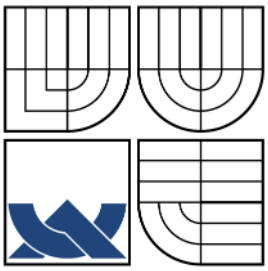
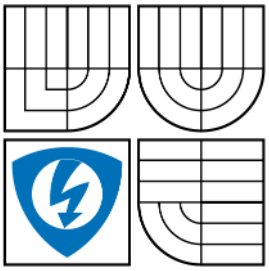


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

BIOMETRICKÉ AUTENTIZAČNÍ METODY

BIOMETRICS AUTHENTICATION METHODS

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE — Jakub Flídr
AUTHOR

VEDOUCÍ PRÁCE — ING. JIŘÍ SOBOTKA
SUPERVISOR

BRNO 2009

VYSOKÉ UČENÍ
TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Student:	Jakub Flídr	***ID:***	73047
Ročník:	3	***Akademický rok:***	2008/2009

NÁZEV TÉMATU:

Biometrické autentizační metody

POKYNY PRO VYPRACOVÁNÍ:

Proveďte rozbor a popis metod autentizace žadatele o přístup do systému pomocí biometrických údajů. Návrhněte systém bezpečné autentizace žadatele pomocí jednoho nebo více biometrických metod. Zároveň otestujte odolnost základních biometrických metod proti nesprávné autentizaci.

DOPORUČENÁ LITERATURA:

[1] Burda, K. Bezpečnost informačních systémů . skripta FEKT, Brno 2005
[2] Ščurek, R. Biometrické metody identifikace osob v bezpečnostní praxi. skripta VŠBTU, Ostrava 2008
[3] Matyáš V. Principy a technické aspekty autentizace. Data Security Management (DSM), roč. 2007, č. 1, ISSN 1211-8737

Termín zadání:	9.2.2009	***Termín odevzdání:***	2.6.2009

Vedoucí práce: Ing. Jiří Sobotka

prof. Ing. Kamil Vrba, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Abstrakt

První část bakalářské práce zahrnuje popis základních pojmů souvisejících s biometrií. Dále jsou zde popsány a rozděleny jednotlivé biometrické metody. Je popsán jejich princip a přibližné výkonnostní parametry. V druhé praktické části je otestována bezpečnost tří rozdílných biometrických metod. Jsou popsány jejich výkonnostní parametry a vlastnosti, uveden princip pokusu o oklamání metody a jeho úspěšnost. Výsledky jsou vyhodnoceny a je uvedeno doporučení pro konkrétní využití metody. Poslední část zhodnocuje získané zkušenosti při návrhu bezpečného autentizačního systému.

Klíčová slova:

Biometrie, biometrický údaj, autentizace, přístupový systém, bezpečnost.

Abstract

The first part of this bachelor thesis includes description of elementary terms in biometrics. Different biometric methods are also described and classified there. It describes the principles of the methods and their approximate performance characteristics. In the second part, practical safety of three different biometric methods is tested. Their performance characteristics and properties are described and also the principle of attempting to mislead the methods and its success is demonstrated. The results are evaluated and recommendations for practical use of the methods is given there. The last part of the thesis evaluates the experience gained in the design of a safe authentication system.

Key words:

Biometric, biometric data, authencitation, access system, security.

Bibliografická citace

FLÍDR, J. Biometrické autentizační metody. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2009. 50 s. Vedoucí bakalářské práce Ing. Jiří Sobotka.

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma Biometrické autentizační metody jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdroj, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením tohoto projektu jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č140/1961 Sb.

V Brně dne ……...

……..…….

podpis autora

Poděkování

Děkuji vedoucímu bakalářské práce ing. Jiřímu Sobotkovi, za velmi užitečnou metodickou pomoc a cenné rady při zpracování práce. A své přítelkyni za pomoc při testech biometrických senzorů.

1 Úvod

Cílem této práce je podat přehled o nejpoužívanějších biometrických metodách využívaných při autentizaci žadatele o přístup do systému. U každé metody se pokusím vysvětlit její princip, implementaci a přibližné parametry. Dále budou otestovány metody autentizace pomocí duhovky, dynamiky stisku kláves a otisku prstů. Poslední část obsahuje návrh bezpečné autentizace pomocí biometrických metod.

Lidé se odpradávna identifikovali pomocí biometrických metod, především podle vzhledu obličeje. Implementovaní biometrických metod do automatických autentizačních systémů umožnil rozvoj počítačové techniky, která nyní nabízí dostatečný výkon i nízkou cenu. Potřebné technologie jsou rychle vyvíjeny a zdokonalovány především díky rozsáhlé podpoře vlád různých zemí. Ty poskytují nejenom rozsáhlé finanční prostředky pro výzkum, ale zároveň největšího odběratele těchto systémů. To láká další soukromé investory do této oblasti a umožňuje to zdokonalování nejen stávajících systémů, ale i objevení nových metod biometrické autentizace. Výhodou těchto systémů je neúplatnost, rychlost autentizace, cena a jedinečnost lidského těla. Uživatel si nemusí nic pamatovat jako u autentizace pomocí hesla nebo vlastnit předmět jako u autentizace předmětem.

2 Základní pojmy

Biometrie –skládá se z řeckých slov "bios", živý, a "metria", měření. Je to tedy vědní obor zkoumající biologické organismy a jejich fyziologické a anatomické parametry a behaviorální vlastnosti.

Biometrika – věnuje se studiu metod sloužících k rozpoznávání člověka na základě jeho biologických parametrů nebo behaviorálních vlastností.

Autentizace – proces, při kterém se ověřuje totožnost uživatele. Výsledkem procesu je pak povolení nebo zamítnutí přístupu do systému.

Identifikace – při tomto procesu systém sejme biometrická data neznámého uživatele, která následně porovná s celou databází. Jedná se tedy o princip „one-to-many".

Verifikace - při tomto procesu uživatel nejdříve zadá systému svoji totožnost (např.: pomocí karty nebo hesla), následně systém sejme biometrická data, která porovná s dříve uloženým etalonem. Jedná se tedy o princip „one-to-one".

2.1 Metody autentizace

Při autentizaci uživatele do systému se využívají tři odlišné podoby:

Autentizace heslem – je nejvíce využívanou možností pro přístup osob do systému. Je to dáno především jednoduchou realizací pomocí softwaru a z toho vyplývající nízkou cenou. Při volbě nebo přidělení hesla se musí pro zvýšení bezpečnosti dodržovat několik zásad. Heslo by mělo obsahovat velká i malá písmena, číslovky, nejlépe by se mělo jednat o shluk nespojitých písmen a číslovek bez slovního významu, popřípadě bez bližšího vztahu k uživateli. Heslo by se mělo v určitých intervalech obměňovat, zároveň by měla být distribuce hesla od administrátora k uživateli dostatečně zabezpečená. I přes to může dojít s pomocí speciálních programů k dešifrování hesla, popřípadě k vysledování neoprávněnou osobou. Velkou roli má také kázeň uživatele, který by neměl mít heslo

nikde napsané nebo ho dokonce vyzradit třetí osobě. Často dochází také k zapomenutí hesla.

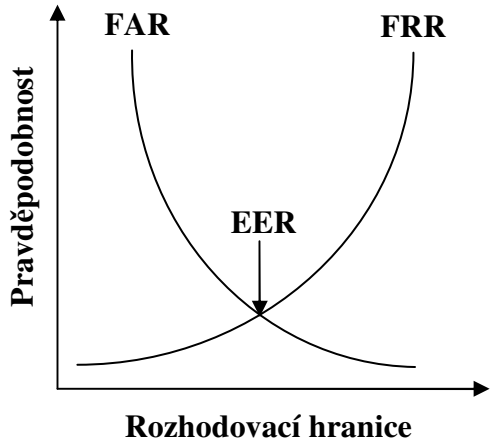
Autentizace předmětem – princip autentizace uživatele spočívá ve vlastnictví určitého předmětu, jenž se obecně nazývá „token“. Mezi jeho hlavní vlastnosti by měla patřit obtížná padělatelnost. Mezi jeho výhody patří žádoucí přenositelnost a vyšší bezpečnost než u autentizace pomocí hesla. Nevýhodou je pak možnost odcizení, a proto je zde žádoucí doplnění této autentizace o heslo nebo biometrickou autentizaci.

Biometrická autentizace – využívá jedinečných tělesných znaků jedince k jeho identifikování. Hlavní výhodou je příznivý poměr bezpečnost/cena, dále pak rychlost a praktičnost, jelikož nelze nic zapomenout ani ztratit. Pokud použijeme vhodné lidské charakteristické znaky, je výhodou i stálost. Bezpečnost můžeme dále zvýšit kombinací několika metod, jež jsou v další části popsány. I tuto metodu autentizace je možno napadnout, ale v současnosti je to nejefektivnější způsob zabezpečení v automatických systémech kontroly vstupů, a nachází proto uplatnění ve všech sektorech a stupních zabezpečení, především pak v docházkových systémech, při celních kontrolách, na letištích, v přístupových systémech bank, na výzkumných pracovištích, ve vojenských objektech a dalších klíčových místech s vysokým stupněm zabezpečení. Ve vývoji a v experimentálním využití jsou pak nově systémy k vyhledávání potencionálních teroristů, založených na identifikaci osob ve skupině lidí na základě výrazu obličeje a chování. Nebo na základě promítání sledu obrázků o délce cca 30 vteřin s různou tématikou (např.: fotografie Usamy Bin Ladina, teroristických činů, atd.) a následného vyhodnocení reakce dotyčného jedince. Tyto systémy jsou experimentálně zkoušeny především ve státech jako Izrael, Velká Británie a Německo.

2.2 Měření výkonnosti biometrických systémů

FAR (**F**alse **A**cceptation **R**ate) – neboli koeficient bezpečnosti. Vyjadřuje pravděpodobnost, že systém neoprávněně povolí přístup identifikované osobě. Jde o kritickou chybu, jelikož systém přijme osobu, jež za normálních podmínek nemá přístup.

FRR (**F**alse **R**ejection **R**ate) **–** neboli koeficient “komfortu“. Vyjadřuje pravděpodobnost, že systém zamítne oprávněné osobě přístup. Tento koeficient tedy nemá vliv na bezpečnost systému, pouze donutí uživatele k opakované identifikaci, což snižuje uživatelský komfort.



Obr. 1: Závislost FAR a FRR na rozhodovací hranici. [1]

EER (**E**qual **E**rror **R**ate) – neboli křížový koeficient. Udává ideální rozložení koeficientů FAR a FRR. Jeho hodnota určuje při jakém nastavení se budou koeficienty FAR a FRR sobě rovnat. Z diagramu (viz obr. 1) je patrné, že pokud nastavíme vyšší zabezpečení (FAR) pak koeficient FRR prudce vzroste, a naopak.

Vícenásobná biometrická autentizace

Jedná se o kombinaci minimálně dvou biometrických metod v jednom systému k identifikaci. Nejčastěji se v praxi využívá identifikace otisků prstů doplněná o další biometrickou metodu v závislosti na požadovaném stupni zabezpečení. Evropská unie například zavádí do cestovních pasů (nově E-pas) elektronický čip s uloženým otiskem prstů a digitální fotografií. Ty jsou nově zaváděny i v České republice. Tyto pasy vyžadují totiž USA k povolení vstupu pro naše občany bez vystavení víza.

U vícenásobné biometrické autentizace je výsledná pravděpodobnost přijetí neoprávněné osoby (FARc) rovna součinu jednotlivých pravděpodobností FARx. .

$$FARc=FAR_1 \cdot FAR_2 \cdot \ldots \cdot FAR_N. \quad (1)\ [2]$$

FRRc neboli výsledná pravděpodobnost odmítnutí oprávněného uživatele je pak rovna součtu jednotlivých pravděpodobností FRRx.

$$FRRc= FRR_1+FRR_2+\ldots+FRR_N. \quad (2)\ [2]$$

2.3 Biometrický etalon

K tomu, abychom mohli uživatele identifikovat nebo verifikovat, je potřeba nejdříve získat referenční vzor jeho unikátních biometrických znaků. Tomuto referenčnímu vzoru se v odborné praxi říká biometrický etalon. Ten se získá opakovaným měřením při zápisu uživatele do systému. Toto měření bývá obvykle prováděno alespoň třikrát, z důvodu získání reprezentativního vzorku a potlačení náhodných jevů. Tyto získané vzory se obvykle zprůměrují. Referenční vzor je potřeba získat v dostatečné kvalitě, jelikož bude při následném používání sloužit k porovnávání se vzorem získaným ze senzoru, nekvalitní vzor by mohl mít za následek chybné odmítnutí žadatele o přístup. Při využívání verifikace je tomuto etalonu přidělen identifikátor, který slouží k jeho opětovnému nalezení v databázi při verifikačním procesu.

Etalon lze uložit v:

1. Tokenu – uživatel nosí svůj etalon nejčastěji na čipové kartě. Není tedy nutná žádná centrální databáze. Nevýhodou je vyšší cena i složitost systému.

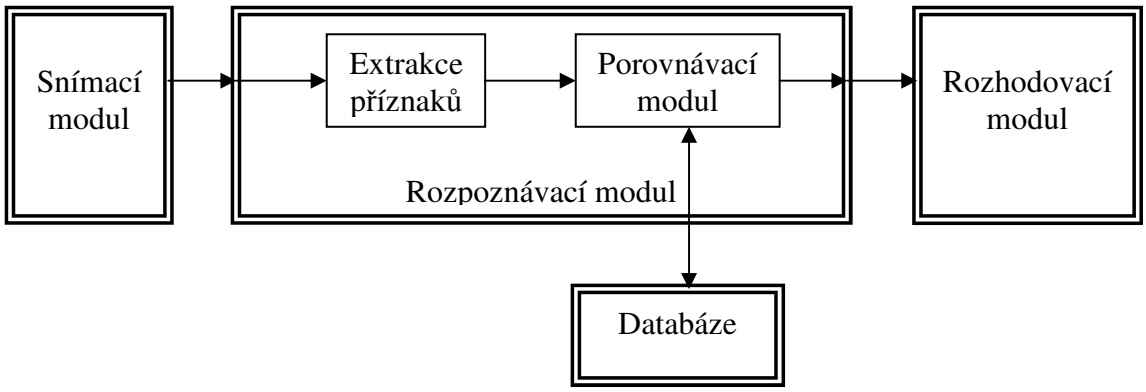
2. Biometrickém čtecím zařízení – databáze s etalony je uložena přímo v biometrcikém čtecím zařízení, díky tomu je proces identifikace rychlý a naprosto nezávislý na okolí.

3. Centrální databázi – etalon je uložen v centrální databázi, což snižuje cenu, ale klade vyšší nároky na spolehlivost a bezpečnost sítě. Zároveň tento způsob umožňuje managementu snadný přehled o oprávněných i neoprávněných identifikacích.

4. Kombinace předchozích možností – tento způsob eliminuje dílčí nevýhody předchozích možností a zaručuje funkčnost systému za všech okolností při vynaložení vyšších výdajů.

2.4 Princip činnosti biometrických systémů

Tyto systémy mají přinést vyšší stupeň zabezpečení, který ale nedosahuje 100% bezpečnosti. Člověk je živý tvor a během života se mění, na což současné biometrické systémy nedokáží reagovat.



Obr. 2**:** Princip činnosti biometrických identifikačních systémů.

Snímací modul – snímá biometrická data uživatele
Rozpoznávací modul *– modul extrakce příznaků* – extrahuje příznaky ze snímaných dat.
– porovnávací modul – porovnává extrahované příznaky s etalonem uloženým v databázi.
Databáze – slouží k uložení biometrických etalonů.
Rozhodovací modul – na základě získaných dat rozhodne o shodě nebo neshodě sejmutých příznaků a etalonu.

Biometrické systémy pracují ve dvou režimech:

Registrační režim – neboli prvotní přístup nového uživatele do biometrického systému, kdy se získává etalon jeho unikátních biometrických vlastností, jenž se uloží do databáze pod určitým ID nebo jménem uživatele, které slouží k jeho pozdější autentizaci.
Autentizační režim – slouží k identifikaci uživatele na základě porovnání nově sejmutých dat ze senzoru s etalonem uloženým v databázi a jejich vyhodnocení.

2.5 Rozděleni biometrických metod

Biometrické metody lze rozdělit do dvou základních skupin:
Biologické metody – identifikují jedince na základě unikátních fyziologických a anatomických parametrů lidského těla.
Behaviorální metody – identifikují jedince na základě jeho unikátních vlastností. Ty jsou dány jednak fyzickými parametry, které člověk získává na základě DNA (pouze jednovaječná dvojčata ji mají naprosto shodnou) a také získanými zkušenostmi během života. Tyto jedinečné vlastnosti nelze napodobit. Nevýhodou je, že se mění poměrně rychle v čase.

3 Biometrické metody

V následujícím textu jsou popsány vybrané biometrické autentizační metody. Mimo tyto existují i další metody založené na identifikaci podle chůze, výrazu tváře a metod využívaných především ve forenzní sféře: identifikace podle plantogramu, parametrů zubů, uchopení a držení zbraně, atd.

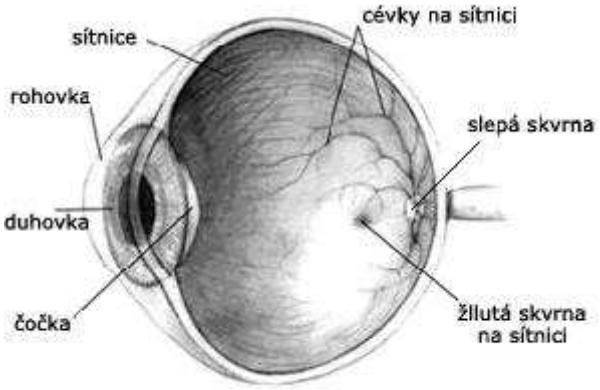
3.1 Biologické metody

3.1.1 Sítnice oka

Tato metoda využívá k identifikaci světločivný systém oka zvaný sítnice. Je to nejvnitřnější vrstva oční koule a pokrývá zadní dvě třetiny její vnitřní plochy s výjimkou místa, kde vychází z oční koule zrakový nerv. Toto místo se nazývá slepá skvrna. Sítnici tvoří receptorové buňky (čípky a tyčinky) pro vnímání světla. Tato technika ale využívá struktury cév vyživujících receptory.

K snímání obrazu sítnice se využívá infračervený zdroj o nízké intenzitě a optoelektronický systém, který zachytí strukturu sítnice v okolí slepé skvrny, nikoliv celou sítnici. Slepá skvrna tedy slouží jako referenční bod. Aby mohl být obraz sejmut, musí uživatel přistoupit ke snímači na velmi malou vzdálenost (2–3cm) a po dobu 1,5–4s se dívat do přesně vymezeného prostoru, což může být pro některé osoby velmi nepříjemné. Při procesu snímání nesmí mít uživatel brýle ani kontaktní čočky. Další nevýhodou je, že většina přístrojů se uchycuje na stěnu, což pro osoby s nevhodnou výškou snižuje uživatelský komfort. Naskenovaný vzorek je poté převeden do podoby 40 bitového čísla.

Přes nespornou přesnost (viz. tab. 1) a téměř nemožnou napodobitelnost je tato metoda v důsledku nízkého komfortu pro uživatele omezena na oblasti nejvyššího stupně zabezpečení a to i v důsledku vysoké ceny.



Obr. 3: Průřez lidského oka. [3]

Tab. 1: Parametry biometrie sítnice oka. [4]

FRR	< 1,0 [%]
FAR	0,0001–0,00001 [%]
rychlost verifikace	0,2 – 1 [s]
míra spolehlivosti	vysoká

3.1.2 Duhovka

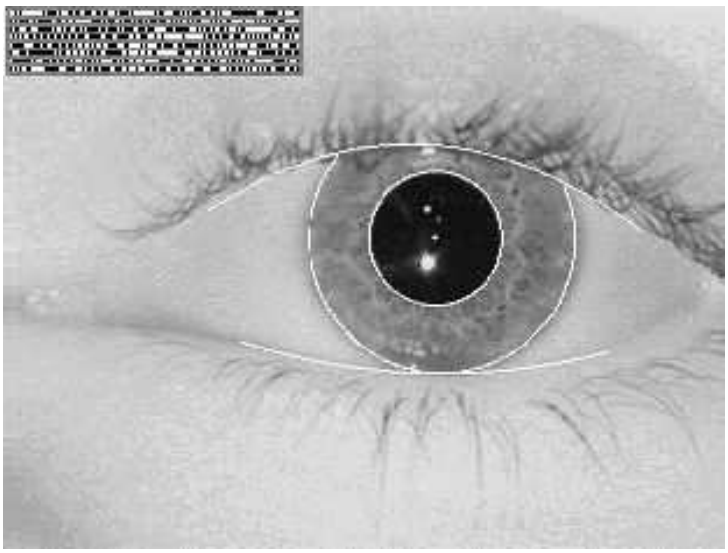
Duhovka je pigmentovaná vnitřní struktura oka obklopující zornici. Oční duhovka je u každého jedince unikátní. Liší se i u jednovaječných dvojčat, dokonce má i každý člověk odlišnou pravou a levou duhovku. Zatímco existuje 60 odlišných forem otisků, tedy markantů, jež mohou být kombinovány na jednom otisku prstu, počet různých forem vzorů duhovky je vyšší než 400. To z ní dělá matematicky nejoriginálnější část těla. Tyto

vzory se vytvářejí v období nitroděložního vývoje (od třetího do osmého měsíce) a nejsou dědičné jako barva a struktura. Duhovka je v čase absolutně neměnná, což z ní dělá nejlepší identifikační metodu.

V roce 1994 si John Daugman nechal patentovat první algoritmus pro identifikaci podle obrazu oční duhovky, který je v současnosti základem většiny systémů tohoto typu. Skutečnost, že tento algoritmus je patentován, navyšuje cenu těchto systémů (např.: docházkový systém pro malou firmu vyjde cca na 150 tis. Kč).

Ke snímání oční duhovky se využívá CCD kamera s vysokým rozlišením, popřípadě doplněná o decentní infračervené osvětlení (750–1000nm) snižující odrazy okolí od rohovky. Při identifikaci je nutná aktivní účast žadatele o přístup. Systém odhalí i brýle či kontaktní čočky, které správné identifikaci nezabrání, stejně tak neovlivňuje spolehlivost ani většina současných očních operací (včetně transplantace rohovky). Identifikace probíhá ze vzdálenosti od 7,6cm do 1m podle použitého přístroje a vyžaduje, aby se žadatel o přístup díval do jednoho konkrétního bodu po dobu 2–3 sekund, během nichž je vytvořena monochromatická fotografie. Následně biometrický systém lokalizuje vnitřní a vnější okraj duhovky a využije několik jasně viditelných charakteristik (např.: pigmentové skvrny, pigmentové záhyby, radiální rýhy, krypty), z nichž sestaví mapu duhovky. Její velikost je 256–512B, což například konkrétní aplikaci IrisCode^{TM} umožňuje porovnat mapu o velikosti 512B s 500 000 jiných map za vteřinu [5].

Při registrování uživatele se vytvoří několik fotografií duhovky (2–4) , aby se minimalizovalo riziko nesprávného vyložení odrazů jako specifických složek duhovky a šablona byla naprosto konzistentní s reálnou skutečností. Následně se uloží pod specifický etalon, kterému se nejvíce podobá, z důvodu urychlení identifikace v rozsáhlých databázích.



Obr. 4: Lokalizace duhovky a její piktografické znázornění. [6]

Využívá se v docházkových systémech, zónách s velmi vysokými nároky na bezpečnost, komerčních organizacích všeho druhu, přístupových systémech, identifikačních systémech (vstup na hranicích do SAE od roku 2001, Liga arabských států od roku 2008, některá vězení v USA).

Tab. 2: Parametry biometrie duhovky. [7]

FRR	0,00066 [%]
FAR	0,00078 [%]
rychlost verifikace	2 [s]
míra spolehlivosti	vysoká

3.1.3 Verifikace pomocí povrchové topografie rohovky

Metodu vynalezl Maria Jongsma a Johnny Brabander v roce 2004. Technologie využívá infračervené světlo malého výkonu vyzařované LED diodou. Ta je zaměřená na střed zornice. Světlo se odráží od rohovky a podle jeho intenzity oko reaguje. Tato reakce je u každého jedince v závislosti na čase a rozšíření zornice jiná. Tato reakce je snímána kamerou a následně porovnána s údaji v databázi.

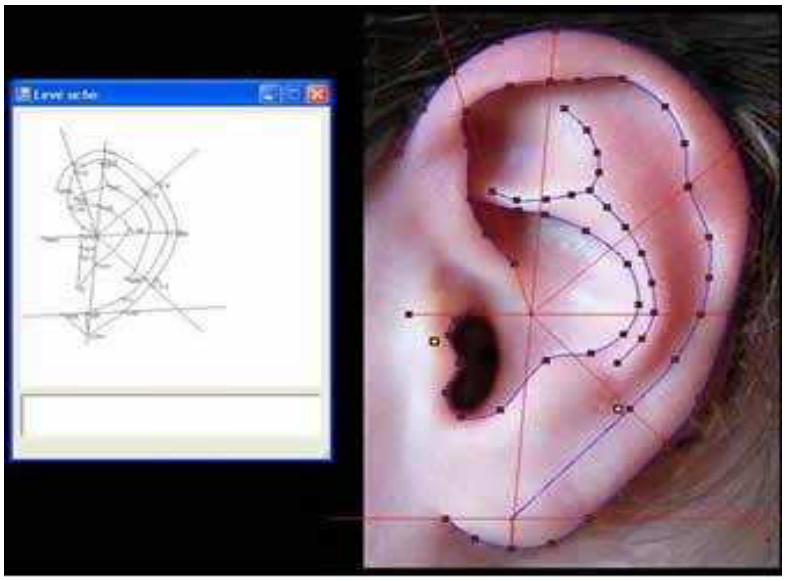
3.1.4 Biometrie ušního boltce

Tato metoda je obdobou identifikace dle obličeje, s podrobnějším zkoumáním. Existují čtyři metody identifikace podle ušního boltce:

1. *Podle morfometrických vztahů* – zkoumá se geometrie ušního boltce a to buď ve 2D nebo 3D formě. Využívá se toho, že každý jedinec má unikátní boltec. U jedince se liší i pravý boltec od levého boltce. Mohou si být pouze podobné. K snímání ze vzdálenosti 0,5–1m, slouží speciální optické zařízení. Ze snímku jsou zjištěny individuální morfometrické vztahy (např.: rozměry, tvary, položení významných bodů, křivky, apod.) a následně porovnány s databází. Při identifikaci je nutná spolupráce uživatele, jelikož vlasy mohou překrývat boltec a znemožnit tak identifikaci.
2. *Podle termografu ušního boltce* – využívá se rozdílné teploty boltce, jež se pohybuje v rozmezí 30–37,2 °C při normálních klimatických podmínkách. Pomocí termokamery se získá snímek boltce a ten se následně porovná s databází.
3. *Podle otisku struktur ušního boltce* – obdoba technologie otisků prstů. Vzhledem k obtížnému snímání a uživatelskému odporu k této metodě se využívá jen ve forenzní oblasti jako doplňková identifikační metoda. Existují čtyři základní tvary boltce: tvar oválný, kulatý, obdélníkovitý a trojúhelníkovitý. Tyto čtyři základní tvary slouží jako základní dělení pro další zpracovaní.
4. *Podle ozvěny vracené kanálkem* – Uživatel přiloží ucho k reproduktoru, který vydává posloupnost klapavých zvuků. Ty se odráží od stěn zvukovodu. Přijímač následně analyzuje příchozí ozvěny, jelikož intenzita pohlcení zvuku je u každého jedince individuální. Metoda by mohla najít uplatnění v ochraně dat mobilních telefonů před zneužitím, popřípadě jako doplňková verifikace přes mobilní telefon

Tab. 3: Parametry biometrie ušního boltce. [8]

FRR	< 1 [%]
FAR	0,1 [%]
rychlost verifikace	3 [s]
míra spolehlivosti	střední



Obr. 5: Biometrické měření parametrů ušního boltce. [9]

3.1.5 Geometrie obličeje

Identifikace podle tváře je nejpřirozenější metodou pro člověka. Proto není překvapením, že patří mezi nejvíce zkoumané metody.

Dostupné systémy se dělí na statické řízené, kdy dochází k vědomé identifikaci a na dynamické neřízené, kdy dochází k identifikaci osoby v davu lidí. Statické řízené systémy mají ulehčenou identifikaci, jelikož se uživatel dívá přímo do snímací kamery, tedy pod nulovým úhlem, dále může být přizpůsobeno osvětlení a barva pozadí. Využívají se pro přístupové a docházkové systémy. U dynamických neřízených systémů se negativně projevuje osvětlení a pozorovací úhel, což mívá často za následek nerozpoznání důležitých rysů obličeje. Těmto systémům je věnována větší pozornost ze strany vlád různých zemí, jež bojují proti terorismu a vynakládají tak na další vývoj značné finanční prostředky. I přes svou nedokonalost se začínají využívat na letištích, vlakových nádražích, bankách a dalších důležitých místech.

V první fázi musí systém lokalizovat ve snímku obličej pomocí barvy kůže. Metoda je založena na předpokladu, že lidská kůže nabývá pouze určitých hodnot barevného spektra. Velmi důležité je vhodné nastavení modelu barvy kůže a jeho přesnosti. Nevýhoda spočívá v chybném vyložení shodné barvy v pozadí jako součást obličeje.

Pro detekci úst se využívá Fischerova lineární diskriminace. Ta vychází z předpokladu, že barevné spektrum rtů je složeno z vysokých hodnot červené a velmi nízkých hodnot modré barvy modelu RGB [10]. Nevýhodou je, že barevné spektrum se může výrazně lišit především u žen, jež používají rtěnku nestandardních barev jako je černá, fialová, atd. Tato skutečnost zabraňuje úspěšné identifikaci. Další problém může nastat, pokud se vyskytuje v pozadí snímku objekt červené barvy, jež může být milně vyhodnocen jako část rtů. Tomu se zabraňuje využitím jistých metod, které mají za úkol potlačit vše mimo obličej identifikované osoby. Další problém nastává, pokud se osoba červená. Tento jev se eliminuje pomocí Gaborovy vlnkové transformace ve vertikálním směru. Díky ní se budou rty jevit jako ostrý přechod barev a budou snadno identifikovatelné.

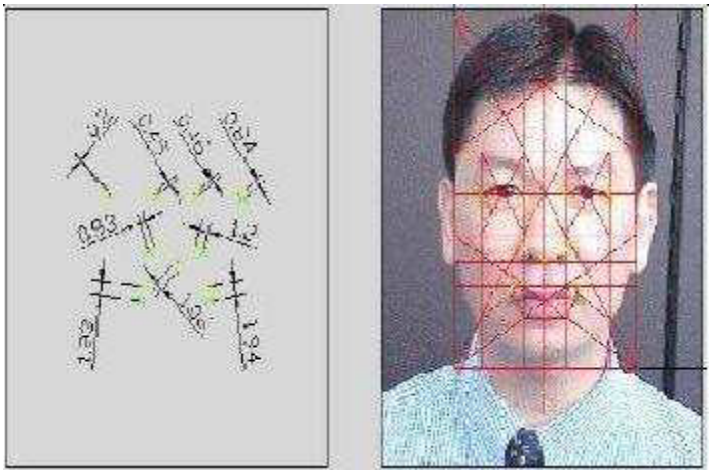
Detekce očí probíhá na obdobném principu jako detekce úst. Využívá se skutečnosti, že barva zornice i bělma očí je u většiny lidí stejná. Záměně se zuby, jež mají obdobné barevné spektrum jako oční bělmo, se zamezí pomocí již známé polohy rtů. Pokud se nepodaří lokalizovat oči, je téměř nemožné identifikovat uživatele.

Po zjištění pozice rtů a očí systém zkontroluje, zda se nacházejí vůči sobě v logických vzdálenostech, a dále pokračuje zjištěním pozic, jež jsou pro jednotlivé systémy rozdílné (např.: obočí, umístění a tvar nosu, uší, atd.) Výhodou je, že se neukládají přesné pozice v obličeji, ale pouze vzdálenosti mezi vybranými body, popřípadě jejich zakřivení (např.: vzdálenost očí, vzdálenost oka od rtů, úhel mezi špičkou nosu a jedním okem).

Velkou slabinou většiny systémů založených na identifikaci obličeje je velká závislost na poloze kamerových systémů a světelných poměrech, dále pak malá spolehlivost daná také závislostí na účesu popřípadě oholení. Systém není samozřejmě ani schopen rozlišit identická dvojčata. Výhodou je pak nízká technologická náročnost pro přístupové systémy, a tedy i cena. Postačí i obyčejná webová kamera (např.: Toshiba Face Recognition). Velikost uloženého etalonu je rovněž nízká, řádově několik bajtů, což zvyšuje rychlost vyhledávání.

Tab. 4: Parametry biometrie geometrie obličeje. [11]

FRR	< 1 [%]
FAR	0,1 [%]
rychlost verifikace	3 [s]
míra spolehlivosti	střední



Obr. 6: Extrahování vybraných vzdáleností lidského obličeje. [12]

3.1.6 Termograf obličeje

Metoda předpokládá unikátní tepelné vyzařování žilního systému a okolních tkání v obličejové části každého jedince. Termogram se získá pomocí infračervené kamery, jež nevyžaduje aktivní účast žadatele o přístup. Jedná se o velmi novou metodu, jež není vědecky ověřená. Výhodou je především unikátnost termogramu a jeho stálost. Nevýhodou je jistá závislost na okolní teplotě, zvláště při přechodu z extremních venkovních teplot do klimatizovaných prostor, kde probíhá identifikace.

Obr. 7: Termogram lidského obličeje. [13]

3.1.7 Geometrie ruky

V roce 1985 si tuto metodu nechal patentovat David Sidlauskas. Je to tedy vůbec nejstarší implementovaný systém, a proto není překvapením, že tato metoda byla použita na Olympijských hrách v Atlantě v roce 1996 k identifikaci osob u vstupu do olympijské vesnice.

Tyto systémy využívají k identifikaci jednoduchá měření ruky z hlediska třídimenzionální perspektivy. Vzhledem k charakteru měření je možné tuto metodu využít pouze u dospělého člověka, kdy se tvar ruky již výrazně nemění. K měření se využívá speciální skener, jež snímá třídimenzionální fotografie, a podložka s pěti kolíky pro zajištění správné polohy ruky, což snižuje riziko neoprávněného zamítnutí. V počátcích této technologie se měření omezovalo pouze na délku prstů. Postupem času ale došlo k navýšení měřených parametrů ruky. Nyní tato technologie snímá délku, šířku a tloušťku prstů a dlaně. Celkem se jedná o 90 měření, které po úpravě mají velikost 9B (Recognition Systems, Inc.) nebo 20B (Biomet Partners).

Tyto systémy nacházejí uplatnění především v docházkových systémech a v přístupových systémech.

Mezi nevýhody patří nízká spolehlivost a hygiena, jelikož je nutný fyzický kontakt. Výhodou tohoto systému je naopak malá velikost etalonu a intuitivnost.

Obr. 8: Snímání geometrie ruky. [14]

Tab. 5: Parametry biometrie geometrie ruky. [15]

FRR	< 0,1 [%]
FAR	0,1 [%]
rychlost verifikace	1–2 [s]
míra spolehlivosti	střední

3.1.8 Struktura žil na ruce

Využívá se individuální struktury žil, jež má u dospělého jedince dostatečnou stálost a jedinečnost i u jednovaječných dvojčat. Tuto skutečnost dokázaly i některé vědecké studie. Obrovskou výhodou této metody je obtížnost zfalšování, jelikož struktura žil je ukryta před zraky případných útočníků, navíc jsou některé systémy schopny rozpoznat, zda v žilách proudí krev. Pozměnit strukturu bez operace je tedy nemožné. Žíly jsou ideální vzory, poněvadž jsou dostatečně velké, stabilní, a jak už bylo řečeno, ukryté. Metoda je komerčně využívána od roku 2000. Existují dvě metody snímaní žil:

1. identifikace podle struktury žil v dorzální části ruky
2. identifikace podle struktury žil na dlani

Identifikace podle struktury žil v dorzální části ruky

Metoda využívá speciální kameru snímající v infračervené oblasti elektromagnetického spektra. Ta získá černobílý obraz krevního řečiště. K dalšímu zpracování se využívá především tvar a tloušťka žil. Zobrazením snímaného místa v infračervené oblasti získáme černobílý snímek ruky s černě vykresleným cévním řečištěm. To je způsobeno odkysličeným hemoglobinem, který pohlcuje světlo o vlnové délce přibližně 760nm, což je hodnota blízká infračervenému světlu. Skutečnost, že IR záření proniká jen do hloubky cca 3mm, má za následek, že se na snímku objeví pouze cévní řečiště dorzální části ruky. Pro získání vzorku pro porovnání s etalonem musí projít snímek čtyřmi fázemi úprav:

1. **Segmentace obrazu** – tento krok slouží k vycentrování snímku. K tomu je nutné oddělit ruku od černého pozadí.
2. **Vyhlazení a redukce šumu** – v tomto kroku dochází k vyhlazení cévního řečiště a potlačení vlivu tvaru dorzální části ruky na získaný snímek.
3. **Lokální prahování** – dochází zde k vyčlenění struktury řečiště na základě specifických metod.
4. **Postprocessing** – po upravení zůstane na snímku pouze struktura žil dorzální části ruky.

Metoda se využívá jak pro verifikaci, tak k identifikaci. Nachází uplatnění v přístupových systémech s vysokou úrovní bezpečnosti. Tato technologie se hojně využívá především v Japonsku, kde slouží k verifikaci osob v nemocnicích, univerzitách a bankomatech.

Mezi velké výhody patří spolehlivost, intuitivnost, bezpečnost a bezkontaktní princip snímání narozdíl od identifikace podle geometrie ruky.

Identifikace podle struktury žil na dlani

Obdoba identifikace podle struktury žil dorzální části ruky, s tím rozdílem, že se využívá struktury žil na dlani. Opět se jedná o bezdotykové snímání pomocí speciální infračervené kamery.

Tab. 6: Parametry biometrie struktury žil na dlani. [16]

FRR	0,01 [%]
FAR	0,00008 [%]
míra spolehlivosti	vysoká

Obr. 9: Snímek dlaně v IR spektru. [17]

3.1.9 Verifikace podle tvaru článku prstu a pěstí

Metodu si nechal patentovat Charles Colbert roku 1997 v USA. K identifikaci se využívají individuální měřitelné parametry prstů na vnější části sevřené pěsti. Obraz sevřené ruky je sejmut pomocí videokamery a pomocí digitálního signálového procesoru je vyhodnoceno až 35 měřitelných parametrů [18]. Na výstupu tedy získáme „vlnu" znázorňující obrys čtyř prstů sevřené ruky, která je následně porovnána s databází. Proces rozhodování je poměrně efektivní, přesto může způsobit zpoždění několika sekund. Pro zkrácení doby ověřování v systémech s vysokým počtem verifikací se využívá zjednodušené ověřování. Hlavní záměr při vývoji metody byl utajení identifikace při vstupu. Využívá se přirozený pohyb při otvírání dveří, kdy uchopíme kliku. K získání přístupu je využit přirozený pohyb ruky spojený s otevřením dveří. Uživatel tedy není informován o probíhající identifikaci jako u některých biometrických metod. Mezi výhody patří jednoduchá mechanická a elektronická část systému a nízká cena. Vzhledem k tomu, že systém využívá k rozhodování především biometrická měření prstních kloubů, nejsou potřebné žádné mechanické prostředky pro správné postavení prstu při verifikaci jako u identifikace pomocí geometrie ruky. Využití se přímo nabízí jako doplňková verifikace při vstupu do zón s vyšším stupněm zabezpečení.

3.1.10 Verifikace podle vrásnění článků prstů

Systém pro identifikaci založený na měření vrásnění na prstech a pozici kloubů představila poprvé firma Toshiba v roce 1998. Využívá elektrostatické kapacitní reaktance měření vrásek na prstu ruky u osob.

3.1.11 Identifikace podle podélného rýhování nehtů

Tuto metodu si nechala patentovat společnost Minnesota Mining and Manufacturing Company v roce 1998. Metoda využívá k identifikaci strukturu rýhování nehtového lůžka. To se nachází přímo pod nehtem a je s ním v podstatě paralelní, není tedy pouhým okem vidět. Zdroj polarizovaného světla vyzařuje paprsky pod určitým úhlem, které dopadají na keratin, jež se nachází mezi nehtem a lůžkem. Keratin je přírodní polymer a tato metoda využívá jeho vlastnosti, že při dopadu světla mění jeho orientaci. Následně můžeme analyzovat fázové změny odraženého paprsku. Po zpracování dostaneme číselnou sekvenci čárového kódu. FAR ani FRR není k dispozici, jelikož je metoda ve fázi vývoje. Nevýhodou pravděpodobně bude nízká odolnost systému proti podvrhům.

3.1.12 Identifikace podle otisků prstů

Identifikace osob podle otisků prstů patří mezi nejstarší, nejrozšířenější a nejznámější biometrické metody. Metodu poprvé použil k identifikaci osob William Herschel v roce 1868, aby zamezil neoprávněnému vyplácení sociálních dávek. O několik let později se metoda začala využívat v kriminalistice, kde pomáhá řešit většinu kriminálních případů [19].

K identifikaci se využívají papilární linie na konečcích prstů ruky. Papilární line se nacházejí i na dlaních a chodidlech. Ty se však v současné době nevyužívají pro přístup do systémů, ale pouze ve forenzní sféře. Papilární line jsou vyvýšené reliéfy, jejichž výška se pohybuje od 0,1–0,4mm a šířka od 0,2–0,7mm [20]. Při identifikaci se využívají změny v průběhu papilárních liniích, těm pak říkáme markanty.

Daktyloskopie zkoumá jakékoli změny v průběhu papilárních linií na konečcích prstů. Identifikace podle otisků prstů je založena na tvaru, umístění a vzdálenosti markantů. Shoda otisku ve forenzní sféře ČR se potvrdí při shodě alespoň patnácti markantů. U komerčních systémů se pak tato podmínka mění v závislosti na stupni zabezpečení. Tato technologie se opírá o tří daktyloskopické zákony:

– neexistují dva jedinci s totožnými papilárními liniemi
– obrazce papilárních linií jsou po celý život relativně neměnné
– obrazce papilárních linii jsou permanentní a lze je změnit, pouze pokud je odstraněna zárodečná vrstva pokožky

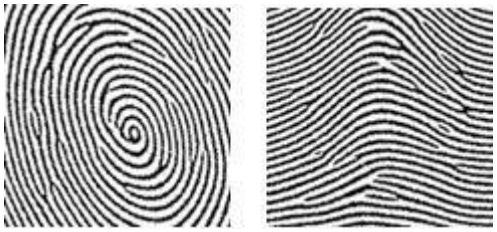
Otisky se mohou získat pomocí statického snímání, kdy se celý prst přitiskne na senzor. Výhodou je intuitivnost. Naopak mezi nevýhody patří nutnost kontaktu se senzorem a možnost zanechání otisku na senzoru. Druhou možností je snímání šablonováním. Kdy uživatel přejíždí prstem po senzoru, ten pak výsledný obraz složí z jednotlivých částí. Výhodou jsou menší rozměry a nižší cena. Rovněž na senzoru nezůstává otisk, jelikož ho pohybem uživatel rozmaže. Nevýhodou je pak nutnost správného postupu při pohybu prstu během skenování.

Při identifikaci se využívá možné rozdělení pomocí základního vzoru papilárních linií. Ty existují tři:

1. Smyčka – Alespoň jedna papilární linie tvoří smyčku mezi deltou a středem centrální oblasti. Tvoří přibližně 60% ze všech otisků.

2. Vír – Tvoří ji minimálně dvě delty, přičemž papilární linie vytvářejí oválné, kruhové nebo spirálovité obrazce s jádrem uprostřed. Tvoří přibližně 30% ze všech otisků.

3. Oblouk – Papilární line zde vytvářejí oblouky. Tvoří přibližně 10% ze všech otisků.



Obr. 10: Základní vzory papilárních linií – vír a oblouk.

Dále se pak zjišťují zvláštnosti papilárních linií neboli markantů. Bylo objeveno více jak šedesát druhů markantů.

Obr. 11: Příklady markantů.

Algoritmy pro rozpoznávání otisků prstů:
I. Podle vzoru – senzor nasnímá otisk prstu. Následně algoritmus zjistí jeho příslušnost k jednomu ze tří základních vzorů a zjišťuje pozici vybraných markantů, popřípadě počet papilárních linií mezi dvěma markanty.
II. Podle podrobností – algoritmus porovnává s etalonem pozici a orientaci jednotlivých markantů v otisku prstu. To klade větší nároky na senzor.

Snímače můžeme rozdělit na – kontaktní
– bezkontaktní

Kontaktní snímače – optoelektronické
– kapacitní
– tlakové
– teplotní
– elektroluminiscenční
– elektronické

Bezkontaktní snímače – ultrazvukové
– optické

Velkou výhodou je množství zdrojů (deset prstů), již existující velká databáze policie, nízká cena a fakt, že tento postup byl v minulosti dostatečně prozkoumán a ověřen.

Nevýhodou pak je možnost obejít systém kopií prstu z odlitku želatiny. Poranění prstu nebo nízká výška reliéfu papilárních linií může mít za následek neschopnost systému identifikovat uživatele.

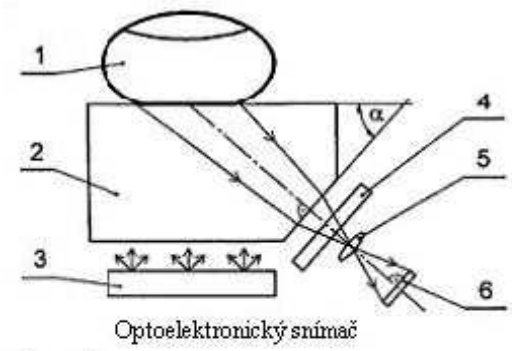
Tab. 7: Parametry biometrie otisků prstů. [21]

FRR	< 1,0 [%]
FAR	0,0001–0,00001 [%]
rychlost verifikace	0,2–1 [s]
míra spolehlivosti	vysoká

Typy snímačů:
Optoelektronické

Princip této technologie je založen na rozdílném lomu světla na hranolu. Přiložením prstu na hranol, dojde k rozsvícení diod. Světlo dopadající na povrch prstu má odlišní lom světla na rozhraní hranol papilární linie a hranol vzduch, dále světlo prochází optickým filtrem, který řeší problémy neostrosti snímaného obrazu a dále na čočku a CCD snímač, který toto světlo digitalizuje a předává výpočetnímu algoritmu pro zpracování obrazu otisku prstu. U některých snímačů se objevuje problém s latentními otisky, které zůstávají na povrchu snímače po předchozí identifikaci. Tím dochází ke zkreslení snímaného otisku a zvýšení pravděpodobnosti neoprávněného odmítnutí vstupu do systému. Tento problém závisí na konkrétním výrobci a provedení povrchové úpravy snímače. Tato skutečnost se může samozřejmě minimalizovat očištěním povrchu snímače. Problém suchých a vlhkých

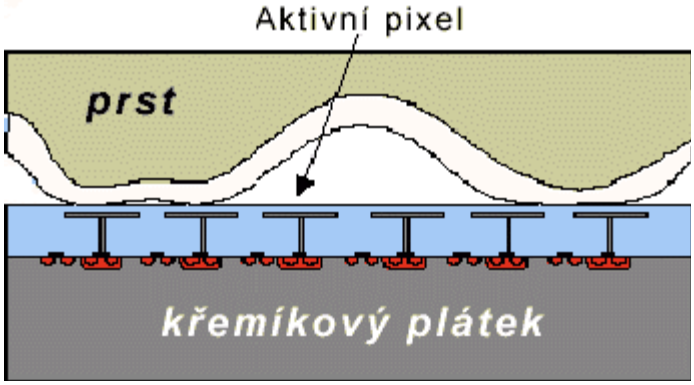
otisků se řeší speciální silikonovou folií na povrchu hranolu a vhodným úhlem nasvícení. Nevýhodou těchto snímačů je že poškození nebo znečištění otisku prstu má velký vliv na snímání, především tmavé nečistoty, které nejlépe pohlcují světlo. Dále větší velikost snímače a tím horší implementace do přenosných zařízení. Výhodou je vysoká kvalita nascenovaného otisku, odolnost proti statickým výbojům, minimální vliv okolního osvětlení a jednoduchá uživatelská obsluha.



Obr. 12: Princip optoelektronického snímače. [22]

Kapacitní snímače

Princip těchto snímačů je založen na měření kapacitního odporu v místě dotyku. Snímač je osázen velkým množstvím mikroelektrod, které tvoří jednu elektrodu a prst druhou. Jedna mikroelektroda tedy tvoří jeden pixel výsledného obrazu. Papilární linie mají tedy větší kapacitní odpor než údolí. Tento odpor má vliv na napětí na kondenzátoru podle, kterého je získán obraz papilárních linií. Z principu tohoto snímače je jasné, že je extrémně závislý na stavu kůže a trápí ho více než ostatní problém suchých a vlhkých otisk prstů, kdy se výrazně mění kapacitní odpor. Výhodou je jejich malá velikost a nízká cena. Nevýhodou pak především nízká životnost vlivem elektrostatických výbojů, která vylučuje použití těchto snímačů v některých provozech.



Obr. 13: Princip kapacitního snímače. [23]

Ultrazvukové snímače

Zařízení vysílá zvukové vlny směrem k přiloženému prstu. Následné odrazy se pak liší podle struktury prstu. Technologie umožňuje získání velmi kvalitního obrazu papilárních linii. Nevýhodou je pak vysoká cena a větší rozměry oproti ostatním metodám.

Elektroluminiscenční snímače

Snímač má vrstvovou strukturu. První vrstvu tvoří sklo s fotodiodami. Nad touto vrstvou je polymerová vrstva, která emituje světlo na základě tlaku. Papilární linie vytvářejí větší tlak než údolí mezi nimi. Další vrstvu tvoří krycí a ochranná vrstva. Nevýhodou těchto snímačů je malá fyzická odolnost a náchylnost na mechanické nečistoty, které zkreslují tvar papilárních linií. Výhodou je pak vysoké rozlišení až 500dpi a z principu tento snímač netrápí problém vlhkých a suchých otisků prstů.

Teplotní snímače

Princip spočívá ve využití pyrodetektoru, tedy velmi citlivého zařízení které snímá rozdíl teplot v našem případě mezi papilárními liniemi a údolími. Prstem se pomalu přejíždí po tomto úzkém snímači a výsledný obraz se tedy získá z několika pásů, tzv. frames. Ty se pak s pomocí speciálního softwaru poskládají do výsledného obrazu. Nevýhodou je že pohyb prstem přes snímač není intuitivní a správné naučení pohybu trvá delší dobu. Také seskládání dílčích frame je obtížnou záležitostí. Tento snímač má také nejhorší kvalitu obrazu, což znesnadňuje identifikaci a odsunuje ho pro použití v systémech s mírnějšími nároky. Výhodou je malá velikost a nízká cena. Jedná se o vůbec nejmenší snímač otisku prstů a také nejrozšířenější především v přenosných zařízeních.

3.1.13 Identifikace pomocí spektroskopie kůže

Optické vlastnosti kůže jsou určeny jejími chemickými a strukturálními vlastnostmi, které jsou unikátní pro každého člověka. Kůže se skládá z několika vrstev a má odlišnou tloušťku nejen na různých částech těla, ale liší se i u každého člověka, přičemž každá vlnová délka se láme a odráží v jiné vrstvě, což je následně vyhodnoceno fotodetektorem. Například krátké vlnové délky jako je modré světlo se odráží od melaninu a krve, světlo delších vlnových délek pak proniká hlouběji do kůže. Tyto optické vlastnosti můžeme změřit pomocí metody rozptýlených odrazů. Biometrický senzor je tvořen 32 LED diodami šestnácti různých vlnových délek v rozmezí 395–940nm a křemíkového fotodetektoru. Vždy dvě pro jednu vlnovou délku na protilehlé straně senzoru a pět křemíkových fotodiod. Diody emitující větší vlnovou délku jsou na vnější straně, diody kratších vlnových délek pak na vnitřní straně. Nejčastěji se senzor zaměřuje na dlaň ruky. Tato metoda není prozatím využívána, ale nabízí dostatečný potenciál ke komerčnímu využití.

Tab. 8: Parametry biometrie spektroskopie kůže. [24]

FRR	3,9 [%]
FAR	1,2 [%]

3.1.14 Identifikace podle pachu

Podle odborníků má každý jedinec pachovou stopu stejně originální jako otisk prstu. Policie využívá pachovou identifikací jako nepřímý důkaz již několik desetiletí.

V kriminalistice je s pojmem „lidský pach“ spojena řada jevů jako je vznik pachových látek, jejich uvolnění, přenos do vzduchu, proces detekce a identifikace pachu. Vědní obor zabývající se zkoumáním pachu se nazývá odorologie. Lidský pach se uvolňuje nepřetržitě a nezávisle na vůli jeho původce. Skládá se až ze třiceti základních chemických sloučenin, jež vytváří podle nejnovějších výzkumů unikátní pach u každého jedince, který nezamaskuje žádná jiná vůně ani požití potravin s výraznou vůní. Nejdůležitějším zdrojem lidského pachu je pot, dále pak kožní maz a odlupovaná zrohovatělá kůže (epidermis). Skladbu lidského pachu ovlivňuje věk, pohlaví, rasa, nemoci, používání léku, charakter potravy, zaměstnání, kosmetické přípravky, konzumace alkoholu a nikotinu. Tyto složky ale pouze doplňují základní geneticky daný pach.

V kriminalistice se využívá spolehlivých schopností psa. Moderní věda má k dispozici zatím dvě nepříliš použitelné metody. Proto se několik subjektů snaží o nalezení nových způsobů spolehlivé identifikace.

Nyní se využívá plynová chromatografie nebo zařízení LIDAR . Prvně jmenovaná metoda je velice přesná a využívá se v kriminalistické technice k analýze organických látek, které je možno převést do plynné povahy. Pach tuto podmínku pravděpodobně splňuje, ale není to prozatím vědecky prokázáno. Další metoda využívá zařízení LIDAR. Z laserového zdroje se vyzařuje monochromatické záření, jež při kontaktu s částicemi vzduchu obsahujícího cizí látky změní svůj charakter. Tuto skutečnost zaznamená detektor a daný algoritmus ji vyhodnotí. LIDAR je tedy svou podstatou obdoba radaru.
Ani jedna z výše jmenovaných metod se však nehodí k identifikaci lidského pachu. Reálné nasazení do přístupových systému je v blízké budoucnosti krajně nepravděpodobné.

3.1.15 Verifikace podle DNA

Žádný jiný údaj nedokáže tak komplexně charakterizovat člověka jako DNA. DNA neboli kyselina deoxyribonukleová se neliší pouze u jednovaječných dvojčat. Počet rozdílů mezi dvěma nepříbuznými jedinci je přibližně 10^6. S pomocí DNA lze bezpečně identifikovat každého jedince a zároveň lze ze získaného genetického profilu vyčíst řadu informací o fyzických charakteristikách daného jedince. Předurčuje vývoj a vlastnosti celého organismu. Metodu identifikace osob pomocí DNA objevil v roce 1984 Alec Jeffreysem. V praxi byla poprvé použita britským Scotland Yardem v roce 1987 k odhalení několikanásobného vraha.
Vzorek DNA můžeme získat z jakékoli části těla, přičemž k identifikování stačí množství DNA odpovídající 50 piko gramům. Nutno podotknout, že v jedné buňce lidského těla je obsaženo množství DNA odpovídající hodnotě 6 piko gramům. K identifikaci se nevyužívá kompletní vzorec, z důvodu složitosti, ale pouze část DNA. Štěpení celé spirály DNA se provádí pomocí enzymu EcoR1. Vzniklé fragmenty DNA jsou štěpeny až do použitelné velikosti a následně se uloží na nylonovou membránu. Po přidání radioaktivních nebo obarvených sond je získán otisk DNA. Vzhledem k podobě s čárovým kódem je jeho následná digitalizace triviální záležitostí. Následně se již může získaný vzorek porovnat s databází.

Největší výhodou DNA je její stálost a nezměnitelnost žádnou dosud známou technologií. Nevýhodou jsou etické pochybnosti a velký zásah do ochrany osobních údajů. Největší překážku ale tvoří časová náročnost, jež znemožňuje využít metodu v reálnem čase. Proto se i nadále bude především využívat ve forenzní oblasti, k identifikaci těl a k určení otcovství.

3.1.16 Bioelektrické pole

Technologie je založena na existenci pasivního bioelektrického pole kolem každého jedince, jež je stejně unikátní jako DNA. Tato pole dokáže identifikovat například přístroj BIOFINDER II & III, který dokáže identifikovat bioelektrické pole jedince na vzdálenost až šesti metrů. Jedinec musí být osamocen, jelikož ve skupině lidi by se jednotlivá pole překrývala. To zabraňuje využívat tuto technologii k širšímu využití. Firma BIOFINDER ji proto nabízí především ke spouštění různých zařízení v domácnosti, především pak pokojového osvětlení. Zajímavostí je, že se unikátní bioelektrické pole jedince může uložit jako *.wav soubor [25].

3.1.17 Biodynamický podpis osoby

Tuto technologii vyvinula a poprvé představila v roce 2006 firma Idesia pod názvem BioDynamic Signature™ zkráceně BDS™. Technologie je založena na dynamických elektrofyziologických vlastnostech každého jedince. Tyto signály jsou samovolně vyzařovány z různých lidských orgánů jako je například mozek, svaly a nervový systém. Tyto bioelektrické signály jsou dostatečně jedinečné i konzistentní na to, aby se mohly využít v praxi. Snímač se skládá ze dvou kovových kontaktních ploch a zesilovače bio-elektrických signálů. Uživatel na každou z nich přiloží jeden prst z každé ruky po dobu několika vteřin. To postačí, aby systém shromáždil dostatek informací o jedincově vzorku, který následně porovná s databází. Při vytváření etalonu je proces poněkud zdlouhavější, jelikož uživatel musí přiložit oba prsty po dobu 10s a to alespoň třikrát.

BDS500 je prozatím jediný produkt na trhu využívající tuto velmi zajímavou technologii. Výhodou je rychlost, jednoduchá implementace, spolehlivost (viz tab. 9), odolnost proti zfalšování a nízká cena.

Tab. 9: Parametry biometrie biodinamyckého podpisu. [26]

Nastavení zabezpečení	FAR [%]	FRR [%]	Čas verifikace [s]
nízké	3	0,5	2-3
střední	1	1	2-4
vysoké	0,2	3	3-5

Obr. 14: BDS500 firmy IDesia. [27]

3.2 Behaviorální metody

3.2.1 Identifikace podle charakteristiky hlasu

Biometrická identifikace podle hlasu patří mezi nejstarší metody. Již několik desetiletí se využívá v kriminalistice a začíná se prosazovat i v komerční oblasti. Lidský hlas vytváří řečové orgány, neboli vokální trakt. Tvoří ho hlasivky, ústní dutina, jazyk a zuby. Jedinečnost je způsobena nejen odlišným tvarem těchto orgánů, ale také subjektivní osobností mluvčího (barva hlasu, rytmus, atd.), akustickou strukturou, gramatikou a skladbou řeči. Díky tomu je hlas jednotlivce dostatečně výjimečný. Je nutné říci, že u této metody je značný rozdíl v pojmech identifikace a verifikace. Identifikace porovnává s databází vyřčené slovo, a pokud odpovídá výslovnosti, je povolen přístup do systému. Naproti tomu verifikace porovnává míru shody mezi vyřčeným slovem a uloženým vzorkem otisku hlasu.

Při vytváření etalonu neboli otisku hlasu můžeme využít i obyčejný mikrofon. Ze zvukového záznamu se za pomocí filtrů získají jedinečné znaky vokálního traktu, jež tvoří vlastní biometrický vzorek. S ohledem na větší odolnost se volí věty, které mají více akustických informací než jednotlivé slovo. Volbou vlastní věty se dále zvyšuje bezpečnost, protože ani sebelepší imitátor není schopen vědět jakou větu má vyslovit. Věty se volí nejčastěji o délce 3 vteřin, jako kompromis mezi paměťovou náročností a dostatkem unikátních akustických informací.

Použití přímo vybízí ke vzdálené verifikaci pro přístup do bankovnictví a jiných systémů přes mobilní telefon.

Moderní systémy jsou navíc schopny rozpoznat nahraný vzorek hlasu. Mezi další výhody patří rychlost, technologická nenáročnost, nízká cena a sociální přijatelnost. Naopak nevýhodou technologie je její závislost na aktuálním stavu mluvčího, jehož lidský hlas může být nepříjemně ovlivněn nemocemi, malá stálost v čase, vliv okolního šumu a jiné zkreslující vlivy.

Tab. 10: Parametry biometrie charakteristiky hlasu v ideálním případě. [28]

FRR	0,01 [%]
FAR	0,28 [%]
rychlost verifikace	0,2–1 [s]
míra spolehlivosti	nízká

3.2.2 Verifikace podle způsobu pohybu očí

Očí jsou jedním z nejdůležitějších orgánů a to platí i o biometrické identifikaci, kde se využívá již řadu let oční duhovka, oční sítnice, nověji oční rohovka a nyní i pohyb očí. Oční pohyby obsahují řadu unikátních informací o každém jedinci. Způsob, jakým se oči pohybují, je velmi komplikovaný. Věda tyto pohyby studuje již více než 100 let. Pohyb očí musí být velmi rychlý, pokud má být obraz získán v reálném čase. K tomu slouží šest očních svalů, které zajišťují vertikální, horizontální a šikmé oční rotace. Ty jsou řízeny z mozku pomocí tří lebečních nervů. Identifikace osob založená na pohybu očí byla představena na konferenci v Londýně v roce 2003 Slezskou univerzitou v Gliwicích z Polska. Metoda je založena na jedinečných behaviorálních a fyziologických vlastnostech oka při sledování pohybujícího se bodu na obrazovce, jelikož způsob zaostřování je důsledek předchozích zkušeností. Pomocí speciálních brýlí, které na principu infračerveného světla snímají pohyb očí a ten pak srovnají s databází, je na

obrazovce vytvořena matice bodů (3x3) [29]. Na rozsvícený bod musí uživatel zaostřit, přičemž se sleduje doba potřebná k zaostření na nový bod. Program začíná a končí uprostřed obrazovky.

Metoda je zatím ve stadiu výzkumu, a proto nejsou výsledky zatím dostatečné pro použití v reálných systémech, i když se jedná o velmi zajímavou metodu, jejíž hlavní výhoda bude nízká cena. Testy byly zatím provedeny na zkušebním vzorku 47 osob rozdílného věku i pohlaví, ale dosáhly nevalných výsledků.

Tab. 11: Parametry biometrie pohybu očí. [30]

FRR	9,4 [%]
FAR	4,84 [%]

3.2.3 Verifikace podle tvaru a pohybu rtů

Metoda je založena na detekci pohybu rtů a využívá obdobnou technologii jako identifikace podle obličeje. Kamera snímá obličej uživatele a speciální software extrahuje tvar rtů a zaznamenává jeho pohyb při vyslovení vstupního kódu, který by měl být individuální u každého člověka.

3.2.4 Dynamika stisku kláves

Již za druhé světové války byla experty porovnávána dynamika psaní morseovky agentů s dříve získaným etalonem. Její plný potenciál se začíná využívat až nyní v oblasti doplňkové verifikace na počítačích. Technologie je založena na měření doby stisku klávesy a doby mezi jednotlivými stisky. U této metody je poněkud komplikovanější získání etalonu. Vzniká zprůměrňováním několika získaných vzorků, minimálně pak osmi různých slov, jež musíme napsat alespoň patnáctkrát. Přičemž slovo by mělo mít aspoň osm znaků. Rozhodovací software je nutno vhodně nastavit pro dosažení přiměřených hodnot FRR a FAR. Na tuto technologii má v současnosti monopol firma Biopassword Inc., což brání většímu rozšíření, stejně jako nedostatečné prověření.

Výhodou je pak jednoduchá implementace a nízká cena vyplývající z potřeby nákupu pouze vyhodnocovacího softwaru. Mezi nevýhody patří nízká spolehlivost, uživatelsky nepříjemné a zdlouhavé získání etalonu. Na spolehlivosti metody se negativně může projevit změna klávesnice, změna stylu psaní především u "počítačových začátečníků", psychický stav jedince a další vlivy. Metoda je tedy naprosto nevhodná k identifikaci, její využití se nabízí spíše jako doplňková verifikace, kdy systém běží na pozadí a v případě odklonu od předlohy vyvolá nový verifikační požadavek. Výrobce neudává koeficienty FRR ani FAR, ale vzhledem k technologii bude hodnota FRR nabývat vysoké hodnoty.

3.2.5 Dynamika pohybu myší

Metoda byla vyvinuta na univerzitě Queen Mary v Londýně. Při verifikaci je uživatel vyzván k nakreslení určeného tvaru, který byl nakreslen při vytváření etalonu. Software získá z nakresleného vzoru specifické znaky jako pozice, rychlost tahu a zaoblení, jež následně porovná s etalonem. Při tvorbě standardního etalonu je potřeba nakreslit obraz alespoň dvacetkrát. Z těchto vzorů je vytvořen průměr, který se pomocí algoritmu převede na 144 vektorů, které jsou následně převedeny a uloženy do databáze ve formě kódu. Vlastnosti i využití jsou obdobné jako u dynamiky stisku kláves. Tedy jednoduchá

implementace, nízká cena. Nevýhody pak jsou nízká spolehlivost a závislost na stavu uživatele. Využití je především v doplňkové verifikaci. Koeficienty FRR a FAR nejsou dostupné z důvodu nedokončeného vývoje.

3.2.6 Dynamika podpisu

Metoda je založena na jedinečnosti kombinace anatomických a behaviorálních vlastností člověka, které se projevují při podpisu. Grafologie jakožto vědecká disciplína zabývající se studiem písma a jeho vztahu k lidskému chování dokázala unikátnost podpisu. Byla vyvinuta v 19. století, ačkoli podpis se jako identifikační charakteristika využívá již několik set let. Díky tomu je veřejností pozitivně vnímána na rozdíl od snímání otisku prstů, který historicky přiřazují k policejní identifikaci. Biometrická identifikace využívá nejen srovnání podpisového vzoru, ale i tlaku a tahu. K tomu slouží speciální tužka a podložka na psaní. Základními dynamickými vlastnostmi jsou rychlost, akcelerace, časování, tlak a směr tahu, které jsou zaznamenávány v trojrozměrném souřadnicovém systému. Díky tomu je tento systém nemožné obelstít. Nikdo není schopen napodobit dynamiku podpisu na rozdíl od metody pro získávání statického obrazu, která využívá pouze geometrických vlastností podpisu.

Výhodou je vysoká bezpečnost, rychlost, uživatelská intuitivnost i přijatelnost. Při použití nové metody vlnkové transformace s ověřováním pomoci algoritmu backpropagation neuronových sítí jsou výsledky vynikající (viz. Tab. 12) ve srovnání s jinými metodami dynamického podpisu.

Tab. 12: parametry dynamiky podpisu [31]

FRR	0 [%]
FAR	< 0,1 [%]

4 Testy biometrických přístupových zařízení

V této části bakalářské práce je mým úkolem otestovat bezpečnost biometrických metod. K dispozici jsem měl tři přístupové systémy založené na odlišných principech biometrické autentizace žadatele o přístup do systému. Jako první, optický snímač otisku prstů od digitalPersona, konkrétně U.are.U 4000 Senzor. Dále kapacitní snímač otisků prstů 200MC od Precise Biometric a jako třetí Panasonic Authenticam™ sloužící k autentizaci uživatele podle duhovky. Z internetu jsem si ještě stáhnul demoverzi BIOPASSWORD v3.1 od BioNet Systems, LLC. Tento produkt slouží k autentizaci uživatele na základě vyplnění správného přihlašovacího jména a hesla napsaného se správnou dynamikou stisku kláves. Jednotlivé systémy budou popsány z hlediska obsluhy, uživatelského prostředí, bezpečnosti a možnosti uplatnění v konkrétních přístupových systémech. Budou též uvedeny jejich parametry. Testy probíhaly na notebooku Toshiba Satellite s procesorem Intel Pentium IV 2,0GHz, 1GB RAM, harddisk 60GB, grafika ATI Radeon X700 128MB a operačním systému Windows XP SP3.

4.1 Optoelektronický snímač otisků prstů

K testování byl využit autentizační systém DigitalPersona® Pro se senzorem U.are.U 4000. Instalace i ovládání programu jsou bezproblémové. S pomocí tohoto autentizačního systému můžeme zabezpečit vstup do počítače, chránit soubory a aplikace před

spuštěním. K tomu je potřeba zaregistrovat alespoň jeden prst z deseti. Biometrický etalon se vytvoří ze čtyř snímků, které musejí být v dostatečné kvalitě. Systém umožňuje také nastavení zkratek shift nebo ctrl plus libovolný zaregistrovaný prst pro spuštění nastavené aplikace. Tento systém ale neumí administrátorskou správu účtů, což je velká nevýhoda. Jednotliví uživatelé si tedy mohou nastavovat zabezpečení ve svých profilech dle své libosti, bez kontroly administrátora. Z toho vyplývá použitelnost především pro domácnosti.

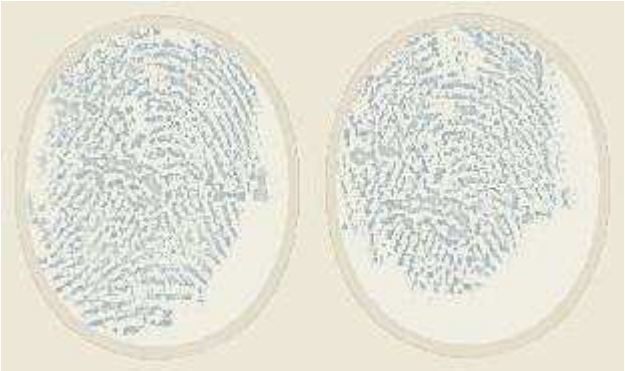
Parametry senzoru U.are.U 4000:
Rozhraní: USB 2.0
Optické rozlišení: 512dpi
Maximální hloubka šedé: 8-bit (256 úrovní šedé)
Obraz: Monochromatický
Osvětlení: čtyři IR diody
Rozměr snímaného obrazu: 15x18mm
Rozměry (ŠxVxH): 4,9x7,9x1,9cm
Provozní teplota: 0–40° C
Provozní vlhkost: 20–80% při 30° C

Obr. 15: U.are.U 4000.

Testování bezpečnosti:
Pro oklamání autentizačního systému jsem se pokoušel vytvořit odlitek prstu z různých hmot. Princip vždy spočíval v obtisknutí prstu do plastelíny a vylitím různé hmoty. Byli vyzkoušeny tyto hmoty:
1. Silikon
2. Vosk
3. Zinkoklih
4. Želatina

1. Silikon
Silikonem se vyplnil obtisk prsti v plastelíně a po 24 hodinách byl odlitek vyjmut. Kvalita otisků byla velmi slabá. To bylo dáno skutečností, že při tuhnutí vytekla ze silikonu voda. Ta zmáčela vytvarované papilární linie. Některé z nich pod tíhou silikonu úplně zanikly. Další nevýhoda silikonu bylo, že zmáčená plastelína v některých částech zůstala přilepená k silikonovému odlitku i po jeho vyjmutí z formy. A při pokusu o její odstranění docházelo zpravidla ke znehodnocení dané části otisku.

Test otisku ze silikonu
Z osmi vytvořených vzorků byli pouze dva z větší části zachované, tři měli jen menší část a tři byli vodou poničeny natolik, že na nich nezůstala jediná papilární linie. Se zbylými dvěma otisky byl proveden neúspěšný pokus o přihlášení. Jejich shoda s originálním otiskem nebyla dostatečná. Jejich kvalita stačila pouze pro vytvoření nového biometrického etalonu (viz obr. 16). Následně se s nimi již pod tento nově vytvořený etalon dalo přihlašovat.



Obr. 16: Silikonové odlitky.

2. Vosk

Na vodní lázni byl v nádobě roztaven obyčejný vosk pleťové barvy a vlit do připravené formy. Po vychladnutí byl odlitek vyjmut. Kvalita takto vytvořeného odlitku je velmi dobrá. Odlitek z této hmoty, ale senzor ignoroval. To je dáno odlišnými optickými vlastnostmi povrchu tohoto odlitku.

3. Zinkoklih

Latinsky: zinci oxidi gelatina mollis.

Česky: měkká zinková želatina.

Tab. 13: Množství surovin pro přípravu 1000g zinkoklihu. [32]

Název suroviny	Množství [g]
Oxid zinečnatý	100
Želatina	400
Glycerol	150
Čištěná voda	350

Vlastnosti: bílá rosolovitá hmota, při opětovném zahřátí taje.

Použití: dříve se připravovalo v lékárně na fixaci obvazu místo sádry .

Postup přípravy: želatina se v nádobě rovnoměrně provlhčí vodou pokojové teploty a nechá se 15min bobtnat. Následně se zahřeje na vodní lázni při teplotě nejvýše 65° C do rozpuštění. V další nádobě smícháme oxid zinečnatý s glycerolem a tuto homogenní směs přimícháme k roztavené želatině.

Popis jednotlivých surovin:

Oxid zinečnatý

Vlastnosti: bílý nebo slabě nažloutlý jemný amorfní prášek bez hrubých částic. Je prakticky nerozpustný ve vodě a v lihu 96%. Rozpouští se ve zředěných minerálních kyselinách. Molární hmotnost 81,38. [33]

Zkouška totožnosti: Při intenzivním zahříváni žloutne, žluté zbarveni po ochlazeni mizí.

Želatina

Vlastnosti: Je to čištěná bílkovina získaná z živočišného kolagenu buď částečnou kyselou hydrolýzou (typ A), nebo částečnou alkalickou hydrolýzou (typ B), může to být i směs obou typů. Nažloutlá až světle žlutavě hnědá pevná látka, bez chuti, obyčejně ve formě průsvitných lístků, útržků, zrn nebo prášku. Je prakticky nerozpustná v běžných organických rozpouštědlech, ve studené vodě bobtná a po zahřátí tvoří koloidní[1] roztok, který po ochlazení přechází ve více nebo méně pevný gel. Izoelektrický bod[2] želatiny typu A je mezi pH 6,3 a 9,2. Želatiny typu B mezi pH 4,7 a 5,2 [34]. Česky lékopis také uvádí další zkoušky a požadavky, např.: ztráta sušením, celkový popel, skladování, označovaní, mikrobiální znečištění nejvýše 103 živých mikroorganismu v 1 gramu. Musí vyhovovat zkoušce na nepřítomnost Escherichia coli a Salmonella.
Mohutnost gelu: Pokud je látka určena pro přípravu globulí, čípků a zinkové želatiny, mohutnost gelu je 150–250g. Mohutnost gelu se vyjadřuje jako množství v gramech potřebné ke vzniku síly, která vtlačí píst o průměru 12,7mm do gelu o koncentraci 6,67 % při 10° C do hloubky 4mm.

Glycerol 85%

Vlastnosti: sirupovitá tekutina, na omak mastná, bezbarvá nebo téměř bezbarvá, čirá, silně hygroskopická[3]. Je mísitelný s vodou a s lihem 96%, těžce rozpustný v acetonu, Prakticky nerozpustný v mastných olejích a v silicích. Je to vodný roztok propan - 1,2,3-triolu. Molární hmotnost je 92,09. Obsahuje 83,5% až 88,5% sloučeniny C3H8O3. [35]

Čištěná voda

Vlastnosit: čirá kapalina, bez barvy a chuti. Jo to voda určená pro výrobu a přípravu léčiv, u nichž není požadováno, že mají být sterilní a prosté pyrogenních látek, pokud není předepsáno a schváleno jinak. Molární hmotnost 18,02. [36]

Výroba: připravuje se destilací, za použití iontoměničů nebo jinou vhodnou metodou z vody, která vyhovuje požadavkům na pitnou vodu (ČSN 75 7111). Skladuje se ve vhodných obalech a skladuje se za podmínek, které zajišťují požadavky na mikrobiologickou jakost. Neobsahuje žádné přísady. Obsahuje maximálně 0,1μg/g těžkých kovů, 10μg/l hliníku, 0,2μg/g amonia a 0,2μg/g dusičnanů.

Výroba otisků ze zinkoklihu: plastelínu, která je po vyndání poměrně tvrdá, krouživými pohyby v dlani změkčíme. Výslednou kuličku položíme na stůl a plochým předmět přimáčkneme. Do vytvořené rovné plochy vtiskneme čistý prst do hloubky alespoň 4mm. Prst opatrně vyjmeme tak abychom obtisk nerozmazali. Ujistíme se, že nejsou nikde v otisku žádné praskliny ani po krajích odkud by mohl zinkoklih po zalití vytéct. V tab.14 je uvedeno množství jednotlivých látek, které jsem použil pro výrobu 50g zinkoklihu. Toto množství vystačí na zhruba 8–10 odlitků otisků prstů. Nejdříve se 20g želatiny v nádobě rovnoměrně provlhčí 17,5g čištěné vody pokojové teploty a nechá se 15min bobtnat. Následně se zahřeje na vodní lázni při teplotě nejvýše 65° C do úplného rozpuštěni. V další nádobě smícháme 5g oxidu zinečnatého se 7,5g glycerolu a tuto homogenní směs přimícháme k rozpuštěné želatině. Stále horkou směs vlijeme do

[1] Vlastnosti jsou mezi homogenní a heterogenní směsí.
[2] Hodnota pH roztoku v němž se elektroneutrální částice nesoucí kladný i záporný náboj nepohybuje v elektrickém poli
[3] Snadno přijímající vodu. Za vlhka měknoucí, za sucha tvrdý.

připravených forem. Necháme 1–2hod tuhnout při pokojové teplotě. Po té můžeme opatrně vyjmout hotové otisky.

Tab. 14: Množství jednotlivých surovin pro odlití 8–10 otisků.

Název suroviny	Množství [g]
Oxid zinečnatý	5,0
Želatina	20,0
Glycerol	7,5
Čištěná voda	17,5

Tab. 15: Náklady na výrobu otisků ze zinkoklihu.

Název suroviny	Množství	Cena [Kč]
Oxid zinečnatý	30g	41,9
Želatina	30g	19,4
Glycerol	50g	27,5
Čištěná voda	600ml	25,0
	Celkem:	**113,8**

Uvedená cena se, ale může lišit podle minimálního množství, které bude daná lékárna prodávat. V tab. 15 je uvedeno minimální množství, které mi prodala lékárna ve Svitavách. K této ceně je potřeba připočítat ještě cenu za plastelínu, kterou pořídíme v kterémkoli papírnictví zhruba za 20Kč.

Test otisku ze zinkoklihu

Vzniklé duplikáty otisků byli kvalitní. Přestože ne všechny odlitky dokázaly senzor oklamat. Úspěšnost kazí především pěna, která se vytváří při výrobě, a i při snaze ji všechnu z povrchu odebrat před zalitím forem, vzniknou v některých duplikátech dírky po těchto vzduchových bublinách. Tyto nepřesnosti pak mají za následek neúspěch při oklamání senzoru. Při prvním pokusu byli odlity čtyři otisky, z nichž dva byli úspěšné při oklamání autetizačního systému. V druhé várce bylo vytvořeno šest otisků. Během výroby zinkoklihu byla odstraněna téměř všechna pěna, i přes to byly úspěšné jen dva otisky. Výhodou jsou stabilnější vlastnosti této směsi. I po měsíci fungují tyto odlitky velmi dobře. Je důležité poznamenat, že po přiložení živého prstu dojde k autentizaci takřka okamžitě, ale při použití odlitku se autentizace ne vždy podaří a je potřeba trocha cviku, ke správnému odhadu intenzity pro přiložení duplikátu otisku. Platí zhruba 75% úspěšnost, že autentizace se povede hned na poprvé. Z obr. 17 je patrné že linie jsou o poznání zřetelnější než u živého nebo želatinového otisku. To je způsobeno nižší vlhkostí na povrchu a tím lepší odrazivostí.

4. Želatina

Výroba otisků ze želatiny: Zachovává se stejný poměr želatiny a čištěné vody jako při výrobě zinkoklihu, tedy 4:3,5. Tento poměr je velice důležité zachovat, jelikož při větším množství vody otisky ztrácejí svoji pevnost a další pro nás důležité vlastnosti. Především to je nižší odpor a horší odrazivost.

Obr. 17: Zleva: živý prst, želatinový prst a prst ze zinkoklihu.

Test otisku z želatiny

Nevýhodou této směsi oproti zinkoklihu je, že po jednom dni jsou otisky nepoužitelné. Otisky totiž postupně osychají a nakonec se zcela vysuší a zdeformují svůj tvar. Tento jev je možné zpomalit udržením vlhkosti okolního prostředí. Byli vyrobeny čtyři várky otisků. První dvě, které měli více vody a proto ani jeden z dvanácti otisků nebyl při oklamání úspěšný. Další dvě várky byly vyrobeny v daném poměru 4:3,5. V první byli úspěšné dva otisky ze tří. Ve druhé všechny tři. Z obr. 17 je jasně patrné, že optické vlastnosti takto vytvořeného otisku jsou téměř shodné s živým prstem. Což dokládá i úspěšnost vyrobených otisků. Co se týče úspěšnosti při autentizaci platí stejná pravidla jako pro zinkoklih. Tedy ne vždy se podaří duplikovaný otisk správně přiložit, aby byla autentizace úspěšná.

Zhodnocení

Vzhledem k určení pro domácnosti není důležité, aby byl systém schopen rozeznat napodobeninu otisku prstu. K tomu jsou určeny jiná propracovanější a dražší zařízení. Tomuto systému plně dostačuje skutečnost, že na světě neexistují dva lidé, kteří by měli stejné otisky. To bylo orientačně ověřeno v rámci testu. Čtyři osoby se pokusili o přihlášení na můj profil, ve kterém jsem měl zaregistrovány všechny prsty, přičemž ani jedné osobě se pod žádným jejím prstem nepodařilo přihlásit. Tím jsem se také pokusil ověřit výkonnost senzoru a algoritmu.

Nověji se v této oblasti začíná uplatňovat multispektrální obraz otisku prstu. Kde využívá senzor několik zdrojů záření o různých vlnových délkách, které se odráží v různé hloubce kůže a dokáží tak získat detailnější informace, dokáží tak lehce rozpoznat a vyhodnotit otisk ze syntetických nebo organických látek. To pomůže k vyšší bezpečnosti, ale za cenu vyšších nákladů a tedy určení pro jinou cílovou skupinu. Součástí testu tohoto senzoru bylo i zjištění minimální plochy potřebné k identifikaci. Pro otisk prstu typu smyčka (viz str.21) byla stanovena jako plocha centrální části prstu kde je nejvíce patrný vzor papilárních linií a také je zde možné získat nejvíce údajů. Potřebná velikost otisku byla stanovena jako čtverec o rozměru 8x8mm. A opačně pokud byla tato oblast prstu zakryta plochou o rozměrech větších jak 4x8mm (ŠxV) byla identifikace neúspěšná.

4.2 Kapacitní snímač otisků prstů

K testování byl využit snímač Precise Biometric 200 MC, bohužel chyběl jakýkoli software i karta, proto jsem musel stáhnout ze stránek výrobce ovladač k senzoru [37] a Precise BioMatch™ Demo 1.7.0 [38]. Jedná se o demoverzi s omezenými schopnostmi. Po spuštění jsou na výběr čtyři možnosti. První slouží k výběru senzoru, v našem případě

zvolíme Precise Biometric 200 MC. Druhá umí vyobrazit přiložený prst a vypíše zda je kvalita dostatečná pro vyhodnocení. Třetí volba umožňuje vytvoření biometrického etalonu, který se může uložit buď na kartu, která bohužel nebyla k dispozici nebo na počítač/virtuální server, tedy na harddisk počítače. Dále vybereme prsty, které budeme chtít zaregistrovat. Následně u vybraných prstů přiložíme dvakrát prst a pokud jsou v dostatečné kvalitě a shodují se je potvrzeno uložení a můžeme pokračovat registrací dalšího prstu (obr. 19). Pokud se otisky dostatečně neshodují jsme vyzváni k opětovnému přiložení prstu. Nakonec se daný profil uloží pod námi zvolené jméno. Čtvrtá volba slouží k simulaci přihlášeni. Musíme nejdříve vybrat odkud budeme brát biometrický etalon. Tedy buď karta nebo počítač/virtuální server. Kartu nemáme k dispozici, proto po zvolení volby počítač/virtuální server musíme vybrat jméno, pod kterým máme uloženy daný biometrický etalon. Následně si vybereme prst a máme 15 vteřin ke správnému přiložení. Po této době dojde u komerčního systému k vyhodnocení neoprávněného pokusu o vstup a k předání této skutečnosti administrátoru.

Parametry senzoru Precise Biometric 200 MC:
Rozhraní: USB 2.0
Optické rozlišení: 508dpi
Maximální hloubka šedé: 8-bit (256 úrovní šedé)
Obraz: Monochromatický
Rozměr snímaného obrazu: 10,4x14,4mm
Provozní teplota: 0–50° C
Provozní vlhkost: 5–93% při 30° C
ESD: + /–15kV

Obr. 18: Registrace.

Testování bezpečnosti:

Pro oklamání autentizačního systému byli vyzkoušeny odlitky prstů ze stejných hmot jako u testování senzoru U.are.U 4000. Proto zde budou uvedeny pouze dosažené výsledky.

Obr. 19: Precise Biometric 200 MC.

1. Silikon

Duplikát otisku z tohoto materiálu senzor ignoroval. To bylo způsobeno odlišným kapacitním odporem vytvořeným v místě dotyku papilárních linií oproti živému prstu.

2. Vosk

Duplikát otisku z tohoto materiálu senzor ignoroval. To bylo způsobeno odlišným kapacitním odporem vytvořeným v místě dotyku papilárních linií oproti živému prstu. To je patrné už z odlišných mechanických vlastností tvrdého voskového odlitku.

3. Zinkoklih

Při použití otisku z této hmoty jsem se přesvědčil, že tento senzor je velmi citlivý na správné přiložení odlitku. Nebýt obrazovky, která ukazuje aktuální stav snímaného otisku bylo by velmi obtížné uspět. Odlitek prstu jsem musel rovnoměrně přitlačit k senzoru za pomocí čtyř prstů, abych byl úspěšný při autentizaci (viz obr. 20). Pokud jsem odlitek přiložil nerovnoměrně, byla autentizace neúspěšná (viz obr. 21). To bylo způsobenou nedostatečným kontaktem papilárních linií s plochou senzoru. Tedy nízkým kapacitním odporem v místech dotyku. Toto odmítnutí bylo stejné pro špatně přiložený odlitek ze zinkoklihu i želatiny a stejně tak i pro vlhký živý prst. Při autentizaci byly úspěšné všechny odlitky, které byli pozitivně použité při testu senzoru U.are.U 4000.

Obr. 20: Zleva: živý prst, želatinový prst a prst ze zinkoklihu.

4. Želatina

Při testování bylo opět nutné velmi citlivě s pomocí obrazovky přiložit odlitek prstu, aby byla autentizace úspěšná (viz obr. 20). Při autentizaci byly úspěšné všechny odlitky, které byly pozitivně použité při testu senzoru U.are.U 4000.

Obr. 21: Špatně přiložený otisk ze zinkoklihu.

Zhodnocení

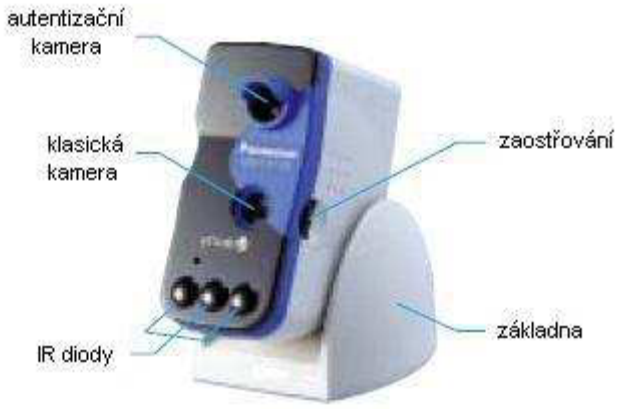
Při testování jsem se přesvědčil, že tento typ senzoru je velmi citlivý na aktuální stav kůže a sám jsem byl několikrát odmítnut z důvodu příliš vlhkých prstů (viz obr 21). Autentizace pomocí zinkoklihu a želatiny byla možná díky podobným vlastnostem jaké má kůže. Tedy obdobný kapacitní odpor. I kdyby se nám podařilo získat odlitek od oprávněného uživatele pořád by nám chyběla karta. Tento systém je totiž založen na dvou faktorech autentizace tedy na vlastnictví předmětu a na biometrické vlastnosti své osoby. V našem případě tedy prst s kartou, na které je uložen náš zakódovaný biometrický etalon. Díky tomu se tato autentizace může využívat v systémech se zvýšenými nároky na bezpečnost. Tento systém je také v USA certifikován pro použití k identifikaci ve státní správě, což dokládá jeho bezpečnost. Součástí testu byl i pokus čtyř osob o přihlášení se pod můj profil, ve kterém jsem měl zaregistrovány všechny prsty, přičemž ani jedné osobě se pod žádným jejím prstem nepodařilo přihlásit

4.3 Autentizace podle duhovky

K testování byla využita kamera Panasonic Authenticam™, využívající k identifikaci software od společnosti Iridian Technologies a I/O software SecureSuite™, umožňující více uživatelům bezpečný přístup k počítači, souborům, složkám a aplikacím. Využívá autentizaci one to one. Tato kamera je mimo jiné určena k integraci s Iridian technologií KnoWho™ autentizačních serverů umožňující autentizaci one to many, ty využívají databáze typu Oracle 8i, Microsoft SQL Server 7.0 nebo Microsoft SQL Server 2000. KnoWho™ autentizační servery mohou přijímat obraz duhovky pocházejících ze systému s certifikací Iridian nebo přímo IrisCode™ záznam. Tato kamera se dá také využít pro video konference. Iridian Technologies nabízí na svých stránkách také Software Developer Kit, umožňující integraci do dalších aplikací. SDK je k dispozici pro C++ a Javu.

Aby zařízení získalo Iridian certifikaci musí splňovat kamera a softwarové řešení minimální systémové požadavky na kritický výkon, součinnost s jinými aplikacemi, bezpečnost, zabezpečení, škálovatelnost, použitelnost, spolehlivost a odolnost. Pozitivní certifikace pro bezpečnost tedy znamená, že zajišťuje dodržování Iridian certifikace a průmyslové standardy pro kryptografickou a fyzickou bezpečnost. Ochranu a

neporušitelnost biometrických údajů v průběhu celého zpracování. V případě kamery znamená certifikace podporu: jednotné Application Programming Interface (např.: z důvodu přístupu do KnoWho™), PrivateID paketové standarty a v případě bezpečnosti využití šifrování 3DES. IrisCode šablony mají velikost 512B nebo možnost uložení přímo obrazu duhovky, kde se velikost pohybuje okolo 12kb. Díky takto malé velikosti IrisCode šablony je schopen systém s procesorem DualCore 2,2GHz prohledat 285.000 záznamů za sekundu.



Obr. 22: BM-DT-120E.

Parametry BM-DT-120E:

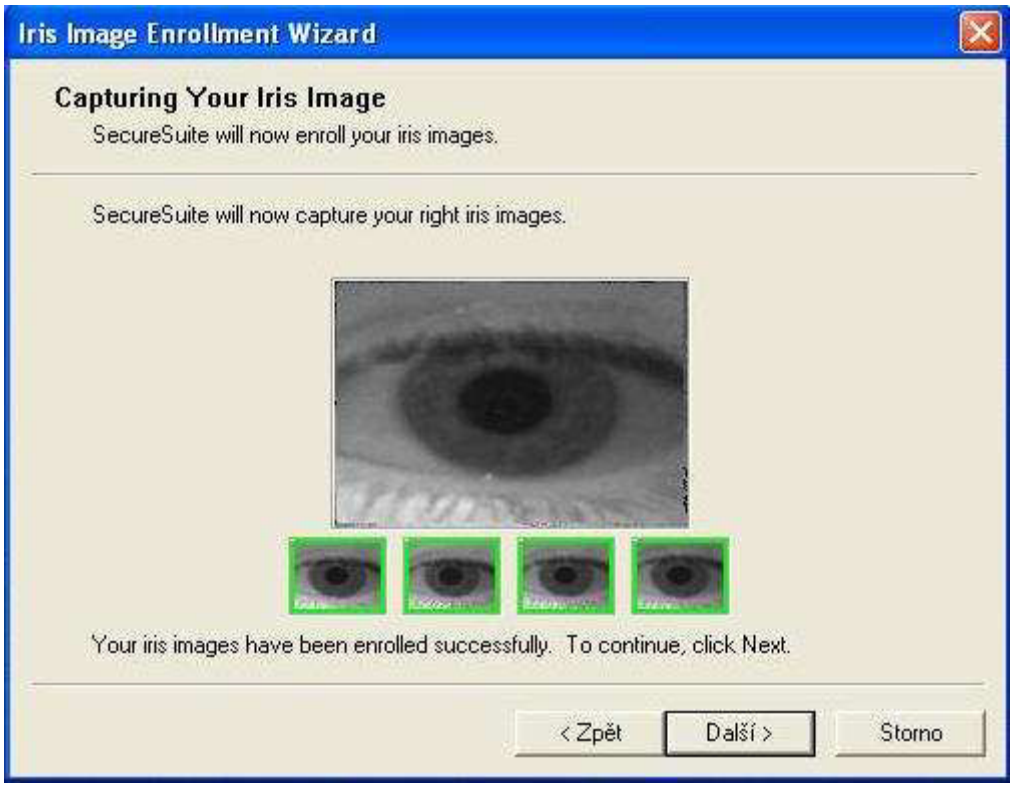
Rozhraní: USB 1.1
Rozlišení CCD: 640x480
Provozní intenzita osvětlení: 40-10000 lux
Maximální hloubka šedé: 8-bit (256 úrovní šedé)
Obraz: Monochromatický
Rozměry (ŠxVxH): 4,2x9x7,4cm
Provozní teplota: 5–35° C
Provozní vlhkost: 20–80 % při 30° C

Systémové požadavky:

CPU Pentium3 450MHz
CD-ROM pro instalaci
256MB RAM
40MB na disku
Microsoft ® Internet Explorer 4.x nebo vyšší pro používání SecureSession

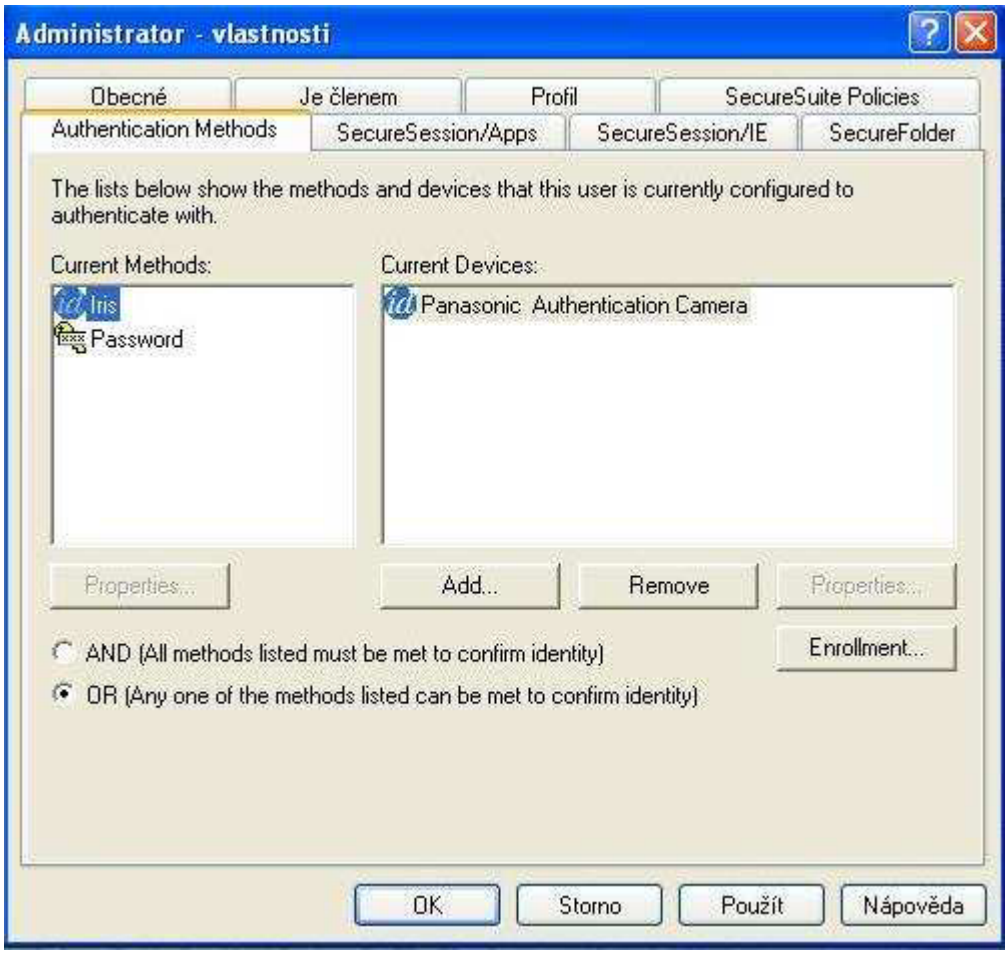
SecureSuite™ tvoří tyto dílčí programy:

-SecureLogon™ pro místní přihlášení k PC, podporuje až šest uživatelů.
-SecureSession™ pro zabezpečení bankovního internetového účtu.
-SecureFolder™ pro zabezpečení složek a souborů.
-SecureApp™ pro zabezpečené spuštění aplikace.



Obr. 23: Registrace duhovky.

V administrátorském režimu po nainstalování SecureSuite 3.1 z přiloženého CD a restartování počítače se spustí software, který vyzve k vytvoření biometrického etalonu. Hned první překážka může být pro některé uživatele fakt, že program je kompletně v angličtině a neumožňuje českou lokalizaci. Jako první musíme zvolit jednu ze tří možností, kterou bude program snímat: levé oko, pravé oko, levé a pravé oko. Po výběru se zobrazí instrukce s vyobrazením. Konkrétně jde o informace o pozici snímaného oka vzhledem ke kameře a to tak, abychom viděli v kameře oranžový kruh kolem černého kotouče. Dále o vzdálenosti, ta by měla být 18–21cm a měli bychom být blíže kameře a pomalu se od ní hlavou vzdalovat dokud oranžový kruh nezezelená a po té vydržet v této poloze zhruba 2–3s, potřebné k sejmutí jednoho snímku ze čtyř. A jako poslední jsou to informace o brýlích, ty bychom měli při vytváření biometrického etalonu odložit. Po potvrzení přečtení informací se nám zobrazí další okno, ve kterém již dochází k samotnému získání snímku duhovky. Je potřeba získat čtyři dostatečně kvalitní snímky oka, jinak budeme vyzváni k opětovnému sejmutí čtyř nových snímků duhovky. Pokud jsme byli úspěšní, tak se z těchto snímků vytvoří IrisCode. Následně spustíme program SecureSuite manager, který slouží ke správě všech účtů na počítači, tedy jak administrátorského tak dalších uživatelů. Zde můžeme aktivovat možnost autentizace pomocí duhovky. Na výběr je samozřejmě i součinnost autentizace pomocí hesla i duhovky. Dále můžeme pro jednotlivé profily povolovat funkce které poskytuje SecureSuite 3.1 (viz výše).



Obr. 24: SecureSuite manager.

Pokud v SecureSuite manageru nastavíme autentizační metodu pomocí hesla i duhovky, budeme vždy při spouštění aplikace nebo systému nejdříve požádání o zadání hesla viz obr. 25. Vyvolání tohoto okna, trvá 15–20 sekund, a pokud se budeme chtít autentizovat duhovkou, musíme stisknout klávesovou zkratku Ctrl+Shift+S. Vyvolání přihlašovacího okna pro oko trvá dalších 5 sekund a samotná autentizace zabere zkušenějšímu uživateli 2 sekundy. Při využívání pouze autentizace oka je tato doba obdobná, tedy 20–25 sekund pro vyvolání autentizačního okna a další 2 sekundy pro rozpoznání duhovky.

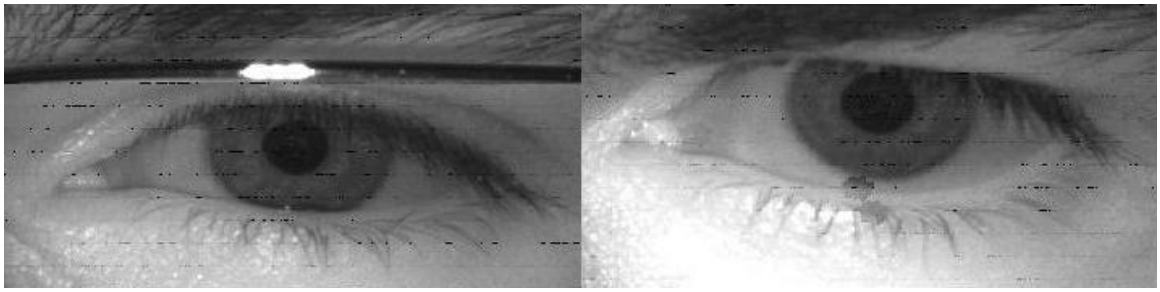
Obr. 25: Žádost o autentizaci.

Testování bezpečnosti:

K pokusu o překonání zabezpečení byla pořízena fotografie detailu oka za obdobných světelných podmínek jako etalon a vytisknuta v poměru 1:1 ke skutečnosti. Fotografie byla vytištěna na matný a lesklý fotopapír, dále pak běžný barevný tisk na inkoustové tiskárně na běžný kancelářský papír. Při pokusu byli všechny fotografie umístěny do předepsané vzdálenosti 19–21cm. Při autentizaci byly poprvé vzorky směrovány podle obrazovky, která ukazuje aktuální snímanou oblast a po druhé byla vyříznuta z fotky zornice skrz, kterou jsem se díval pro určení správné pozice. Ani v jednom případě však nebyl zaznamenán úspěch. To je způsobeno využitím tří infradiod, které vyzařují záření z pásma NIR (Near Infrared=780–2400nm). Obvykle se pro naše účely využívá vlnová délka 750–1000nm, ale výrobce žádnou hodnotu neudává. Oko spolu s částí obličeje je ozářeno tímto zářením a podle odrazivosti, která je dána vztahem

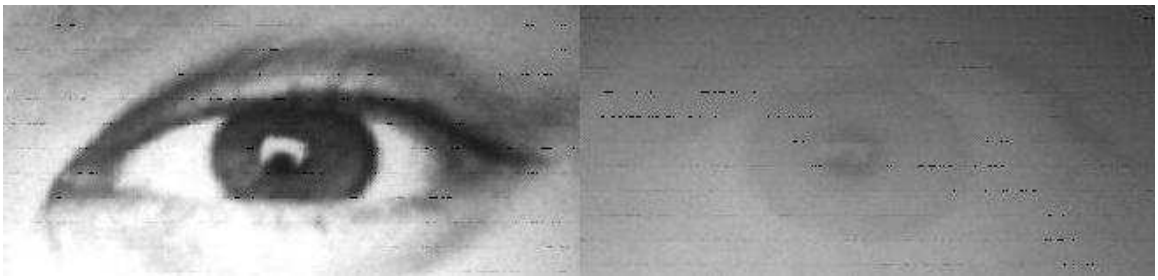
$$\rho = \frac{\Phi_o}{\Phi} \ [-], \qquad (3) \ [39]$$

kde Φo je odražený světelný tok a Φ je dopadající světelný tok. Toto záření odráží v různé míře na CCD snímač, takže získáme obraz ve stupních šedé. Nejsvětlejší místa tedy odpovídají bodům s největší odrazivostí, tmavá naopak. Je nutné si uvědomit, že intenzita odraženého záření je modulována odrazivostí snímaných předmětů, vlnová délka dopadajícího a odraženého záření se však nemění. Monochromatické světlo se také využívá z důvodu lepšího rozeznání detailů tvaru a jasu. Z principu kamery je jasné, že by bylo nutné vytvořit fotografii se stejnou nebo velmi podobnou odrazivostí jakou má skutečná duhovka. To by bylo velmi obtížné jelikož odrazivost se určuje velmi obtížně, proto jsem vyzkoušel dostupné možnosti a dále se již tímto nezabýval.



Obr. 26: Zleva: oko s brýlemi a oko bez brýlí.

Součástí bezpečnostního testu byl i pokus o přihlášení pod můj profil dalšími pěti osobami. Tyto pokusy byli neúspěšné. U pěti osob byla rovněž ověřena pravdivost tvrzení, že člověk má odlišnou pravou a levou duhovku. Tato skutečnost se potvrdila.

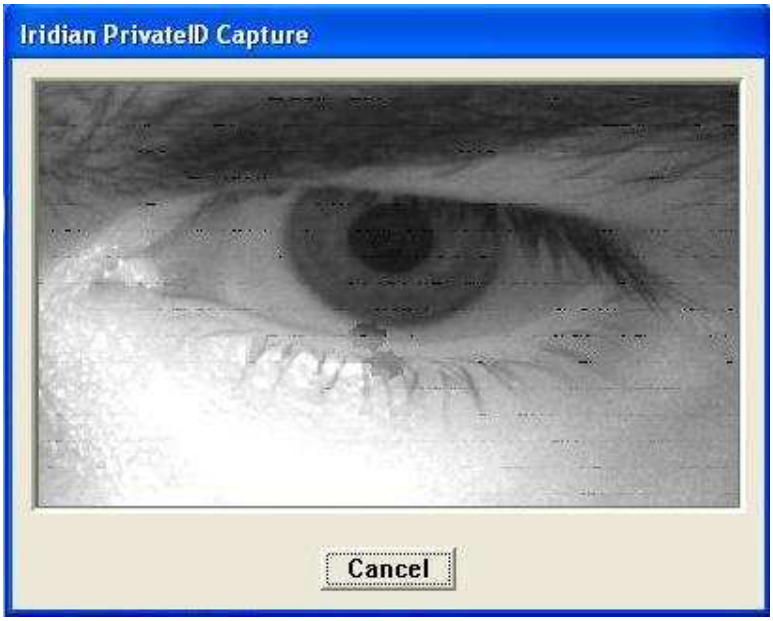


Obr. 27: Zleva: oko na klasickém 80g/m^2 papíru a oko na fotografickém papíru.

Zhodnocení:

Při instalaci z důvodu poškozeného CD, došlo ke zhroucení Windows. Naštěstí bylo k dispozici jiné CD s ovladači. Sejmutí biometrického etalonu musí být bez přerušení. Pokud má někdo problémy s očmi a po dvou nasnímaných obrazech si bude potřebovat odpočinout, byť jen na krátkou dobu, bude vytvoření etalonu neúspěšné. Osobně jsem měl s tímto také problém, jelikož jsem nikdy před tím neměl s touto autentizaci zkušenost a ani ze široka otevřené oko nestačilo ke správnému sejmutí duhovky musel jsem si prsty víčka od sebe odtáhnout, což je velmi nepříjemné a spolu s hledáním správné polohy vedlo k tomu, že jsem musel sejmutí opakovat hned několikrát, než jsem byl úspěšný. Program SecureSuite má strohou grafiku, ale přehledné ovládání, což je nejdůležitější. Ovládání účtů i nastavování funkcí bylo naprosto bezproblémové, je však potřeba říci, že doba potřebná ke spuštění autentizační obrazovky, ať při spouštění aplikace nebo zakódování souboru je velmi dlouhá a pokud budeme využívat autentizaci duhovky a ne jenom hesla což je velmi pravděpodobné tak, tato doba dále narůstá. Při autentizaci jsem již nemusel mít rukou rozevřené oko, což vede ke zlepšení uživatelské pohodlí, i samotná autentizace je rychlejší a při větší zkušenosti to je otázka dvou vteřin, tedy zhruba na stejné úrovni jako autentizační systém od digitalPersona.

Po zkušenosti si myslím, že se jedná o velmi bezpečný autentizační systém (výrobce udává hodnotu FAR 0,0000833), který by ale měl pracovat na silnějších strojích, aby prodleva při spuštění autentizace nebyla příliš velká. Využití je především v oblastech se zvýšenými nároky na bezpečnost, než pro domácí využití.



Obr. 28: Snímání duhovky při autentizaci.

4.4 Dynamika stisku kláves

Na internetu se mi podařilo objevit na stránkách firmy Biopassword Inc. demoverzi jejich autentizačního programu. Pro stáhnutí z internetu [40] musíte mít emailový účet od společnosti Google nebo Yahoo. Následně jsem již nainstaloval demoverzi, která je určené pouze k vyzkoušení principu autentizace pomocí dynamiky stisku kláves. Po spuštění programu je nutné se zaregistrovat. K tomu je potřeba zadat přihlašovací jméno a heslo, obojí s minimální délkou osmi znaků a to vše zopakovat patnáctkrát. Čím vícekrát se zopakuje právě toto zadávání tím lépe dokáže algoritmus zjistit Vaši dynamiku stisku

kláves při psaní daného slova. Tento parametr je však pro potřeby demoverze nastaven na hodnotu 15 stejně jako úroveň bezpečnosti, která je nastavena na hodnotu 4. Ani jednu z těchto hodnot nelze změnit. Úroveň bezpečnosti se jinak může nastavovat v rozmezí 1–10, přičemž hodnota 10 znamená největší úroveň zabezpečení, tedy co nejvíce požadovaná shoda s etalonem. Je škoda, že demoverze neumožňuje nastavení úrovně bezpečnosti, ale pro obraz o schopnostech této biometrické metody to postačí.

Obr. 29: Registrace.

Pro potřeby otestování programu, byli zvoleny dvě přihlašovací sekvence. Jedna s běžným slovem: laborator, které sloužilo zároveň jako přihlašovací jméno a heslo. Důvod volby byl především jednoduchost pro psaní majitele hesla, protože toto přihlašovací jméno a heslo již delší dobu využívá v práci. Díky tomu byl dán předpoklad, že se dále nebude měnit rychlost ani styl psaní tohoto slova. Zjištěná hodnota FRR by tedy měla být menši než pro druhou přihlašovací sekvenci. Dále byla zjištěna hodnota FAR pro útočníka. Tato hodnota byla zjištěna pro případ znalosti hesla a v druhém případě byla zjištěna při znalosti hesla a rytmu úhozů majitele hesla. Druhá přihlašovací složitější sekvence byla tvořena pro majitele dosud nepoužívaným řetězcem slov, pro přihlašovací jméno: xflidr02 a pro heslo: Project2009. Pro obě tyto sekvence platí, že týden po registraci byli zjištěny hodnoty FRR a FAR. Tato ochranná doba byla volena z důvodu simulace, kdy přihlášení opět využijeme až několik dní po registraci. K zjištění dynamiky úhozů byl natočen záznam pomocí fotoaparátu Nikon Coolpix S51c, ze vzdálenosti 1m od klávesnice a pod úhlem 45° proti rovině stolu s notebookem a bočním úhlem 45° proti přímce LCD klávesnice. Útočník měl k dispozici 20 minut pro cvičné naučení dynamiky stisku kláves z pořízeného záznamu. Následně došlo ke spuštění programu BioPassword a 25 pokusům o přihlášení se.

Obr. 30: Zamítnutí, z důvodu špatné dynamiky úhozů.

Pro první přihlašovací sekvenci vychází pro majitele hesla FRR 8% (viz tab. 16). Následně se útočník se znalostí hesla pokusil o přihlášení. Byla zjištěna hodnota FAR 4%. V případě znalosti dynamiky stisku kláves z pořízeného záznamu byla zjištěna hodnota FAR 40%.

Tab. 16: Jednoduší přihlašovací sekvence.

	Majitel hesla	Útočník bez znalosti úhozů	Útočník se znalostí úhozů
Počet úspěšných přihlášení	23	1	10
Počet neúspěšných přihlášení	2	24	15

Pro druhou přihlašovací sekvenci vychází pro majitel hesla FRR 8% (viz tab. 17). Útočník měl k dispozici stejné podmínky jako v předchozím případě. Bez znalosti dynamiky úhozů byla zjištěna hodnota FAR 24% a se znalostí dynamiky úhozů byla hodnota FAR 16%.

Tab. 17: Obtížnější přihlašovací sekvence.

	Majitel hesla	Útočník bez znalosti úhozů	Útočník se znalostí úhozů
Počet úspěšných přihlášení	23	8	4
Počet neúspěšných přihlášení	2	17	21

Zhodnocení

Jedná se o velmi zajímavou metodu, která navyšuje bezpečnost přihlášení klasickým heslem. Velká výhoda spočívá v možnosti utajení pro útočníka, který nemusí mít zdání o tom, že na pozadí běží tato autentizace a samozřejmě ve snadné implementaci do stávajících klasických přihlašovacích systémů, nevyžadující žádné další hardwarové prvky. Uživatelský komfort a bezproblémové přihlášení budou mít především zkušenější uživatelé, kteří již mají ustálený rytmus dynamiky stisku kláves. Dosažené výsledky byli zjištěny pro nastavení bezpečnosti na hodnotu 4. Zjištěná hodnota FRR 8% je nad očekávání dobrá. Překvapila i skutečnost, že tato hodnota zůstala stejná pro novou dosud nepoužívanou přihlašovací sekvenci. Hodnoty FAR nabývají bez znalosti dynamiky úhozů hodnot 4–24%. Znalost dynamiky stisku kláves je možné zužitkovat jen částečně. Postačí pouze k částečné korekci rozložení pozice prstů při psaní, avšak samotná dynamika je i přes to velmi těžko napodobitelná, a závisí především na podobnosti stylu

psaní těchto dvou osob a štěstí útočníka. Napodobení majitele hesla se povedlo při jednodušší přihlašovací sekvenci, kdy byla zjištěna hodnota FAR 40%, při obtížnější 16% to bylo dokonce méně než bez znalosti.

Z tohoto výsledku je jasně patrná křehká hranice mezi úspěchem a odmítnutím při pokusu o napodobení majitele hesla. Tyto výsledky je nutno brát jen jako orientační, jelikož se jedná o metodu, která patří do skupiny behaviorálních metod. Proto by při opakování testu vyšly tyto hodnoty pro útočníka odlišně.

5 Návrh systému bezpečné autentizace

Pod slovem bezpečná autentizace je možné si představit různá řešení. Je důležité před vlastním návrhem znát požadavky, které budeme klást na takový autentizační systém, tedy jak velká budou bezpečnostní rizika. Jsou zde ale i další požadavky a to technické a finanční.

Do technických požadavků můžeme zařadit kvalitu zpracování, standardizaci, tedy splnění biometrických norem BS ISO/IEC 19794-X[4], záruku a podporu na zakoupený systém, obtížnost obsluhy a rychlost autentizace.

Do finančních pak řadíme pořizovací cenu, školení, upgrade softwaru, logistickou podporu a cenu provozu.

Do bezpečnostních patří parametry FAR a FRR. Dále použité kódování, šifrovaní a protokol pro přenos sítí. Výkonný přehledový management sítě a zabezpečení pro rozpoznání živého biometrického znaku.

Při předpokladu využívání systému i staršími osobami, kteří nemusejí mít zkušenost s počítačem mohu rovnou pominout autentizaci pomocí dynamiky stisku kláves. Pro ně už bývá problém zapamatovat si heslo a po zkušenosti aby tato autentizace měla smysl, musela by být totožnost dynamiky úhozů s etalonem velmi podobná, což by pro laiky bylo velmi obtížné a koeficient FRR by byl neúnosně vysoký.

Stejně tak mohu vypustit autentizaci pomocí sítnice a duhovky, kde je vyžadována velká míra spolupráce. Obecně lze tedy říci, že čím vetší je míra spolupráce vyžadována, tím zkušenější musí být uživatel. Taková autentizace využívaná širokou veřejností může být možná pouze s asistencí. Osobně si myslím, že se hodí spíše ke kontrole osob při vstupu do přísně střežených objektů finančních společností, výzkumných ústavů, věznicích a vojenských objektů. Bezpečnost by se určitě navýšila, pokud by byla součástí osobních dokladů, ať už cestovních pasů, pracovních povolení pro cizince, občanských průkazů nebo databáze vyhoštěných osob cizí národnosti. Vzhledem k unikátnosti a extrémně vysoké ne-li nemožné možnosti padělání, vidím uplatnění především při zjišťování totožnosti policií a úřady, kde je možná asistence vyškoleného personálu. Pro příklad lze uvést využití autentizaci pomocí duhovky v SAE při kontrole na hranicích zda dotyčná osoba nepatří do databáze nevyžádaných nebo hledaných osob.

Při autentizaci pomocí otisku prstu, která je v dnešní době nejrozšířenější a je založena na vysoké jedinečnosti každého otisku prstu, je důležité, aby systém disponoval technologií, která s jistotou rozpozná padělek otisku a také výkonným senzorem, který dokáže získat co nejvíce jedinečných znaků a minimalizovat na co nejmenší míru hodnotu koeficientu FAR. Teprve poté bude takový systém naprosto bezpečný. Toto by mohla splňovat multispektrální technologie snímání otisku (viz str.34). Tu jsem ale neměl

[4] V současné době je deset norem, definují především způsob měření jedinečných biometrických znaků, jejich ukládání a předávání.

možnost ověřit. Výhodou autentizace pomocí otisku prstu, je její převaha na trhu a díky tomu nízká cena.

Osobně mě nejvíce z používaných biometrických metod zaujala verifikace pomocí struktury žil na ruce (viz str.19). Sice jsem neměl možnost jí vyzkoušet, ale i přes to si myslím, že tato metoda splňuje většinu požadavků, které se od autentizačního systému požadují. Vysoká míra jedinečnosti dokládá rozsáhlé využití této biometrické metody v Japonsku k verifikaci osob v nemocnicích, univerzitách a bankomatech. Bezkontaktní princip má vysokou míru hygieničnosti. Princip spočívá ve snímání cévního řečiště, které je ukryto v ruce. Je obtížná jeho duplikace a výhodou je také intuitivnost při verifikaci, kdy stačí přiložení ruky pod senzor.

6 Závěr

Na začátku práce se jsem se zaměřil na popis obecných postupů při získávání etalonu, možnosti jeho uložení a obecné činnosti biometrických autentizačních systémů. Podařilo se mi popsat většinu dosud známých biometrických metod využívaných v současnosti pro autentizaci žadatele o přístup do systému. U jednotlivých metod jsem se pokusil uvést historii jejich vývoje, princip, vlastnosti a příklad využití v praxi. U některých metod se mi nepodařilo zjistit jejich výkonnostní parametry z důvodu nedokončeného ověření spolehlivosti nebo monopolu některých firem na danou technologii a neochoty zveřejňovat dosažené parametry.

Při testování biometrických metod byla zjištěna největší bezpečnost u autentizace pomocí duhovky, kterou se jako jedinou z testovaných nepodařilo oklamat. Byla potvrzena odlišnost levé a pravé duhovky, stejně jako jedinečnost duhovky u každého člověka, kdy se testu účastnilo šest osob. Autentizace pomocí dynamiky kláves navyšuje bezpečnost používaných hesel, bez nutnosti jakýchkoli hardwarových nároků, což umožňuje její snadnou implementaci. Pro dvě přihlašovací sekvence byla zjištěna hodnota FRR a FAR při znalosti hesla. Hodnota FRR v obou případech nabývala hodnoty 8%. Hodnota FAR byla v prvním případě 4% a ve druhém 24%. Velký rozptyl hodnoty FAR je daný nastavením zabezpečení na hodnotu 4 z maximálního možného nastavení bezpečnosti při hodnotě 10. Velký vliv má také podobnost stylu psaní a náhoda při změně dynamiky stisku kláves s cílem docílit shody s majitelem hesla. V případě autentizace pomocí otisku prstů bylo zjištěno, že odlitek otisku prstu z želatiny nebo zinkoklihu dokáže nahradit živý prst při autentizaci a to jak u kapacitního snímače tak optoelektronického snímače. Pro optoelektronický snímač, jež snímá plochu o rozměru 14x18mm byla stanovena minimální plocha potřebná k identifikaci prstu se vzorem papilárních linií typu smyčka jako plocha centrální části otisku o rozměru 8x8 mm. Bylo také zjištěno, že při zastínění centrální části stejného prstu plochou o rozměrech větších jak 4x8mm nebude identifikace úspěšná. U kapacitního snímače byla zjištěna velká závislost na stavu kůže, kdy několikrát došlo k neúspěšné autentizaci z důvodu vlhkých prstů. Součástí testu bylo i ověření jedinečnosti otisku, kdy se čtyři osoby neúspěšně pokusili o přihlášení pod můj vytvořený profil, ve kterém byli zaregistrovány všechny mé otisky.

Při návrhu bezpečné biometrické autentizace byli zužitkovány poznatky získané při praktických testech a teoretické znalosti o biometrických metodách. Jako optimální vidím autentizaci pomocí struktury žil na ruce a s výhradami autentizaci pomocí otisku prstu. Pro velmi vysoké zabezpečení pak pomocí duhovky. Systém využívající jednu z těchto metod není potřeba jistit další biometrickou metodou, jelikož všechny tyto metody využívají dostatečně jedinečné znaky člověka. Důraz musí být proto kladen na kvalitní snímač a algoritmus pro vyhodnocení.

Použitá literatura

[1] MIROSLAV, Skoumal. IDENTIFIKACE ČLOVĚKA POMOCÍ BIOMETRICKÝCH ÚDAJŮ. [s.8.], 2007. 50 s. Vedoucí bakalářské práce PaedDr. Zdeněk Pejsar Ph.D. Dostupný z WWW: <http://minsky.ic.cz/veci/identifikace_cloveka_pomoci_biometrickych_udaju.pdf>.

[2] ŠČUREK PH.D., Mgr. Ing. Radomír. Biometrické metody identifikace osob v bezpečnostní praxi. Studijní text. 2008, č. čj, s. 18.

[3] Oko [online]. c1996-2008 , 2008 [cit. 2008-12-12]. Dostupný z WWW: <http://encyklopedie.seznam.cz/heslo/141448-oko>.

[4] RNDR.KROLUPPER, Filip. Biometrie oční sítnice [online]. 2005-2008 , 2008 [cit. 2008-12-11]. Dostupný z WWW: <http://www.biofs.com/cs/s2.php>.

[5] DICKSON, Goh. Multi-Screen Technologies [online]. 2005. 2008 , 2008 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: <http://multiscreentech.com/Technology.htm>.

[6] DAUGMAN, Dr. John. IRIS RECOGNITION [online]. 1998-2008 , 2008 [cit. 2008-12-12]. Angličtina. Dostupný z WWW: <http://www.icdri.org/biometrics/iris_biometrics.htm>.

[7] WILLIAMS, G.. Iris recognition technology [online]. c2005-2008 , 1996 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: <http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel3/4087/11967/00551842.pdf?arnumber=551842>.

[8] RNDR.KROLUPPER, Filip. Biometrie oční sítnice [online]. 2005-2008 , 2008 [cit. 2008-12-11]. Dostupný z WWW: <http://www.biofs.com/cs/s6.php>.

[9] SCHMIDTOVÁ, RNDr. Jana. Morfometrický fotokomparační software [online]. 2006 [cit. 2008-12-12]. Dostupný z WWW: <http://www.biofs.com/cs/mfs.php>.

[10] VLACH, Ing. Jan. Lokalizace obličeje v obraze s komplexním pozadím [online]. 2007 , 2008 [cit. 2008-10-15]. Dostupný z WWW: <http://www.elektrorevue.cz/file.php?id=200000112-66258671fa>.

[11] GOH, Alwyn, NGO, David CL. Computation of Cryptographic Keys from Face Biometrics [online]. 2005 , 2006 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: <http://security.polito.it/cms2003/Program/Goh07/1Goh.pdf>.

[12] GOH, Alwyn, NGO, David CL. Computation of Cryptographic Keys from Face Biometrics [online]. 2005 [cit. 2008-12-12]. Dostupný z WWW: <http://security.polito.it/cms2003/Program/Goh07/1Goh.pdf>.

[13] MAINGUET, Jean-François. Face recognition / Reconnaissance du visage : Facial thermogram / Thermogramme du visage [online]. 2006-2008 , 2008 [cit. 2008-12-12]. Dostupný z WWW: <http://pagesperso-orange.fr/fingerchip/biometrics/types/face.htm>.

[14] ARUN, JAIN, PANKANTI. A Hand Geometry-Based Verification System [online]. 2004 , 2008 [cit. 2008-10-15]. Angličtina. Dostupný z WWW: <http://biometrics.cse.msu.edu/hand_proto.html>.

[15] ŠČUREK PH.D., Mgr. Ing. Radomír. Biometrické metody identifikace osob v bezpečnostní praxi. Studijní text. 2008, č. čj, s. 58.

[16] WATANABE, Masaki, et al. Palm vein authentication technology and its applications [online]. Fujitsu Laboratories Ltd., c2005-2008 , 2008 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: < http://www.biometrics.org/bc2005/Presentations/Conference/1%20Monday%20September%2019/Poster%20Session/Watanabe_1568964435_BioSymposium_2005.pdf >.

[17] ŠČUREK PH.D., Mgr. Ing. Radomír. Biometrické metody identifikace osob v bezpečnostní praxi. Studijní text. 2008, č. čj, s. 29.

[18] Knuckle profile indentity verification system [online]. c2004-2008 , 2008 [cit. 2008-12-12]. Angličtina. Dostupný z WWW: <http://www.patentstorm.us/patents/5594806/claims.html>.
[19] JIROTKA, Antonín. Obrázky prstů [online]. c2005 , 2005 [cit. 2008-12-12]. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/2003/casopisy/pol/0503/afis305_info.html>.
[20] Obrazce a znaky kůže [online]. 2006 , 2003 [cit. 2008-12-12]. Dostupný z WWW: <http://sweb.cz/krimi-spk/02_exper/expertiz/02a_dakt/02a_kuze.htm>.
[21] RNDR.KROLUPPER, Filip. Biometrie otisků prstů [online]. 2005-2008 , 2008 [cit. 2008-12-11]. Dostupný z WWW: <http://www.biofs.com/cs/s3.php>.
[22] POLÁČKOVÁ, Zuzana. Rešerše algoritmů pro snímání a zpracování otisku prstů [online]. c2008 [cit. 2009-02-15]. Dostupný z WWW: <https://dip.felk.cvut.cz/browse/pdfcache/polacz1_2008bach.pdf>.
[23] ĎÁSEK, Milan. Biometrika [online]. 2003 , 26.2.2003 [cit. 2009-05-15]. Dostupný z WWW: <http://www.volny.cz/pretorian/biometrika.html#x81>.
[24] [NIXON, CORCORAN, ROWE. Biometric Identity Determination using Skin Spectroscopy [online]. 2004 , 2008 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: <http://www.lumidigm.com/PDFs/Biometric%20Identity%20Determination%20using%20Skin%20Spectroscopy.pdf>.]
[25] OLIVADOTI, William. FORGET FINGERPRINTS [online]. 2006 , 2008 [cit. 2008-12-12]. Angličtina. Dostupný z WWW: <http://homeautomation.0catch.com/_webimages/homeautomation.html>.
[26] YARNITZKY, Prof. David. BDS™ Application Kit & BDS™ SDK [online]. 2006-2008 , 2008 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: <http://www.idesia-biometrics.com/products/app_kit.html>.
[27] BioDynamic Reader [online]. 2004 [cit. 2008-12-12]. Angličtina. Dostupný z WWW: <ftp://ftp.aladdin.com/pub/marketing/eToken/Factsheets/FS_eToken_BDReader.pdf>.
[28] [Voice Key Technology [online]. c2007 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: <http://www.speechpro.com/eng/company/processing-technologies/voice-key-tech>.]
[29] KASPROWSKI, Paweł, OBER, Jozef. Enhancing eye movement based biometric identification method by using voting classifiers [online]. 2007 [cit. 2008-12-12]. Dostupný z WWW: <http://cat.inist.fr/?aModele=afficheN&cpsidt=17134800>.
[30] KAPCZYńSKI, KASPROWSKI, KUźNIACKI. Modern access control based on eye movement analysis and keystroke dynamics [online]. 2006. 2007 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: <http://www.proceedings2006.imcsit.org/pliks/126.pdf>. ISSN 1896-7094.
[31] [LEJTMAN D., GEORGE E., Handwritten signature verification using wavelets andback-propagation neural networks [online]. 2001. c2008 , 2008 [cit. 2008-12-11]. Angličtina. Dostupný z WWW: <http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/7569/20622/00953934.pdf?temp=x>.]
[32] [Český lékopis 2002. Sv. 5. Praha : Grada Publishing a.s., 2002. ISBN 80-247-0464-1. Zince oxidi gelatina mollis, s. 5646–5647.]
[33] [Český lékopis 2002. Sv. 4. Praha : Grada Publishing a.s., 2002. ISBN 80-247-0464-1. Zinci oxidum, s. 4604–4605.]
[34] [Český lékopis 2002. Sv. 3. Praha : Grada Publishing a.s., 2002. ISBN 80-247-0464-1. Gelatina, s. 2702–2705.]

[35] [Český lékopis 2002. Sv. 3. Praha : Grada Publishing a.s., 2002. ISBN 80-247-0464-1. Glycerolum 85%, s. 2753–2755.]
[36] [Český lékopis 2002. Sv. 2. Praha : Grada Publishing a.s., 2002. ISBN 80-247-0464-1. Aqua purificata, s. 1495–1497.]
[37] Precise Biometric [online]. 5.11.2007 , 14.5.2009 [cit. 2009-05-15]. Dostupný z WWW: <http://www.precisebiometrics.com/drivers.aspx>.
[38] Precise Biometric : Driver [online]. c2000 , 14.5.2009 [cit. 2009-05-15]. Dostupný z WWW: <http://www.precisebiometrics.com/demo.aspx>.
[39] DOBROVOLNÝ, Petr. Spektrální chování objektů [online]. 2005 [cit. 2009-05-15]. Dostupný z WWW: <http://www.geogr.muni.cz/archiv/vyuka/DPZ_CVICENI/Texty/DPZ_03_spektralni_chovani.pdf>.
[40] Smart Advisors [online]. c2005 [cit. 2009-05-15]. Dostupný z WWW: <http://smartadvisors.net/biopassword/demo.php>.

Seznam zkratek

BDS	BioDynamic Signature
DNA	Deoxyribonukleová kyselina
ERR	Křížový koeficient
FAR	Koeficient neoprávněného přijetí
FRR	Koeficient nesprávného odmítnutí
IR	Infračervené záření
LCD	Liquid crystal display
RGB	Červená-zelená-modrá
SAE	Spojené arabské emiráty
SDK	Software Developer Kit