Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Biometrické autentizační metody

Ivana Staňková

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Ivana Staňková

Veřejná správa a regionální rozvoj

Název práce

Biometrické autentizační metody

Název anglicky

Biometric authentication methods

Cíle práce

Cílem této závěrečné práce je zejména vytvořit přehled aktuálně používaných autentizačních metod založených na biometrice včetně používaných technologií snímačů biometrických příznaků, vyhodnocování a chybovost autentizace atd. Také prozkoumejte praktické využití biometrických autentizačních metod a navrhněte libovolnou aplikaci.

Metodika

Seznámení se s problematikou autentizace člověka pomocí biometrických příznaků, prostudování používaných metod a vypracování jejich podrobného přehledu. Rovněž se autor zaměří na návrh identifikačního systému, který by bylo možné použít v praxi a porovná jej s běžně používanými systémy. Dále za pomoci dostupných prostředků vybrané běžné autentizační metody otestuje proti neoprávněné autentizaci.

Doporučený rozsah práce

40

Klíčová slova

biometrie, biometrické metody, verifikace, přístupový systém, zabezpečení

Doporučené zdroje informací

DAUGMAN, J. How iris recognition works. Proceedings of 2002 International Conference on Image Processing, pp. 33-36, 2002.

DODDINGTON, G. R. Speaker recognition – Identifying people by their voices. Proceedings of IEEE, vol. 73, no. 11, pp. 1651-1664, 1985.

ROSS, A. – JAIN, A. K. Human Recognition Using Biometrics: An Overview. Annals of Telecommunications, vol. 62, no. 1-2, pp. 11-35, 2007.

ŘÍHA, Z. – RAK, R. – MATYÁŠ, V. *Biometrie a identita člověka ve forenzních a komerčních aplikacích.* Praha: Grada, 2008. ISBN 978-80-247-2365-5.

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 19. 11. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 20. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 05. 03. 2017

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Biometrické autentizační metody" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 15. března 2017 _____

Poděkování

Děkuji svému vedoucímu práce, Ing. Tomášovi Vokounovi, za cenné rady při vypracování této práce a odborné vedení.

Biometrické autentizační metody

Souhrn

Tato práce se zabývá popisem a výčtem používaných biometrických metod za účelem autentizace uživatele. Z dostupných informací a softwarových nástrojů byly vybrány čtyři biometrické parametry, které byly dále prakticky otestovány na vytvořené databázi o rozsahu 20 osob. Z provedených experimentů dosáhla nejlepších hodnot efektivity identifikace metoda analýzy otisku prstu. Rozpoznání mluvčího, identifikace uživatele dle hlasu, taktéž získala zajímavé výsledky, leč ve srovnání s biometrií otisku prstu dosáhla o přibližně o třetinu menší hodnoty efektivity. Z naměřených výsledků byly rovněž vypočteny intervaly příslušných statistických parametrů pro objektivnější zhodnocení metod. I přes velice dobré výsledky se biometrické metody ukázaly jako příliš časově náročné a ne příliš spolehlivé, aby je bylo možné aplikovat pro praktické využití např. ve společnosti. Z tohoto důvodu je tedy nutné ještě jejich další vývoj, avšak je lze momentálně doporučit jako další úroveň zabezpečení pro jednotlivé uživatele.

Klíčová slova: biometrie, rozpoznávání, autentizace, identifikace, verifikace, otisk prstu, dynamika stisku kláves, obličej, hlas

Biometric authentication methods

Summary

This thesis is focused on the list of used biometric methods and their description in the case of user authentication. From available software tools and information, four biometric parameters were chosen to further practical testing on created database containing 20 persons. By performed experiments, the fingerprint analysis achieved the best efficiency results and the speaker identification obtained promising results as well, but significantly lower than for fingerprint analysis. The intervals of probability for desired statistical parameters were calculated from experimentally achieved results for their conclusion in more objective point of view. Despite the interesting results were achieved, biometric authentication methods cannot be recommended to be fully implemented in some practical cases, e.g. in companies, because of its latency and recognition efficiency. Thus, they have to be more developed, but for single user, they can be recommended as a higher level of current security.

Keywords: biometry, recognition, authentication, identification, verification, fingerprint, keystroke dynamics, face, voice

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Bezpečnost může být definována jako odolnost člověka /věci/ komunity, apod. vůči nepříznivým vlivům, zneužitím, atd. To znamená, že bezpečnost je vztažena zejména tam, kde by mohlo dojít k poškození čehokoliv zranitelného a cenného. Jindy je bezpečnost definována jako forma ochrany, která je tvořena separací subjektu od hrozby. Tato separace je obecně nazývána kontrolou a obsahuje vztahové změny právě mezi subjektem a hrozbou (ISECOM, 2016).

Hlavním cílem této bakalářské práce je zaměření se právě na vytvořenou separační (kontrolní) část, kterou obecně nazýváme zabezpečením. V dnešní době, kdy má majetek nejen materiální, ale i značně se rozvíjející virtuální hodnotu, je velice aktuální téma tzv. kyberbezpečnosti, a jak již z názvu této bakalářské práce vyplývá, kyberbezpečnost, resp. počítačové zabezpečení využívající biometrické informace bude zde detailně popisováno a analyzováno.

I když je zabezpečení založené na biometrii na vzestupu, je však nejprve nutné prozkoumat ostatní metody zabezpečení, aby bylo možné počítačové zabezpečení využívající biometrické informace vhodně zařadit, neboť otázka zabezpečení sahá daleko do historie- až k samotným počátkům člověka.

2 Cíl práce a metodika

2.1 Cíl práce

Jak již bylo nastíněno zadáním této bakalářské práce, jejím hlavním cílem této je zejména vytvořit přehled aktuálně používaných autentizačních metod založených na biometrice včetně používaných technologií snímačů biometrických příznaků, vyhodnocování a chybovost autentizace, a zejména praktické otestování dostupných vhodných softwarových nástrojů. Praktické poznatky budou vyhodnoceny vzhledem k aktuálnímu zabezpečení jedné vybrané společnosti.

2.2 Metodika

Za pomoci dostupných poznatků a sofwarových nástrojů bude vybráno několik biometrických metod, které dále budou testovány z hlediska úspěšnosti autentizace a pohodlnosti pro uživatele při zadávání jeho identity, resp. efektivity snímání. Všechny dostupné nástroje, které budou mít potencionální využití pro praktickou aplikaci ve vybrané společnosti, budou důkladně otestovány na vytvořené databázi tvořenou 20 osobami.

3 Teoretická východiska

3.1 Zabezpečení

Jak bylo v samotném úvodu k této práci zmíněno, kořeny otázky zabezpečení sahají daleko do historie několik milionů let před naším letopočtem. Ochranu majetku tedy můžeme najít už od doby, kdy začal člověk brát rozum, kdy se začal usazovat na jednom místě a kdy začal shromažďovat materiální věci.

Z počátku byla za účelem zabezpečení člověka a jeho okolí využívána zvířata (zejména psi) a jednoduché mechanické nástroje, které se postupem času stávaly více sofistikovanými a rozměrově menšími. Chronologický vývoj nejstarších mechanických metod zabezpečení lze lehce naznačit např. takto:

Palisáda, kterou lze definovat jako kolovou hradbu z kmenů zaražených do země těsně u sebe, byl velmi významný obranný prvek, který však nedokázal dlouho odolávat trvalému obléhání či ohni.

Padací most můžeme označit jako zabezpečovací prvek obranného opevnění, který umožňuje zamezení nepovolaného přístupu pomocí zvednuté mostové části.

Závora – prvek se značně omezenou zabezpečovací schopností, které je spíše informativní charakteru, resp. k varování na neoprávněný přístup, neboť jej lze snad prolomit i bez jakéhokoliv poškození. Závora je díky efektivnosti předání varování o nepovoleném vstupu a jednoduchosti využívána dodnes, zejména u železničních přejezdů, přístupových cest na zemědělské pozemky atd. Vhodné je také zmínit, že postupem času prošla závora určitým vývoje, a tak je nyní často poháněna elektřinou a ovládána řídící jednotkou.

Mechanický zámek prošel oproti předchozím příkladům mechanického zabezpečení značnou minimalizací, která je doprovázena vysokou efektivitou poskytnutí zabezpečení proti neoprávněnému přístupu. Mechanický zámek můžeme naleznout ve dvou variantách, a to jako pevný či visací. Oba tyto druhy je možné naleznout na dveřích, nábytku, vozidlech apod. Důležité je také zmínit, že mechanický zámek se používá jako primární zabezpečení elektronických zařízení před jejich odcizením. Obvykle se uvolňuje klíčem nebo číselnou kombinací.

Důležitým milníkem pro rozvoj používaných metod zabezpečení byl objev elektrického proudu a jeho následná distribuce. Příklad tohoto progresu byl již zmíněn výše u závory, ale mnohem důležitější dopad měl elektrický proud na vývoj elektroniky, která byla následně

používána či přímo implementována do zabezpečovacích zařízení. Díky tomuto rozvoji bylo možné zabezpečovací prvky rozměrově zmenšit, ale také značně zvýšit jejich účinnost, neboť používání diskrétních (digitálních) signálů u elektroniky umožňuje použití komplikovanějších otevíracích posloupností, využití dalších prvků (příznaků) k prolomení zabezpečení či využití vyššího stupně zabezpečení (šifrování) pro ochranu klíče před zneužitím.

Elektronický zámek má tedy stejnou funkci jako klasický mechanický. Skládá se ze dvou částí- řídící jednotky a klíče, který je nosičem identifikátorů a slouží k odemknutí zámku. Klíč může mít jak fyzickou (přístupová karta), tak i imaginární podobu (např. číselný kód). Obdobné formy realizace může mít i samotný zámek, kdy nemusí mít pouze hardwarovou podobu, ale může to být i pouhý software, který můžeme najít u různých aplikací od internetového obchodu počínaje přes firemní systém plánování dovolené až u elektronického bankovnictví konče. U elektronických zámků je tedy nejdůležitější softwarová, popř. firmwarová část, která se stará o vyhodnocování a zabezpečení daného objektu za použití zvolených příznaků. Nejvíce sofistikované elektronické zámky využívají zabezpečení na základě biometrických znaků, kdy je za použití vhodného čidla (snímače) převeden požadovaný fyziologický parametr na digitální signál, který je pak dále zpracován a analyzován. Příklad elektronického zámku, který využívá a nevyužívá biometrické příznaky, je zobrazen na Obr. 1.

Obr. 1 Příklad elektronických zámků (TechFresh, 2011), (Zicom, 2014).

3.2 Vyhodnocování přístupu

Vyhodnocování přístupu je velice důležitou procesní částí zabezpečení. Na základě špatné klasifikace během vyhodnocovací fáze může dojít k neoprávněnému přístupu (ekvivalent tzv. missed detection) či chybnému zamítnutí přístupu (ekvivalent tzv. false

alarm). V této fázi zabezpečení je využíváno několik různých klasifikátorů, od nejjednodušších, které jsou založené na přímém porovnání vzoru s aktuální hodnotou, až po složitější vyhodnocovací nástroje, které využívají neuronové sítě či strojové učení pro udělení či zamítnutí přístupu na základě zkoumaných příznaků. V problematice zabezpečení je vyhodnocovací stupeň složen ze dvou dílčích částí, autorizace a autentizace, jejichž vlastnosti a rozdíly jsou rovněž popsány níže.

3.2.1 **Identifikace**

Dle literatury (Rak, 2008), je identifikace definována jako využití jedinečných, měřitelných, fyzikálních nebo fyziologických znaků (příznaků) nebo projevů subjektu k jednoznačnému zjištění identity. Pro identifikační účely se tedy využívají anatomické nebo fyziologické charakteristiky, které jsou pro každý subjekt co nejvíce unikátní a časově neměnné. Identifikace je proces porovnávání a ztotožnění (v zahraničních referencích nazýván jako One–To–Many–Matching (Krhovják, 2007), tzn. jeden k mnoha či 1:*n* recognize) nasnímaného subjektu. V našem případě rozpoznávání osob dochází k porovnání biometrického vzorku se všemi referenčními šablonami, které jsou uložené v databázi (seznamu, apod.) a vedou ke zjištění, který referenční vzor z databáze odpovídá zkoumanému subjektu. Identifikující biometrická aplikace tedy rozpozná totožnost zkoumané osoby.

Identifikaci dále dělíme na pozitivní a negativní v závislosti na požadovaném výstupu identifikačního procesu. Jednotlivé typy identifikace jsou definovány následovně:

Pozitivní identifikace - Cílem pozitivní identifikace je zabránit používání identity jedné osoby dalšími osobami (to znamená, že je nezbytné zabránit, aby docházelo k prokazování se osob pomocí jiné identity). Z toho tedy vyplývá, že pokud biometrická aplikace využívající princip pozitivní identifikace v procesu porovnávání nenajde shodu mezi šablonou předkládaného (např. biometrického) vzorku s žádnou referenční šablonou uloženou v databázi, výsledkem je odmítnutí přístupu či oprávnění uživatele do objektu, počítačové sítě apod. Ztotožnění obou šablon naopak znamená přijetí uživatele (Rak, 2008).

Negativní identifikace - Naopak negativní identifikace má za cíl vyloučení nežádoucího stavu, kdy jeden subjekt využívá identitu více subjektů, což znamená např. zabránění osobě vydávat se za jinou osobu. Jestliže biometrická aplikace, která využívá princip negativní identifikace v procesu porovnání, nenajde shodu mezi šablonou uloženou v databázi, výsledkem je přijetí přístupu (oprávnění) uživatele. Ztotožnění vzoru a aktuálního posloupnosti naopak znamená odmítnutí uživatele (Rak, 2008).

Princip funkčnosti pozitivní a negativní identifikace je pro větší přehlednost znázorněn v Tab. 1.

Tab. 1 Charakteristika rozdílu mezi pozitivní a negativní identifikací (Rak, 2008).

Pozitivní identifikace	**Negativní identifikace**
Cílem je prokázat, že „já jsem“ již registrován v systému, databázi apod.	Cílem je dokázat, že „já nejsem“ registrován v systému, databázi (a není tam registrován ani nikdo jiný s touto identitou).
Porovnání mnou předložené šablony s jedinou referenční šablonou. Jedná se o verifkaci.	Mnohonásobné porovnání mnou předložené šablony se všemi podobnými s cílem vyloučit nalezení případného duplikátu šablony.

3.2.2 **Verifikace**

Proces verifikace může být definován jako ověření identity člověka, tedy proces přímého porovnávání (tzv. One–To–One Matching, jeden ku jedné, či 1:1 autentizace) jediné šablony, která je vytvořena ze získaných příznaků subjektu, s jedinou referenční šablonou/vzorem, který právě náleží zkoumanému subjektu. V našem případě opět považujeme za subjekt nějakou konkrétní osobu, a zkoumané příznaky mají biometrický charakter. Cílem verifikace je tedy zjistit, zda zkoumaný subjekt je skutečně tím, co tvrdí, za kterou se vydává či se jinak navenek jeví. Detailnější popis verifikace lze nalézt v literatuře, např. v (Jain, 2008) či (Mlýnková, 2015).

3.2.3 **Identifikace vs. Verifikace**

Jak již bylo zmíněno, v běžném životě jsou tyto dva rozlišovací procesy zaměňovány. Z tohoto důvodu je na místě velmi lehce nastínit ty nejpodstatnější rozdíly a vlastnosti, které rozlišují identifikaci od verifikace a naopak. Ve stručnosti lze tedy říci, že:

Identifikace – jde o porovnávání aktuálního subjektu se subjekty v databázi. Tento proces je velmi často označován jako One-To-Many, a pracuje na principy vyhledávání co největší (největšího počtu) shody, aby určil přesnou identitu aktuálního prvku pomocí vytvořené databáze. Proces identifikace je typicky využíván ve forenzních aplikacích, lékařské diagnostice atd.

Verifikace – je přímý proces ověřování totožnosti aktuálního subjektu s přímým vzorem. Jedná se tedy o porovnání typu One-To-One. Verifikačním procesem nedochází k zařazení subjektu jako v případě identifikace, ale k ověření, zda-li se skutečně jedná o vzorek s oprávněním k autentizaci. Proces verifikace můžeme typicky nalézt v bezpečnostních aplikacích komerční sféry.

3.2.4 **Autentizace**

Prvním stupněm vyhodnocovací fáze v oblasti zabezpečení se nazývá autentizace, kterou můžeme jednoduše definovat jako samotný proces ověření identity zkoumaného objektu. V běžném životě se s autentizací setkáváme např. na úřadech při prokazování totožnosti na základě identifikačních dokumentů, při ověřování platnosti webových stránek na základě digitálních certifikátů, pravosti předmětů na základě výskytu unikátních značek a jejich tvaru, apod. Je tedy patrné, že se s procesem autentizace lze setkat v nejrůznějších situacích. V oblasti informačních technologií je proces autentizace spojován s žádostí udělení přístupu k některým datům či funkcím používaného systému.

Metody autentizace můžeme rozdělit do tří skupin:

První skupina metod využívá pro samotnou autentizaci důkazy třetích stran, které jsou důvěryhodné a dokážou potvrdit či vyvrátit identitu zkoumaného subjektu. V praxi si tak můžeme představit svého kamaráda, nadřízeného, rodinného příslušníka či jiného svědka. V digitálním světě využívají tyto metody svědectví certifikačních autorit, pomocí kterého jsou některé webové stránky označeny jako tzv. web of trust, či identita jednotlivců může být potvrzena digitálním podpisem využívajícím schválené kryptografické klíče.

Druhá skupina metod využívá přímé porovnání parametrů a jeho vzoru. V této skupině si tedy můžeme představit např. stanovení stáří předmětu na základě chemické spektroskopie, určení pravosti listinného dokumentu na základě jeho čitelnosti a výskytu obrazových artefaktů, určení identity osoby na základě jeho otisku prstů, rozboru řeči či jiných biometrických parametrů.

Třetí skupina metod využívá tzv., řetěz důkazů, pomocí kterého je stanovena identita subjektu. V běžném životě lze tuto skupinu metod naleznout ve forenzních aplikacích (policejní či detektivní vyšetřování atd.), během kterých je získává sled (posloupnost) důkazů vedoucí k prokázání či vyvrácení identity šetřeného subjektu. V oblasti informačních technologií využívá tato skupina záznamy o průběhu jednotlivých kroků procesu, tzv. logu, aby byla ověřena pravost výstupního signálu, resp. vytěžených dat.

Všechny výše uvedené tři skupiny autentizačních metod využívají pro svou správnou funkčnost pozorování určitých faktorů, které napomáhají ke správnému výsledku celého ověřovacího procesu. Tyto faktory jsou nazývány jako autentizační faktory, které dále můžeme rozdělit do tří různých skupin (Čermák, 2009):

Vědomostní faktory (knowledge factors), mezi které se řadí informace, jež subjekt zná, jako jsou heslo (celé či jen část), vstupní formule (např. „Sezame, otevři se!“), PIN (u bankovních karet, SIM karet atd.) či bezpečnostní otázka, resp. správná odpověď na ní (např. v případě zapomenutého hesla u e-mailové schránky).

Vlastnické faktory (ownership factors), mezi které se řadí především dokumenty prokazující dané oprávnění. Tyto dokumenty mohou míst různou formu. Nejčastěji se jedná o přístupové karty/odznaky (firemní řešení) a softwarové či hardwarové přístupové klíče (tokeny).

Dědičné faktory (inheritance factors), mezi které se řadí zejména již dříve zmíněné biometrické prvky (otisk prstů, povrch duhovky, řeč, DNA a jiné unikátní bioelektrické signály) či podpis.

Z předchozího stručného seznamu je patrné, že lze využít mnoho různých autentizačních faktorů ze tří různých skupin. Je obecně dáno, že robustní autentizační systémy využívají analýzu faktorů nejméně ze dvou skupin. Úroveň autentizačního procesu také záleží na stupni zabezpečení, kde je používán set jednoho či několika faktoru z jedné či více skupin (viz výše). Se samotnou myšlenkou autentizace v oblasti informačních technologií přišla v 70. letech minulého století firma IBM, která navrhla, aby byl uživatel ověřen na základě něčeho, co zná, co vlastní, nebo na základě jeho fyzické charakteristiky.

Podle počtu použitých faktorů a autentizačních metod, rozlišujeme jednofaktorovou (nejslabší), dvoufaktorovou (silnější) či multifaktorovou (nejsilnější) autentizaci. Podrobný popis těchto jednotlivých typů autentizace je uveden v literatuře, např. v (Ross, 2007).

Autentizaci také dále dělíme podle způsobu ověřování subjektu na identifikaci a verifikaci. V praxi jsou velmi často tyto dva procesy zaměňovány, a tudíž je nezbytné vysvětlit mezi nimi zásadní rozdíl.

3.2.5 Autorizace

Autorizaci lze považovat za druhou část vyhodnocovacího stupně. Jedná se o udělení oprávnění (získání přístupu) k dané operaci, kterou může být např. přístup ke konkrétním

datům, do určitých prostor, přístup k funkcím atd. V oblasti informačních technologií je autorizace využívána pro řízení přístupu k souborům a adresářům, nastavení změn systému a jeho funkcí atd., aby se zabránilo možnému zneužití dat či odvádění pozornosti zaměstnanců stranou od pracovní činnosti.

3.3 Biometrie

Jak již bylo zmíněno výše při popisu jednotlivých ověřovacích metod, k určení pravosti subjektu jsou vybírány nejvíce unikátní příznaky v rámci zkoumané databáze. To znamená, že korelace vybraných příznaků nabývá co nejnižší kladné (či co nejvyšší záporné) hodnoty korelace napříč databází/populací. Ideálně je hodnota korelace rovna nule. Tohoto předpokladu, že pro každého člověka jsou některé příznaky zcela unikátní a neměnné, využívá právě biometrie, kterou lze definovat jako metodu autentizace založenou právě na biologických příznacích (morfologické a fyziologické).

Slovo biometrie je odvozeno z řeckých slov bios (život) a metron (měření), z čehož vyplývají právě předchozí tvrzení. I přes uvedená pozitiva má biometrie značnou nevýhodu v tom, že v případě vyzrazení charakteristik zkoumaných parametrů, nelze je měnit tak jako je tomu např. u hesel, čipů atd. Detailnější popis biometrie včetně výkladu a popisu jednotlivých částí kaskády biometrické autentizace lze nalézt v příslušné literatuře (Jain, 2008).

Obecně má tento proces biometrického ověření identity několik fází. První, či nultá fáze, je definování zkoumaných příznaků. To znamená, že je nutné si uvědomit náročnost, chybovost a využitelnost dané autentizační aplikace v požadovaném prostředí. Ne vždy je vhodné (ať už z finančních či efektivních důvodů) používat analýzu otisku prstu, povrchu duhovky atd. Autentizační proces využívající zvolené biometrické příznaky se skládá z následujících úrovní:

- Snímání (sběr vstupních dat)
- Přenos dat a analýza příznaků
- Klasifikace
- Uložení dat (vytvoření tzv. logu)

Následující část práce popisuje jednotlivé biometrické (fyziologické či morfologické) příznaky, které jsou v dnešní době využívány ať už komerčně, či pouze ve výzkumné fázi.

3.3.1 **Biometrické příznaky**

Jelikož jsou v běžné praxi jednotlivé kroky autentizačního procesu (viz předchozí strana) skryty pod co nejvíce sofistikovaným zařízením, které se skládá z hardwarové části (snímač, napájení, řídící elektronika atd.) a softwarové části (zpracování vstupních signálů, klasifikace, vytvoření logu atd.), tak se tato část bakalářské práce bude věnovat právě samotným biometrickým příznakům. U jednotlivých příznaků bude samozřejmě uveden i princip vytěžování jednotlivých příznaků, použité snímače pro jejich konkrétní vytěžení atd.

V zahraničních publikacích se lze setkat s termínem feature, který právě stojí za českým ekvivalentem příznak. Biometrické příznaky lze tedy rozdělit do dvou skupin, dle jejich charakteristiky, a to na:

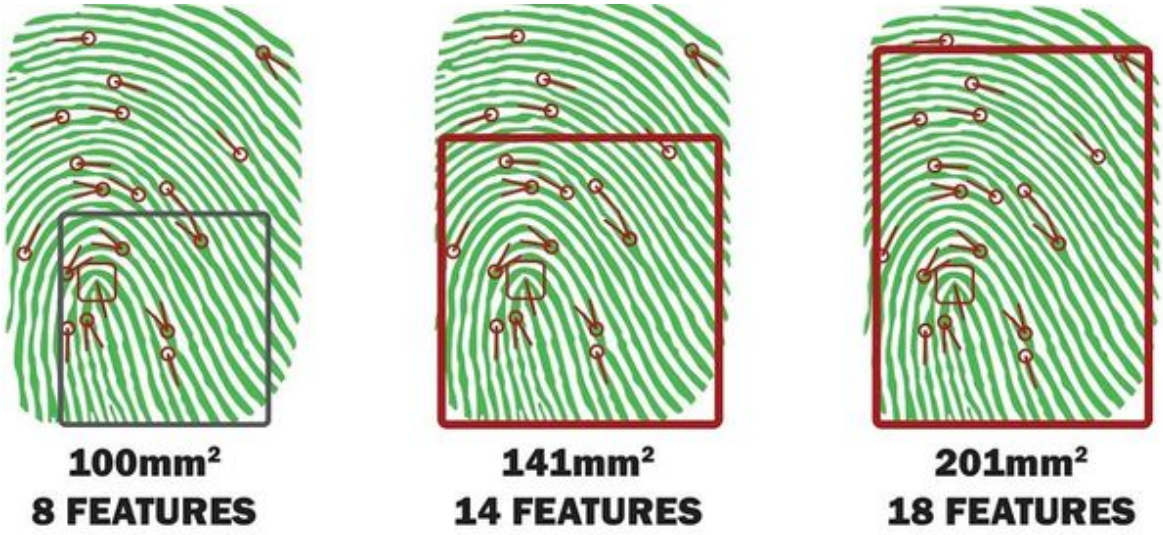
Biologické, které popisují jedince na základě jeho unikátních fyziologických/anatomických parametrů.

Behaviorální, které popisují jedince na základě jeho unikátních vlastností (chování). Tyto příznaky zcela evidentně nejsou dány pouze fyzickými parametry, ale i zkušenostmi, které jedinec nabývá během života. Jak již bylo u biometrických příznaků obecně napsáno, tyto parametry jsou unikátní, avšak jejich nevýhodou je, že jsou proměnné v čase (Flídr, 20009).

3.3.2 **Otisk prstu**

Otisk prstu je nejrozšířenější biometrickou metodou autentizace. Je zde využívána analýza papilárních linií každého otisku prstu, resp. jsou zde vyhledávány prohlubně a hřebeny snímaného otisku prstu. Obr. 2 červeně znázorňuje příznaky získané na základě analýzy papilárních linií, a také jak moc velký set těchto příznaků je možné analyzovat v závislosti na velikosti snímače, což zajisté vede k možné větší robustnosti autentizačního systému. Jakmile je získán obraz daného otisku prstu, je pak dále zpracován a analyzován jako dvourozměrný objekt (obraz). Metody, princip zpracování a analýza obrazů je detailně popsána např. v [Russ, Image processing handbook].

Princip činnosti používaným snímačů je převod optické informace na informaci elektrickou (data). Na základě pohybu ruky při snímání otisku prstu můžeme senzory rozdělit na statické, u kterých je prst pouze přiložen na kontaktní plochu snímače po dobu alespoň 1 s, a dynamické, u kterých dochází k přejetí (tzv. swipe) posledního článku prstu od jeho kořene po špičku určitou rychlostí. Statické snímače můžeme naleznout např. na mobilních telefonech, a dynamické se často používají na noteboocích.



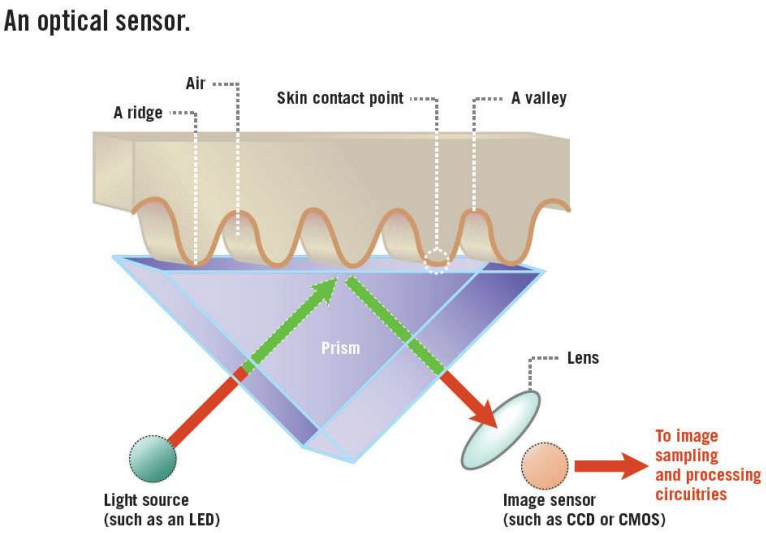
Obr. 2 Počet příznaků otisku prstu na analyzované ploše (Next Biometrics, 2016).

Na základě získávání elektrické informace, jednotlivé typy snímačů rozlišujeme na:

Optické – tyto senzory považujeme za nejstarší v oblasti snímání tisků prstů. Princip získání otisku prstu je stejný jako u fotografie akorát s tím rozdílem, že je tento snímač, na rozdíl snímače integrovaného ve fotoaparátu, více kontrastnější z toho důvodu, aby byl obraz papilár správně pořízen. Stejně jako u digitálních fotoaparátů, i zde platí, že vyšší rozlišení snímače je schopné pojmout více detailů otisku prstu, což se může promítnout ve výsledku autentizačního procesu. Papilární linie, které jsou na snímku zachyceny, jsou pak dále analyzovány vhodně zvolenými algoritmy. Nedílnou součástí tohoto typu snímače jsou i LED diody, které přiložený prst vhodně osvětlí, aby byly papiláry co nejkvalitněji zachyceny.

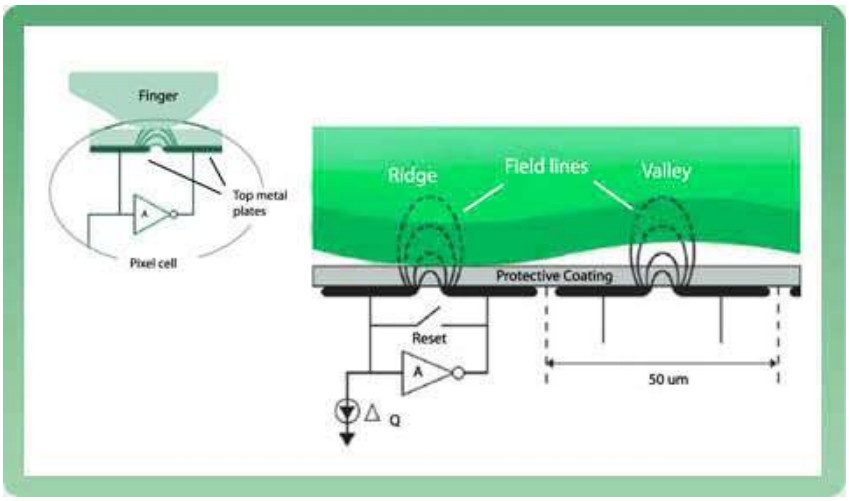
Důležité je zmínit, že tento typ senzorů může být oklamán např. vytištěným otiskem prstu či nějakou jinou vhodnou kopií. Na druhou stranu není výroba toho typu snímače nákladná, a tudíž může být aplikovatelný i tam, kde je kladen velký důraz na cenu oproti zabezpečení.

Princip činnosti optických senzorů otisků prstu je ilustrován na Obr. 3.



Obr. 3 Příklad principu optického snímače (Android Authority, 2016).

Kapacitní – tyto senzory využívají vzniklých kapacit mezi vrcholkem a prohlubní papilární linie pro získání představy jak otisk prstu ve skutečnosti vypadá. Principiálně se tedy nevytváří obraz otisku prstu, ale uchovávají se informace o velikosti uchovaného náboje v síti kapacitorů (kondenzátorů) snímače, resp. v místě dotyku vrcholku otisku prstu dochází ke změně náboje na snímači, kdežto v prohlubni nikoliv. Každá změna je pak následně za pomoci analogově/digitálního převodníku zpracována na vhodný formát elektrické signálu pro další zpracování. Tento princip je znázorněn na Obr. 4.



Obr. 4 Příklad principu kapacitního snímače otisku prstů (Zvetco Biometrics, 2016).

Kapacitní snímač je obecně velmi bezpečný, neboť k jeho prolomení je potřeba nejen stejný motiv otisku, ale i materiál se stejnými vlastnostmi (např. permitivitou) jaké má lidská tkáň. Výroba tohoto druhu snímače je nákladnější, a tudíž i ve výsledku je vyšší prodejní cena. Kapacitní snímače otisku prstů se momentálně používají zejména v mobilních telefonech.

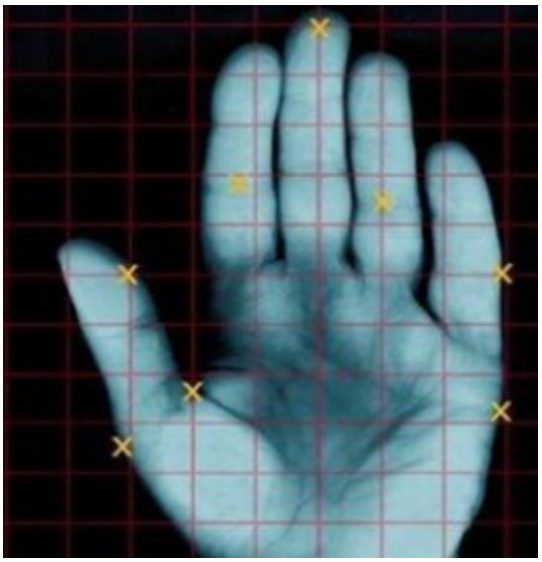
Ultrazvukové – tyto snímače se řadí mezi nejnovější technologie v oblasti pořizování snímku papilárních linií. Jejich velké pozitivum lze spatřit v tom, že pro správné pořízení snímku papilárních linií není zapotřebí zcela čistých a suchých rukou jako v předchozích případech. Ultrazvukový snímač využívá pro detekci výskytu vrcholků a prohlubní papilárních linií odrazu ultrazvukové vlny. Tedy, v případě prohlubně urazí odražená vlna větší vzdálenost než v případě vrcholku, a tudíž později dopadá na povrch snímače. Z principu jeho činnosti je tedy patrné, že každý snímač má v sobě integrován generátor ultrazvukového vlnění. Jelikož se jedná o stále vyvíjenou technologii, je nasazení ultrazvukových snímačů otisků prstu v praxi minimální, a jejich pořizovací cena je vysoká. Toto je však vykoupenou vysokou spolehlivostí a efektivitou v autentizačních procesech.

3.3.3 Geometrie ruky

Rozměr dlaně a prstů je další biometrický znak, který může vést k úspěšné autentizaci osob. Jelikož se obvykle měří celá ruka, resp. její délka, šířka a tloušťka včetně jednotlivých prstů, tak použitý snímač nabývá větších rozměrů oproti senzoru otisků prstů, což se promítne i na finální ceně zařízení. Oproti tomu je prolomení této metody autentizace téměř nemožné, neboť je zapotřebí opatřit celý snímek ruky, což není vůbec snadné.

Jak již bylo zmíněno, uvedená metoda autentizace na základě příznaků vytěžených ze snímku geometrie ruky je velmi spolehlivá, ale i finančně nákladná. Proto se tento způsob zabezpečení používá ve zvláštních či výjimečných případech, např. k zamezení přístupu do strategicky významných objektů apod.

Běžně se pro pořízení obrazu ruky používají opto-elektrické CCD snímače, které lze nalézt např. v digitálních fotoaparátech. Zachycený snímek ruky je zobrazen na Obr. 5, kde je červeně ilustrován rastr a žlutými křížky jsou vyznačeny významné body (příznaky) zachycené ruky.

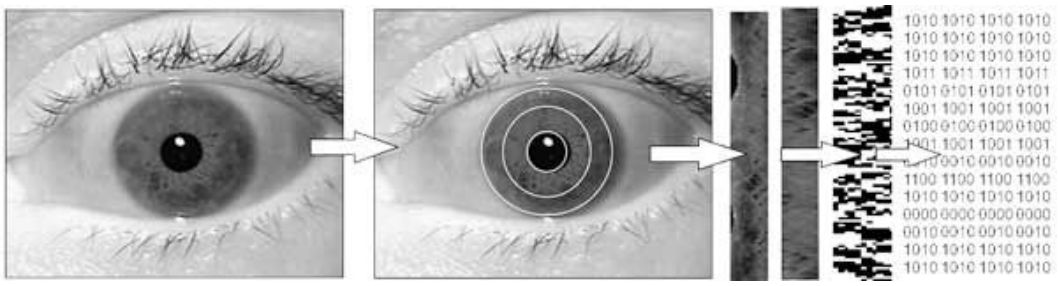


Obr. 5 Snímek geometrie ruky s vyznačenými významnými body (All In One Computing And Electronics, 2016).

3.3.4 **Duhovka**

Oční duhovka patří rovněž mezi unikátní ukazatele identity člověka. Konkrétně se u této metody zkoumá obrazec (pattern) povrchu duhovky, neboť právě motiv povrchu duhovky je pro každého člověka unikátní (Daugman, 2002).

Cílem této metody je za použití až 266 vytěžených příznaků, což je několikanásobně více než u jiných biometrických metod, provést správně autentizační proces. Obraz duhovky je pořízen ze vzdálenosti několika decimetrů snímačem, resp. monochromatickou kamerou, která využívá infračerveného záření k eliminaci odrazů a jiných nechtěných zobrazovacích jevů, a taktéž pomocí tohoto záření dokáže detailně rozlišit strukturu duhovky i u silně pigmentovaných (tmavých) očí. Obrázek 6 znázorňuje analýzu zachyceného povrchu duhovky včetně lokalizace zornice atd.



Obr. 6 Princip analýzy duhovky (Baker, 2010; upraveno).

Tato biometrická autentizační metoda je sice neinvazivní, ale je zapotřebí, aby zkoumaná osoba netrpěla žádnou oční patologickou vadou a měla sundané brýle. Naopak dioptrické kontaktní čočky robustnost této metody nijak zvlášť nedegradují na rozdíl od kosmetických (barevných) kontaktních čoček (Baker, 2010). Autentizaci na základě biometrie duhovky je velice těžké a finančně nákladné integrovat, avšak ve Spojených arabských emirátech je rutinně používána imigračními úřady od roku 2001 a na některých letištích ve Velké Británii, USA a Kanadě byl zahájen její testovací provoz. V současné době je ale nezbytné provést další výzkum a vývoj, aby byla autentizace pomocí duhovky snadněji aplikovatelná a robustnější. Detailnější popis této i jiných biometrických metod lze nalézt např. v (Jain, 2007).

3.3.5 **Sítnice**

Biometrické metody založené na rozpoznávání sítnice disponují mnohem vyšší spolehlivostí a robustností než v případě analýzy duhovky neboť dosud nebyl představen či odkryt způsob jak by bylo možné sítnici duplikovat, neboť každý člověk má unikátní rozprostření cév vycházející z očního nervu do sítnice. Důležité je zmínit, že sítnice se vyvíjí do osmého měsíce života, a od té doby její podoba zůstává unikátní a neměnná po celý život i v případě onemocnění jako je cukrovka, glaukom a jiné.

Sítnice je snímána a dále analyzována podobně jako duhovka. Rovněž se jedná o nízkoenergetické infračervené záření, které prochází do oka subjektu, které je přiloženo blízko snímače. Jelikož cévy na sítnici absorbují jinak tento druh záření než okolní tkáně, je nezbytné, aby toto záření pronikalo do oka cca 15 s. Zajisté je toto velmi dlouhý časový interval, který značně znevýhodňuje použití scanu sítnice při běžných aplikacích stejně tak jako vysoká pořizovací cena. Proto je nezbytný, jako v případě u duhovky, další výzkum a vývoj v této technologické oblasti.

V současnosti se obraz cév sítnice využívá pouze ve vládních autentizačních aplikacích u FBI, CIA a NASA, ale také ve zdravotnictví, neboť podle scanu sítnice je možné diagnostikovat AIDS, neštovice, malárii, atd. Více o využití snímků sítnice v biometrii lze nalézt v literatuře, např. v (Bujnošková, 2011).

Obr. 7 znázorňuje zachycenou sítnici včetně rozložení cév, které jsou v ní obsaženy.

Obr. 7 Snímek sítnice (Wikimedia Commons, 2016).

3.3.6 **Obličej**

Tyto autentizační systémy využívají příznaky geometrie obličeje jako je vzájemná vzdálenost očí, jejich tvar, šířka nosu, relativní výška čela atd. pro účely biometrické identifikace či verifikace. Autentizační metody založené na analýze obličeje může rozdělit v závislosti na použitém snímači na dvou a trojrozměrné.

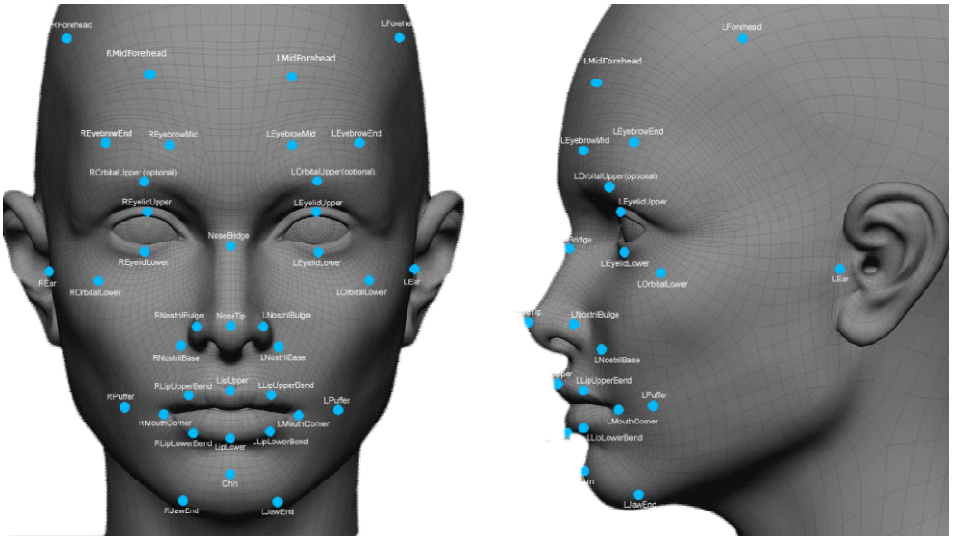
Dvourozměrná analýza obličejových příznaků spočívá ve zpracování fotografie či krátkého úseku videa. Z tohoto principu je patrné, že autentizační systém lze oklamat fotografií, či naopak systém může chybně vyhodnotit obličej ve stínu atd. Pro eliminaci těchto jevů bylo proto zavedeno 3D snímání.

Trojrozměrná analýza obličeje eliminuje předchozí zmínky o vlivu fotografie či stínu na vyhodnocení autentizačního procesu a to v tom důsledku, že je zde měřena a dále vhodně zpracovávána i hloubka určitých částí obličeje jako je třeba oční důlek, velikost brady, hloubka obličeje atd. Také je ohromnou výhodou trojrozměrného snímání fakt, že je možné provést autentizační proces téměř při jakémkoliv úhlu natočení obličeje. Moderní 3D systémy využívají ke snímání obličeje rovnou tři CMOS kamery- jedna frontální, druhá profilová a třetí je naproti frontální natočená ve vhodném úhlu. Jednotlivé snímky jsou pak dále společně analyzovány v průběhu autentizačního procesu. Velkou nevýhodou trojrozměrného snímání obličeje je alespoň částečná spolupráce subjektu při pořizování vhodných snímků jeho obličeje.

Využívané příznaky při biometrické analýze obličeje jsou znázorněny pomocí modrých bodů na Obr. 8. Obecně není autentizace pomocí analýzy obličeje považována za úspěšnou,

neboť její výsledek lze snadno ovlivnit aktuální expresí obličeje, make-upem, stárnutím atd., a tak se mnohdy přechází k analýze textury kůže či analýze obličeje termálními kamerami.

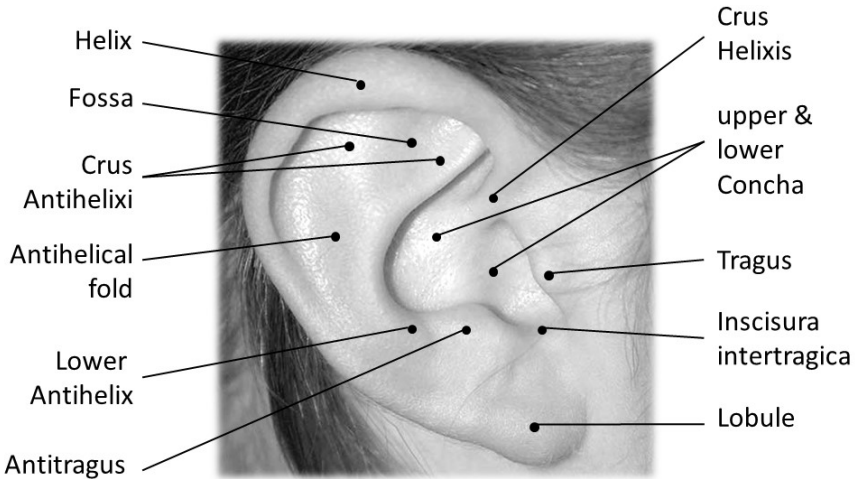
Z výše uvedených důvodů je autentizace pomocí obličejových příznaků zatím využívána pouze na zábavní úrovni či v případech nedůležitého zabezpečení a to ve formě software, který např. poskytují firmy Apple, Adobe, Google, aj. Detailnější informace o biometrii obličeje lze dohledat v literatuře (Jafri, 2009).



Obr. 8 Ilustrace analýzy obličeje (The Privacy Surgeon, 2016).

3.3.7 **Ucho**

Biometrická analýza vnější ucha může velmi úspěšně posloužit pro autentizační účely. Mnohdy se uvádí, že biometrie vnější ucha dosahuje výrazně lepších výsledků než analýza obličeje. Snímání vnějšího ucha je jednoduše proveditelné za pomoci obyčejné kamery či fotoaparátu. Získaný snímek je dále segmentován, zpracován, a za pomoci detekce hran a příslušných algoritmů jsou lokalizovány zkoumané příznaky (viz Obr. 9). Jednotlivé příznaky jsou pak dále zpracovávány a analyzovány jako v předchozích případech a opět je i zde potřebná spolupráce zkoumaného subjektu. Více lze o autentizačních metodách využívající biometrii ucha nalézt v příslušné literatuře, např. v (Pflug, 2012).

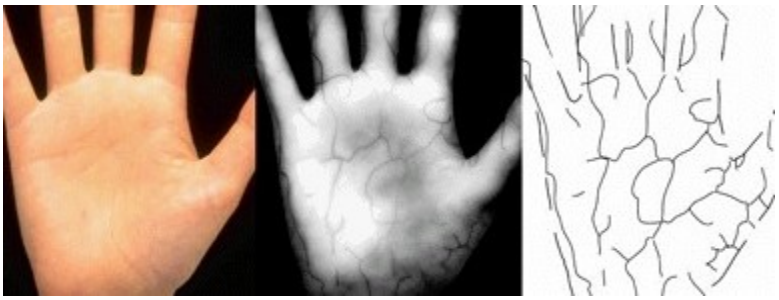


Obr. 9 Významné body analýzy ucha (Pflug, 2012).

3.3.8 **Krevní řečiště**

Analýza krevního řečiště je podobná autentizačním metodám využívající biometrie sítnice s tím rozdílem, že na snímač produkující infračervené záření je přiložen prst či celá ruka. V případě snímání celé ruky pak může skenování krevního řečiště probíhat na dlani či na hřbetu ruky.

Stejně jako u jiných infračervených metod je zachycený snímek krevního řečiště černobílý, resp. v odstínech šedi. V tomto snímku je pak dále zobrazeno rozložení žil, a v této síti jsou pak dále vyhledávány vhodné příznaky pro autentizační proces. Jednotlivé snímky (fáze) analýzy krevního řečiště dlaně jsou zobrazeny na Obr. 10. Detailní popis analýzy krevního řečiště pro biometrické účely je publikován např. v (Lu, 2014).



Obr. 10 Snímek ruky a jejího krevního řečiště (Lu, 2014).

3.3.9 **DNA**

Biometrická analýza DNA za účelem autentizace subjektu je značně časově náročná, a tudíž je pro přístupové procesy, kde je požadována autentizace téměř v reálném čase,

nepoužitelná, a navíc její realizace je velice finančně nákladná. Z tohoto důvodu je používána především ve speciálních, forenzních, aplikacích, které vyžadují autentizaci osoby téměř se 100% jistotou, a nepožadují krátkou dobu ke stanovení výsledku.

I přesto, že je analýza DNA považována za nejspolehlivější autentizační metodu, není vůbec obtížné její potencionální zneužití, neboť v některých případech je snadné získat DNA, za pomocí slin, vlasu, kožního fragmentu, krve, atd., od kýžené osoby. Tudíž je nezbytné vyřešit i tuto otázku (nejen finanční a časovou náročnost) před praktickou aplikací autentizace na základě příznaků DNA v komerční sféře.

Více informací o analýze DNA pro účely biometrie lze nalézt v literatuře, např. v (Jain, 2006).

Předchozí části této sekce popisovaly biologické biometrické znaky. Jak již bylo v úvodu této sekce zmíněno, druhou skupinou biometrických znaků jsou znaky behaviorální, které jsou popsány níže.

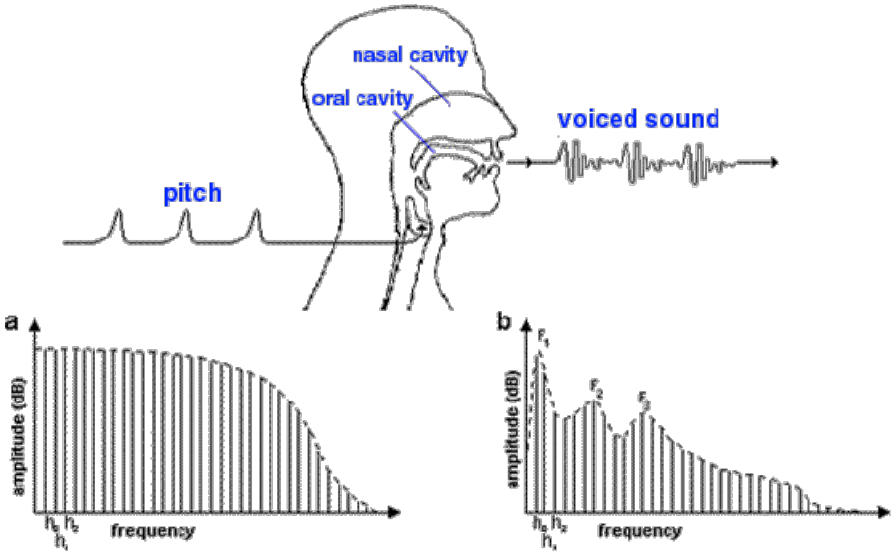
3.3.10 **Hlas**

Hlas můžeme zařadit jak do biologických, tak i do behaviorálních příznaků. Nejprve je nutné pořídit záznam hlasu za pomoci mikrofonu, který slouží v našem případě jako hlavní snímač. Dále je pak tento záznam digitálně analyzován především ve frekvenční oblasti (spektru), kde jsou vyhledávány nejrůznější příznaky jedinečné pro každý subjekt (mluvčího).

Autentizační proces mluvčího probíhá za pomoci analýzy nejrůznějších spektrálních koeficientů či formantů, které lze definovat jako rezonanční frekvence určitý dutin lidského těla. Poloha těchto formantových kmitočtů (především těch vyšších) je unikátní pro každého jedince kvůli unikátnosti stavby těla. Z tohoto důvodu lze biometrii hlasu zařadit i do biologické skupiny.

Pro účely autentizace za použití parametrů hlasu je také používán např. základní kmitočet, který je rovněž někdy označován jako nultý formant. Základní kmitočet určuje, jakou rychlostí kmitají hlasivky, a jelikož je závislý na intonaci, aktuálním emočním stavu, alkoholovém opojení, stresu a lze jej lehce imitovat, je tento parametr užíván pouze jako doprovodný příznak při autentizačních procesech. Analýza základního tónu je naopak běžně používána v detektorech lži, prokázání alkoholové či jiné intoxikace, apod. Obrázek 11 znázorňuje vzájemný vztah mezi hlasovým traktem, příslušnými dutinami, základním tónem a formantovými kmitočty.

Také je možné využívat pro účely autentizace na základě hlasu vyhledávání a analýzu typických slov či parazitních projevů („ehm“, „eeee“, atd.) pro konkrétní osobu.



Obr. 11 Příklad principu autentizace za pomoci hlasu (Saquib, 2010).

Obecně je autentizace na základě analýzy hlasu velmi citlivá na kvalitě pořízeného záznamu, resp. je třeba vytvořit robustní metody, které budou odolávat okolnímu ruchu a budou správně analyzovat zaznamenaný hlas mimo dynamický rozsah v důsledku vysoké hlasitosti zdroje atd. Více informací o biometrii hlasu lze dohledat např. v (Saquib, 2010) či v (Doddington, 1985).

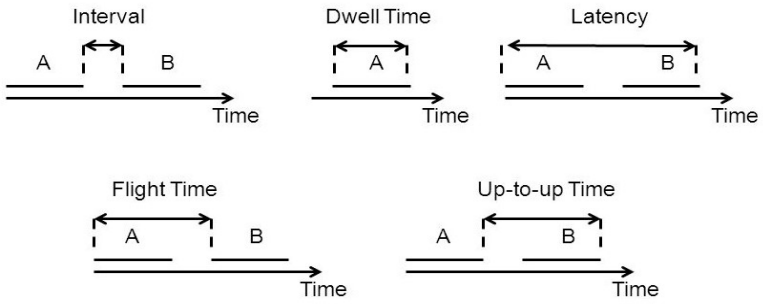
3.3.11 **Psaní na klávesnici**

Analýza psaní, resp. dynamiky, úhozů sloužila dříve pro autentizaci v telegrafických otázkách, kdy byly zkoumány přenášené znaky Morseovy abecedy, resp. doba trvání čárky atd. S technologickým pokrokem je možné tento biometrický parametr analyzovat téměř na každém zařízení.

Rozlišujeme dva druhy analýzy psaní na klávesnici - dynamický a statický. Dynamický styl je definován analýzou dlouhého textu, kde jsou zkoumány zvyky subjektu při psaní, jak daný subjekt používá kontrolní klávesy, jakých překlepů se obvykle dopouští, jakou rychlostí píše atd. Jelikož je nezbytné pro dynamický druh analýzy dynamiky psaní na klávesnici zachytit velké množství textu, není moc vhodné jej používat v přístupových systémech.

Statická analýza dynamiky psaní na klávesnici využívá zadání určitého krátkého textu- i pouze jednoho slova (heslo). Statická analýza dynamiky úhozů je většinou používána jako doprovodná úroveň zabezpečení při zadávání hesla. Díky tomuto faktu je možné vytvořit silnější autentizační systém, protože je zkoumáno, jaký uživatel je a co uživatel ví zároveň. Statická analýza dynamiky u zadávání krátkého textu/hesel se nazývá jako password hardening.

Mezi biometrické příznaky, zaznamenávané pro účely autentizace v rámci analýzy dynamiky psaní na klávesnici, jsou jednotlivé časové intervaly. Konkrétně: doba mezi stiskem a uvolněním klávesy, doba mezi uvolněním první a stiskem druhé klávesy, doba od stisku první a uvolnění druhé klávesy, interval mezi uvolněním první a stiskem druhé klávesy, a doba mezi stiskem první a druhé klávesy. Všechny tyto situace jsou zobrazeny na Obr. 12, kde A označuje první klávesu a písmeno B druhou klávesu.



Obr. 12 Analyzované intervaly stisků klávesnice (Dohnálek, 2012; upraveno).

Markantní výhodou analýzy dynamiky psaní na klávesnici je jednoduchá a diskrétní integrace do již existujících systémů bez zásadních změn použitého HW a SW. Jejich nevýhodou je však nutnost přeučení klasifikátoru v závislosti na zkušenostech a rozvoji v oblasti psaní na klávesnici (např. naučení se psát všemi deseti prsty či rychleji atd.) zkoumaného subjektu.

Detailnější popis biometrie dynamiky psaní na klávesnici lze nalézt např. v (Dohnálek, 2012).

3.3.12 **Podpis**

Vlastnoruční podpis je další biometrický parametr, jehož vlastnosti lze zkoumat v rámci autentizačních procesů. Konkrétně lze analyzovat u podpisu příznaky, jako jsou: velikost písmen a jejich vzájemný poměr, sklon písma, uzavřené oblasti atd. Tyto parametry jsou

označovány jako statické, a jsou získávány a analyzovány obdobně jako u oční duhovky atd. Tedy získaný snímek podpisu je zpracováván jako běžný dvojrozměrný snímek.

Aby došlo k vyšší preciznosti autentizačního procesu, dochází u podpisu také ke zkoumání dynamických příznaků (např. rychlost a síla tahu). Tyto příznaky jsou vyjádřené příslušnými vektory, a tak je potřebné dodat i třetí rozměr do příslušného snímače.

Jelikož jsou snímače tvořeny dotykovými obrazovkami, digitálním perem, tabletem (pero a podložka), apod., je nutné je do příslušného autentizačního procesu zakomponovat. I přes relativně nízkou cenu vstupních zařízení, není tato technologie moc rozšířená. Její detailnější popis lze naleznout v literatuře (Sangekar, 2014).

3.3.13 **Pohyb**

Pohyb, zejména chůze, je také považována za jeden možný biometrický parametr. Jelikož záznam pohybu můžeme chápat jako posloupnost fotografií, využívá se k jeho snímání klasická kamera. Dále jsou pak jednotlivé obrazy analyzovány jako statické snímky, a následně dochází k analýze diferencí významných bodů. Tyto diference jsou právě zkoumané příznaky.

Vhledem k tomu, že tato technologie není moc prozkoumaná a její výskyt je prakticky jedinečný, není proto momentálně vhodná pro běžnou komerční aplikaci. Více informací o biometrii chůze lze naleznout např. v (Zhang, 2011).

4 Vlastní práce

Tato část bakalářské práce pojednává o skutečných nástrojích pro účely biometrické autentizace, resp. o jejich vhodnosti zařazení do běžné praxe (Zeman, 2011). Jako modelový příklad, na který budou vybrané způsoby dodatečného zabezpečení aplikovány, byla vybrána jedna nejmenovaná firma z ČR, která se zabývá vývojem softwarového vybavení civilních i vojenských letadel. Jelikož se jedná o firmu, která vytváří produkty citlivé na výrobní tajemství, je zcela nezbytné, aby se žádné informace nedostaly do nesprávných rukou.

Z tohoto důvodu je využíváno k ochraně všech údajů a dat trojstupňové zabezpečení:

První úroveň je na úrovni docházkového systému, kde každý zaměstnanec vlastní svou identifikační kartu. Aby se zaměstnanec dostal ke svému pracovnímu místu, musí několikrát prokázat svou identitu pomocí této karty na jednotlivých terminálech. Avšak, jednotliví zaměstnanci mají omezený přístup do všech prostor, resp. je nemožné se dostat kamkoliv do budovy. Vždy je potřeba nejprve požádat o přístup do daného prostoru s odůvodněním. Tato žádost je procesována přes několik kompetentních osob, a pokud je od všech obdrženo kladné vyjádření, zpřístupní se žadateli přístup do požadované místnosti. Celý tento proces trvá několik dní.

Druhá úroveň zabezpečení je na softwarové bázi, kdy každý počítač využívá zabezpečení od firmy McAfee. Konkrétně antivir, firewall a také nástroj na šifrování e-mailové komunikace a celého pevného disku, což značně znemožňuje neoprávněný přístup k datům. Uživatel je navíc každé 2 měsíce vyzván ke změně hesla, která se mohou opakovat až po uplynutí dvou let, a navíc musí splňovat určitá kritéria (min. 1 speciální znak, min. 2 velká písmena, min. 1 číslice, min. jedno malé písmeno a minimální délka hesla je stanovena na 10 znaků). Z výše uvedených informací je patrné, že data jsou velmi dobře ochráněna tímto softwarovým nástrojem proti zneužití,

Třetí úroveň zabezpečení je mechanického rázu. Konkrétně je každý počítač zabezpečen uzamykatelným řetězem proti neoprávněnému zcizení či přemístění.

Praktická část této práce má objasnit, zda-li by bylo vhodné již tak kvalitní zabezpečení vytvořených dat a firemního know-how vylepšit za pomoci autentizačních biometrických metod. Proto budou dostupné autentizační metody založené na biometrii vhodně vybrány a aplikovány na výše uvedenou firmu, která čítá přibližně 120 zaměstnanců.

4.1 Příznaky a software

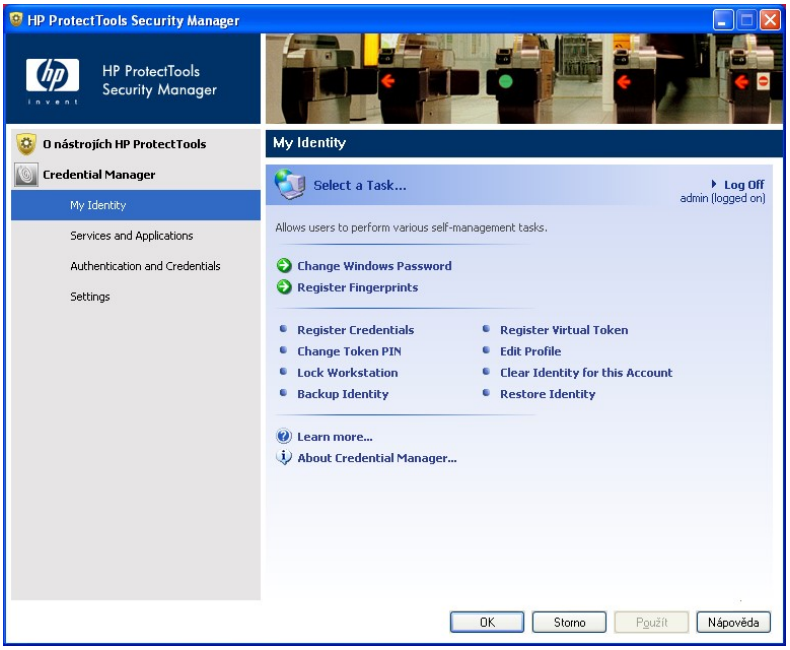
Jak již bylo naznačeno v teoretickém úvodu této bakalářské práce, využitelnost některých biometrických příznaků v běžné praxi je zcela vyloučena z důvodu jejich snímání, zpracování atd. Z tohoto důvodu byly zvoleny čtyři biometrické parametry (otisk prstu, dynamika úderu, obličej a hlas), jež by bylo vhodné aplikovat do běžné praxe k zvýšení robustnosti zabezpečení.

Následující část této práce tedy popisuje jednotlivá aplikační řešení.

4.1.1 Otisk prstu

HP Credential Manager - Prvním ze skupiny softwaru pro biometrickou autentizaci založenou na analýze otisku prstu by zvolen software HP Credential Manager, který byl standardně dodáván výrobcem Hewlett Packard ke svým počítačům. Výhodou tohoto zabezpečení jsou nulové náklady na jeho pořízení. Tato výhoda je však kompenzována omezenou funkčností softwaru, která je zaměřena pouze na přihlášení či odhlášení uživatele od konkrétního počítače, jelikož nemá v sobě integrované žádné části pro síťovou komunikaci atd.

Přívětivé uživatelské rozhraní tohoto software je ilustrováno na Obr. 13, kde je patrné že uživatel je schopný se během krátké chvíle přesunout na správu svého uživatelského účtu, jeho zabezpečení, obnovení vzoru svých otisků prstů atd.

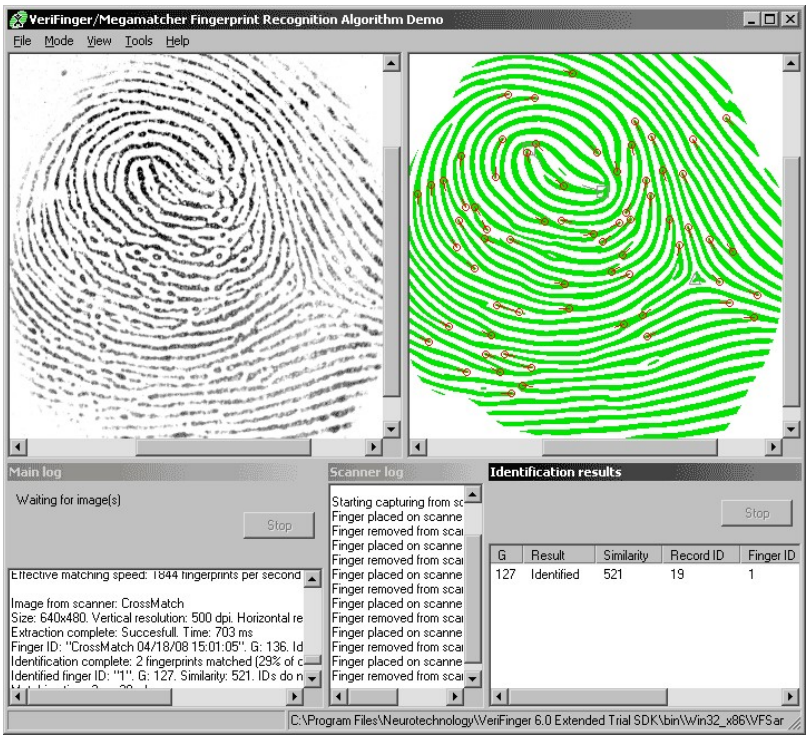


Obr. 13 HP Credential Manager – uživatelské prostředí (Software Informer, 2016).

Původně bylo zamýšleno použití obdobného přihlašovacího managera od společnosti DELL, který by byl otestován na notebooku DELL D620, jelikož firma, na kterou bude zaměřeno zhodnocení praktické aplikace vybraných biometrických, využívá počítače právě této značky. Bohužel se nepodařilo na stránkách výrobce získat funkční software, a tak bylo zvoleno řešení právě ve formě HP Credential Manager, který bude otestován, na notebooku HP Compaq NX6125, což nebude vadit k tomu, abychom ověřili úroveň a účinnost zabezpečení za pomoci otisku prstů.

VeriFinger - Dalším testovaným softwarovým nástrojem pro analýzu otisku prstu a zabezpečení, např. počítače, založené právě na tomto biometrickém příznaku je program VeriFinger od firmy NeuroTechnology. Tento software umožňuje přístup k jednomu či více počítačům/zařízením na základě zakoupené licence, ke kterým je nutné připojit rovněž senzor této firmy. Jednotlivé ceny licencí a nutných periferií lze nalézt na (NeuroTechnology, 2016), kde je taktéž uveden jejich detailní popis.

Pro praktické účely této bakalářské práce byla zvolena demo verze tohoto software, jehož grafické uživatelské rozhraní je zobrazeno na Obr. 14.

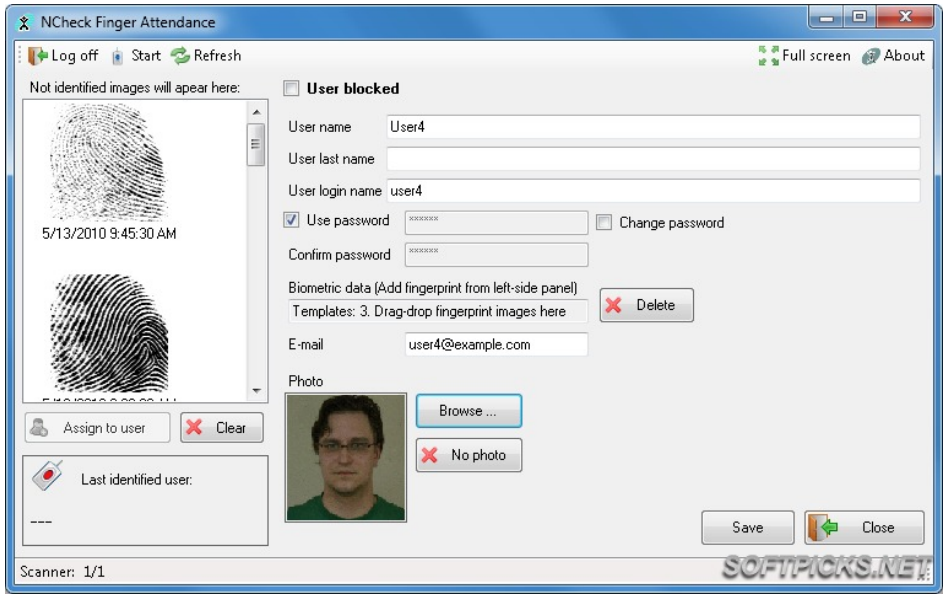


Obr. 14 VeriFinger - ilustrace prostředí (NeuroTechnology, 2016).

NCHECK Finger Attendance - Tento software byl zvolen jako další testovaný softwarový nástroj v této bakalářské práci. Sám výrobce na svých stránkách (Biometric Solutions, 2016) uvádí, že tento nástroj je vhodný především do malých či středně velkých

firem, kde je požadovat pouze na autentizaci příchodu a odchodu. Další využití tohoto nástroje je značně omezené, neboť v sobě neobsahuje žádné síťové rozhraní, a tak komunikace se vzdáleným serverem není možná.

Velkou výhodou tohoto softwarového nástroje je cena licence, která činí pouhých 95 EUR, a výrobcem deklarovaná kompatibilita s běžnými čtečkami otisků prstů. Jako v předchozím případě, i zde výrobce nabízí 30denní verzi software k vyzkoušení zdarma. Skutečnou podobu tohoto programu zachycuje Obr. 15.



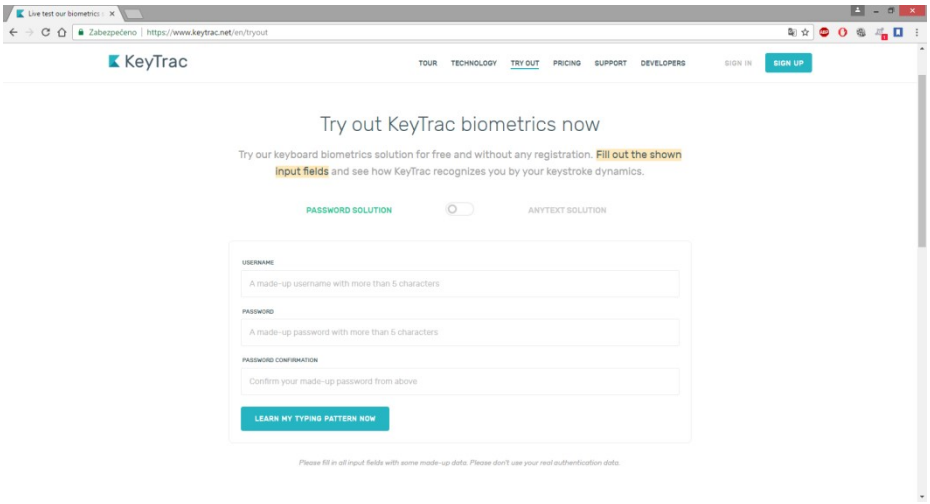
Obr. 15 NCHECK Finger Attendance – uživatelské prostředí (SoftPicks, 2016).

AWARE NexaRecognition - Posledním možným SW řešením zabezpečení za pomoci otisku prstu může být některý program firmy Aware z programové řady NexaRecognition. Tato řada softwarových nástrojů nabízí nejen analýzu otisku prstu, ale taktéž analýzu obličeje, duhovky atd. Jelikož je kompletní zabezpečení realizováno formou na klíč, není možné dohledat cenu jednotlivých produktů, jejich následný servis/udržitelnost, apod. Rovněž není možné ani stažení zkušební verze jakéhokoliv SW od výrobce Aware, a tudíž jej nelze prakticky otestovat a porovnat jeho úspěšnost s konkurencí. Vzhledem k tomu, že se jedná o velmi zajímavou realizaci zabezpečení na základě biometrických příznaku, je vhodné jej zde uvést pro představu, jak mohou další SW produkty vypadat a jak mohou být aplikovány. Více informací o tomto softwarovém nástroji je uvedeno přímo na stránkách výrobce (Aware, 2016)

4.1.2 **Dynamika úderu**

Mezi první rozšíření, které dělají zadávání běžného hesla na PC mnohem robustnější pomoci analýzy dynamiky úderů kláves, byl zvolen softwarový nástroj KeyTrac. Tento software je možné zakoupit již od $0 měsíčně (licence pro soukromé účely), pro účely naší výše popsané firmy by s přehledem dostačovala licence Startup za $199 měsíčně, která pokryje až 200 uživatelů, a nabízí jako vyšší licenční verze denní zálohy, e-mailovou podporu, 256bit SSL šifrování atd. V případě specifických nároků uživatele, resp. firmy, lze licenci i nabízené služby značně individualizovat.

KeyTrac navíc lze natrénovat pomocí jakéhokoliv textu či přímo konkrétním heslem. V našem případě se bude jednat o konkrétní heslo, které bude uživatel zadávat do webového rozhraní tohoto softwarového nástroje, viz Obr. 16.



Obr. 16 Úvodní obrazovka systému KeyTrac.

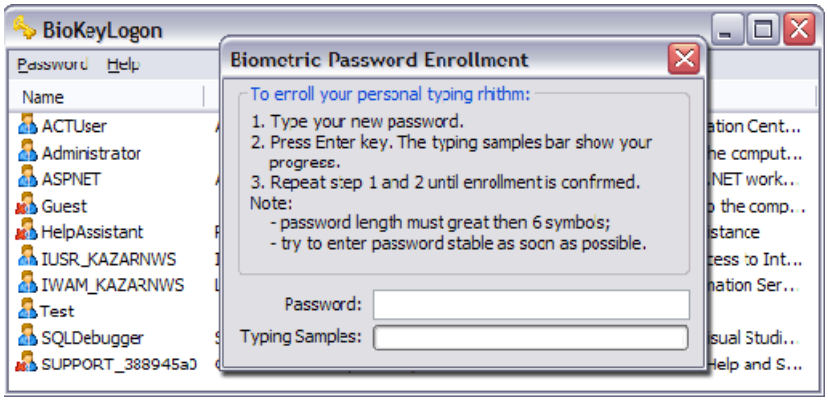
Autentizace uživatele je provedena, pokud je shoda aktuálně zadaného hesla s jeho vzorem více než 95 %. V opačném případě je uživatel zamítnut, resp. vyzván k novému zadání hesla, i když heslo bylo zadáno správně. Celkově lze KeyTrac charakterizovat jako moderní softwarový nástroj, který lze modifikovat přesně dle požadavků zákazníka, a navíc zvýší robustnost přístupu k datům/počítači atd. Více informací o tomto programu je uvedeno na stránkách výrobce (KeyTrac, 2016)

BioKeyLogon - Dalším softwarovým nástrojem, který byl v rámci této bakalářské práci zvolen k praktickému testování, je BioKeyLogon (ve verzi 2.0). Tento program je výrobcem nabízen v 15 denní trial verzi a za cenu necelých $20 lze pořídit plnou verzi pro jeden počítač. Tento softwarový nástroj neobsahuje žádné další funkcionality, a tak pouze umožňuje větší

robustnost vůči neoprávněnému přihlášení do operačního systému Windows, pro který je primárně určen.

Uživatel nejprve vytvoří svůj profil do příslušné databáze, a následně několikrát vyzván k zadání svého hesla aby byl vytvořen dostatečný vzor dynamiky úderu pro budoucí klasifikaci, viz Obr. 17.

Více informací o tomto softwarovém nástroji lze naleznout např. na (Softpedia, 2016), kde je rovněž možné tento program zakoupit.



Obr. 17 BioKeyLogon – ukázka prostředí (Softpedia, 2016).

BioPassword Enrolment - Jako poslední ze skupiny programů, které využívají pro autentizaci uživatele dynamiku úderu kláves, byl vybrán BioPassword Enrolment. Tento software je nabízen na trhu přibližně od roku 2000 a je neustále vyvíjen. Jeho poslední verze Enterprise Edition je nabízena právě pro firemní použití, kdy za cenu 19 dolarů ročně je možné zakoupit licenci pro jednoho uživatele.

Co se týká popisu funkčnosti celého programu, tak jej lze naleznout pro jeho starší verzi Protection v4.5. Z popisu chování tohoto software je zřejmé, že je potřeba pro inicializaci tohoto programu a vytvoření příslušných vzorů hesel, resp. úderů, konkrétního uživatele administrátorských oprávnění. Dále je uživatel vyzván k zadání svého hesla o minimálním počtu 4 znaků (doporučeno 8-16 znaků). Uživatel zadá své heslo celkem patnáctkrát, při čemž nesmí být použit klávesa backspace v případě přehmatu. Vždy je potřeba restartovat celý inicializační proces, neboť by v opačném případě došlo ke zkreslení dynamiky i rychlosti úderů. Tento počet (15) zadání hesla umožňuje vytvoření vhodného otisku uživatele do databáze přístupu.

Pro správu uživatelů a hesel, program disponuje grafickým uživatelským rozhraním, viz Obr. 18, kde lze např. nastavit ochranu spořiče obrazovky pomocí této biometrické autentizační metody, atd. Více o tomto software lze dohledat např. v (Patrick, 2009).

Obr. 18 Ilustrace software BioPassword Enrolment (Patrick, 2009).

4.1.3 **Obličej**

Další biometrický znak, který bude prakticky otestován, byl vybrán obličej subjektu. Resp. příznaky vytěžené z obličeje zkoumané osoby, které jsou dále zpracovávány a vyhodnocovány. Jak již ale bylo v úvodu této bakalářské práce zmíněno, je zapotřebí dodržet korektní snímání obličeje, což může v určitých situacích problém.

Betaface API - Jako první softwarový nástroj využívající obličejových příznaků pro autentizaci, který byl vybrán pro praktické otestování, se nazývá Betaface API. Tento nástroj využívá odesílání pořízených snímků obličeje na server, kde je prováděna analýza a následná klasifikace zkoumaného subjektu. Veškerá komunikace je zabezpečena pomocí HTTPS protokolu.

Cena měsíční licence tohoto produktu začíná na 199 Euro při měsíčním zpracování 40.000 snímků. Za 399 Euro lze měsíčně zpracovat až 100.000 snímků atd. Pokud postačuje zpracovat 500 a méně snímků denně, je cena licence nulová.

V popisu funkčnosti tohoto software lze najít, že pro vyhodnocování identity subjektu je analyzováno 22 obličejových příznaků, jako je např. barva pleti a vlasů, stáří, přítomnost vousů či brýlí atd. Detailnější popis tohoto nástroje lze naleznout na stránkách výrobce (BetaFace API, 2016).

Pro účely našeho praktické vyhodnocování však bude vyzkoušena demo verze tohoto programu, která se snaží rozpoznat slavné osobnosti. Pro jednotlivé osobnosti tedy bude pořízeno z internetových zdrojů několik fotografií, na kterých bude zachycena proměna obličeje (stářím, stylem úpravy, apod.), a bude tedy zkoumána úspěšnost identifikace. Tento jev nám pomůže objasnit, zda-li a jak často je nutné aktualizovat vzorové snímky osob v databázi, a zda-li má změna vzhledu osobnosti zásadní vliv na výsledek autentizačního procesu.

KeyLemon je softwarový nástroj, který bude taktéž podroben praktickému testování v této bakalářské práci. Tento program využívá biometrie obličeje pro autentizační proces. KeyLemon lze zakupit ve třech variantách- Basic, Bronze a Gold, kde cena Bronze licence je necelých 20 Euro, Gold stojí téměř 40 Euro a Basic licence je zdarma.

Funkční rozdíl mezi licencemi ale není nijak zásadní. Basic licence dokáže odemknout počítač při úvodním přihlašovacím procesu, Bronze navíc umožňuje automatické uzamknutí počítače, pokud se uživatel po delší dobu nenachází před jeho obrazovkou, a Gold verze nabízí lepší autentizační výsledky za různých světelných podmínek, a také umožňuje nastavit úroveň zabezpečení. V případě vyšší úrovně zabezpečení v Gold verzi, je uživatel vyzván k mrknutí oky, což podle výrobce tohoto software znemožňuje použití videa či fotografie pro prolomení autentizačního procesu.

Detailní popis prakticky testovaného produktu KeyLemon lze nalézt na stránkách výrobce (Biometric Solutions, 2016).

4.1.4 **Hlas**

Posledním biometrickým znakem, který bude prakticky otestován v rámci této bakalářské práce je hlas. Hlas byl vybrán z toho důvodu, že vývoj autentizačních metod založených na analýze hlasu je stále v počátku a nepřináší žádné stabilní a důvěryhodné výsledky (viz teoretický úvod této bakalářské práce), a tak je vhodné je porovnat s ostatními produkty využívající jiné biometrické příznaky.

VeriSpeak - Z omezeného výběru softwarových produktů, které využívají analýzu hlasu pro účely autentizace, byl zvolen program VeriSpeak. Tento program pro rozpoznání identity subjektu (mluvčího) existuje ve dvou verzích- klasický program a webová aplikace.

Z popisu výrobce (NeuroTechnology, 2016) je patrné, že úspěšnost autentizace je závislá na hlučnosti prostředí, použitém hardwaru (výrobce nedoporučuje, aby se lišily

mikrofony pro běžnou autentizaci a pro pořízení vzorové nahrávky), aktuálním emočním a zdravotním stavu mluvčího, rychlost projevu atd. Tudíž je patrné, že tyto požadavky značně omezují možné praktické nasazení autentizačních metod, využívajících analýzu hlasu, v běžných situacích.

Výrobce programu VeriSpeak samozřejmě neprozrazuje, které hlasové příznaky analyzuje, ale uvádí, že VeriSpeak je možné používat v textově závislém (známá fráze) či nezávislém režimu. VeriSpeak také využívá tzv. dvou-faktorovou autentifikaci, která využívá kontroly hlasových příznaků, aby bylo zabráněno neoprávněné autentizaci za pomoci hlasového záznamu.

I ceny licence software VeriSpeak jsou značně vysoké. Standard licence stojí 339 Euro a Extended licence má cenu 859 Euro, přičemž se liší pouze v počtu (1 či 3) vybraných komponent. Pro každý další počítač nad uvedený počet v rámci zakoupené licence je vždy potřeba pořídit kýžené komponenty za poplatek.

Výrobce však na svých stránkách nabízí program VeriSpeak v 30denní testovací trial verzi, která bude použita v rámci této bakalářské práce.

5 Výsledky a diskuse

Jak již bylo v předchozích sekcích této bakalářské práce nastíněno, nyní se dostáváme k její praktické části, kde bude výše vybraný software otestován. Pro tyto účely byla zvolena databáze dobrovolníků ať už řad rodinných příslušníků, spolupracovníků či kamarádů, čítající celkově 20 subjektů. Konkrétně 12 žen a 8 mužů ve věkovém rozmezí 26 až 57 let. Pro přehlednější práci s naměřenými výsledky jsou jednotlivé subjekty označovány písmenem Z pro ženu nebo M pro muže a příslušným pořadovým číslem.

Nyní už však dochází k přesunutí se k prakticky získaným výsledků.

5.1 Otisk prstu

Prvním biometrickým znakem, který byl prakticky otestován na vytvořené databázi dvaceti dobrovolníků, byl otisk prstu. K tomuto účelu byl použit notebook HP Compaq NX6125 s integrovanou čtečkou otisku prstu, operačním systémem Microsoft Windows XP Professional a Microsoft Windows 10 Education.

5.1.1 HP Credential Manager

Tento program, který poskytuje společnost ke svým notebookům (zakoupených především v minulosti) byl vybrán jako první software pro praktické testování. Na testovacím notebooku bylo vytvořeno celkem 20 uživatelských účtu. Každý uživatel si svůj účet zabezpečil jak jednoduchým heslem, tak i pomoci svých otisků prstů.

Pro správné vyhodnocení a uvedení do databáze vzorů, bylo potřeba celkem 3 prsty (prostředníček, ukazováček a prsteníček) čtyřikrát otisknout pro každou ruku. Tento inicializační krok je zobrazen na Obr. 19.

Obr. 19 HP Credential Manager – prvotní zadávání otisků uživatele.

První měření úrovně zabezpečení bylo provedeno uzamčením počítače, a následným přihlášením ke svému uživatelskému účtu za pomoci otisku prstu. Celkový počet pokusů pro přihlášení každého uživatele byl 10, a to tak, že se uživatel nejprve snažil přihlásit za pomocí každého svého zaznamenaného prstu (celkem 6), a pak následující 4 přihlašovací pokusy si uživatel zvolil sám, který prst použije.

V následující tabulce, Tab. 2, jsou uvedeny poměry počtu úspěšných přihlášení k celkovému počtu přihlašovacích pokusů. Tab. 2 může být interpretována tak, že v řádcích jsou uvedeni uživatelé, kteří se pokusili přihlásit ke svému účtu, a ve sloupcích jsou účty, ke kterým se aktuální uživatel přihlásil.

Tab. 2 Otisk prstu - výsledky autentizace uživatelů.

	Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8	Z9	Z10	Z11	Z12	M1	M2	M3	M4	M5	M6	M7	M8
Z1	0.8																			
Z2		1.0																		
Z3			0.8																	
Z4				0.6																
Z5					1.0															
Z6						0.5														
Z7							0.3										0.1			
Z8								0.7												
Z9									0.7											
Z10										0.8										
Z11											0.9									
Z12												0.4								
M1													0.8							
M2														1.0						
M3															0.1					
M4													0.1			0.2				
M5																	0.6			
M6																		0.9		
M7																			0.9	
M8																				0.7

Z výše získaných výsledků je patrné, že ve většině úspěšných případů se uživateli podařilo přihlásit ke svému účtu. Pouze ve dvou případech se podařilo uživateli přihlásit k jinému uživatelskému účtu za pomoci snímku otisku prstu. Konkrétně čtvrtý muž (M4) se v jednom případě úspěšně přihlásil k účtu uživatele M1, a sedmá žena (Z7) se přihlásila k účtu M5. Toto přihlášení bylo pouze náhodného charakteru, a po pokusu jej zopakovat (natočení prstu, rychlost snímání atd.), se jej nepodařilo znovu navodit.

Z Tab. 2, je rovněž patrné, že některým uživatelům dělalo problém sejmout v pořádku svůj otisk prstu, a tudíž tyto pokusy nebyly akceptovány pro přihlášení, např. 6 pokusů u Z7, 7 pokusů pro M4 atd.

Po odečtení obou neoprávněných případů přihlášení lze vypočítat průměrnou hodnotu poměru mezi úspěšným přihlášením a celkovým počtem pokusů, která je 0,685, tedy přibližně 69 %. Toto číslo tedy reprezentuje přibližně situaci, kdy je potřeba třikrát sejmout otisk prstu, abychom byli úspěšně přihlášeni ke svému účtu. Hodnota tohoto čísla bude samozřejmě časem narůstat, neboť uživatel si zvykne na celý proces snímání otisků prstů, a navíc bude používat pouze ty prsty, u kterých si je nejvíce jistý, že proběhne bezproblémové přihlášení.

Odečteme-li od hodnoty 1 (reprezentující hodnotu 100 %) poměr mezi celkovým neoprávněným přihlášením (0,2) a celkovým počtem úspěšných přihlášení (13,9), získáme hodnotu úspěšné identifikace subjektu, která má hodnotu přibližně 98,6 %. I přes to, že je tato hodnota úspěšnosti velice vysoká, je potřeba dbát v potaz, že její hodnota klesne při aplikaci na celou populaci, neboť byla získána pouze pro 20 osob. Nicméně, i takto lze hovořit o velice vysoké hodnotě úspěšnosti.

Tab. 3 Vypočtené hodnoty efektivity.

	ANO	***NE***	**CELKEM**	***ε* [%]**
Z1	0	190	190	100
Z2	0	190	190	100
Z3	0	190	190	100
Z4	1	190	191	99,5
Z5	0	190	190	100
Z6	0	190	190	100
Z7	0	190	190	100
Z8	2	190	192	98,9
Z9	0	190	190	100
Z10	0	190	190	100
Z11	0	190	190	100
Z12	0	190	190	100
M1	1	190	191	99,5
M2	0	190	190	100
M3	0	190	190	100
M4	0	190	190	100
M5	3	190	193	98,4
M6	0	190	190	100
M7	0	190	190	100
M8	0	190	190	100

Efektivita autentizace tohoto softwarového nástroje byla rovněž otestována dalším praktickým způsobem, a to tak, že na testovacím počítači byl zaveden pouze jeden uživatelský účet, který byl zabezpečen snímky otisků prstů (přesně jako v předchozím případě). Ostatní uživatelé z databáze se právě k tomuto účtu snažili připojit pomocí svých otisků libovolných prstů a to tak, že každý měl 10 pokusů, a v případě, že některý pokus o neoprávněné přihlášení byl úspěšný, mohl jej znovu zopakovat. Získané výsledky tímto praktickým měřením jsou uvedeny v Tab. 3.

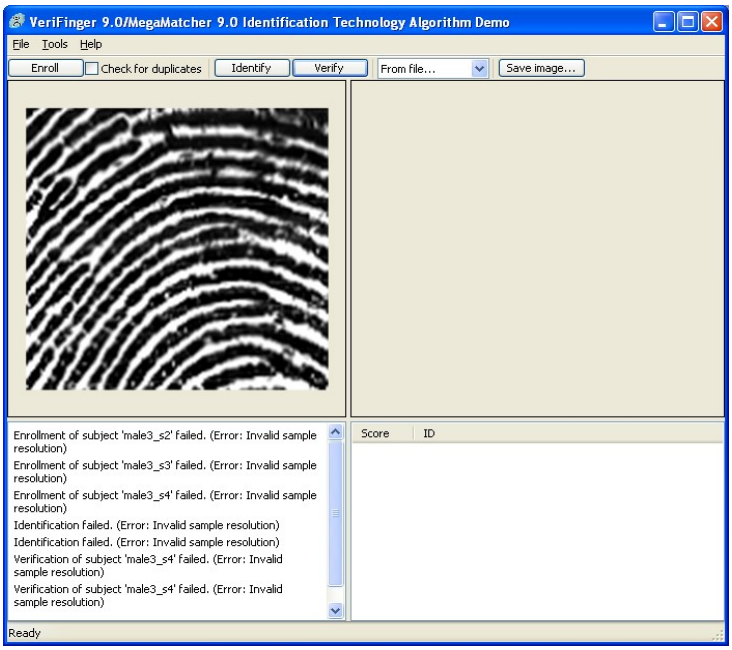
Z výsledků, uvedených v Tab. 3, je patrné že celkově pouze v sedmi případech došlo k neoprávněnému přihlášení k cizímu uživatelskému účtu za pomoci snímku otisku prstu. Hodnota výše uvedené efektivity zabezpečení ε je definována vztahem

$$\varepsilon_i = \frac{NE_i}{ANO_i + NE_i} \cdot 100\ [\%]$$

kde *NE* je počet neúspěšných pokusů přihlášení a *ANO* je počet úspěšných přihlášení pro subjekt *i*. Takto získaná efektivita zabezpečení má průměrnou hodnotu přibližně 99,8 %, a z jejích stabilních výsledků je patrné, že se jedná o velice robustní formu zabezpečení.

5.1.2 **VeriFinger**

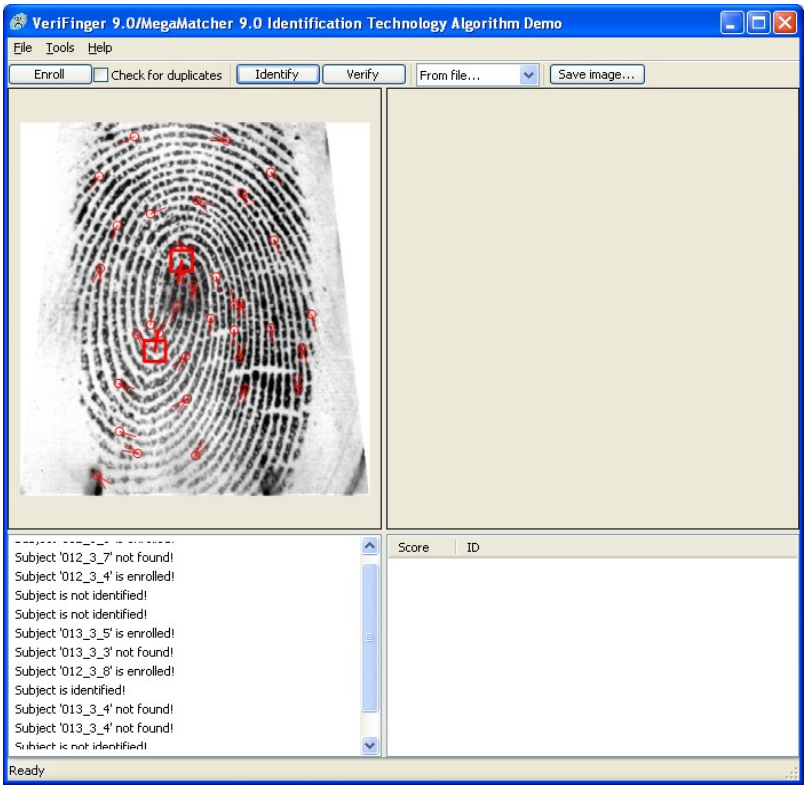
Dalším prakticky otestovaným softwarovým nástrojem pro autentizaci za pomoci otisku prstu měl být program VeriFinger, který se bohužel nepodařilo zprovoznit tak, aby jej bylo možné otestovat podobně jako program HP Credential Manager. Zkušební verze programu VeriFinger se potýkala hlavně s problémy při zpracování otisků, které byly zachyceny za pomoci integrované čtečky v notebooku. Z Obr. 20 je patrné, že program VeriFinger nepracoval původně správně kvůli nesprávnému rozlišení pořízeného snímku.



Obr. 20 VeriFinger – načtení vlastního snímku otisku.

Nicméně, aby byla otestována efektivita rozpoznávání tohoto softwarového nástroje, byly staženy dvě databáze snímků otisků prstů „Cross_Match_Sample_DB“ a „UareU_sample_DB“, na které se výrobce programu VeriFinger odkazuje, a umožňuje jejich bezplatné stažení (NeuroTechnology, 2006).

V tomto případě již byl nahraný snímek otisku prstu správně nahrán a analyzován, ale bohužel programu chyběla hlubší funkcionalita, která např. vyhledávala stejný otisk prstu z vybrané databáze atd. Vždy bylo nutné manuálně zvolit snímek, se kterým má být vzor porovnáván, a shoda byla pouze tehdy, pokud byly oba snímky zvoleny jako stejné. Jak již bylo řečeno, pro testování by bylo potřeba tento program doplnit hlubší (vhodnější) funkcionalitou, či doplnit databáze o snímky stejných otisků prstů, které jsou nějakým způsobem zdeformovány (otočení, neúplnost, rozmazání atd.). Jelikož k tomuto testovanému programu není poskytována žádná podpora ve formě nápovědy či technické dokumentace, bylo od jeho testování upuštěno. Obrázek 21 zachycuje nalezenou shodu na zpracovaném snímku otisku prstu z databáze včetně červeně označených analyzovaných příznaků otisku.



Obr. 21 VeriFinger – načtení otisku z databáze.

5.1.3 NCHECK Finger Attendence

Program NCHECK Finger Attendance měl být posledním otestovaným softwarovým nástrojem. Bohužel toto nebylo možné, jelikož instalační soubor, který je poskytován na stránkách výrobce, je poškozen, a tudíž celá instalace neproběhne až do konce, a tak jej není možné následovně spustit. Tato chyba se objevila jak pod operačním systémem Windows XP, tak i pod Windows 10. Funkční instalační soubor nebylo možné získat z jiného zdroje. Je však předpoklad, že pokud by byl zájem o zakoupení licence, podpora tohoto programu by uvedený problém vyřešila, aby byl plně funkční.

5.2 Dynamika úderu

Dalším biometrickým znakem, který byl prakticky otestován za účelem možné aplikace ve vybraném prostředí, je dynamika úderu. Síla a funkčnost autentizace toho biometrického parametru měla být původně otestována pomocí 3 softwarových nástrojů, které měly být poskytnuty výrobcem. Ovšem realita je někde úplně jinde, a tak detailní popis možnosti/nemožnosti otestování jednotlivých nástrojů je uveden dále v příslušných sekcích.

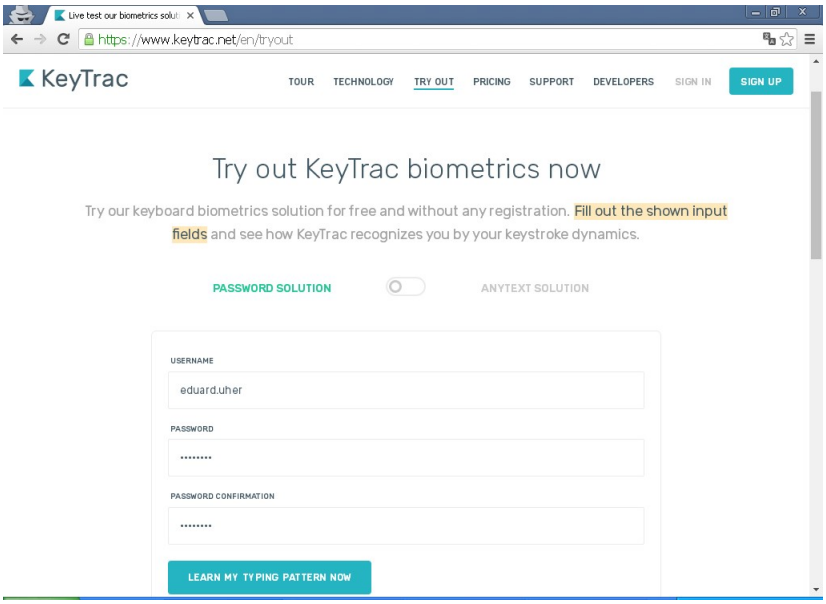
5.2.1 KeyTrac

Prvním softwarovým nástrojem, který umožňuje autentizaci uživatele pomocí dynamiky úhozů, je KeyTrac. Tento program je možné otestovat bez nutnosti instalace pouze prostřednictvím internetového připojení, jak již bylo v popisu tohoto nástroje zmíněno. Nevýhodou tohoto testovacího řešení je vytvoření pouze jednoho uživatelského profilu. Z tohoto důvodu si tedy nejprve každý uživatel vytvořil svůj uživatelský účet, zadal své libovolné heslo, které následně potvrdil, a pak se pokusil celkem desetkrát přihlásit ke svému účtu tímto heslem. Po každém přihlašovacím pokusu byla zobrazena shoda mezi aktuálně zadaným heslem a jeho vzorem. Jak již bylo uvedeno u popisu tohoto software, uživatel je úspěšně autentizován, pokud je shoda se vzorem vyšší nebo rovna hodnotě 95 %. Z tohoto důvodu jsou úspěšné autentizace označeny zelenou barvou v Tab. 4, kde jsou uvedeny všechny získané hodnoty shod a také celková hodnota efektivity, která je vypočtena jako podíl počtu úspěšných přihlášení k celkovému počtu přihlašovacích pokusů v procentech.

Tab. 4 KeyTrac – získané hodnoty efektivity.

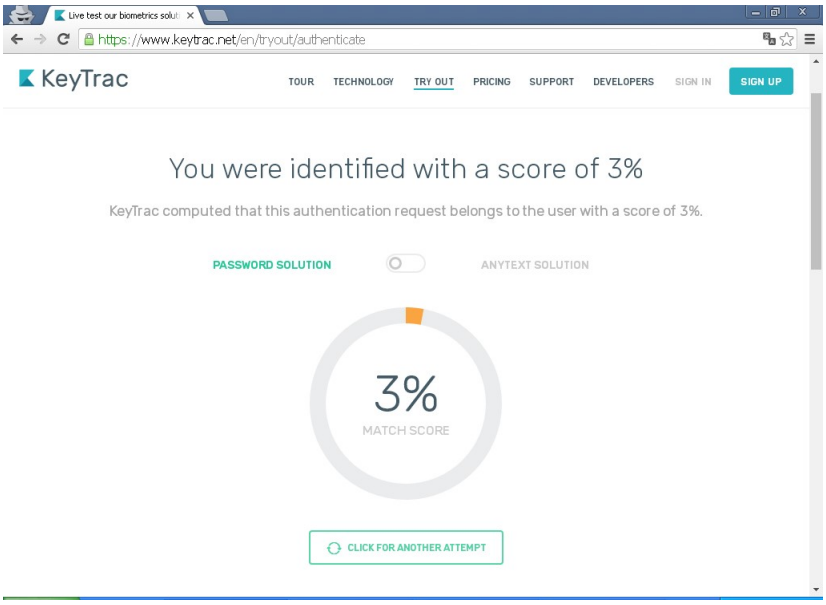
	SHODA [%]										ε [%]
Z1	88	99	6	98	98	100	56	77	91	97	50
Z2	76	58	78	81	81	89	74	79	92	92	0
Z3	75	0	80	97	43	5	43	80	45	35	10
Z4	45	75	100	71	34	82	86	90	90	92	10
Z5	85	87	82	82	82	84	88	92	84	84	0
Z6	67	72	77	72	72	72	74	69	66	72	0
Z7	56	59	48	54	86	97	79	64	46	65	10
Z8	63	54	58	69	67	87	89	67	77	54	0
Z9	54	67	69	17	72	89	39	39	59	74	0
Z10	69	90	93	94	94	94	96	89	92	91	10
Z11	99	85	89	82	85	86	90	91	97	92	20
Z12	87	75	79	76	72	81	83	90	91	82	0
M1	87	89	91	93	92	89	83	89	65	90	0
M2	65	87	89	82	89	90	88	84	85	77	0
M3	51	62	71	64	8	71	63	72	38	35	0
M4	58	39	77	89	72	48	67	96	87	75	10
M5	99	93	96	96	96	100	100	98	98	99	90
M6	89	90	88	91	92	93	93	93	96	95	20
M7	47	26	40	49	57	60	68	58	69	67	0
M8	68	87	89	86	87	80	82	79	73	74	0

Z Tab. 4 je zcela evidentní, že někteří uživatelé by se bohužel nedokázali vůbec přihlásit ke svému účtu i přes to, že zadané heslo bylo správné. Schopnost zopakování stejných pohybů/dynamiky při zadávání hesla je tedy zcela individuální. Průměrná hodnota efektivity je v tomto případě 11,5 %, což není vůbec uspokojivá hodnota. Tuto hodnotu by bylo zvýšit snížením prahové úrovně shody (následek je zvýšení rizika neoprávněné autentizace), která je potřebná pro úspěšnou autentizaci, nebo pomoci rozsáhlejší nácviku zadaného hesla při zakládání uživatelského účtu, viz Obr. 22.



Obr. 22 KeyTrac – vytvoření profilu uživatele.

Dalším praktickým otestováním funkčnosti tohoto software bylo za pomoci vytvořeného fiktivnímu účtu, kdy všichni uživatelé z databáze znali přihlašovací jméno uživatele i heslo (délka 8 znaků), ale neznali způsob zadání hesla, což může být zcela běžná situace, např. pokud se někdo neoprávněný dostane k vašim přihlašovacím údajům. Každý subjekt z databáze byl vyzván k tomu, aby se desetkrát pokusil zadat heslo jakýmkoliv způsobem. Obrázek 23 ilustruje zaznamenanou hodnotu shody aktuálně zadaného hesla se vzorem, která nenabývala (dle předpokladu) nijak vysokou hodnotu.



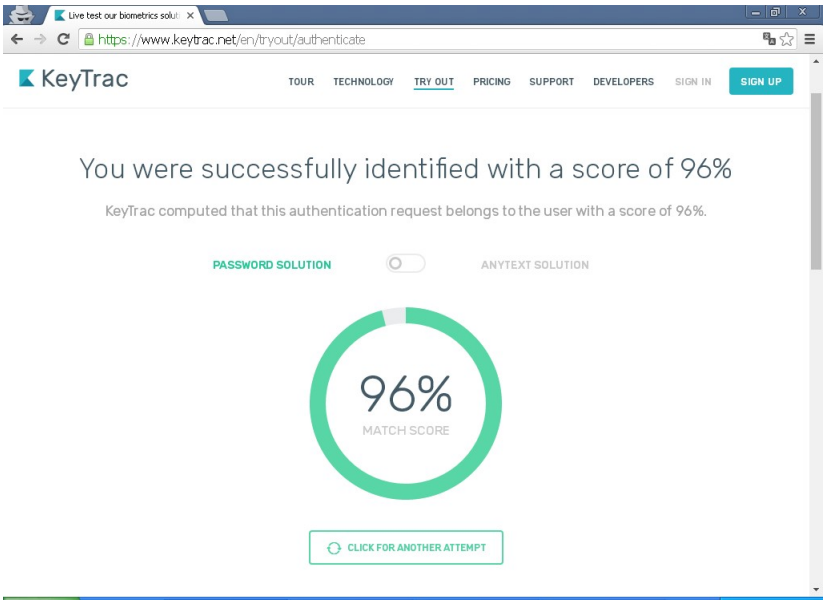
Obr. 23 KeyTrac – neúspěšné přihlášení uživatele.

Všechny získané hodnoty shody v případě známého hesla a jeho neznámého způsobu zadávání jsou uvedeny v Tab. 5, kde je patrné, že ani jednou nedošlo k neoprávněné autentizaci uživatele. Průměrná hodnota shody je v tomto případě přibližně pouhých 23 %.

Tab. 5 KeyTrac – získané hodnoty shody.

	SHODA [%]									
Z1	3	1	2	25	0	12	15	12	11	19
Z2	0	0	0	0	0	8	0	6	17	25
Z3	5	8	6	2	0	9	11	31	15	7
Z4	1	3	0	1	7	5	62	23	34	22
Z5	52	33	45	22	23	18	20	28	22	16
Z6	3	4	3	3	3	3	4	4	0	0
Z7	22	26	45	23	40	5	38	21	46	53
Z8	6	1	45	4	34	41	54	55	3	22
Z9	50	31	53	39	49	40	14	33	63	28
Z10	19	56	13	56	7	5	16	18	39	47
Z11	13	39	6	20	20	28	27	16	18	23
Z12	43	24	23	36	8	17	29	18	44	4
M1	23	14	18	9	9	53	32	60	40	8
M2	11	46	29	20	0	50	40	25	26	32
M3	46	36	30	48	33	17	34	43	12	10
M4	27	61	31	37	60	1	22	63	64	25
M5	35	8	55	11	30	20	2	19	0	1
M6	29	16	2	13	39	38	28	11	61	19
M7	27	21	28	14	0	11	48	42	34	18
M8	4	31	45	17	16	13	57	8	58	37

Posledním způsobem, jak ověřit robustnost tohoto nástroje, bylo zveřejnění i způsobu zadávání hesla (rytmus a akcenty úderů kláves při jeho zadávání). Každý subjekt z databáze byl pak tedy desetkrát vyzván k zadání hesla tak, jako tomu bylo v předchozím případě. Obr. 24 znázorňuje případ rapidního nárůstu shody aktuálně zadaného hesla se vzorem.



Obr. 24 KeyTrac – úspěšné přihlášení uživatele.

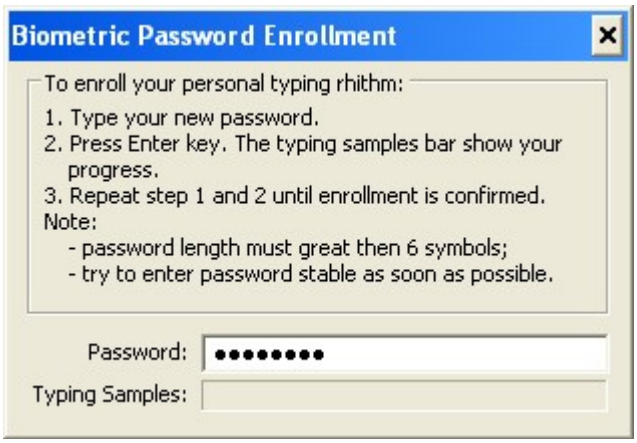
Tab. 6 KeyTrac – shoda a efektivita pro známé heslo i styl.

	SHODA [%]										ε [%]
Z1	4	46	97	99	99	99	99	100	99	99	80
Z2	6	8	4	14	7	15	46	67	18	85	0
Z3	77	75	90	68	82	63	84	74	64	94	0
Z4	98	65	100	93	63	71	90	86	92	66	20
Z5	85	95	90	63	64	89	83	87	81	98	20
Z6	99	70	74	65	81	77	86	91	73	68	10
Z7	62	60	69	70	91	89	100	65	96	72	20
Z8	96	79	64	81	73	71	89	78	72	69	10
Z9	13	9	9	16	15	65	61	93	76	77	0
Z10	83	63	85	100	79	75	62	65	60	81	10
Z11	65	71	98	93	67	73	80	86	100	88	10
Z12	92	88	66	85	78	84	76	77	72	97	10
M1	93	98	89	79	83	71	99	92	86	69	20
M2	62	65	94	80	99	75	96	61	66	92	20
M3	97	92	89	62	96	83	70	94	72	85	20
M4	100	70	82	83	92	75	100	99	66	79	30
M5	8	6	11	16	9	14	14	16	12	13	0
M6	70	85	77	74	71	79	90	75	73	80	0
M7	67	74	80	94	71	92	87	84	78	82	0
M8	79	64	97	80	88	81	75	91	99	90	20

Všechny takto získané hodnoty shody jsou uvedeny v Tab. 6, kde je její rapidní nárůst zcela patrný a úspěšné autentizační pokusy (shoda vyšší než 95 %) jsou označeny zeleně. O nějaké robustnosti systému vůči neoprávněnému přihlášení nelze v tomto případě mluvit, neboť průměrná hodnota (15 %) efektivity je téměř shodná s efektivitou pro prvotní individuální přihlášení uživatele (11,5 %). Z tohoto důvodu je nezbytně nutné chránit nejen přihlašovací údaje, ale i způsob, jakým jsou zadávány, neboť i rytmus zadávání údajů může být lehce odposlouchán v případě hlučnější klávesnice atd.

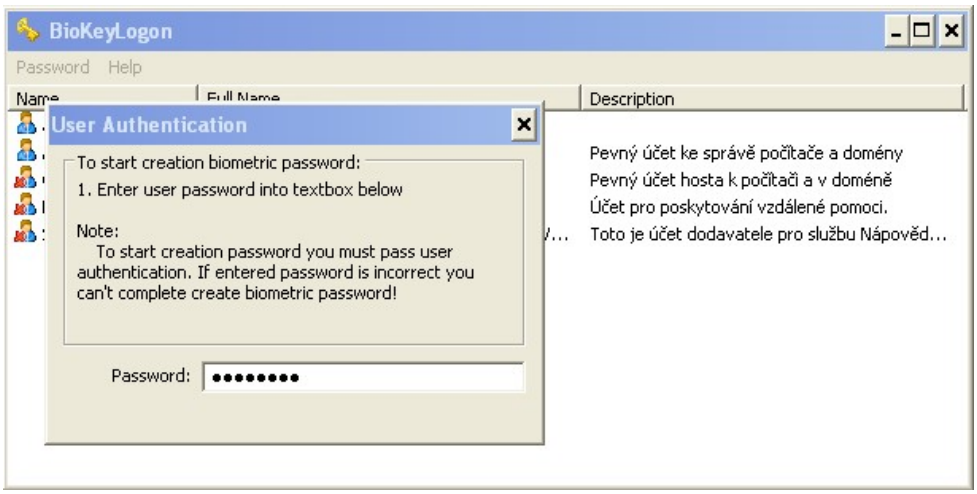
5.2.2 **BioKeyLogon**

Dalším testovaným softwarem, který umožňuje autentizaci za pomoci dynamiky úderů do kláves, měl být BioKeyLogon. Bohužel se tento nástroj nepodařilo otestovat, neboť způsoboval značnou nestabilitu operačního systému, a pouze v nouzovém režimu pro Windows XP bylo možné přiřadit pouze inicializační heslo, viz Obr. 25, ale při fázi nacvičení vzoru zadávání hesla pro vybraného uživatele (Obr. 26) došlo vždy ke zhroucení operačního systému.



Obr. 25 Praktické testování BioKeyLogon.

Tento jev přetrvával až do odinstalování tohoto softwarového nástroje jak pro operační systém MS Windows XP, tak i pro MS Windows 10. Po jeho odstranění byl systém opět stabilní. Tento problém by se dal s největší pravděpodobností vyřešit ze strany výrobce tohoto softwarového nástroje v případě zakoupení licence.



Obr. 26 BioKeyLogon – zadávání hesla uživatele.

5.2.3 BioPassword Enrolment

Jako poslední softwarový nástroj poskytující autentizaci za pomoci dynamiky úderů kláves byl vybrán program BioPassword Enrolment. Tento nástroj bohužel nebylo možné prakticky otestovat, neboť odkaz pro jeho stažení byl nefunkční, a navíc se jej nepodařilo dohledat z jiného zdroje. Opět je možné tvrdit, že pokud by se jednalo o novější program s placenou licencí, bylo by možné napsat na podporu výrobce o nápravu, ale jelikož se jedná o bezplatný a starší nástroj, šance sjednání nápravy výrobcem může být téměř mizivá.

5.3 Obličej

Předposledním biometrickým znakem, který byl prakticky otestován, je obličej. Následující část popisuje výsledky či pozorování z testování dvou různých softwarových nástrojů, kde u každého nástroje byly využity jeho možnosti využity naplno, a navíc každý nástroj byl otestován různým způsobem.

5.3.1 BetaFace API

Jako první otestovaný softwarový nástroj, sloužící pro autentizaci na základě biometrických příznaků obličeje, byl zvolen BetaFace API. Jelikož tento online nástroj umožňuje několik různých módů (např. popis osoby na základě analýzy obličeje), tak byl vybrán nejvíce zajímavý režim, kdy obličej na vstupní fotografii porovnáván a vyhledán v databázi obličejů slavných osobností.

Hlavním důvodem, proč byl zvolen právě tento režim, je ten, že hlavním cílem bylo otestovat úspěšnost rozpoznávání identity mezinárodně slavné osobnosti, která je zachycena

na fotografiích v různém věku či v různé úpravě svého zevnějšku (např. vousy, změna barvy vlasů, apod.).

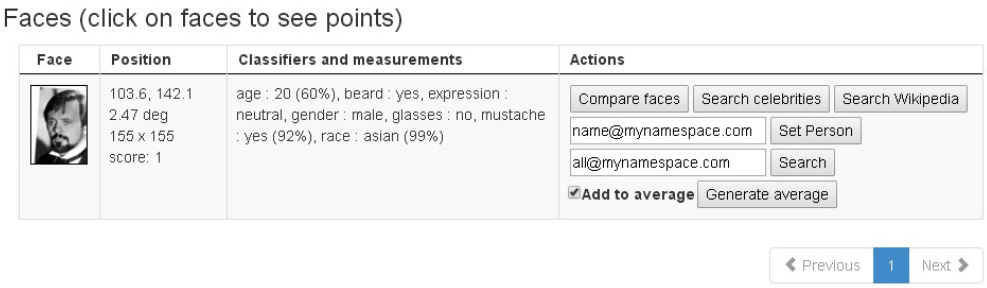
Pro tyto účely bylo tedy potřeba vytvořit novou databázi. Záměrně byly vybrány ty osobnosti, které působí na scéně již dlouhou dobu, či ty, které změnili svůj vzhled nějakým radikálnějším způsobem. V této databázi je opět celkem 20 osob – 10 žen a 10 mužů, a pro každou osobu byly vybrány dvě různé fotografie. Seznam vyhledávaných osob z databáze a získané výsledky jsou uvedeny v Tab. 7.

Tab. 7 Betaface API – výsledky identifikace.

jméno	foto 1		foto 2		poznámka
	rok	pořadí/jistota	rok	pořadí/jistota	
Keanu Reeves	1999	1/77%	2016	1/61%	
Hugh Jackman	1990	2/52%	2016	nenalezen	
Anthony Hopkins	1980	6/52%	2005	1/72%	asiat
Sean Connery	1970	1/76%	2010	1/67%	
Colin Farrell	1999	1/95%	2015	1/61%	
Johnny Depp	1990	1/59%	1999	1/61%	
Axl Rose	1984	1/53%	2011	nenalezen	žena
Paul McCartney	1964	1/68%	2014	1/72%	žena
Freddie Mercury	1975	5/48%	1991	nenalezen	žena
Brad Pitt	1994	1/72%	2014	1/60%	
Jennifer Lawrence	2012	nenalezen	2015	3/52%	
Tilda Swinton	2005	1/75%	2015	1/71%	
Marilyn Monroe	1950	2/55%	1960	8/54%	
Julia Roberts	1990	1/72%	2015	1/66%	
Nicole Kidman	1990	1/59%	2016	1/67%	
Meryl Streep	1980	4/56%	1985	5/44%	
Jane Fonda	1980	1/66%	2000	1/61%	
Tina Turner	1970	2/52%	1990	3/53%	
Cher	1982	2/57%	2002	1/70%	věk 12 let
Margaret Thatcher	1970	1/57%	2000	1/61%	

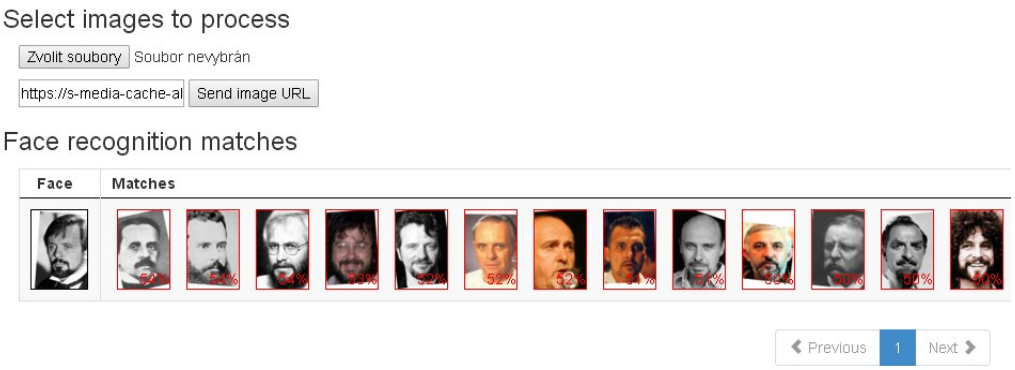
Z výše uvedené tabulky je patrné, že pouze v jednom případě (foto 1 pro Colina Farrella) byla jistota autentizace velmi vysoká. Tento případ je v Tab. 7 vyznačen zelenou barvou. V ostatních případech nedosahovala jistota (eventuelně účinnost- závisí na úhlu pohledu) uspokojivých hodnot, které by potvrzovaly její robustnost pro použití v praxi.

V některých případech nebyl obličej osobnosti přiřazen ke své identitě ani do desátého místa- tyto situace jsou v Tab. 7 zobrazeny červeně. V posledním sloupci Tab. 7 je uvedena poznámka, která uvádí nějakou zvláštnost v případě rozpoznávání zadaného obličeje. Např. Anthony Hopkins byl s velmi vysokou pravděpodobností vyhodnocen na fotografii číslo 1 jako asiat (viz Obr. 27).



Obr. 27 Ukázka výsledku analýzy fotografie.

Z této fotografie byl také Anthony Hopkins identifikován až na šestém místě s hodnotou jistoty rozpoznání 52 %. Tento výsledek byl ovlivněn tím, že v dané databázi nebyla uložena vhodná fotografie, která by zvýšila účinnost rozpoznávání (viz Obr. 28).



Obr. 28 Neúspěšná identifikace software BetaFace API.

Z podobného důvodu byla nízká jistota identifikace i u ostatních osob z databáze. V tomto případě, pro praktické nasazení a zvýšení účinnosti autentizace, je potřeba udržovat aktuální fotografie v databázích a úprava rozpoznávacích algoritmů, které budou více adaptibilní na radikální změnu vzhledu (vousy, změna barvy vlasů, podlitiny atd.).

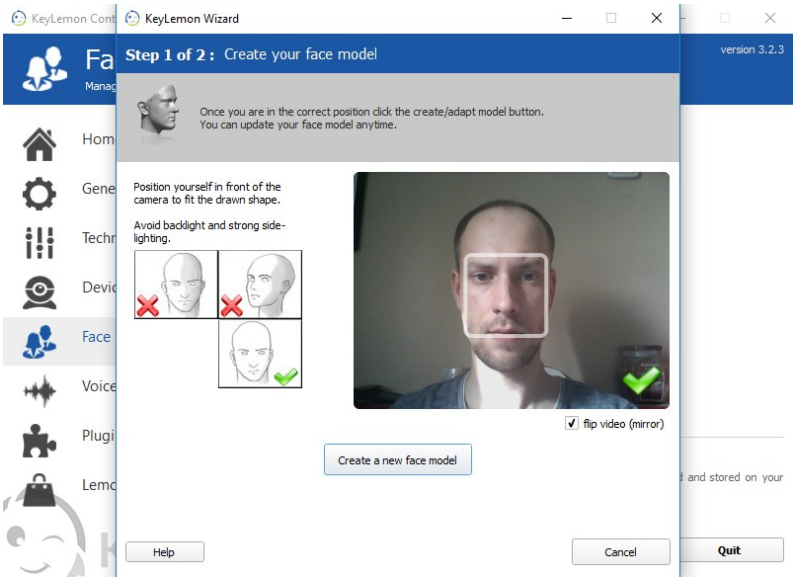
5.3.2 **KeyLemon**

Dalším programem, který poskytuje autentizaci za pomoci analýzy biometrie obličeje je KeyLemon. Tento software navíc nabízí i několik dalších možností biometrické autentizace,

které však závisí na zakoupené licenci. Funkčnost tohoto softwarového nástroje byla opět otestována na notebooku HP Compaq NX6126 s operačním systémem MS Windows 10 a připojenou kamerou Logitech přes USB port.

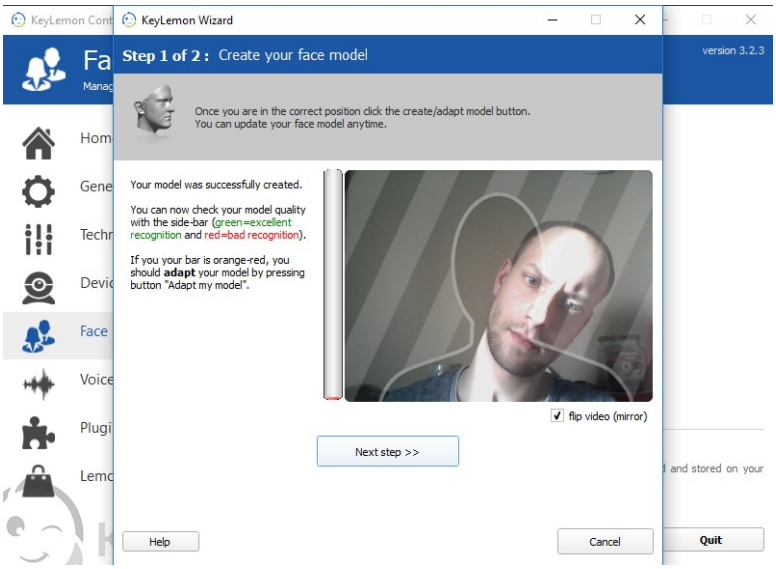
Licence tohoto programu, která je poskytována zdarma, měla značné problémy při rozpoznávání obličeje v případě více uživatelských účtů na testovacím počítači. Proto byl tento problém vyřešen vytvořením jednoho univerzálního uživatelského účtu, ke kterému byl ověřován přístup prostřednictvím biometrických příznaků obličeje. Samozřejmě byla pro každého uživatele z databáze (databáze subjektů stejná jako např. v části, která se zabývá praktickou analýzou otisku prstu) aktualizována vzorová fotografie pro přístup ke svému účtu.

Na Obr. 29 je znázorněno prvotní pořízení vzorové fotografie, ve které je potřeba korektního postavení obličeje ve snímku, které je znázorněno zelenou značkou v levém dolním rohu snímku.



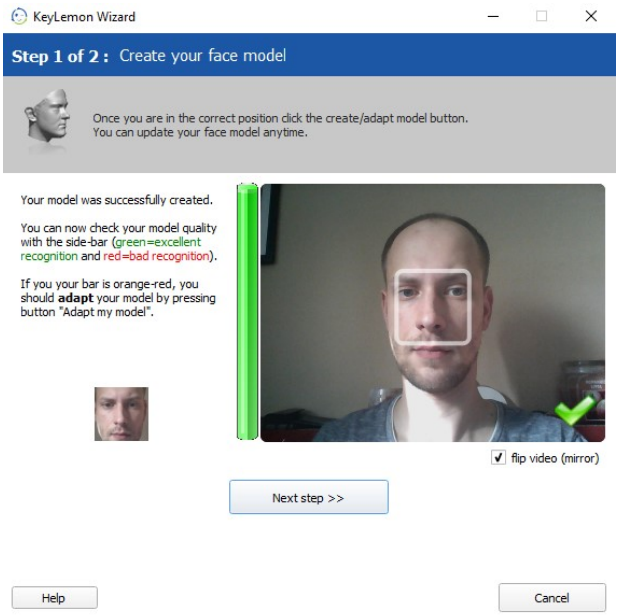
Obr. 29 Správně postavení obličeje.

Dále je potřeba sejmutí další fotografie pro vytvoření obličejového modelu. V tomto případě je nutné držet ramena i hlavu ve správné poloze, kterou znázorňuje šablona. Na Obr. 30 je patrné že kvalita (sloupec vlevo od snímku) je radikálně ovlivněna nakloněním/umístěním hlavy mimo vyznačenou oblast. V tomto případě by kvalita vytvořeného obličejového modelu byla minimální.



Obr. 30 Chybné postavení obličeje.

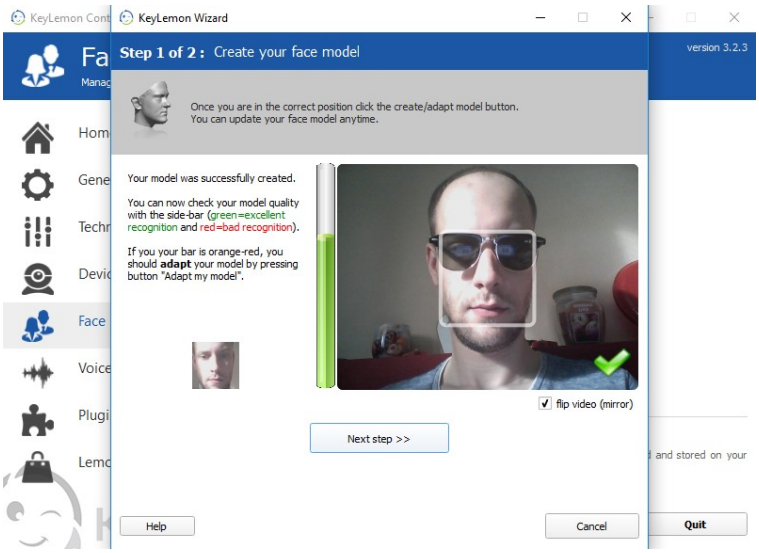
Obr. 31 ilustruje opačnou situaci, kdy obličej je posazen správně do snímku. Plně zelený sloupec vlevo od snímku znázorňuje potenciální vytvoření velmi kvalitního obličejového modelu.



Obr. 31 Vytvoření kvalitního obličejového modelu.

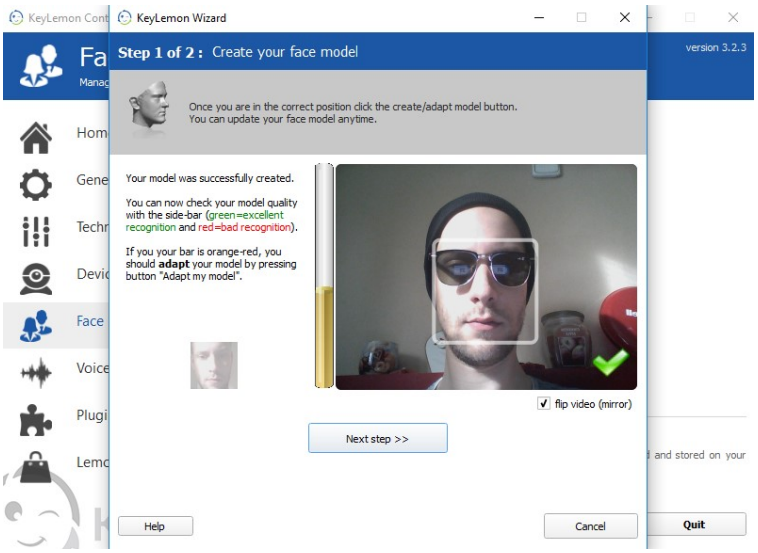
Jelikož nebylo nijak možné při přihlašovacím procesu k uživatelskému účtu kvantifikovat kvalitu rozpoznávání, tak byl proveden následující experiment. Obr. 32 prezentuje, že pokud

jsou nějakým způsobem zdeformovány, v tomto případě znehodnocení představují sluneční brýle, příznaky pouze v jedné části obličeje, tak úroveň rozpoznání, resp. vytvoření obličejového modelu, nabývá stále slušných hodnot. Tento jev je symbolizován zeleným sloupcem vlevo od pořízeného snímku.



Obr. 32 Degradace kvality obličejového modelu brýlemi.

Pokud dojde k deformaci i druhé obličejové části- v tomto případě čepice, tak dochází k značné degradaci úrovně rozpoznávání, které je znázorněno nízkou úrovní oranžového sloupce vlevo od analyzovaného snímku (viz Obr. 33). Pokud dojde k deformaci i ve třetí části obličeje (ústa, brada, apod.), spadne ukazatel kvality možného rozpoznání na své minimum podobně jako v Obr. 30.



Obr. 33 Degradace kvality pořízení modelu obličeje čepicí.

Jak již bylo zmíněno, úspěšnost rozpoznávání uživatele tímto softwarovým nástrojem nemohla být nijak kvantifikována, a ani nijak kvalitativně měřena. Z tohoto důvodu byl měřen pouze čas od zadání příkazu k identifikaci uživatele až po potvrzení autentizace. Jelikož by byly dosažené výsledky značně zkreslené, došlo se pouze ke globálnímu závěru tohoto testování. Závěr je tedy takový, že všichni uživatelé byli úspěšně rozpoznáni a přihlášeni ke svému účtu za dobu menší než 6 s. Tato doba byla hlavně závislá na aktuálním osvětlení (vytváření parazitních stínů na obličeji) a na prvotním natočení hlavy. Samozřejmě je možné tento interval snížit za pomoci uniformního prostředí a zvyknutí si uživatele jak se správně postavit před snímací kameru.

Obecně lze říci, že jde o kvalitní nástroj, pokud je na počítači vytvořen pouze jeden uživatelský účet, ke kterému je přiřazena autentizace za pomoci biometrických příznaků obličeje. Důležité je sdělit, že neoprávněný přístup byl také ověřen s tím výsledkem, že žádnému uživateli z databáze se nepodařilo přihlásit do operačního systému, pokud nebyl model jeho obličeje nastaven jako vzorový.

5.4 Hlas

Posledním biometrickým parametrem, který měl být prakticky otestován, je hlas. Jelikož je celkově oblast zpracování řeči ve vývoji, dostupných nástrojů pro autentizaci za pomoci analýzy hlasu je minimum, jelikož každé zlepšení efektivity si výrobce pečlivě střeží.

5.4.1 VeriSpeak

Jako první software, který měl být prakticky otestován, byl vybrán VeriSpeak. Po stažení 30denní trial verze se bohužel nepodařilo tento program zprovoznit ani na jednom operačním systému či jiném notebooku. Z tohoto důvodu byl otestován další softwarový nástroj, který umožňuje autentizaci na základě analýzy hlasu.

5.4.2 KeyLemon

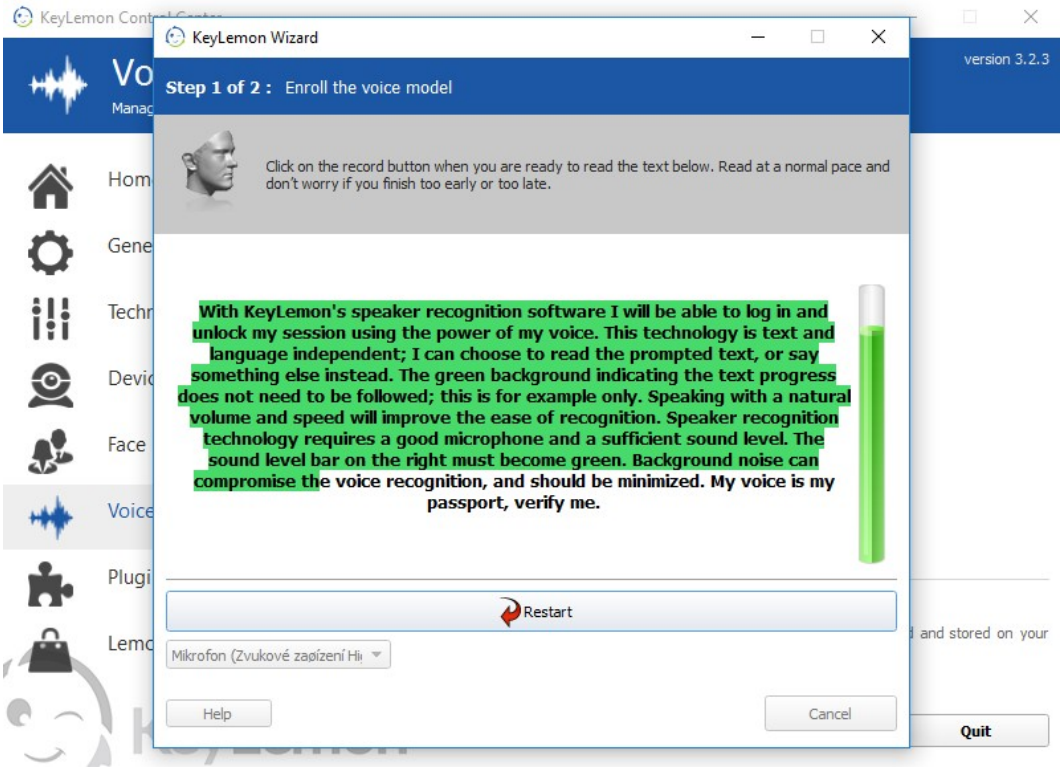
KeyLemon je tedy komplexní software, který obsahuje i část poskytující autentizaci pomocí analýzy hlasu uživatele. Tato část byla prakticky otestována v této bakalářské práci jako náhrada za software VeriSpeak, který se bohužel nepodařilo zprovoznit.

Jelikož je zabezpečení uživatelského účtu plně rozvinuto až v nejvyšší (Gold) licenci software KeyLemon, byly otestovány pouze jeho omezené možnosti, které se skládaly

z vytvoření hlasového vzoru mluvčího, a otestování, zda-li byl úspěšně identifikován či nikoliv.

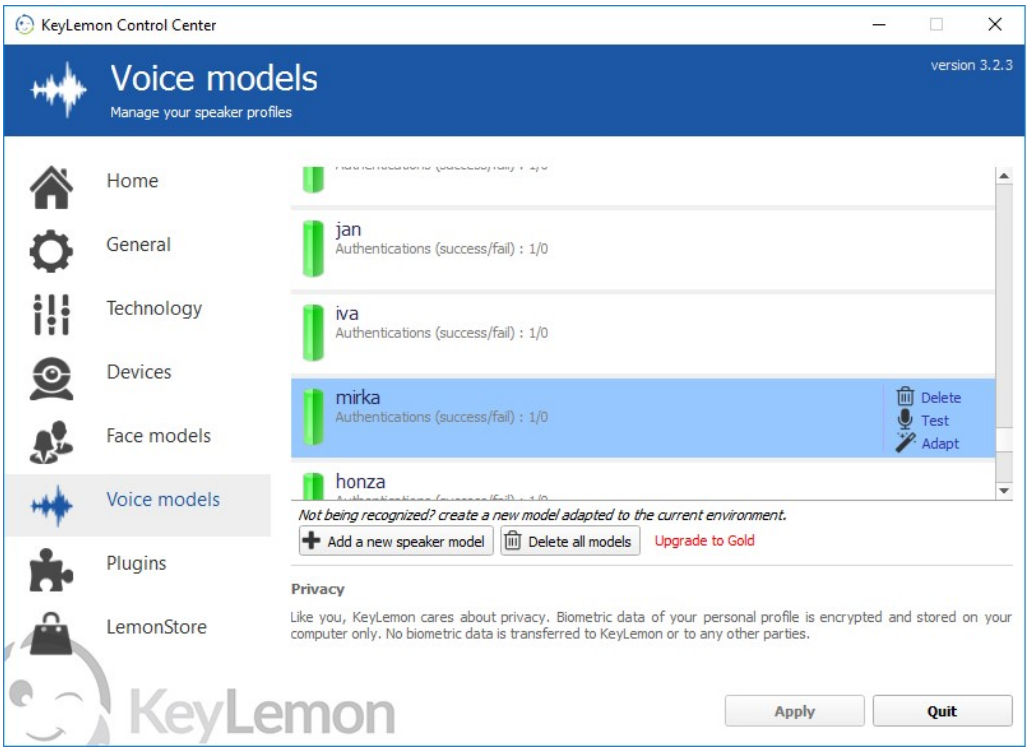
Pro vytvoření hlasového vzoru je nejprve nutné, aby uživatel hovořil po delší dobu (cca 1 minutu) vhodnou intenzitou hlasu, jejíž úroveň je znázorněna pravým sloupcem, viz Obr. 34. Vhodná úroveň dynamiky hlasu je zobrazena zelenou barvou.

Vzhledem k tomu, že je tento nástroj textově i jazykově nezávislý, je skutečně potřeba, aby uživatel mluvil v prvotní fázi co nejdelší dobu. Pro tento účel může předčítat uvedený text, který je zeleně podbarvován, aby naznačil tempo řeči, anebo uživatel může samozřejmě mluvit libovolný text.



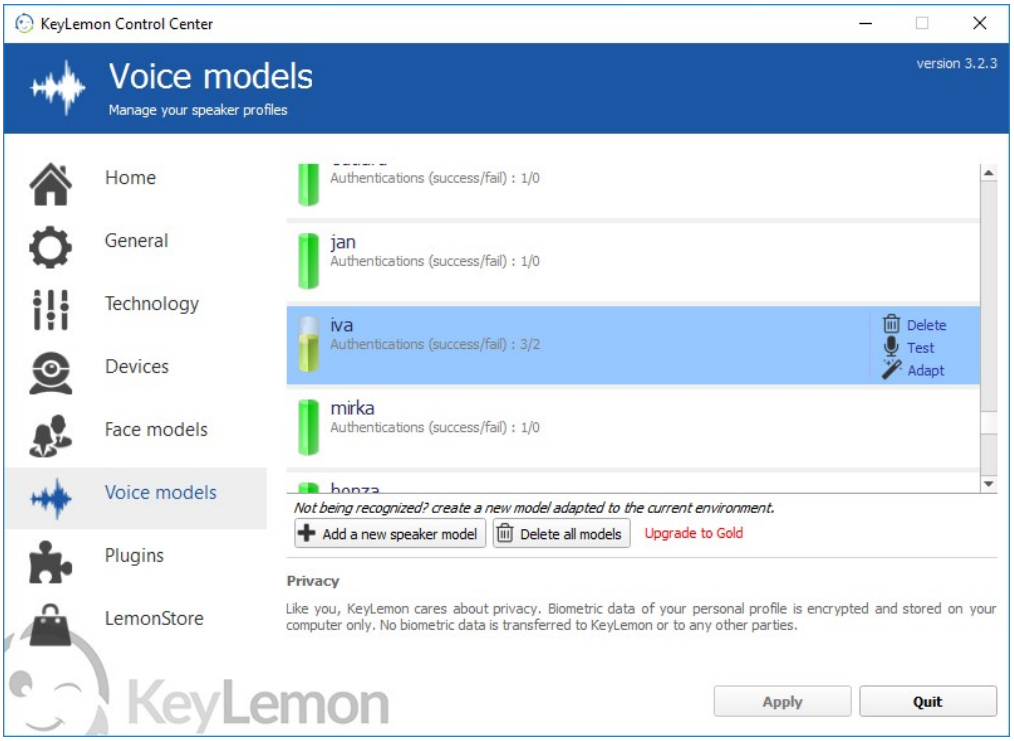
Obr. 34 KeyLemon – pořizování hlasového vzoru.

Po vytvoření uživatelské účtu a hlasového „razítka“ je možné v základní verzi KeyLemon pouze otestovat, zda-li je uživatel rozpoznán či nikoliv. Tato situace je zobrazena na Obr. 35.



Obr. 35 KeyLemon – verifikace mluvčích

Pokud je uživatel otestován, je k jeho jménu uvedena statistika kolikrát byl úspěšně a neúspěšně identifikován, viz Obr. 36.



Obr. 36 KeyLemon – průběžné výsledky testování.

Vzhledem ke značně omezeným testovacím možnostem této části software KeyLemon, byla zvolena následující metodika otestování efektivity autentizace. Každý uživatel z již dříve popsané databáze si nejprve vytvořil svůj hlasový vzor. Po zkompletování všech vzorů, každý uživatel byl jednotlivě otestován tak, že byl vyzván k tomu, aby pronesl úsek řeči o délce cca 10 s. Poté byl tento úsek zanalyzován a porovnán s příslušným vzorem, jehož výsledek mohlo být zamítnutí (NE) identity uživatele, její potvrzení (ANO), a nebo vyzvání k opakovanému otestování (ZNOVU).

Každý uživatel byl testován tak, že bylo potřeba, aby byla celkem desetkrát potvrzena jeho identita, přičemž byl zaznamenáván počet ANO, NE a ZNOVU. Naměřené hodnoty jsou uvedeny v Tab. 8, kde jsou hodnoty úspěšnosti a efektivity vyšší než 90 % vyznačeny zeleně. Tyto hodnoty jsou velice uspokojivé.

Úspěšnost můžeme definovat jako převrácenou hodnotu nutného počtu pokusů na jedno úspěšné přihlášení. Jinak řečeno- snadnost přihlášení. Úspěšnost α je tedy definována pro *i*-tého mluvčího vztahem

$$\propto_i = \frac{ANO_i}{ANO_i + NE_i + ZNOVU_i} \cdot 100\ [\%]$$

kde *ANO, NE* a *ZNOVU* jsou příslušné počty potvrzení či zamítnutí uživatele, či vyzvání k opakování pokusu o autentizaci. Efektivitu ε můžeme v tomto případě definovat jako falešný poplach, resp. zamítnutí oprávněné autentizace v procentech. Efektivita ε je pro mluvčího *i* popsána rovnicí

$$\varepsilon_i = \frac{ANO_i}{ANO_i + NE_i} \cdot 100\ [\%]$$

Z omezených možností testované programu nebylo možné vyzkoušet robustnost této části vůči chybné detekci, kdy je nesprávně potvrzena identita uživatele.

Tab. 8 KeyLemon – hlas, získané výsledky.

	ANO	*NE*	*ZNOVU*	*α* [%]	*ε* [%]
Z1	10	0	5	67	100
Z2	10	9	4	43	53
Z3	10	0	7	59	100
Z4	10	3	8	48	77
Z5	10	0	3	77	100
Z6	10	1	0	91	91
Z7	10	2	8	50	83
Z8	10	5	2	59	67
Z9	10	0	3	77	100
Z10	10	5	6	48	67
Z11	10	8	0	56	56
Z12	10	0	3	77	100
M1	10	11	5	38	48
M2	10	0	7	59	100
M3	10	7	1	56	59
M4	10	0	4	71	100
M5	10	0	3	77	100
M6	10	3	3	63	77
M7	10	3	7	50	77
M8	10	4	2	63	71

Průměrná hodnota dosažené efektivity autentizace za pomoci analýzy hlasu byla v tomto případě 81,3 %, což by bylo možné hodnotit jako velice slušnou hodnotu, kdyby nebyly dosaženy nízké hodnoty efektivity např. u M1, Z11 atd.

5.5 Zpracování výsledků

Vzhledem k omezenému počtu testovaných osob v databázi je vhodné naměřené hodnoty efektivity ε aplikovat na celou populaci. Za tímto účelem je využívána statistická metoda MLE (Maximum Likelihood Estimation), která je v češtině známá jako metoda maximální věrohodnosti. Její matematický i detailní popis lze nalézt v literatuře, např. v (Dupač, 2005) nebo v (Harris, 1998). Obecně lze říci, že např. za pomoci odhadu průběhu kumulativní pravděpodobnosti, jsou odhadovány základní parametry výsledného rozdělení, u kterého je předpoklad normálního rozložení. Odhad výsledného průběhu kumulativní pravděpodobnosti se řídí maximalizací logaritmické hodnoty pravděpodobnosti. Při dosažení tohoto maxima, popř. uspokojivé hodnoty, je možné s určitou pravděpodobností považovat získané hodnoty odhadnutého rozložení za relevantní. Jelikož nebyl k dispozici

žádný vhodný sofwarový nástroj, který by složitý matematický popis metody značně zjednodušil, tak bohužel nebylo možné odhadnout v rámci této bakalářské práce parametry MLE, které by byly získané aplikací na hodnoty efektivity ε analýzy otisku prstu (Tab. 3) a analýzy hlasu (Tab. 8).

Z tohoto důvodu teoretické hodnoty výše zmíněných hodnot efektivity ε posuzovány pouze z hlediska intervalových odhadů průměru μ a směrodatné odchylky σ za předpokladu normálního rozdělení a 95% intervalu spolehlivosti.

Intervalový odhad střední hodnoty μ je dán vztahem

$$P\left(\mu_\varepsilon - \frac{\sigma}{\sqrt{n-1}} \cdot u_{1-\frac{\delta}{2}} < \mu < \mu_\varepsilon + \frac{\sigma}{\sqrt{n-1}} \cdot u_{1-\frac{\delta}{2}}\right) = 1 - \delta$$

kde n je počet analyzovaných prvků souboru (v tomto případě 20), δ je interval chyby (aktuálně 5 %, resp. 0,05), u je příslušný kvantil normovaného normálního rozdělení, a μ_ε a σ_ε jsou reálné hodnoty průměru a směrodatné odchylky získané efektivity.

Intervalový odhad směrodatné odchylky je dán vztahem

$$P\left(\sqrt{\frac{n \cdot \sigma^2}{\chi^2_{\frac{\delta}{2}}(n-1)}} < \sigma < \sqrt{\frac{n \cdot \sigma^2}{\chi^2_{1-\frac{\delta}{2}}(n-1)}}\right) = 1 - \delta$$

kde χ^2 značí příslušný kvantil chí kvadrát rozdělení.

Naměřené hodnoty střední hodnoty a směrodatné odchylky efektivity ε je uvedena v Tab. 9.

Tab. 9 Základní statistické údaje vybraných efektivit.

	ε [%]	
Software	μ	σ
HP Credential Manager	99,815	0,42341
KeyLemon - Hlas	81,3	18,0447

Z těchto hodnot jsou vypočtené hodnoty příslušných intervalových odhadů uvedeny v Tab. 10.

Tab. 10 Intervalové odhady statistických parametrů vybraných efektivit.

Software	ε [%]	
	Intervalový odhad μ	**Intervalový odhad σ**
HP Credential Manager	$P(99{,}625 < \mu < 100) = 0{,}95$	$P(0{,}343 < \sigma < 0{,}578) = 0{,}95$
KeyLemon - Hlas	$P(73{,}186 < \mu < 89{,}414) = 0{,}95$	$P(14{,}617 < \sigma < 24{,}672) = 0{,}95$

Pomocí intervalových hodnot lze tedy dospět k dalšímu dílčímu závěru, ve kterém bude zejména zdůrazněna stabilita dosažených výsledků autentizace za pomoci analýzy otisku prstu, kdy s 95% spolehlivostí bude střední hodnota efektivity ε z rozsahu 99,625 až 100 % a hodnota směrodatné odchylky efektivity ε z rozsahu 0,343 až 0,578 %. I když lze předpokládat, že reálně získané výsledky pro co nejvyšší možný počet osob budou dosahovat nižší hodnoty střední hodnoty, resp. vyšší hodnoty směrodatné odchylky, představuje tento intervalový odhad, že biometrie otisku prstu představuje velmi robustní řešení autentizace. Tento jev však momentálně neplatí o analýze hlasu, kdy je s 95% pravděpodobností střední hodnota efektivity autentizace o cca 10 až 30 % nižší než pro otisk prstu, a intervalový odhad směrodatné odchylky je několikanásobně vyšší. I přes tento fakt a předpoklad, že reálné výsledky budou nabývat horší hodnot než uvedených v Tab. 10 lze tvrdit, že biometrie analýzy hlasu dosáhla velice slušných výsledků efektivity, které však naznačují ještě další nutný vývoj v této oblasti biometrické autentizace.

5.6 Diskuse

Touto praktickou částí byla za pomoci pěti různých softwarových nástrojů otestována autentizace za pomoci analýzy jednoho ze čtyř vybraných biometrických znaků. Jak je patrné z naměřených výsledků, všechny metody mají největší slabinu v rychlosti zpracování analyzovaného biometrického znaku, v jeho korektním pořízení pro následnou správnou autentizaci a rovněž v efektivitě autentizačního procesu. Vzhledem k původně zamýšlené aplikaci v menší/střední firmě a velikosti potencionální rizika s přístupy uživatelů k počítačům či do kýžených prostor, nelze žádnou z vybraných biometrických autentizačních metod doporučit pro celkové zabezpečení společnosti, ale pouze pro individuální zabezpečení jako další stupeň ochrany před neoprávněným přístupem. Toto tvrzení je samozřejmě postavené na základě výsledků, které byly získány dostupnými bezplatnými licencemi testovaných softwarových nástrojů, a může se změnit v závislosti na zakoupení komerční

licence, kdy bude plně využívána podpora jednotlivých nástrojů. Je však zcela diskutabilní a na zcela na místě, zda-li by se nějak rapidně zvýšila efektivita a rychlost jednotlivých biometrických metod, aby se snížilo zdržení při autentizačním procesu a minimalizovala pravděpodobnost chybné autentizace. Tedy je zcela evidentní, že dosavadní řešení zabezpečení přístupu pomoci velmi silných hesel a přístupových karet je nejen dostačující, ale efektivnější a spolehlivější než jakákoliv výše prezentovaná biometrická autentizační metoda.

6 Závěr

Tato bakalářská práce se zabývala rozborem, otestováním a praktickým nasazením autentizačních metod, které využívají analýzu biometrických znaků. Po důkladném prozkoumání momentálně analyzovaných biometrických znaků a možností nabízených softwarových nástrojů, byly vybrány čtyři biometrické znaky, které byly dále prakticky otestovány, resp. jejich účinnost atd. Konkrétně se jednalo o otisk prstu, dynamiku stisku kláves, obličej a hlas. Bohužel se až postupem času ukázalo, že některé nástroje, které výrobci poskytují k vyzkoušení, nelze v pořádku otestovat či stáhnout. Z tohoto důvodu, došlo k otestování menšího počtu softwarových nástrojů, než bylo původně naplánováno. O to však důkladněji byl každý nástroj otestován za pomoci vhodně vytvořené databáze čítající 20 jedinců.

Z praktického otestování jednotlivých biometrických parametrů dopadl nejlépe otisk prstu, u kterého bylo dosaženo průměrné hodnoty efektivity správného rozpoznání identity uživatele o velikosti přibližně 99,8 % (za pomoci HP Credential Manager). I když došlo v ojedinělých případech k chybné detekci uživatele, je tato metoda nejvíce spolehlivá, a tudíž jako jediná připravená k praktické aplikaci. Její nevýhodou je však možné zdržení při přihlašovacím procesu, neboť (jak bylo prakticky dokázáno) někteří uživatelé mají značné problémy se správným přejetím prstu přes čtečku otisků.

Jako dalším použitelným biometrickým znakem pro praktickou aplikaci se osvědčila dynamika úderů klávesnice. Vzhledem k nutné znalosti hesla a způsobu jeho zadávání, je tato metoda velice robustní, a to tak, že i většina uživatelů z databáze měla problémy s přihlášením ke svému účtu. Tento fakt by bylo možné potlačit snížením prahové hodnoty podobnosti aktuálně zadaného hesla se vzorem či důkladnějším naučením zadávání přihlašovacího hesla uživatele. Právě z tohoto důvodu není příliš vhodné aplikovat analýzu tohoto biometrického znaku mezi větší množství uživatelů, např. firma, aby se předešlo možné integraci vzniklých problémů s přihlášením či přístupem.

Obličej a hlas byly zvoleny jako další biometrické znaky, které byly prakticky ověřeny. I když se jedná o velmi zajímavá řešení autentizace, není je dle mého názoru vhodné prakticky aplikovat mezi více uživatelů z časových i bezpečnostních důvodů, avšak se jedná o velice zajímavé a pohodlné řešení soukromého zabezpečení operačního systému.

Vzhledem k dosaženým praktickým poznatkům, cenám nabízených softwarových nástrojů a původní plánované aplikaci, nelze doporučit nasazení těchto metod k běžnému používání ve vybrané menší firmě o počtu cca 120 zaměstnanců. Dosavadní řešení

zabezpečení přístupu do počítačů i prostor za pomoci velmi silných přístupových hesel, jejich časté obměny, a přístupových karet je dostatečné řešení, které je časově velmi efektivní a málo problémové. Přihlédneme-li však k faktu, že vývoj autentizačních metod založených na biometrických znacích je stále ve svém rozmachu, třeba bude za několik (desítek) let jiná situace, kdy tyto metody budou zcela bezpečné a natolik efektivní, že upustí od zabezpečení běžnými hesly, přístupovými kartami, apod. Momentálně tomu však není, i když se jedná o velice zajímavou a v budoucnu určitě perspektivní aplikaci informačních komunikačních technologií.

7 Seznam použitých zdrojů

Knižní publikace

DUPAČ, V. - HUŠKOVÁ, M. *Pravděpodobnost a matematická statistika*. Praha: Nakladatelství Karolinum, 2005. ISBN 80-246-0009-9

HARRIS, J. W. - STOCKER, H. *Maximum Likelihood Method, Handbook of Mathematics and Computational Science*. New York: Springer-Verlag, 1998.

JAIN, A. K. - BOLLE, R. M. - PANKATI. S. *Personal Identification in Networked Society*. New York: Springer-Verlag, 2006. ISBN 978-0-387-32659-7

JAIN, A. K. - FLYNN, P. - ROSS, A. *Handbook of Biometrics*. New York: Springer-Verlag, 2008. ISBN 978-0-387-71041-2

RAK, R. - MATYÁŠ, V. - ŘÍHA, Z. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: GRADA, 2008. ISBN 978-80-247-2365-5

Příspěvek ve sborníku a článek v seriálové publikaci

BAKER, S. E. – HENTZ, A. – BOWYER, K. W. – FLYNN, P. Degradation of iris recognition performance due to non-cosmetic prescription contact lenses. *Computer Vision and Image Understanding*, 2010, vol. 114, no. 9, p. 1030–1044.

DAUGMAN, J. How iris recognition works. *Proceedings of 2002 International Conference on Image Processing*, 2002, p. 33-36.

DODDINGTON, G. R. Speaker recognition – Identifying people by their voices. *Proceedings of IEEE*, 1985, vol. 73, no. 11, pp. 1651-1664.

JAFRI, R. A Survey of Face Recognition Techniques, *Journal of Information Processing Systems*, 2009, vol. 5, no. 2, pp. 41-68.

JAIN, A. K. Biometric recognition: Q&A. *Nature*, 2007, no. 449, p. 38–40.

KRHOVJÁK, J. - MATYÁŠ, V. Autentizace a identifikace uživatelů. *Zpravodaj ÚVT MU*. 2007, p. 1-5. ISSN 1212-0901

LU, Y. – GONGPING, Y. – YIN, Y. – LIZHEN, Z. A Survey of Finger vein recognition. *Lecture Notes in Computer Science*, 2014, vol. 8833, p. 234-243.

PFLUG, A. – BUSCH, C. Ear biometrics: A survey of detection, feature extraction and recognition methods. *IET Biometrics*, 2012, vol. 1, no. 2, p. 114-129.

ROSS, A. - JAIN, A. K. Human Recognition Using Biometrics: An Overview. *Annals of Telecommunications*, 2007, vol. 62, no. 1-2, p. 11-35.

RUSS, J. C. - WOODS, R. P. The Image Processing Handbook. *Journal of Computer Assisted Tomography*, 1995, vol. 19, no. 6, p. 979-981.

SANGEKAR, S. S. - DHAWANI, D. C. Survey of Various Techniques for Signature Recognition and Verification. *International Journal of Science and Research*, 2014, vol. 3, no. 11, pp. 1520-1522. ISSN 2319-7064

SAQUIB, Z. - SALAM, N. - NAIR, R. P. - PANDEY, N. - JOSHI, A. A Survey on Automatic Speaker Recognition Systems. *Communication and Information Science*, 2010, vol. 123, pp. 134-145. ISBN 978-3-642-17641-8

ZHANG, Z. - HU, M. - WANG, Y. A Survey of Advances in Biometric Gait Recognition, *Lecture Notes in Computer Science*, 2011, pp. 150-158.

Webové stránky a příspěvky na webových stránkách

ALL IN ONE COMPUTING AND ELECTRONICS. *Biometric Installation* [online]. 2016. [cit. 2016-6-22]. Dostupné z: http://www.aioc.co.uk/biometric.php

ANDROID AUTHORITY. *UMIDIGI Z Pro international giveaway!* [online]. 2016. [cit. 2016-11-8]. Dostupné z: http://www.androidauthority.com/umidigi-z-pro-international-giveaway-754766

AWARE. *Nexa fingerprint recognition* [online]. 2016. [cit. 2016-11-8]. Dostupné z: http://www.aware.com/biometrics/nexa-fingerprint-recognition

BETAFACE API. *BetaFace API* [online]. 2016. [cit. 2016-11-8]. Dostupné z: https://www.betafaceapi.com/demo.html

BIOMETRIC SOLUTIONS. *Review: Keylemon face recognition* [online]. 2016. [cit. 2016-10-30]. Dostupné z: http://www.biometric-solutions.com/review-keylemon-face-recognition.html

BIOMETRIC SOLUTIONS. *Review NCheck finger attendance* [online]. 2016. [cit. 2016-11-6]. Dostupné z: http://www.biometric-solutions.com/review-ncheck-finger-attendance.html

ČERMÁK, M. *Autentizace* [online]. 2009. [cit. 2016-5-8]. Dostupné z: http://www.cleverandsmart.cz/autentizace/

ISECOM. *Open Source Security Testing Methodology Manual (OSSTMM)* [online]. 2016. [cit. 2016-7-8]. Dostupné z: http://www.isecom.org/research

KEYTRAC. *KeyTrac* [online]. 2016. [cit. 2016-11-8]. Dostupné z: https://www.keytrac.net/en

NEUROTECHNOLOGY. *VeriFinger* [online]. 2016. [cit. 2016-11-8]. Dostupné z: http://www.neurotechnology.com/verifinger.html

NEUROTECHNOLOGY. *VeriSpeak* [online]. 2016. [cit. 2016-9-12]. Dostupné z: http://www.neurotechnology.com/verispeak.html

NEXT BIOMETRICS. *Fingerprint* [online]. (JPG). 2016. [cit. 2016-11-8]. Dostupné z: http://nextbiometrics.com/filarkiv/article_images/_green_all5_text.jpg

PATRICK, A. *BioPassword* [online]. 2009. [cit. 2016-11-8]. Dostupné z: http://www.andrewpatrick.ca/biometrics/biopassword/biopassword.shtml

SOFTPEDIA. *BioKeyLogon* [online]. 2016. [cit. 2016-11-8]. Dostupné z: http://www.softpedia.com/get/Security/Security-Related/BioKeyLogon.shtml

SOFTPICKS. *NCheck finger attendance* [online]. 2016. [cit. 2016-11-8]. Dostupné z: http://www.softpicks.net/software/Business/Miscellaneous/NCheck-Finger-Attendance-Trial-118935.htm

SOFTWARE INFORMER. *Credential manager for HP ProtectTools* [online]. 2016. [cit. 2016-11-30]. Dostupné z: http://credential-manager-for-hp-protecttools.software.informer.com

TECHFRESH. *Samsung EZON digital door lock series* [online]. 2011. [cit. 2016-7-8]. Dostupné z: http://www.techfresh.net/samsung-ezon-digital-door-lock-series

THE PRIVACY SURGEON. *MasterCard will begin trials of face recognition software to authorize payments - let the travesty begin!* [online]. 2016. [cit. 2016-7-22]. Dostupné z: http://www.privacysurgeon.org/blog/incision/mastercard-will-begin-trials-of-face-recognition-software-to-authorize-payments-let-the-travesty-begin

WIKIMEDIA COMMONS. *Right eye retina* [online]. 2016. (JPG). [cit. 2016-7-22]. Dostupné z: https://commons.wikimedia.org/wiki/File:Righ_eye_retina.jpg

ZVETCO BIOMETRICS. *P6500 Fingerprint device* [online]. 2012. [cit. 2016-7-22]. Dostupné z: http://www.zvetcobiometrics.com/Products/P6500/features.php

ZICOM. *Fingerprint lock* [online]. 2014. [cit. 2016-7-8]. Dostupné z: http://zicom.com/fingerprint-locks/finger-print-lock.html

Vysokoškolské kvalifikační práce

BUJNOŠKOVÁ, E. *Využití snímků sítnice v biometrii*. Brno, 2011. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Vedoucí bakalářské práce doc. Ing. Radim Kolář, Ph.D.

DOHNÁLEK, T. *Průběžná verifikace osob na základě dynamiky stisku kláves*. Brno, 2012. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Michal Doležel.

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

MLÝNKOVÁ, B. *Databáze nebiometrických a sekundárních biometrických znaků osob*. Brno, 2015, Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií. Vedoucí práce Ing. Pavel Dvořák, Ph.D.

ZEMAN, T. *Aplikace biometrických systémů*. Praha, 2011. Bakalářská práce. Bankovní institut vysoká škola v Praze. Vedoucí práce Mgr. Miroslav Široký, DiS.