost tohoto řešení. Přes malou podlouhlou plochu senzoru musí uživatel přetáhnout prst "přiměřenou konstantní rychlostí". Oproti jiným technologiím je tedy zapotřebí uživatele zaškolit a je zde předpokládána dostatečná šikovnost uživatele.

Senzory tohoto typu vyrábí například společnost Bergdata Biometrics GmbH [20], jejíž řešení je založeno na senzoru Atmel FingerChip (TM) od Atmel Corporation [18].

E-Field senzor měří změny elektrického pole tvořené vrcholy a údolími papilárních linií.

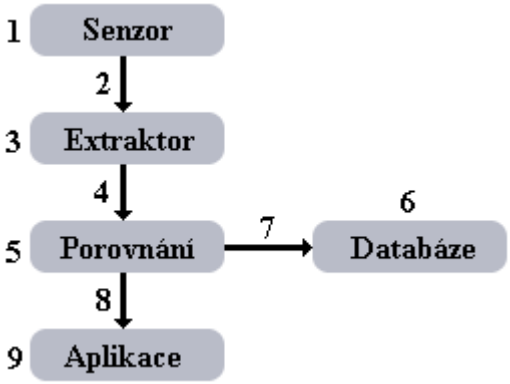
Tento typ senzoru snáze pracuje i s prsty jejichž otisky by například kapacitní senzory měly problémy zaznamenat. Na druhou stranu nevýhodou je nízké rozlišení a malá plocha senzoru, což vede ke zvýšení hodnoty EER.

Tento typ senzoru vyrábí AuthenTec, Inc. [19].

Nejpoužívanější typy senzorů byly také často testovány, zda akceptují i umělý nebo neživý prst. Bohužel, falešné nebo neživé prsty byly velmi často akceptovány. Tyto testy jsou však několik let staré a je možné, že nejnovější senzory již nejsou tak snadno oklamatelné. Rozhodla jsem se proto podrobit mně dostupné senzory jednoduchému testu, jehož výsledky uvádím v části 5.2.

2.2 Obecný biometrický systém

Senzory, kterými jsme se doposud zabývali, jsou ale pouze jednou z několika částí, ze kterých se skládá celý biometrický systém, viz. obrázek 2.4.



Obrázek 2.4: Schéma biometrického systému. Čísla na obrázku odpovídají slabým místům diskutovaným v textu.

Senzor sejme biometrický vzor (v našem případě otisk prstu), který dále putuje do extraktoru k extrakci markantů a vytvoření šablony. Výsledná šablona je vstupem pro porovnávací jednotku. Aby bylo možné šablonu porovnat, je potřeba přístup do databáze, která slouží k uchovávání šablon otisků prstů. Výsledkem porovnání je procentuální shoda, která se dle nastaveného prahu změní na Ano nebo Ne (v případě verifikace) nebo na nalezenou identitu (v případě identifikace). Tento výsledek je pak předán aplikaci, která buď povolí nebo odmítne dané osobě přístup.

Biometrický systém používáme ve dvou různých specifických režimech. První přichází na řadu registrace uživatele do systému. Jedná se o sejmutí biometrického vzoru a uložení výsledné šablony do databáze, kde bude připravena k použití při porovnání. V tomto případě je většinou nejprve ověřena identita uživatele na základě nějakých neelektronických dokumentů (např. občanského průkazu). Registrace uživatele do systému probíhá většinou pod dozorem pověřené osoby, která uživatele zaregistruje. Tento člověk by měl zároveň dohlédnout na správný průběh, tedy aby na senzor nebyla přiložena napodobenina lidského prstu nebo dokonce prst odejmutý jiné osobě a aby nebylo s přístrojem manipulováno. Musí také zkontrolovat zda vytvořená šablona je použitelná, zda neobsahuje příliš málo markantů (špinavý či opotřebovaný prst) nebo naopak mnoho markantů (uživatel při snímání pohnul prstem). Pokud by tahle nekvalitní šablona byla uznána, pak by se díky ní mohla bez problému do systému přihlásit neoprávněná osoba.

Druhým režimem je identifikace nebo verifikace uživatele, při které se využije funkce všech částí systému. Biometrický systém jako celek má v zásadě devět slabých míst [2, 1] (očíslovaných dle obrázku 2.4) :

1. **Podvržení biometrické vlastnosti.** Místo toho, aby na plochu senzoru přiložil svůj prst živý člověk, je přiložen uměle vyrobený nebo odejmutý prst.

2. **Replikace dat.** V tomto případě dojde k zaslání dříve nasnímaných otisků prstů a tedy k obejití senzoru.

3. **Modifikace extraktoru.** Jedná se o situaci, kdy za určitých specifických podmínek modifikovaný extraktor bude generovat předem připravený vektor rysů (šablonu). Tento způsob útoku na biometrický systém se nazývá Trojský kůň.

4. **Vlastní šablona.** Zde se jedná o obejití procesu získání dat a nalezení markantů. Porovnávací jednotce je přímo zaslána předem připravená šablona.

5. **Modifikace porovnávací jednotky.** V tomto případě dojde k modifikaci prahu, dle kterého je vydáván výsledek. Například pokud je nastaven extrémně nízký práh u verifikace, útočníkovi je pak potvrzena libovolná identita.

6. **Změna šablony v databázi.** Jedná se o neoprávněnou modifikaci jedné nebo více šablon v databázi. Osobě, jejíž šablona byla změněna, pak není povolen přístup, ale místo ní pak systém umožní vstup cizí osobě, které přísluší data změněné šablony.

7. **Blokování přístupu k databázi** Bez přístupu k databázi není biometrický systém schopen porovnávat otisky prstů se šablonami v databázi, všem osobám tak bude odepřen přístup. Jedná se o útok typu Denial of Service (DoS). Na první pohled nevypadá, že by tento typ útoku přinesl útočníkovi nějakou výhodu. Avšak v případě, že biometrický systém nefunguje, musí identifikační (nebo verifikační) proceduru jím vykonávanou převzít jiný prvek. Tuto náhradní identifikaci (verifikaci) pak může být pro neoprávněnou osobu snazší oklamat.

8. **Změna výsledku porovnání.** Dojde k zaslání předem vybraného výsledku aplikaci, která na jeho základě povolí přístup neautorizované osobě.

9. **Modifikace aplikace.** Neoprávněný uživatel v tomto případě obejde celý systém získání otisku, extrakce markantů i porovnání. Napojí se přímo na aplikaci, která mu povolí přístup.

Modifikaci extraktoru, porovnávací jednotky nebo aplikace lze zabránit řádnou konstrukcí biometrického systému, kdy nebude možné, aby útočník měl k těmto částem systému přístup, mohl je modifikovat a poté uvést systém zpět do provozu. Pro posílení bezpečnosti může být celý systém pod dohledem pracovníka ostrahy, ať již přímo nebo prostřednictvím kamerového systému.

Pro zajištění bezpečné komunikace mezi jednotlivými částmi systému je zapotřebí použít kryptografii. Důležité je to zejména v případě komunikace mezi porovnávací jednotkou a databází šablon, protože databáze bývá umístěna mimo místnost se senzorem. Tato komunikace je tedy snáze napadnutelnější než například komunikace mezi extraktorem a porovnávací jednotkou, která se odehrává v rámci jednoho přístroje. Všechny komunikační kanály lze také chránit řádným návrhem a konstrukcí celého biometrického systému a dozorem jak bylo popsáno v předchozím odstavci.

Abychom zamezili modifikaci šablon přímo v databázi je nutno opět využít kryptografie. V tomto případě je nutné zajistit důvěrnost a integritu dat. Abychom zajistili integritu dat je nutné, aby data byla zašifrována soukromým klíčem patřícím biometrickému systému (nejlépe registračnímu modulu). Pro zajištění důvěrnosti je zapotřebí zašifrovat data veřejným klíčem patřícím danému uživateli. Data tedy nemůže neoprávněně změnit ani uživatel, kterému patří, ani někdo se znalostí soukromého klíče registračního modulu, natož někdo bez těchto znalostí.

Výše uvedená řešení slabých míst jsou v praxi široce využívána. Zbývá tedy poslední slabé místo biometrického systému, možnost podvržení biometrické vlastnosti při snímání senzorem. Z tohoto důvodu je zapotřebí při snímání biometrické vlastnosti provádět zároveň i testování živosti. Toto řešení je však v praxi málokdy použito. Některé senzory otisků prstů nemají testování živosti implementováno vůbec, jiné jen částečně a jen několik málo z nich

testování živosti implementuje plně. Většina firem v současnosti nesděluje podrobnosti jimi implementovaného řešení testování živosti. Tato politika bývá často nazývána "Security through obscurity" (zajištění bezpečnosti utajením) a na celý biometrický systém bývá nahlíženo jako na černou skříňku. Již v 19. století, ale holandský kryptolog Kerckhoffs dokázal, že tento princip v kryptografii neplatí a dle mého názoru můžeme dnes jeho tvrzení aplikovat i na testování živosti u biometrických systémů. Není přeci možné věřit systému, o kterém pouze jeho výrobci tvrdí, že je bezpečný a přitom nebyl otestován žádnou nezávislou třetí stranou.

Pokud není testování živosti dostatečně implementováno je možné zvýšit bezpečnost biometrického systému dohledem vyškoleného pracovníka ostrahy. Díky dozoru je obtížnější použít umělý nebo mrtvý prst, ale není to nemožné, a také dozorem není možno řešit případy velmi tenkého otisku prstu nalepeného na živý prst. Další možností zvýšení bezpečnosti je používání tzv. multimodálního biometrického systému, což je systém využívající více biometrických vlastností (např. duhovka a otisk prstu), nebo kombinace biometrického systému s jinou formou identifikace (např. pomocí čipové karty). Multimodální biometrický systém je oproti unimodálnímu bezpečnější, protože je jednodušší kvalitně napodobit jednu biometrickou vlastnost než napodobit dvě. Jedná se však jen o způsob jak obejít problém a ne jak jej vyřešit, což nás přivádí zpět k testování živosti.

Kapitola 3

Testování živosti

3.1 Využitelné charakteristiky

Pro testování živosti využijeme jednu nebo více vlastností charakteristických pro živé lidské tělo. V tomto okamžiku bychom mohli namítnout, že již samotné získání biometrické informace je testováním živosti, protože při jejím snímání využíváme vlastností lidského těla. To je sice pravda, nicméně toto "slabé testování živosti" nestačí. Je zapotřebí silnějších a spolehlivějších testů, neboť jak bylo uvedeno dříve, mnoho dnešních senzorů je velmi snadné ošálit.

Při testování živosti je důležité, abychom testovali živost stejné oblasti lidského těla, která byla snímána. Je nesmyslem testovat například reakci zorničky v případě, že provádíme identifikaci na základě otisků prstů. Uživatel pokoušející se o neoprávněný přístup za pomoci umělého prstu bude mít reakci zorničky stejně v pořádku jako oprávněný uživatel. Testování živosti musí být také prováděno současně se snímáním biometrické charakteristiky, jinak by mohlo dojít k záměně nasnímaného umělého prstu za reálný při přechodu ze snímací fáze k testování živosti. Tento fakt zužuje množinu vhodných řešení, protože metoda testování živosti nesmí narušovat průběh snímání otisku a obráceně. Je také zapotřebí, aby tato vlastnost nebyla snadno nebo nejlépe vůbec napodobitelná. V neposlední řadě je nutné, aby testování živosti bylo možné snadno hardwarově nebo softwarově implementovat, aby nezvýšilo příliš cenu tohoto bezpečnostního řešení a přitom nesnížilo jeho použitelnost například dlouhou dobou čekání na výsledek.

Lidské tělo nám poskytuje mnoho vlastností, které můžeme pro naše účely využít. Ne všechny se však hodí pro testování živosti u otisků prstů. V zásadě můžeme tyto vlastnosti rozdělit do tří základních kategorií [5, 1]:

1. **Vnitřní vlastnosti.** Jedná se o vlastnosti živého lidského těla, v případě otisků prstů jde o vlastnosti různých vrstev kůže, případně tkání nebo jiných součástí těla skrytých pod kůží.

   (a) **Fyzické/mechanické.** Do této kategorie lze zařadit hustotu nebo například elasticitu pokožky. Elastičnost pokožky je vyžadována u všech typů senzorů, u kterých je zapotřebí přitisknout prst na plochu senzoru, tedy 3D prst díky elastičnosti je částečně převeden na 2D obraz. Tuto vlastnost lze však i dále využít. Vlivem vzrůstajícího tlaku lze pozorovat změnu šířky papilárních linií. Je tedy možné implementovat softwarové řešení testování živosti, které bude založeno na porovnání šířky papilárních linií před a po silnějšímu přitlačení prstu na plochu senzoru.

(b) **Elektrické.** Zde můžeme uvažovat kapacitanci, impedanci, rezistenci pokožky nebo její vodivost či dielektrickou konstantu. Na měření těchto veličin jsou založeny principy snímání kapacitního nebo E-Field senzoru, v jejich případě se ale nejedná o testování živosti. Pokožka živého člověka má v porovnání s jinými materiály rozdílné elektrické vlastnosti, čehož využíváme pro testování živosti. Pro hardwarovou implementaci je potřeba k senzoru přidat systém elektrod a vyhodnocovací jednotku, které budou pracovat souběžně se snímáním otisku prstu.

Vodivost pokožky je závislá na podmínkách prostředí (např. vlhkost vzduchu), klimatu a také na charakteru pokožky (vlhké nebo suché prsty). Výsledkem je široký interval přípustných hodnot, kterého může být v praxi snadno zneužito.

Dielektrická konstanta se nachází v podobné situaci. Stejně jako vodivost je závislá na podmínkách prostředí, zejména na vlhkosti. Pro ošálení tohoto typu testování živosti by prý stačilo namočit umělý otisk do roztoku alkoholu a vody v poměru 9:1 [7]. Alkohol by se vypařoval rychleji než voda a dielektrická konstanta této směsi by se pomalu posouvala do hodnot odpovídajících živému lidskému prstu.

Testování elektrických vlastností pokožky bylo použito v senzoru FIU-500 společnosti Sony [5]. Tento optický senzor obsahoval jednotku pro měření kapacitance pokožky. Tento typ senzoru byl vyráběn kolem roku 2000, později však společnost Sony tento směr opustila a pokud je mi známo, v současnosti její senzory neobsahují testování živosti.

(c) **Vizuální.** Pro účely testování živosti u otisků prstů je zde možné využít pouze barvu nebo průhlednost pokožky. Samotnou barvu nemá smysl testovat. V dnešní době není nijak obtížné vyrobit umělý prst, který bude barevně zcela odpovídat reálnému. Tato vlastnost se dá využít lepším způsobem. Barva pokožky je v normálním stavu načervenalá, pod vlivem tlaku však zbělá. Tento fakt můžeme změřit jako změnu odrazivosti světla ve viditelné části spektra, zejména pak vlnové délky odpovídající modré a zelené barvě.

(d) **Spektrální.** Do této kategorie patří schopnost pohlcovat, propouštět nebo odrážet elektromagnetické záření různých vlnových délek. Pomocí těchto vlastností můžeme snadno rozlišit jednotlivé materiály, ze kterých může být umělý prst vyroben, a mrtvou tkáň od živého prstu. Na tomto principu je založena technologie firmy Lumidigm [13, 14], kterým se budu zabývat v podkapitole 3.3.

Další možnosti využití těchto vlastností spočívají v měření změn absorbce (pulsní oxymetrie) či odrazivosti světla (např. při změně tlaku). Na měření změn odrazivosti ultrazvukových vln je založena i detekce živosti u ultrazvukových senzorů. Amplituda i celkový charakter senzorem přijaté vlny u živého prstu se totiž významně liší od případu použití umělého prstu.

(e) **Tělní tekutiny.** Pod tímto pojmem je možno si představit různé složky krve, její nasycenost kyslíkem, DNA či další vlastnosti. Co se týče DNA, práce s ní trvá minimálně půl hodiny (což je pro přístupový systém nepoužitelné) a samozřejmě by se pak DNA dala sama o sobě použít k jednoznačné identifikaci osoby a tím pádem by již senzor snímající otisky prstů nebyl zapotřebí.

Nasycenost krve kyslíkem lze pro testování živosti použít. Vyžaduje to ovšem hardwarovou implementaci, založenou na principu pulsního oximetru, který se dnes v medicíně běžně používá. Princip pulsního oxymetru je založen na Lambert-Beerově zákoně [15], dle kterého je absorbce světla o jisté vlnové délce přímo

úměrná koncentraci dané látky. V našem případě se používá světlo dvou různých vlnových délek: červené (660 nm) a infračervené (940 nm). Detekovanou látkou je nasycený a nenasycený hemoglobin, jehož množství se navíc kvůli tepu periodicky mění.

Nevýhodou pulsního oxymetru je čas potřebný pro skenování, který se pohybuje kolem 5 sekund. Tuto detekci živosti lze navíc obelstít, pokud se umělý prst bude pohybovat nebo bude-li mít vlastní zdroj světla blikající s frekvencí odpovídající tepu. Navíc v případě velmi tenkého umělého otisku nalepeného na skutečný prst by snadno mohlo dojít k jeho zanedbání a testování skutečného prstu za ním.

2. **Generované signály.** Jedná se o skupinu signálů, kterou nevědomě a neovlivnitelně generuje živý člověk.

   (a) **Puls.** Tato vlastnost je pro člověka charakteristická a vypadá jako velmi nadějný kandidát pro testování živosti. Musíme však vzít v potaz, že tep se pro jednotlivé osoby velmi liší. Navíc není stejný ani pro jednotlivce. Závisí na emocionálním stavu člověka a také na předcházející fyzické námaze. Normální tepová frekvence odpovídá přibližně 60 až 90 tepům za minutu. Maximální tepová frekvence se pohybuje v rozmezí 200 až 220 tepů za minutu (dle [31]) v závislosti na věku.

   Senzory detekující tep pracují na principu pulsního oximetru, jehož princip byl podrobněji popsán výše (u detekce nasycení krve kyslíkem). I v tomto případě jej lze ošálit pohybem prstu, zdrojem světla nebo při použití velmi tenkého falešného otisku prstu nalepeného na živý prst.

   (b) **Teplota.** Nejjednodušší možností by bylo přímé změření tepoty. Teplota lidské pokožky na konečcích prstů se pohybuje v rozmezí 26 až 30°C. Teplota je závislá na zdravotním stavu (např. horečnatá onemocnění). Navíc existuje velká skupina lidí majících vlivem špatné cirkulace krve studené, někdy až skoro ledové ruce. Lidé z této široké skupiny by byli odmítáni, zatímco velmi tenký umělý otisk prstu nalepený na útočníkův skutečný prst by se vcelku rychle zahřál téměř na teplotu lidského těla a nebyl by pro něj problém tento druh testu živosti obejít.

   (c) **Pot.** Testování živosti u otisků prstů založené na zkoumání zda se prst potí bylo již softwarově implementováno. Výzkumem v této oblasti se zabývá zejména profesorka Shuckersová z laboratoře BioSAL (Biomedical Signal Analysis Laboratory na Clarkson University a West Virginia University) [6, 10, 11, 12]. Jedná se o velmi rozsáhlé téma, které podrobně popisuji v podkapitole 3.2.

   (d) **Odlučování staré kůže.** Pokožka živého člověka odlučuje své odumřelé buňky a lidem se tedy loupe kůže. Tato vlastnost je sice nesporná, nicméně si neumím představit její využití v praxi.

3. **Reakce na podnět.** Jedná se o reakce na podnět vydaný v rámci senzoru snímané oblasti.

   (a) **Ovlivnitelné.** Do této skupiny patří reakce vykonávané vědomě, můžeme je tedy ovlivnit. V případě testování živosti u otisků prstů nemá ze zřejmých důvodů smysl testovat reakce na zvukové nebo visuální podněty, zbývají nám pouze podněty dotekové.

   Jednou z možností je zahřát nebo naopak ochladit dotekovou plochu senzoru a uživatele pak požádat, aby stiskl např. modré tlačítko je-li plocha studená

nebo červené je-li teplá. Na první pohled je zřejmé, že osoba používající např. umělý prst k ošálení systému sice netuší jestli je plocha senzoru chladná nebo teplá, nicméně i tak má padesátiprocentní šanci to uhodnout. Tento princip je nevyhovující a v současnosti nevím o žádném systému, který by jej používal.

(b) **Neovlivnitelné.** Jedná se o reakce, které naše tělo vykonává nevědomě a my nemáme možnost je ovlivnit. Příkladem může být reakce na světlo u zornice oka nebo pohyb kolene při úderu do správného reflexního bodu pod ním.

V případě testování živosti u otisků prstů můžeme sledovat reakci prstu na studený nebo naopak teplý podnět. Na horký podnět reaguje organismus rozšířením periferních cév a dojde tedy ke zvětšení amplitudy průtoku krve. Reakce na studený podnět je opačná. Vzhledem k tomu, že lidé na tento podnět reagují velmi citlivě, je možné snížit teplotní podnět na člověkem nezaznamenatelnou úroveň.

Další možností je sledovat odpověď na malý impuls proudu. Tuto metodu vymyslel pan Peter Kallo spolu se svými spolupracovníky a v roce 2001 si ji nechali patentovat (US Patent 6,175,641) [5]. V praxi tohoto principu využívaly senzory dnes již neexistující firmy Guardware Systems Ltd.

3.2 Pot

Testováním živosti založeném na pocení pokožky se zabývali v laboratoři BioSAL pod vedením profesorky Shuckersové (viz. [1, 10, 11, 12]). Výhodou této metody je čistě softwarová implementace, na rozdíl od jiných způsobů testování živosti není zapotřebí žádný dodatečný hardware. Tato metoda byla nejprve vyvinuta pro kapacitní senzory (citlivé na vlhkost), posléze byla s úspěchem odzkoušena i na optických a elektrooptických senzorech.

Na vrcholcích papilárních linií se ve vzdálenosti asi 0.5 mm od sebe nacházejí potní póry. Jejich pozice se v průběhu života nemění, stejně tak, jako zůstává neměnné samotné uspořádání papilárních linií. Na čtverečním centimetru je možno nalézt přes 90 potních pórů (600 na palec čtvereční) [1]. Mezi suchými a mokrými (zpocenými) oblastmi kůže je velký rozdíl v elektrické vodivosti a dielektrické konstantě, díky čemuž lze vytvořit elektrický model kůže.

Obrázek 3.1: Změna snímků otisků prstů v čase [12].

Metoda profesorky Shuckersové je založena na měření změny vlhkosti (potu) v čase (jak

je vidět na obrázku 3.1). Pot je vlastní pouze živým lidským bytostem, nevyskytuje se u umělých ani odejmutých prstů, a tudíž je možné jej použít pro detekci živosti u otisků prstů.

Postup vyžaduje pro porovnání sejmout otisk prstu dvakrát. Poprvé je otisk sejmut po přiložení prstu na senzor. Typicky vypadá tečkovaně, pot je shromážděn v nejbližším okolí potních pórů. Samotný potní pór může být na snímku vidět jako suchá (bílá) tečka. Po pěti sekundách je sejmut otisk podruhé. Dochází k rozptýlení potu podél papilárních linií do původně polosuchých oblastí. Na snímku se tak celý otisk jeví tmavší. U umělých nebo odejmutých prstů samozřejmě tento jev není pozorovatelný, snímky otisků zachycené v obou časových okamžicích se zde jeví jako téměř identické.

Ačkoliv popis principu testování živosti založeném na detekci potu vypadá jednoduše, samotná implementace algoritmu však snadná není. V první fázi je zapotřebí vstupní snímek otisku prstu předzpracovat a zvýšit tak kvalitu obrazu pro samotné zpracování. Nejprve je odstraněn šum pomocí mediánového filtru a posléze je celý obraz upraven pomocí ekvalizace histogramu.

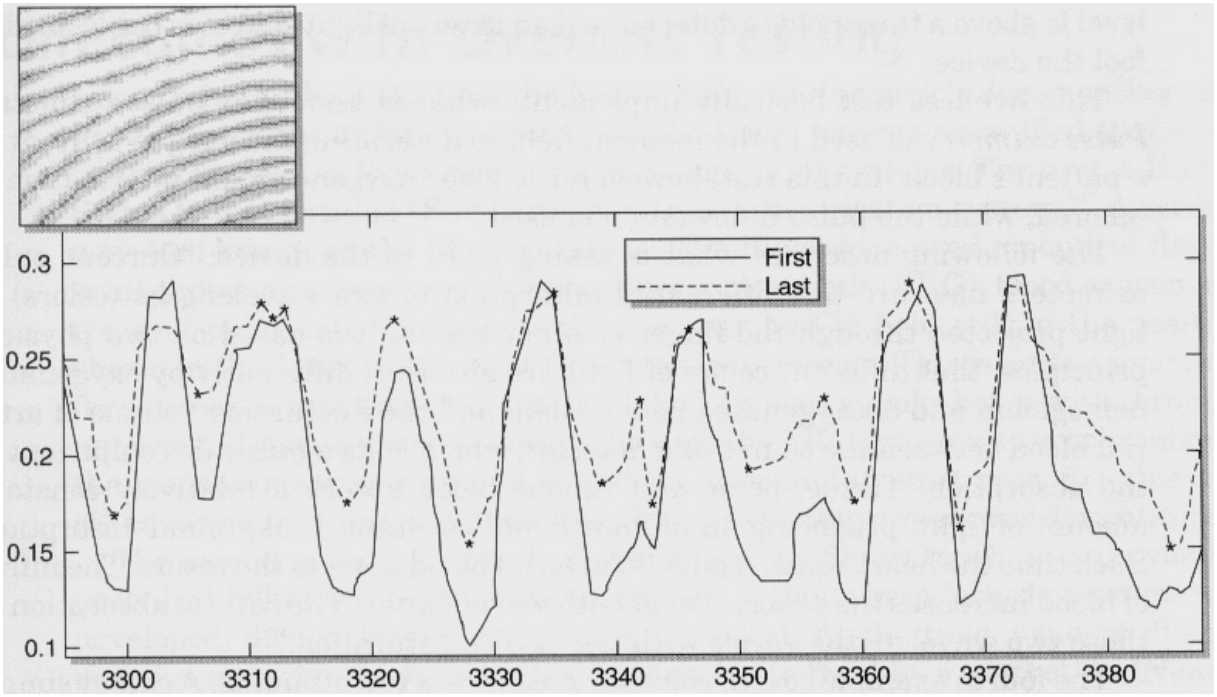
V druhé fázi probíhá samotné zpracování. Dochází zde k mapování dvourozměrného otisku prstu na signál, jehož hodnota reprezentuje úroveň šedé ve vstupním obrazu. Tento signál je vypočten pro oba dva zachycené snímky. Poté je provedeno jedno statické a několik dynamických měření. Statické měření spočívá v aplikaci Fourierovy transformace a je zaměřeno na vzdálenost mezi jednotlivými póry. Dynamická měření jsou založena na srovnání těchto dvou snímků. V případě, že oba signály zakreslíme do stejného grafu (obr. 3.2) je zde zřetelně vidět rozlévání potu podél vrcholků papilárních linií. Celková energie signálu je pak u prvního snímku větší než u druhého. U prvního snímku můžeme také pozorovat větší výkyv (rozdíl mezi hodnotou lokálního maxima a minima) než u druhého. Zatímco lokální maxima nabývají u obou snímků přibližně stejných hodnot, zatímco hodnoty lokálních minim bývají u druhého snímku výrazně větší. Obecně lze také pozorovat, že výkyv bývá u živého prstu větší než u umělého nebo odejmutého.

Ve třetí fázi dochází k rozhodnutí, zda testovaný vzorek pochází ze živého prstu. Výsledné rozhodnutí by mohlo být složením všech jednotlivých (statických i dynamických) měření. Tento způsob ale není příliš efektivní a algoritmus pak dosahuje vyšší hodnoty EER. Jako mnohem lepší se v této fázi ukázalo použití neuronové sítě Back Propagation. Vstupy sítě jsou výsledky jednotlivých měření, výstupem je 1 (v případě přijetí) nebo -1 (v případě odmítnutí).

Pro testování úspěšnosti této metody testování živosti bylo zapotřebí nejprve vymyslet způsob ošálení senzorů, tedy způsob výroby umělých prstů schopných senzor ošálit. Pro výrobu byly jako materiály použity plastelína (PlayDoh) a jílovitá hmota. V obou případech se jedná o vcelku vlhké materiály, což bylo důležité vzhledem k tomu, že tato metoda testování živosti je na vlhkosti založena.

Dalším krokem bylo samotné testování. Nejprve byly prováděny testy pouze na kapacitním senzoru. Testovací množina se skládala z 18 vzorků "živých prstů" osob ve věku 20-29 let, 18 umělých prstů z plastelíny (PlayDoh) a 18 odejmutých prstů. Pro neuronovou síť bylo stanoveno 2/3 vzorků z každé kategorie pro trénink, zbývající vzorky byly použity pro testování úspěšnosti. Síti bylo dopřáno libovolného počtu iterací pro učení (nebyl tedy stanoven maximální počet iterací). Ohromujícím výsledkem testování byla 100% úspěšnost.

Později proběhly rozsáhlejší testy na kapacitním, optickém a elektrooptickém senzoru. Došlo také ke snížení doby mezi snímky na 2 sekundy, přidání dvou nových dynamických měření a pro rozhodování byly použity i jiné metody než jen neuronová síť. Skupina testovaných prstů byla také značně rozšířena. V tomto případě se jednalo o 33 lidí v různém věku (někteří i starší padesáti let). Pro úplnost studie zde byli zastoupeni lidé různých etnik i



Obrázek 3.2: Výsledné signály odpovídající průběhu rozlévání potu [5].

pohlaví. Dále bylo použito 33 umělých a 14 odejmutých prstů. Pro učení byla použita první polovina vzorků a pro testování druhá. Výsledkem byla průměrně 90% úspěšnost.

Ačkoliv bylo testování této metody oproti původním testům rozšířeno a zpřesněno, stále ještě existují aspekty, které by bylo dobré prozkoumat. Vzhledem k tomu, že z každého typu technologie byl použit pouze jeden senzor, stálo by za úvahu rozšířit testování na více senzorů z každé technologie, pokud možno od různých výrobců. Pro oklamání senzoru byly sice k výrobě umělých prstů využity vlhké materiály, nicméně nebyl testován žádný umělý prst snažící se imitovat samotný proces pocení. Možná by nebylo špatné otestovat i podmínky okolního prostředí za jakých je testování prováděno. Nicméně vzhledem k dosaženým výsledkům vypadá tato metoda velmi slibně.

3.3 Spektroskopie

Testování živosti založené na spektrálních vlastnostech vyvinuli ve společnosti Lumidigm, Inc (viz. [1, 13, 14, 24]). Tato metoda je čistě hardwarová a lze ji použít pro testování živosti pomocí hardwarového rozšíření u již existujících optických či jiných vhodných senzorů nebo může být začleněna již při výrobě tzv. multispektrálního optického senzoru.

Lidský prst se skládá z mnoha vrstev, z nichž každá má odlišné spektrální vlastnosti. Uměle vyrobené prsty mají odlišnou strukturu a jsou vyrobeny z jiných chemických látek, proto je jejich spektrální charakteristika odlišná. Stejně snadno rozpoznatelné jsou i odejmuté prsty, protože v lidské tkáni po přerušení krevního oběhu dochází k mnoha nevratným chemickým reakcím, které výslednou spektrální charakteristiku výrazně změní.

Princip této metody spočívá v nasvícení prstu světlem různých vlnových délek (viditelné

světlo až infračervené záření, tedy 395 nm - 940 nm). Každá vlnová délka pak dokáže proniknout do různé hloubky pod povrch prstu a je v rozdílné míře pohlcena a rozptýlena tkání. Například modré světlo (nejkratší vlnová délka) nepronikne příliš hluboko, naopak světlo vlnové délky odpovídající červené (nebo dokonce infračervené záření) pronikne nejhlouběji pod povrch prstu. Vlnové délky jsou pečlivě voleny, aby odpovídaly jednotlivým součástem živých tkání (melaninu, bilirubinu, hemoglobinu, kolagenu, atd.).

Existují různé implementace tohoto principu. V jedné z nich je k nasvícení použito 32 LED diod [1], které jsou zapínány v přesném pořadí. Mezi nimi je pak umístěno 5 křemíkových fotodiod pro zachycení odraženého světla. Pokročilejší možností je pak použití 72 LED diod [13] pro emitování světla různých vlnových délek a zachycení odraženého světla pomocí CCD nebo CMOS kamery.

V roce 2004 proběhlo rozsáhlé testování tohoto principu [1]. Testovacími subjekty bylo 169 lidí ve věku 19-86 let. Dále bylo vyzkoušeno 19 substancí pro výrobu falešných prstů, například různé druhy či barvy silikonu, pěny, plastelíny (PlayDoh), latexu, dřeva nebo zvířecích produktů. Tloušťka použitých materiálů však prý byla vcelku silná. Vyhnuli se tak možnosti, že by paprsky prošly materiálem a výsledné procento zachyceného odraženého světla by charakterizovalo prst za tímto umělým materiálem. Všechny výše uvedené materiály byly touto metodou snadno detekovatelné jako neživý subjekt (nejvíce živé lidské kůži odpovídala pěna a světle hnědá plastelína) a dokonce byly rozlišitelné i mezi sebou.

Ačkoliv tato metoda byla oproti ostatním testována mnohem šířeji, stále není testovací vzorek dostatečný. Bylo by vhodné použít většího počtu lidí a zahrnout i členy různých skupin dle barvy kůže, muže i ženy, nebo i lidi mající nějakou chorobu, která by mohla spektrální vlastnosti ovlivnit. Také jsem nenalezla výsledky testů zkoumající úspěšnost odhalení podvodu při použití odejmutého prstu.

Kapitola 4

Nový senzor

Studium charakteristik lidského těla využitelných pro testování živosti mne inspirovalo k vytvoření nového senzoru pro otisky prstů, který bude zároveň obsahovat testování živosti dvou charakteristických vlastností. Když jsem poté hledala na internetu, zda již někdo podobný senzor nevytvořil, narazila jsem na dva patenty: US Patent 5,088,817 a US Patent 6,292,576. Každý z nich testuje pouze jednu ze dvou mnou využívaných vlastností. V prvním případě se však jedná o jiný způsob testování a tedy i odlišnou konstrukci senzoru, v případě druhého patentu dochází k testování jiného aspektu druhé vlastnosti.

Došla jsem tedy k závěru, že mnou navržený senzor je konstrukčně ojedinělý a spolu s vedoucím mé práce panem Ing. Dipl.-Ing. Martinem Drahanským, Ph.D. jsme se dohodli, že by bylo na místě podat žádost o přidělení užitného vzoru pod názvem:

TESTOVÁNÍ ŽIVOSTI PRSTŮ VYVOLÁNÍM OPTICKÝCH ZMĚN.

Podíl na tomto řešení máme oba: můj je nápad a návrh senzoru, pan Drahanský je pak autorem technického návrhu řešení. Tuto nabídku předmětu průmyslového vlastnictví jsme zaslali na Ústav transferu technologií VUT v Brně, který jej vede pod evidenčním číslem 2007/002.

4.1 Návrh senzoru

Vzhledem k tomu, že tato diplomová práce je již z principu přístupná širokému okruhu lidí, nemohu zde zveřejnit návrh senzoru, protože by to bylo v rozporu s prohlášením o mlčenlivosti, které jsem spolu s nabídkou předmětu průmyslového vlastnictví musela podepsat. Kompletní popis tohoto senzoru je tedy obsažen pouze v tajné části této práce.

4.2 Program pro demonstraci funkce senzoru

Pro demonstraci funkce tohoto senzoru jsem vytvořila program v jazyce C++ s využitím OpenGL. Vzhledem k tomu, že tento senzor existuje pouze ve formě návrhu (výroba prototypu je plánována na příští až přespříští akademický rok), musela jsem pro zachycení snímků otisků prstů využít dostupné vybavení laboratoře.

S využitím sejmutých otisků a tohoto programu jsem experimentálně stanovila meze obou charakteristických vlastností, ve kterých se nachází živý lidský prst. Tyto meze byly ovšem stanoveny pouze na základě sejmutých otisků několika prstů jedné osoby, což je

ovšem pouze provizorní záležitost. Do budoucna je plánováno rozsáhlejší testování tohoto principu, kde by měl být použit co nejširší vzorek testovaných osob (tedy osoby různého věku, pohlaví i různého etnických skupin), aby bylo možné potvrdit univerzalitu těchto dvou charakteristických vlastností a také lépe stanovit jejich meze pro živý lidský prst. Osobně však nepředpokládám, že by se tyto vlastnosti i v rámci takto široké skupiny lidí nějak výrazněji lišily.

Dále bude zapotřebí otestovat princip senzoru oproti pokusům o podvržení biometrického vzoru. Po pečlivém prostudování známých metod oklamání senzoru (viz. část 5.1 této práce) však nepředpokládám, že by některá z nich mohla být u tohoto senzoru úspěšná.

Vzhledem k výše uvedeným faktům (především kvůli neexistenci prototypu senzoru) je tento demonstrační program uzpůsoben pouze pro offline testování živosti. Vzhledem k obtížnosti zpracování obrazu v tomto případě program vyžaduje při určování hranic jedné z metod asistenci uživatele. Do budoucna se počítá s úpravou programu (vylepšením a vyladěním algoritmů zpracování obrazu) tak, aby mohl celý program zpracovat požadavek na testování živosti v reálném prostředí (online) a bez nutnosti zásahu uživatele.

Kompletní popis programu se nachází v tajné části této práce.

Kapitola 5

Testy oklamání senzorů

5.1 Možnosti oklamání senzoru

Existuje mnoho metod podvržení biometrické charakteristiky – oklamání senzoru. Pro některé z nich je zapotřebí vyrobit umělou napodobeninu schématu papilárních linií člověka za kterého se chcete vydávat, pro jiné stačí pouze využít otisku zanechaného na snímací ploše senzoru (latentní otisk). Podle obtížnosti jsem tyto metody rozdělila následovně:

1. **Reaktivace latentního otisku prstu.** Zde se jedná o znovupoužití otisku prstu, který byl zanechán na senzoru.

   (a) **Dýchnutí.** Pro reaktivaci latentního otisku u senzorů stačí skutečně jen lehké dýchnutí na plochu senzoru. Vodní pára obsažená v dechu zkondenzuje na povrchu senzoru a v kombinaci s mastnotou latentního otisku způsobí změnu kapacitance, kterou senzor chápe jako pokyn k zahájení snímání otisku. Je však nutné podotknout, že tato metoda není stoprocentně úspěšná a kvalita takto získaných snímků není nijak vysoká, nicméně k oklamání senzoru to stačí.

   (b) **Sáček s vodou.** Tato metoda je v principu obdobou předchozí. Opět dochází ke kontaktu vody s latentním otiskem prstu, nicméně v tomto případě se voda na plochu senzoru nedostane dýchnutím, ale prostřednictvím přiložení tenkostěnného igelitového sáčku naplněného vodou. V tomto případě je voda rozprostřena rovnoměrněji a kvalita sejmutého otisku je oproti předchozímu případu vyšší. Metoda sama má také vyšší spolehlivost.

   (c) **Grafitový prášek.** Další možností je poprášení latentního otisku grafitovým práškem a přelepení lepicí páskou. Poté je na pásku lehce zatlačeno a senzor otisk bez problému sejme. Výsledkem jsou snímky vysoké kvality a stoprocentní úspěšnost metody. Modificací této metody je možnost použití latentního otisku i například ze sklenice nebo CD. Tento otisk je opět poprášen grafitovým práškem tak, aby prášek zůstal pouze v místech papilárních linií. Takto upravený otisk je poté přelepen lepicí páskou. Grafitový prášek v místech papilárních linií zůstane na pásce i po odlepení od původního podkladu a může být použit pro oklamání senzoru stejně jako v předchozím případě.

Tyto tři výše uvedené metody oklamání senzorů byly v roce 2002 úspěšně odzkoušeny na kapacitních senzorech společností Infineon, STMicroelectronics a Veridicom [9].

Obecně platí, že reaktivace latentního otisku je možná pouze u těch senzorů na jejichž povrchu lze tento otisk zanechat. Tím jsou vyloučeny bezdotykové metody snímání otisků prstů (jako například některé ultrazvukové senzory) a také termický senzor, kdy je prst snímán při přetahování přes pyroelektrickou buňku a tudíž otisk zanechat nelze. Dále pak můžeme vyloučit tlakový a elektrooptický senzor, kdy otisk sice zanechat lze, ale tento senzor vyžaduje trojrozměrný model papilárních linií ke snímání, a tudíž zde reaktivace není možná.

Posypání latentního otisku by mohlo fungovat u optického senzoru, nicméně je zde menší komplikace. V případě, že by byl tento otisk posypán grafitovým práškem a pak například překryt papírem, senzor by černá místa chápal nikoliv jako papilární linie, ale jako údolí mezi nimi. Aby tento model byl úspěšný musí dojít k reverzi otisku, což zatím pokud je mi známo nikdo neodzkoušel.

Tyto tři metody využití latentního otisku prstu by dle mého názoru mohly fungovat i pro E-Field senzor, protože je ve svém principu vcelku podobný kapacitnímu senzoru.

2. **Tisk/fotografie prstu.** Obecně panuje tvrzení, že pro ošálení optického senzoru stačí použít na papír vytištěný otisk prstu. Tato možnost vypadá pravděpodobně, nicméně nenašla jsem žádný publikovaný test, který by tuto možnost vyzkoušel. U ostatních typů senzorů není díky jejich principu pravděpodobné, že by se takovouto jednoduchou metodou nechaly oklamat.

3. **Razítko.** Jedná se o jednodušší obdobu výroby umělého prstu, o které se velmi často mluví jako o jedné z možností pro oklamání různých druhů senzorů. Stejně jako v předchozím případě jsem ani zde nenašla žádný publikovaný test a tak jsem se rozhodla tuto metodu vyzkoušet sama. Výsledky tohoto testu uvádím v části 5.2.

4. **Umělý prst.** Pro výrobu umělého prstu můžeme použít dva možné přístupy: prst lze vyrobit buď s nebo bez asistence uživatele. Obecně platí, že výroba s pomocí uživatele je snazší a výsledný prst má vyšší kvalitu, nicméně ne vždy je to možné a i výroba prstu například z latentního otisku zanechaného někde na sklenici je možná a její výsledky jsou bez problémů použitelé. V praxi bylo otestováno několik materiálů z nichž byly umělé prsty vyrobeny:

   (a) **Silikon.** S tímto materiálem pracovala spolu se svými kolegy paní Lisa Thalheim [9]. Forma pro tento prst byla vyrobena pomocí vosku, do kterého byl otištěn prst. Forma byla poté vyplněna běžně dostupným silikonem. Tyto prsty byly testovány na zařízeních obsahujících optické senzory od společnosti Identix, kterými byly akceptovány ve 100 procentech případů. Dále pak byly testovány na termickém senzoru společnosti Atmel. V případě termického senzoru byl tento prst schopen senzor oklamat až po jisté době, protože při práci s termickými senzory je obecně potřeba jisté praxe.

   Se silikonovými umělými prsty pracoval také pan Putte s panem Keunigem [7], kterým se pomocí tohoto modelu podařilo oklamat optické i kapacitní senzory mnoha společností. Pro oklamání kapacitního senzoru však musel být umělý prst naslíněn, aby jeho elektrické vlastnosti více odpovídaly živému lidskému prstu a senzor mohl otisk sejmout. Pro výrobu formy na silikon byla použita sádra (v případě kooperace s uživatelem) nebo plošný spoj s fotocitlivou vrstvou (v případě výroby z latentního otisku).

(b) **Želatina.** Tento druh umělých prstů zkoumal profesor Matsumoto se svými spolupracovníky [8]. V případě výroby umělého prstu ve spolupráci s uživatelem byl pro výrobu formy využit materiál freeplastic do něhož byl prst otištěn. Jednalo-li se o výrobu bez spolupráce s uživatelem, byl použit na skle zanechaný latentní otisk, jehož viditelnost byla vylepšena za použití kyanoakrylátového lepidla. Otisk byl posléze vyfocen a po upravení v grafickém programu vytištěn na průhlednou fólii. Pro formu samotnou byl poté použit plošný spoj s fotocitlivou vrstvou. Přes tento spoj byla položena fólie s potiskem prstu a pomocí UV záření a následných úprav byla forma vyrobena. Do takto vyrobených forem byla poté vlita tekutá želatina a formy byly zchlazeny v ledničce.

Takto vyrobené umělé prsty jsou téměř průhledné s jantarovým zabarvením a mají jednu překvapivou výhodu oproti ostatním materiálům. Želatina je požívatelná a tudíž může útočník, který ji použije pro získání neoprávněného přístupu, v případě hrozícího prozrazení sníst a zničit tak případný důkazní materiál.

Želatinové umělé prsty (profesorem Matsumotem nazývané "gummy fingers") byly testovány na šesti optických (senzory společností Identix, Mitsubishi, NEC, Omron, Sony a SecuGen), čtyřech kapacitních (Fujitsu, Infineon, NEC a Sony) a jednom elektrooptickém senzoru společnosti Ethentica. Ve všech případech byly senzory velmi snadno oklamány a nasnímaly umělý prst.

(c) **Plastelína.** Další možností je výroba umělých prstů z plastelíny (PlayDoh), čímž se zabýval kolektiv profesorky Shuckersové z laboratoře BioSAL [11]. Tento materiál byl vybrán kvůli relativně vysoké vlhkosti, protože hodně senzorů pro snímání otisků prstů je na vlhkost citlivých. Tímto způsobem se podařilo ošálit optické, elektrooptické i kapacitní senzory.

5. **Odejmutý prst.** Obtížněji detekovatelným podvodem je použití prstu odejmutého uživateli, jak je často k vidění v různých, převážně akčních, filmech. Tento způsob oklamání senzoru studoval kolektiv profesorky Shuckersové z laboratoře BioSAL [11]. Pomocí těchto prstů byly úspěšně oklamány kapacitní, optické i elektrooptické senzory.

6. **Velmi tenký umělý otisk prstu.** Tato metoda je obecně považována za nejhůře detekovatelnou ze všech možností oklamání senzoru. Tenké otisky prstu jsou obecně vyráběny ze stejných materiálů jako celé umělé prsty a přebírají tedy i jejich výhody při ošálení senzorů. Navíc zde hraje roli i jejich malá tloušťka, která může při testování živosti způsobit zanedbání umělého otisku a testování živého prstu za ním.

   Vzhledem k nenápadnosti této metody tak pro zvýšení bezpečnosti nepomůže ani instalace kamer ke snímači otisků prstů nebo dohled pracovníka ostrahy, protože takto vyrobený padělek může být na záznamu kamery nerozeznatelný a i člověk jej může snadno přehlédnout.

5.2 Testování s využitím razítka

Rozhodla jsem se otestovat, zda je pravdivé tvrzení, že senzory otisků prstů se dají ošálit pomocí obyčejného razítka.

Pro tento účel jsem si nechala vyrobit razítko s otiskem prstu (viz. obrázek 5.1) o velikosti 17x13 mm. Nechat si vyrobit tento typ razítka je nad očekávání snadné. Stačí jen zanést do obchodu disketu s fotografií otisku prstu (upravenou do černobílé podoby)

Obrázek 5.1: Razítko s otiskem prstu.

nebo dokonce stačí i otisk na papíře. Za dva až tři dny si pak můžete přijít pro razítko. Takto získaný umělý otisk prstu je ve velmi vysoké kvalitě (záleží samozřejmě na předloze) a výroba razítka stojí pouhých 100 Kč.

Ve školní laboratoři jsem vyzkoušela čtyři senzory otisků prstů, každý z nich používal jinou technologii snímání otisků. První z nich byl optický senzor společnosti Suprema SFM-3020. Dle očekávání bylo velmi snadné jej oklamat pomocí razítka . Na obrázku 5.2 vidíte vlevo otisk sejmutý senzorem z razítka, vpravo pak pro porovnání otisk sejmutý z živého prstu. Jak je zřetelně vidět, oba tyto otisky jsou dostatečně kvalitní.

Obrázek 5.2: Test optického senzoru. Vlevo otisk sejmutý z razítka, vpravo ze živého prstu.

Dalším testovaným senzorem byl kapacitní senzor Suprema SFM 3050. U kapacitních senzorů obecně hodně záleží na vlastnostech materiálu, ze kterého je umělý prst vyroben. Předpokládala jsem sice, že senzor bude možné obelstít, nicméně jsem si nebyla jistá kvalitou takto získaného otisku. Výsledek testu je na obrázku 5.3.

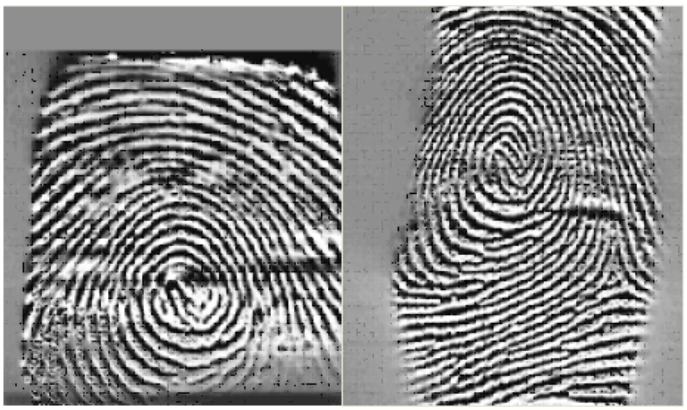
Na obrázku se senzorem sejmutými otisky je patrné, že guma použitá pro výrobu razítka není pro oklamání kapacitního senzoru zrovna ideálním materiálem, protože výsledný otisk je poněkud světlý, ale pro obelstění senzoru je to dostatečné.

Třetí senzor, na kterém jsem použití razítka testovala, byl termický senzor společnosti Bergdata FCAT 100. V tomto případě bylo oklamání senzoru poněkud komplikovanější. Razítko má sice šířku otisku 13 mm, nicméně tento otisk je umístěn na podstavě o šířce

Obrázek 5.3: Test kapacitního senzoru. Vlevo otisk sejmutý z razítka, vpravo ze živého prstu.

přibližně 2 cm. Takto široké prsty tento senzor neočekává a nebylo možné takto senzor otestovat. Oproti dále testovanému E-Field senzoru je však senzor firmy Bergdata rozebíratelný. Po obnažení snímacího mechanismu a krátkém tréninku už nebyl problém s oklamáním senzoru. Výsledek je vidět na obrázku 5.4.

Vlevo je opět otisk získaný za použití razítka, vpravo pak otisk sejmutý ze živého prstu. Na první pohled vypadají tyto otisky odlišně, ale opak je pravdou. Musíme vzít v úvahu nesnadný a uživatelsky velmi nepřívětivý způsob práce s termickým senzorem. V případě, že otisk vypadá poněkud sraženě, znamená to, že uživatel přetáhl prst přes senzor rychleji než by bylo vhodné. Pokud naopak otisk vypadá protáhle (jako na obrázku 5.4 v případě živého prstu) znamená to, že prst byl naopak přetažen přes senzor moc pomalu. Odhadnout správnou rychlost je obtížné, ale dalo by se říci, že se jedná o věc cviku. Porovnávací algoritmy pro termické senzory musí být schopny roztažení nebo naopak smrštění otisku v této ose kompenzovat a proto je možné říci, že tyto dva otisky jsou ekvivalentní.



Obrázek 5.4: Test termického senzoru. Vlevo otisk sejmutý z razítka, vpravo ze živého prstu.

Posledním senzorem, který jsem chtěla testovat byl E-Field senzor Suprema SFM 3000. Zde jsem ovšem narazila na problém. Snímací plocha je zasazena do rámečku o rozměrech

13x13 mm. Razítko má ovšem délku 17 mm a tak není možné jej přiložit na plochu senzoru tak, aby dostatečná část razítka přiléhala k ploše a bylo tak započato snímání otisku. Vzhledem k podobnosti E-Field a kapacitní technologie předpokládám, že i E-Field senzor by mohl být oklamán za pomoci razítka, nicméně pro otestování tohoto předpokladu bude zapotřebí nechat vyrobit menší razítko.

Obecně lze tedy říci, že pomocí razítka lze oklamat senzory založené na optickém, kapacitním i termickém principu. Je však důležité si před zadáním výroby razítka zjistit rozměry senzorů a tomuto uzpůsobit nejen rozměry gumového otisku, ale podstavce na kterém bude tento otisk upevněn.

5.3 Testování nového senzoru

Princip nově navrženého senzor byl podroben několika testům. V rámci pokusu o oklamání senzoru zde bylo vyzkoušeno razítko testované v předcházející části mé práce. Ze všech testů vyšel tento senzor vítězně, což vzhledem k principu na kterém je založen se dalo očekávat.

Podrobnosti jsou uvedeny v tajné části mé práce.

Kapitola 6

Závěr

V této práci jsem se zabývala testováním živosti u otisků prstů. Po nastudování potřebných podkladů (uvádím je v seznamu použité literatury) jsem se zde pokusila podat ucelený přehled v současnosti známých metod testování živosti. Tento úkol také vyžadoval vysvětlit funkci celého biometrického systému (včetně jeho slabých míst), aby bylo možno názorněji ukázat, proč je testování živosti vlastně tak důležité. Dále bylo nutné pochopit principy jednotlivých typů senzorů, protože tyto senzory samy o sobě představují takové velmi slabé testování živosti. Bez této znalosti by pak bylo obtížné pochopit silné metody testování živosti (konkrétně proč se daná metoda hodí jen pro některé typy senzorů) nebo naopak hledat slabá místa senzorů a tedy i možnosti jejich oklamání. Teprve po uvedení těchto informací jsem mohla přistoupit k samotnému popisu jednotlivých hardwarových i softwarových metod testování živosti u otisků prstů. Uvedla jsem celkový přehled těchto metod a poté jsem se speciálně věnovala softwarové metodě založené na pocení pokožky a hardwarové metodě založené na spektroskopických vlastnostech kůže.

Studium metod testování živosti mne inspirovalo k vytvoření nového senzoru pro snímání otisků prstů, který má v sobě zabudováno testování dvou různých charakteristických vlastností živé lidské tkáně. Pomocí dostupného vybavení jsem pak funkci senzoru ověřila a sestavila program pro demonstraci této metody. Díky neexistenci prototypu senzoru je tento program zatím určen pouze pro offline testování živosti a v současné době vyžaduje asistenci uživatele při určování hranic pro jednu z metod.

Tato práce se tak stává základním stavebním kamenem pro vývoj nového typu senzoru otisků prstů, nicméně k výslednému senzoru vede ještě dlouhá cesta. Nejprve bude zapotřebí zdokonalit použité algoritmy pro zpracování obrazu, aby testování živosti probíhalo automaticky (bez zásahu uživatele). Mimo konstrukci samotného prototypu bude také nutné vypracovat algoritmy pro extrakci markantů a jejich porovnání s uloženou šablonou, aby byl tento prototyp plnohodnotným senzorem a ne jen rozšířením obsahujícím test živosti. Poté bude zapotřebí otestovat funkci tohoto řešení na co nejširším vzorku populace a také testovat co nejpestřejší možnosti ošálení senzoru. Díky tomu bude možné přesněji stanovit hranice pro živost prstů a také potvrdit nebo vyvrátit můj názor (založený na výsledcích dosavadních testů), že tento senzor je se současnými prostředky prakticky nemožné ošálit.

Literatura

[1] Kluz, M.: Liveness testing in biometric systems. Master thesis. Brno, Masaryk University Brno Faculty of Informatics 2005.

[2] Drahanský, M.: Biometrické systémy BIO Studijní opora. Verze 01.2006. Vysoké učení technické v Brně Fakulta informačních technologií. Dokument dostupný na URL https:// www.fit.vutbr.cz/study/courses/BIO/private/BIO_Studijni_opora.pdf (30. prosince 2006).

[3] Hanáček, P.: Bezpečnost informačních systémů. 2006. Vysoké učení technické v Brně Fakulta informačních technologií. Dokument dostupný na URL https://www.fit.vutbr.cz/study/courses/BIS/private/bis.htm (30. prosince 2006).

[4] Zemčík, P.: Zpracování obrazu. 2006. Vysoké učení technické v Brně Fakulta informačních technologií.

[5] Valencia, V. S., Horn, Ch.: Biometric Liveness Testing. Biometrics, 2003, s. 139-149.

[6] Shuckers, S., Abhyankar, A.: Detecting Liveness in Fingerprint Scanners Using Wavelets: Result of the Test Dataset. Biometric Authentication, Springer, 2004, s. 100-110.

[7] Putte, T. van der, Keuning, J.: Biometrical Fingerprint Recognition: Don't get your fingers burned. IFIP TC8/WG8.8 Fourth Working Conference on Smart Card Research and Advanced Applications, s. 289-303, Kluwer Academic Publishers, 2000. Dokument dostupný na URL http://www.keuning.com/biometry/Biometrical_Fingerprint_Recognition.pdf (11. listopadu 2006).

[8] Matsumoto, T., Matsumoto, H., Yamada, K., Hoshino, S.: Impact of Artificial "Gummy" Fingers on Fingerprint Systems. Proceedings of SPIE, Vol. 4677, Optical Security and Counterfeit Deterrence Techniques IV, San Jose, February 2002. s. 275-289. Dokument dostupný na URL http://cryptome.org/gummy.htm (11. listopadu 2006).

[9] Thalheim, L., Krissler, J., Ziegler P.-M.: Body Check, Biometric Access Protection Devices and their Programs Put to the Test in c't magazine. 11/2002. s. 114. Dokument dostupný na URL http://www.heise.de/ct/english/02/11/114/ (11. listopadu 2006).

[10] Derakhshani, R., Parthnasardi, S., Hornak, L., Shuckers, S.: Perspiration for Detecting Liveness in Fingerprint Scanners-Comparison of Different Classifiers. Dokument dostupný na URL http://people.clarkson.edu/∼biosal/research/perspiration.html (29. října 2006).

[11] Parthnasardi, S., Derakhshani, R., Shuckers, S., Hornak, L.: Spoofing Fingerprint Devices. Dokument dostupný na URL http://people.clarkson.edu/∼biosal/research /spoofingfingerprint.html (29. října 2006).

[12] Shuckers, S., Hornak, L., Norman, T., Derakhshani, R., Parthnasardi, S.: Issues for Liveness Detection in Biometrics. West Virginia University. Dokument dostupný na URL http://www.biometrics.org/html/bc2002_sept_program2_bc0130 _DerakhshabiBrief.pdf (30. prosince 2006).

[13] Ennis, M. S. aj.: Multispectral Sensing for High-Performance Fingerprint Biometric Imaging. Lumidigm, Inc. Dokument dostupný na URL http://www.lumidigm.com /PDFs/Multispectral_Fingerprint_Imaging.pdf (29. října 2006).

[14] Rowe, R. K.: A Multispectral Sensor for Fingerprint Spoof Detection. Lumidigm, Inc. Dokument dostupný na URL http://www.lumidigm.com/PDFs/SEN1-13-05e.pdf (29. října 2006).

[15] Havlík, J.: Pulsní oxymetrie. Katedra teorie obvodů FEL ČVUT v Praze. Dokument dostupný na URL http://noel.feld.cvut.cz/vyu/31lt1/Lectures/PulsniOximetrie.pdf (18. listopadu 2006).

[16] Tuč, D.: Review of commercial fingerprints sensors. Semestral project. Brno University of Technology, Faculty of Information Technology 2005.

[17] Lodrová, D.: Textová rešerše - Testování živosti u technologie otisků prstů. Vysoké učení technické v Brně Fakulta informačních technologií 2005.

[18] Atmel Corporation. http://www.atmel.com (11. listopadu 2006).

[19] AuthenTec, Inc. http://www.authentec.com (11. listopadu 2006).

[20] Bergdata Biometrics GmbH. http://www.bergdata.com (11. listopadu 2006).

[21] BMF Corporation. http://www.bm-f.com (11. listopadu 2006).

[22] Elsys Corporation. http://www.elsys.ru/delsy_e.php (30. prosince 2006).

[23] L-1 Identity Solutions, Inc. http://www.l1id.com/ (7. února 2006).

[24] Lumidigm, Inc. http://www.lumidigm.com (11. listopadu 2006).

[25] Optel, Ltd. http://www.optel.pl (11. listopadu 2006).

[26] SecuGen Corporation. http://www.secugen.com (11. listopadu 2006).

[27] Security First Corporation. http://www.securityfirstcorp.com (30. ledna 2007).

[28] Ultra-Scan Corporation. http://www.ultra-scan.com/ (7. února 2006).

[29] Upek, Inc. http://www.upek.com (11. listopadu 2006).

[30] Veridicom International. http://www.veridicom.com (11. listopadu 2007).

[31] Wikipedia. http://www.wikipedia.org/ (11. listopadu 2006).

Slovníček pojmů

Bilirubin. Žlutooranžová látka nacházející se v krvi (žlučové barvivo). Vzniká štěpením jedné ze složek hemoglobinu.

BioSAL. Biomedical Signal Analysis Laboratory na Clarkson University a West Virginia University v USA. Laboratoř se zaměřením na zpracování a interpretaci signálů generovaných lidským tělem.

CCD. Charge-Coupled Device – zařízení pro pořizování obrazu umístěné nejčastěji ve videokamerách či fotoaparátech. Oproti CMOS se jedná o starší technologii, která nemůže být jednočipová.

CMOS. Complementary Metal Oxide Semiconductor – zařízení pro pořizování obrazu podobné CCD technologii. Oproti ní má však horší kvalitu obrazu.

Daktyloskopie. Nauka o papilárních liniích. V kriminalistice se používá pro identifikaci osob.

DELSY. Dactyloscopic Electronic Systems – divize ruské společnosti ELSYS Corp. zabývající se daktyloskopickými systémy.

Dielektrikum. Jedná se o izolant, který má schopnost být polarizován.

DoS. Denial of Service – útok způsobující nedostupnost služby.

Důvěrnost dat. K datům mají přístup pouze autorizované subjekty.

EER. Equal Error Rate – jedná se o průsečík křivek znázorňující chybné přijetí a chybné odmítnutí uživatele. Pokud na tuto hodnotu nastavíme rozhodovací práh, pak bude chybně přijato statisticky stejné množství osob jako chybně odmítnuto.

Hemoglobin. Červené krevní barvivo obsažené v červených krvinkách. Distribuuje po těle kyslík a odvádí oxid uhličitý.

Identifikace. Porovnání sejmutého vzorku (např. otisku prstu) se všemi vzorky v databázi (porovnání 1:N). Oproti verifikaci tedy uživatel nezadává svůj login ani nijak jinak nezadává svou identitu.

Infračervené záření. Elektromagnetické záření s vlnovou délkou 760nm - 1mm, tedy vlnovou délkou větší než viditelné světlo.

Integrita dat. Data nemohou být neoprávněně změněna.

Jednobitový obraz. Barva každého pixelu je určena pouze jedním bitem, může tedy nabývat pouze hodnot 1 a 0 reprezentující černou a bílou barvu.

Kolagen. Bílkovina, která je základní stavební hmotou pojivových tkání. Ve formě kolagenových vláken je složkou mezibuněčné hmoty.

Latentní otisk prstu. Jedná se o otisk zanechaný při doteku na povrchu předmětu. Dobře vidět je to například na sklenici.

LED. Light-Emitting Diode – světlovyzařující dioda.

Markant. Významný bod, změna papilární linie. Může se jednat o rozdvojení nebo ukončení linie, či některé jejich poddruhy.

Melanin. Pigment podmiňující barvu pokožky.

Multimodální biometrický systém. Nepoužívá pouze jeden příznak jedné biometrické vlastnosti, ale buď více vlastností nebo více příznaků jedné vlastnosti. Například otisk prstu a duhovka oka nebo statická a dynamická charakteristika podpisu.

Osmibitový (šedý) obraz. Barva každého pixelu může nabývat hodnot 0 až 255, což představuje 256 úrovní šedi.

PlayDoh. Modelovací hmota podobná naší plastelíně.

Pulsní oxymetr. Běžný lékařský přístroj měřící tepovou frekvenci a nasycenost krve kyslíkem. Nejčastěji se měření provádí na prstu.

Senzor. Zařízení konvertující jev (fyzikální, chemický, ...) na elektrický signál.

Ultrazvuk. Zvuk s frekvencí vyšší než 20 kHz. Lidské ucho jej nedokáže zachytit, vnímají jej však například delfíni.

Verifikace. Porovnání vstupního vzorku (např. otisk prstu) s odpovídajícím vzorkem v databázi (1:1). Uživatel například zadá svůj login a nechá si sejmout otisk prstu, který je poté porovnán s otiskem patřícím k zadanému loginu.

Dodatek A

Tabulka metod testování živosti

Vlastnost	**SW/HW**	**senzor**[1]	**výhody**	**nevýhody**
elasticita pokožky	SW	kapacitní	SW metoda	
elektrické char.	HW	optický		lze snadno obelstít
barva pokožky	SW/HW	optický	SW metoda	špinavé prsty
spektrální char.	HW	optický		
nasycenost kyslíkem	HW	optický	běžná technologie	5 sekund
DNA	HW		pak by nebyly otisky zapotřebí	
puls	HW	optický	běžná technologie	5 sekund
teplota	HW			studené ruce
pot	SW	kapacitní	SW metoda	suché, vlhké prsty
odlučování kůže			dosud nenavržena implementace	
ovlivnitelné reakce	HW			uhádnutí reakce
neovlivnitelné reakce	HW			

Tabulka A.1: Tabulka vlastností využitelných pro testování živosti.

[1]Příklad typu senzoru, u kterého by může být tato metoda testování živosti použita.

Dodatek B

Tabulka senzorů pro otisky prstů

Typ senzoru	výrobce [1]	t. ž.[2]	výhody	nevýhody
ultrazvukový	Optel, Ltd.	ano	implicitní test živosti, bezdotykový senzor	složitější algoritmus, vyšší cena
optický (1 druh LED)	SecuGen Corporation	ne	nízká cena	snadno oklamatelný, latentní otisky prstů
optický (multisp.)	Lumidigm, Inc.	ano	implicitní test živosti	latentní otisky prstů
elektrooptický	Elsys Corp.	ne	suché i mokré prsty, vysoké rozlišení	vyšší citlivost na fyzické poškození a znečištění
kapacitní	Veridicom International	ne	SW implementace testování živosti (pot)	snadno oklamatelný, suché a mokré prsty
tlakový	BMF Corporation	ne	mokré i suché prsty, nízká spotřeba elektřiny	jednobitový obraz
termický	Bergdata Biometrics	ne	suché i mokré prsty, bez latentních otisků	uživatelsky nepřívětivý, vyšší spotřeba elektřiny
E-Field	AuthenTec, Inc.	ne		nízké rozlišení, menší plocha senzoru

Tabulka B.1: Tabulka senzorů pro otisky prstů.

[1] Příklad výrobce senzoru.

[2] Testování živosti - zda senzor již ze svého principu obsahuje některou z hardwarových metod testování živosti.

Dodatek C

Tabulka metod oklamání senzorů otisků prstů

Metoda/typ senzoru:	Kapacitní	Optický	Elektooptický	Termický	Nový[4]
Dýchnutí	A[1]	tN[3]	tN	tN	tN
Sáček s vodou	A	tN	tN	tN	tN
Grafitový prášek	A	tA[2]	tN	tN	tN
Tisk/foto	tN	A	tN	tN	tN
Razítko	A	A	tA	A	tN
Silikonový prst	A	A	tA	A	tN
Želatinový prst	A	A	A	tA	tN
Plastelínový prst	A	A	A	tA	tN
Amputovaný prst	A	A	A	tA	tN

Tabulka C.1: Tabulka metod oklamání senzorů otisků prstů.

Ne všechny typy senzorů jsou v tabulce uvedeny. Nenašla jsem žádnou práci, kde by byl testován tlakový senzor, obecně však předpokládám, že vzhledem k principu na kterém je založen jej půjde oklamat stejnými metodami jako elektrooptický senzor. Stejná situace panuje v případě E-Field senzoru, který by měl být oklamatelný stejnými způsoby jako kapacitní senzor (kvůli podobnosti principů na kterých jsou tyto senzory založeny).

Posledním typem senzoru, který zde není uveden je ultrazvukový senzor, který také není příliš rozšířen a nemám informace, že by byl testován. Jeho princip se však nepodobá žádnému z výše uvedených senzorů a proto si netroufnu přesně odhadnout, které metody by jej mohly ošálit. Jisté je pouze to, že ultrazvukový senzor v bezdotykové verzi nebude možné oklamat žádnou z metod využívajících latentních otisků prstů, protože v tomto případě není žádná plocha senzoru, kde by bylo možné otisk zanechat.

[1] Ano - je vyzkoušeno, že tento senzor lze danou metodou oklamat.

[2] teoreticky Ano - vzhledem k principu tohoto senzoru je pravděpodobné, že by senzor mohl být danou metodou oklamán. Nebylo to ovšem (pokud je mi známo) doposud otestováno.

[3] teoreticky Ne - vzhledem k principu tohoto senzoru není (dle mého názoru) možné aby byl danou metodou oklamán.

[4] Nový typ senzoru, který jsem navrhla.