MASARYKOVA UNIVERZITA
FAKULTA INFORMATIKY

Srovnávací testy vybraných biometrických zařízení

BAKALÁŘSKÁ PRÁCE

Lukáš Adamec

Brno, Jaro 2009

Prohlášení

Prohlašuji, že tato práce je mým původním autorským dílem, které jsem vypracoval samostatně. Všechny zdroje, prameny a literaturu, které jsem při vypracování používal nebo z nich čerpal, v práci řádně cituji s uvedením úplného odkazu na příslušný zdroj.

Poděkování

Rád bych poděkoval všem osobám, s jejichž pomocí tato práce vznikla. Předně bych rád poděkoval doc. RNDr. Václavu Matyášovi, M.Sc., Ph.D. za cenné rady, ochotu a vedení práce. Dále bych chtěl poděkovat Ing. Mgr. Zdeňku Říhovi, Ph.D. za podporu týkající se technických záležitostí. V neposlední řadě patří mé poděkování také všem dobrovolníkům, díky kterým bylo možné provést testování biometrických zařízení a bez nichž by tato práce nebyla realizovatelná.

Shrnutí

Tato bakalářská práce se zabývá biometrickými metodami autentizace osob. Důraz je kladen především na otisky prstů a rozpoznávání tváře.

Cílem práce je otestování několika systémů založených na výše zmíněných biometrikách. Testování se snaží simulovat použití biometrických metod pro autentizaci uživatelů a řízení přístupu v běžných aplikacích bezpečnostního inženýrství, kde by biometriky mohly být použity jako alternativa k autentizaci pomocí hesel nebo tokenů. Jednotlivé systémy jsou následně srovnány jak v rámci samostatných technologií, tak i obě technologie mezi sebou.

Klíčová slova

Biometrika, otisk prstu, tvář, autentizace, FAR, FRR

Obsah

Kapitola 1

Úvod

Autentizace neboli proces ověření a ustavení identity patří už od pradávna k základním principům využívaným při zajišťování bezpečnosti a řízení přístupu v mnoha oblastech lidského života [1]. Archeologické nálezy dokazují, že již obyvatelé prehistorické Číny využívali jedinečnosti otisků prstů k ověření identity osoby [2]. Příklady využití autentizačních metod v dnešní době mohou být řízení přístupu do objektů či místností, používání platebních karet, zadávání přístupových hesel v počítačových aplikacích nebo i pasová kontrola.

Proces ověření identity (autentizace) umožňuje prokázat, že osoba předkládající nějaké tvrzení o své totožnosti je skutečně tou osobou, za kterou se vydává. Ověření identity lze v zásadě provést jednou ze tří základních autentizačních metod:

- *Něco, co známe.* Metoda stavějící na znalosti tajné informace známé pouze oprávněné osobě. Typicky se jedná o znalost hesla nebo PINu.
- *Něco, co máme.* Uživatel vlastní nějaký technický prostředek, tzv. token. Může jím být například klíč nebo čipová karta.
- *Něco, co jsme.* Identifikace na základě biometrických charakteristik člověka, například otisku prstu.

Každá z uvedených metod má své výhody i nevýhody. Proto lze jednotlivé metody vzájemně kombinovat za účelem dosažení vyšší úrovně bezpečnosti a záruky za správné ověření identity. Příkladem může být kombinace čipové karty a PINu [3]. Bližší informace týkající se autentizace jsou obsahem druhé kapitoly.

Ve své práci se zaměřuji na biometrické metody autentizace osob. Jsou založeny na automatizovaném měření a porovnávání biometrických charakteristik člověka. Biometrické charakteristiky (biometriky) jsou měřitelné fyziologické nebo behaviorální (na chování založené) vlastnosti, které jsou pro každého člověka jedinečné a tudíž využitelné k ověření identity. Mezi měřitelné fyziologické charakteristiky lze zařadit otisk prstu, vzor oční duhovky nebo obličejové rysy. Mezi behaviorální vlastnosti patří například dynamika podpisu nebo hlasové charakteristiky [4, 5]. Podrobněji jsou biometriky a biometrické technologie popsány v kapitole 3.

Cílem této práce je, jak již název napovídá, srovnání vybraných biometrických zařízení na základě mnou navržených a provedených testů. Konkrétně se jedná o srovnání biometrických zařízení dostupných v Laboratoři bezpečnosti a aplikované kryptografie Fakulty informatiky Masarykovy univerzity. V laboratoři jsou využívány technologie založené na srovnávání otisků prstů a rozpoznávání tváře. V rámci této práce testuji čtyři zařízení pro snímání otisků prstů a dva softwarové produkty pro rozpoznávání obličeje na základě obrazu získaného pomocí webové kamery, resp. pro další testování nahraného z uloženého obrazu.

Kapitola 4 se zabývá popisem testovaných biometrických zařízení. V oblasti otisků prstů se jedná o zařízení Microsoft Fingerprint Reader a APC Biopod, což jsou čtečky otisků prstů určené pro běžné uživatele počítačů jako alternativa k autentizaci pomocí hesel. Do stejné oblasti dále spadají zařízení Bioscrypt V-Pass a Cross Match Verifier 300 LC2. Tyto čtečky se řadí mezi kvalitnější typy běžně využívané na profesionální úrovni, například jako autentizační metoda

zajišťující řízení přístupu do objektů. Ve druhé oblasti testování, kterou je rozpoznávání obličeje, se zájem soustředí na software VeriLook od společnosti Neurotechnology, konkrétně na jeho aktuální verzi VeriLook 3.2 Standard SDK. Snímání obličeje probíhá prostřednictvím webové kamery Creative WebCam Live! Motion. Druhým zástupcem v této oblasti je software od společnosti Luxand, a to ukázková aplikace demonstrující využití knihovny pro detekci a rozpoznávání tváře Luxand FaceSDK 1.7.

Testování má dvě části. V první části analyzuji možnosti jednotlivých biometrických autentizačních systémů. To se týká zejména správné konfigurace zařízení prostřednictvím dostupných softwarových nástrojů, správy otisků prstů, procesu registrace osob a možností následné autentizace zaregistrovaných osob.

Druhou částí je otestování systémů na netriviálním počtu osob. Pro účely této práce bylo stanoveno rozmezí 30–50 osob. Na základě provedené analýzy systémů jsem testování navrhl tak, že každá osoba projde procesem registrace a následně absolvuje minimálně pět pokusů o autentizaci na každém z testovaných zařízení. Deset z těchto osob se dále autentizuje s časovým odstupem jednoho měsíce. Na základě těchto testů srovnávám jednotlivé systémy z hlediska chybovosti, uživatelské přívětivosti a náročnosti na administrativu systému. Testování a vyhodnocení výsledků se věnuje kapitola 5.

V závěru práce hodnotím, který systém je vhodný pro případné nasazení v praxi jako náhrada za jinou autentizační metodu a který naopak vhodný není, protože jeho použití by mohlo vést k nespokojenosti uživatelů nebo snížení bezpečnosti. Zároveň se pokouším přiblížit, jak může podobné testování přispět k rozvoji technologií založených na biometrikách.

Kapitola 2

Autentizace

V každodenním životě se často setkáváme se situacemi, které vyžadují ověření naší identity (autentizaci), tedy co možná nejpřesnější určení, kdo daná osoba ve skutečnosti je. Důležitým požadavkem při ověřování identity osoby je spolehlivost takového procesu, která umožňuje rozlišit oprávněné osoby od útočníků nebo jiných hrozeb, čímž zvyšuje bezpečnost daného systému a poskytuje vyšší míru ochrany před zneužitím neoprávněnou osobou.

Požadavky na zajištění bezpečnosti se systém od systému liší. Jiné požadavky budou kladeny na systém řízení přístupu do jaderné elektrárny, kde selhání bezpečnostního systému může vést až k vážnému ohrožení lidských životů a jiné pro řízení přístupu studentů do počítačové studovny.

2.1 Základní terminologie

Při ověřování identity osoby je nutné rozlišit mezi pojmy autentizace a autorizace.

- *Autentizace* – proces ověření a tím i ustavení identity osoby s požadovanou mírou záruky, tzn. že osoba předkládající nějaké tvrzení o své totožnosti je skutečně tou osobou, za kterou se vydává. [6]

- *Autorizace* – proces přidělení určitých oprávnění (na základě identity uživatele) a určení povolených aktivit, které může uživatel v systému vykonávat. Proces autorizace obvykle navazuje na úspěšnou autentizaci uživatele. [6]

Příklad rozdílu mezi výše zmíněnými pojmy: Zaměstnanec jménem Bob dá výpověď. Následně je mu odebrán přístup k firemním zdrojům, ke kterým měl jako zaměstnanec přístup. Firemní počítače mohou Boba stále spolehlivě autentizovat, avšak nyní již bez povolení přístupu k dříve používaným zdrojům informací. [1]

K autentizaci uživatele se zpravidla využívá jeden z následujících přístupů. Jedná se buďto o verifikaci (autentizaci), nebo o identifikaci.

- *Verifikace (autentizace)* – 1:1; proces ověření identity, kdy osoba předkládá tvrzení o své identitě. Databáze autentizačních informací se neprochází celá. Systém vyžaduje od uživatele vstupní data (typicky uživatelské jméno nebo token), čímž se získá jeden záznam v databázi. Následně uživatel poskytne informaci, která umožní ověření jeho identity (např. heslo, PIN, biometrický vzorek). Na základě srovnání uživatelem zadané autentizační informace s autentizační informací u uživatelem definované identity systém rozhodne o úspěšné, resp. neúspěšné autentizaci. [1, 6]

- *Identifikace* – 1:N; osoba tvrzení o své identitě nepředkládá. Systém prochází všechny záznamy v databázi, aby našel patřičnou shodu a identitu osoby sám rozpoznal. Systém může být navržen tak, že vyhledá nejlepší shodu, nebo označí všechny možné shody a

uspořádá je podle pravděpodobnosti. V případě, kdy databáze uchovává velký počet vzorků, může být identifikace časově náročná. [1, 6]

2.2 Autentizační metody

Autentizace uživatelů se typicky provádí jednou ze tří základních autentizačních metod. Liší se prostředky, které se pro autentizaci uživatele využívají. Jedná se o autentizaci tajnými informacemi (typicky hesla, PINy, passphrase), autentizaci tokeny (čipová karta) a autentizaci na základě biometrických charakteristik (otisk prstu, vzor oční sítnice, aj.).

Každá metoda má své výhody i nevýhody. Pro eliminaci slabin, které jednotlivé metody vykazují, se často v reálných systémech využívají kombinace výše zmíněných metod, tzv. vícefaktorová autentizace.

2.2.1 Autentizace uživatelů tajnými informacemi

Metoda autentizace uživatelů tajnými informacemi spočívá ve znalosti tajné informace, která je známá pouze oprávněné osobě a na základě její znalosti se daná osoba autentizuje v systému. Často také označována jako *„něco, co známe“*. Jedná se o nejběžnější a nejpřirozenější způsob ověřování identity osoby. V dnešní době se s touto metodou setkáváme především v počítačových aplikacích.

Tajnou informací jsou typicky textové informace – hesla, PINy nebo passphrase (přístupová fráze).

- *Hesla* – typicky se jedná o textový řetězec 6–10 znaků, který je sdružený s každým uživatelem a uživatel by si jej měl pamatovat. To tvoří sdílené tajemství mezi uživatelem a systémem. K získání přístupu do systému uživatel zadá dvojici <login, heslo>, kde *login* určuje identitu uživatele a *heslo* slouží k ověření této identity. Systém ověří, zda se heslo shoduje s daty uloženými pro daný login a uživateli je povolen přístup do systému.

  Volba hesel se často řídí pravidly, která musí být splněna, aby se snížila pravděpodobnost jejich odhalení útočníkem. Zpravidla se jedná o minimální délku hesla, požadavek, aby každé heslo obsahovalo alespoň jeden číselný, nealfabetický znak a alespoň jedno velké písmeno – obrana před slovníkovým útokem. Dalším požadavkem může být periodická změna hesel – obrana před „stárnutím hesla“ – čím déle se heslo používá, tím roste pravděpodobnost, že bude odhaleno. [7]

  Při volbě hesla často řešíme dilema zapamatovatelnost (krátká, jednoduchá hesla) vs. bezpečnost (co nejdelší, nejsložitější hesla). Praxe ukazuje, že nejvhodnější jsou lehce zapamatovatelná a zároveň obtížně uhodnutelná hesla – hesla založená na delší, lehce zapamatovatelné frázi (např. psmVTCOo24Z = Polámal Se Mraveneček, Ví To Celá Obora, O Půlnoci Zavolali). [6]

- *Passphrase* – krátká fráze, jejíž výhodou je lepší zapamatovatelnost oproti heslu

- *PIN* – Personal Identification Number; často používány spolu s fyzickým předmětem – tokenem. Jedná se o krátké číselné kódy, typicky 4–8 znaků dlouhé. K získání přístupu do systému je nezbytné předložit token a následně zadáním správného PINu prokázat identitu oprávněného držitele tokenu (např. SIM karta + PIN). Toto opatření zabraňuje zneužití tokenu v případě jeho ztráty nebo odcizení. Ochranou proti útokům hrubou silou

(vzhledem k malému prostoru možných kombinací) jsou doplňková procedurální omezení, např. omezení počtu pokusů pro zadání PINu. [7]

Útoky využívané k odhalení hesel [6, 7]:

- *Slovníkový* – použitelný k odhalení hesel, které jsou obsaženy v online slovníku nebo dostupných seznamech slov
- *Permutační* – permutace písmen s několika znaky a typickými náhradami (S – 5, atd.)
- *Slova, data, číslice související s uživatelem*
- *Hrubou silou* – všechny možné kombinace

Mezi nevýhody autentizace tajnými informacemi patří možnost zapomenutí hesla nebo jeho prozrazení. Uživatelé často volí jednoduchá hesla, která souvisí s jejich osobou (jméno, adresa, datum narození, atd.) nebo, pokud už mají složité heslo, často si jej poznamenávají na papír. Dalšími problémy jsou nedostatečná změna při vyžadovaných periodických změnách hesla, sdílení hesla s jinou osobou nebo používání stejného hesla ve více systémech. Všechny tyto přístupy snižují úroveň bezpečnosti systému.

2.2.2 Autentizace uživatelů tokeny

Metoda označovaná také jako *„něco, co máme“*. Uživatel vlastní nějaký předmět, tzv. token, který je vyžadován při ověřování identity osoby. Nejčastěji využívanými tokeny jsou karty a autentizační kalkulátory. Tokeny mívají specifické fyzické vlastnosti, obsahují tajné informace a mohou provádět (kryptografické) výpočty.

Při použití tokenů vyvstává dilema týkající se ceny výroby jednoho kusu při výrobě mnohakusové série, která by měla být co nejmenší vs. ceny padělání jednoho kusu za účelem vniknutí do systému, která by naopak měla být co největší (přestává platit, pokud se vyplatí výroba mnohakusové série padělků). Náklady na výrobu klesají při výrobě větších sérií. Náklady na padělaní navíc ovlivňuje, zda útočník získá stejně výrobou jednoho nebo několika padělků, jakou dobu a kolik musí mít k dispozici původních tokenů, existence legislativního postihu samotného padělání. [6, 8]

- *Karty* – nejvíce používaný autentizační token, např. platební karty, SIM karty, identifikační karty pro řízení přístupu do objektů. Podle použité technologie je lze rozdělit na karty s magnetickým proužkem a karty čipové (kontaktní nebo bezkontaktní).

  Karty s magnetickým proužkem obsahují třístopý magnetický proužek, který uchovává uložené informace. Nevýhodou těchto karet je, že se poměrně jednoduše kopírují, informaci je možné kdykoliv přepsat (i neúmyslně).

  Čipové karty se dělí na karty paměťové, paměťové se speciální logikou (ochrana PINem, čítače) a procesorové. Mohou mít podobu klasických (platebních) karet, SIM karet nebo USB tokenů. Další dělení je na karty kontaktní, vyžadující kontakt se čtečkou, která zároveň plní roli zdroje energie, a bezkontaktní, které mají vlastní zdroj energie a komunikují se čtečkou pomocí silného magnetického pole. Bezkontaktní karty jsou vhodné např. pro fyzickou kontrolu přístupu. Čipové karty s procesorem mají nezanedbatelnou výpočetní sílu a je možné na nich implementovat kryptografické algoritmy a protokoly.

- *Autentizační kalkulátory* – jedná se o specializovaná zařízení, typicky využívající protokol výzva-odpověď. Odpověď je funkcí tajné informace – klíče a výzvy. Komunikace s uživatelem probíhá buď přes manuální rozhraní prostřednictvím klávesnice a displeje, nebo automaticky pomocí optiky, čárového kódu a infračerveného portu. Standardní je použití PINu.

  Tokeny založené na hodinách bývají součástí autentizačních kalkulátorů. V daném okamžiku dávají správnou hodnotu, která je jedinečná pro každý přístroj, platná pouze po určitou dobu a tuto hodnotu umí spočítat i autentizační server.

Hlavními výhodami tokenů jsou rychlá zjistitelnost ztráty, možnost autentizace pouze s použitím tokenu (autentizační informaci nelze sdílet tak jednoduše jako heslo), obtížné kopírování a schopnost tokenů zpracovávat, uchovávat nebo přenášet další informace.

Mezi jejich nevýhody patří potřeba speciální čtečky nebo vycvičené osoby, bez tokenu není autentizace možná. Token musí být dostatečně složitý pro zajištění dostatečné obtížnosti zkopírování. Může se porouchat, což nemusí být vždy jednoduše zjistitelné uživatelem. [6, 8]

2.2.3 Autentizace uživatelů pomocí biometrik

Biometriky jsou automatizované metody identifikace nebo ověření identity osoby na základě měřitelných fyziologických nebo behaviorálních charakteristik, které jsou pro každého člověka jedinečné. Typickými zástupci biometrik jsou otisky prstů, geometrie ruky, tvář, hlas, podpis, aj.

Tato metoda autentizace uživatelé, označovaná také jako *„něco, co jsme“*, byla původně používána ve specializovaných zabezpečovacích aplikacích (kriminalistika, vojenství), v současné době se však stále více prosazují i ve veřejném sektoru (pasová kontrola, bankovnictví, aj.). [9]

Podrobně o biometrikách v následující kapitole.

2.2.4 Vícefaktorová autentizace

Autentizační systém je vyroben člověkem, a proto může být člověkem také prolomen. Hesla mohou být odposlechnuta, tokeny mohou být ukradeny, biometriky okopírovány. Každý autentizační systém má tedy slabiny. Z toho důvodu se v reálných systémech často využívá tzv. vícefaktorová autentizace, která kombinuje alespoň dvě z dříve uvedených autentizačních metod. Typickým příkladem je platební karta, při jejímž použití (např. v bankomatu) musí uživatel navíc znát odpovídající PIN. [1]

Kapitola 3

Biometriky

Každý člověk disponuje přirozenou schopností rozeznávat lidi podle hlasu, tváře a dalších charakteristik. Naproti tomu stroje musí být k rozpoznávání lidí na základě takových charakteristik naprogramovány. Technologické pokroky v biometrikách stále více přibližují strojové rozpoznávání lidskému vnímání. Hlavním přínosem použití biometrik je schopnost přesně rozlišovat osoby – s větší spolehlivostí, rychlostí, pohodlím a zároveň nižší cenou. Jednotlivé biometrické metody se od sebe v mnohém odlišují a spolu s rozvojem nových technologií poskytují stále více možností. [1]

3.1 Historie biometrik

Prvotní využití biometrických údajů k ověření identity se datuje do doby před více než tisíci lety. Hrnčíři ve východní Asii používali otisky prstů na svých výrobcích jako prvotní formu obchodní značky. V Egyptě byli obchodníci identifikováni na základě fyzických charakteristik jako výška, barva očí a barva pleti. Starý Zákon popisuje první příklady využití rozpoznávání hlasu, umožňující mužům rozpoznat nepřítele na základě vyslovení předem určeného slova.

V 19. století se kriminalisté a výzkumníci snažili nalézt lepší cestu k identifikaci osob kvůli potřebě identifikovat zločince. Ve Francii vyvinul Alphonse Bertillon metodu měření rozmanitých fyzických charakteristik lidského těla (vzdálenost od loktu ke špičce ukazováku velikost ušního boltce, aj.), spolu se zaznamenáváním zvláštních znaků osoby (jizvy, tetování). V počátcích slavila metoda úspěch, nicméně vyžadovala složité vybavení, vykazovala vysokou chybovost a navíc měřené charakteristiky nebyly pro každou osobu unikátní. Ve Velké Británii se díky policejním orgánům pozornost soustředila především na otisky prstů. Ty se později staly spolehlivým identifikátorem v kriminalistice, kde se využívají dodnes.

Biometrická technologie, ve smyslu automatizované metody ověřování identity, se poprvé objevila jako aplikace pro řízení přístupu. Tato evoluce s sebou přinesla spolehlivější a efektivnější autentizaci pro fyzický přístup. Jedna z prvních komerčních aplikací biometrik byla použita v roce 1972 na Wall Street a jednalo se o zařízení snímající otisk prstu pro kontrolu docházky. Od tohoto roku se biometriky neustále zdokonalují a stále více se rozšiřují i do běžného života. [1]

3.2 Vlastnosti biometrik

Ne všechny fyziologické nebo behaviorální vlastnosti člověka můžeme považovat za biometriky. Charakteristiky, které můžeme použít jako biometriky musí splňovat následující požadavky [2, 4]:

- *Univerzalita* – každá osoba by měla mít danou charakteristiku; v praxi je tato vlastnost obtížně dosažitelná, např. nedostatečně kvalitní otisk prstu, proto se povoluje určitá tolerance

- *Jedinečnost* – žádné dvě osoby by neměly být stejné ve smyslu měřené charakteristiky; problém může nastat např. u jednovaječných dvojčat. Důležitou roli hraje velikost skupiny, v rámci které srovnáváme.
- *Stálost* – charakteristika by se neměla časem měnit; změny mohou být způsobeny stárnutím, nemocí, zraněním, vykonávanou prací. Především behaviorální charakteristiky se mohou během života měnit (hlas, podpis)
- *Měřitelnost* – charakteristika by měla být opakovaně měřitelná, jednoduše přeložitelná snímači
- *Výkon* – dosažitelná přesnost identifikace, zdroje vyžadované k dosažení požadované přesnosti a faktory ovlivňující přesnost
- *Přijatelnost* – míra ochoty uživatelů používat biometrický systém
- *Bezpečnost* – obtížnost úspěšného oklamání systému podvodnými technikami

Následující tabulka poskytuje přehled biometrických technologií vzhledem k výše uvedeným vlastnostem. Každá vlastnost je ohodnocena *low*, *medium*, nebo *high*, kde *low* označuje nedostatečné a *high* reprezentuje velmi dobré splnění dané vlastnosti.

Biometrics	Univer-sality	Unique-ness	Perma-nence	Collect-ability	Perfor-mance	Accept-ability	Circum-vention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

H=High, M=Medium, L=Low

Tab. 3.1: Přehled biometrických technologií [10]

Dalšími vlastnostmi, které mohou ovlivnit volbu biometrického systému jsou:

- *Cena* – náklady na pořízení potřebného vybavení, náklady na provoz systému a jeho údržbu
- *Chybovost* – biometrická data, narozdíl od jiných autentizačních metod, nejsou nikdy 100% shodná. Z toho důvodu musíme povolit určitou variabilitu mezi registračním vzorkem a později získanými biometrickými údaji, což může vést k chybám.

Chybovost biometrických systémů závisí na řadě faktorů. Jedná se o typ snímače, vlivy prostředí, ve kterém je systém používán, nastavení systému (minimální kvalita vzorků, počet pokusů) a nezanedbatelný vliv mají také samotní uživatelé (nováčci/trénovaní, úředníci/dělníci). [6]

Více o chybovosti a popis jednotlivých typů chyb v kapitole 3.7 Chybovost.

3.3 Model použití biometrik

Použití každé biometrické technologie má svá specifická úskalí, základní operace jsou velmi podobné a vytvářejí obecný postup použití biometrického systému. [11]

3.3.1 Registrace

- *Prvotní získání biometrického vzorku* – biometrický vzorek osoby je získán prostřednictvím vstupního zařízení. Kvalita tohoto vzorku je velmi důležitá, protože podstatně ovlivňuje úspěšnost následných autentizací tohoto uživatele. Může se stát, že někteří uživatelé nemohou být zaregistrováni do systému (lidé s nedostatečně kvalitními vzorky, lidé s chybějícími prsty apod.). Tito lidé vytvářejí tzv. *„fail to enroll“* (FTE) skupinu. Lidé často nemají žádné předchozí zkušenosti s používáním biometrického systému, proto by prvotní snímání mělo být řízeno proškoleným personálem.

- *Vytvoření registračního vzorku* – prvotní vzorek je po sejmutí zpracován. Jsou z něj získány charakteristické znaky, které danou osobu jednoznačně identifikují. K vytvoření registračního vzorku je často vyžadováno více prvotních měření biometrických dat (3–5) , aby se dosáhlo co možná největší kvality registračního vzorku.

- *Uložení registračního vzorku* – biometrické vzorky nejsou ukládány ve formě snímaného obrazu, ukládají se pouze získané charakteristiky. Existuje několik možností uložení registračního vzorku: v tokenu (čipová karta), v centrální databázi na serveru nebo v biometrické čtecím zařízení

Jakmile je uživatel zaregistrován do systému, může systém používat k verifikaci nebo identifikaci. Tento proces je obvykle plně automatizován.

3.3.2 Verifikace/Identifikace

- *Získání biometrického vzorku* – pokud je vyžadována autentizace uživatele, uživatel poskytne systému svá biometrická data prostřednictvím vstupního zařízení, která budou následně porovnána s registračním vzorkem. Často se požaduje ověření, zda vzorek pochází od živé osoby (tzv. *testování živosti*). Testování živosti může být prováděno buď hardwarově (přímo snímačem, např. otisk prstu), nebo softwarově (vzorkováním v čase, např. rozpoznávání tváře).

- *Vytvoření charakteristik* – zpracování získaného vzorku. Obvykle je k dispozici pouze jeden vzorek, tudíž počet a kvalita charakteristických znaků je menší než při registraci.

- *Srovnání charakteristik* – nové charakteristiky jsou srovnány s charakteristikami získanými při registraci. Při verifikaci se nové charakteristiky srovnávají pouze s jedním registračním vzorkem, který uživatel předem specifikuje. Při identifikaci se prochází celá databáze registračních vzorků.

- *Rozhodnutí* – finální rozhodnutí, zda bude uživateli umožněn přístup do systému. Provádí se na základě porovnání míry shody porovnávaných vzorků s *prahovou hodnotou*. Míru shody udává tzv. *skóre*, prahová hodnota udává míru shody mezi registračním vzorkem a nově získanými daty. Nastavení prahové hodnoty je závislé na oblasti nasazení systému. Systémy s vysokým FAR (False Acceptance Rate) vykazují vysokou míru nesprávných přijetí – nízká úroveň bezpečnosti. Systémy s vysokým FRR (False Rejection Rate) vykazují vysokou míru nesprávných odmítnutí v prostředí s vysokými nároky na bezpečnost, což vede k nespokojenosti uživatelů, kteří často musí k úspěšné autentizaci podstoupit několik pokusů.

3.4 Výhody/nevýhody biometrik

Stejně jako každá jiná autentizační metoda i autentizace pomocí biometrických údajů má své světlé i stinné stránky. Jaké výhody a nevýhody s sebou tedy biometriky přináší? [11]

3.4.1 Výhody

Hlavní výhodou je, že biometriky autentizují přímo uživatele tím, že k autentizaci používají skutečné lidské fyziologické a behaviorální charakteristiky, které jsou relativně stálé a neměnné.

Uživatel nemusí nic nosit u sebe ani si pamatovat mnohdy složité tajné informace.

Uživatelé nemohou předat biometrické charakteristiky jiné osobě jako tokeny nebo hesla.

Biometriky nemohou být narozdíl od tokenů nebo jiných předmětů používaných k autentizaci ukradeny. Biometriky nejsou tajné, a proto jejich dostupnost nenaruší bezpečnost tak, jako v případě prozrazení hesla. Dokonce ani použití falešné biometriky by nemělo útočníka (nesprávně) autentizovat.

Biometriky nemohou být ukradeny ani ztraceny, což snižuje náklady na údržbu systému (vydávání nových hesel, tokenů).

Další výhodou může být rychlost. Proces autentizace pomocí biometriky může být rychlejší než při použití jiné metody autentizace, např. přiložení prstu na snímač vs. hledání správného klíče od dveří.

3.4.2 Nevýhody

Biometrické systémy jsou stále ve fázi vývoje, především co se týče přesnosti a rychlosti. Systémy s FRR pod 1% a zároveň s nízkým FAR jsou spíše výjimkou, většina dostatečně spolehlivých systémů (v souvislosti s nízkým FAR) je vhodná pouze pro verifikaci.

Dalším problémem je nemožnost registrace některých osob (lidé s chybějícími orgány apod.), kteří nemohou takový systém používat, musí se zavádět dodatečná opatření, která zvyšují náklady a složitost systému a snižují bezpečnost.

Biometrická data nejsou tajná a bezpečnost systému nemůže být založena na utajení biometrických charakteristik uživatelů. Biometrická data musím být vždy aktuální a snímány v průběhu autentizace. To způsobuje, že vstupní zařízení musí být důvěryhodné.

Biometrické senzory, které přichází do kontaktu s uživatelem mají omezenou životnost, musí se udržovat čisté.

Biometrické systémy mohou narušit soukromí uživatele. Biometriky mohou obsahovat mnoho citlivých informací, např. z DNA lze zjistit náchylnost uživatele k chorobám, tělesný pach může poskytovat informace o nedávných aktivitách.

Biometrické systémy způsobují ztrátu anonymity, všechny aktivity jsou jednoznačně spojeny s danou osobou.

Někteří uživatelé mohou mít k biometrikám odpor, nechtějí se podrobit měření nebo nechtějí, aby jejich biometriky byly ukládány v systému.

3.5 Rozdělení biometrik

Biometrické technologie mohou být založeny na fyziologických nebo behaviorálních charakteristikách člověka. [1, 6]

- *Fyziologické charakteristiky* – též nazývané *statické*; biometrická data jsou získávána přímým snímáním části lidského těla. Do této kategorie patří např. otisk prstu, geometrie ruky, vzor oční sítnice, vzor oční duhovky, tvář, DNA.

- *Behaviorální charakteristiky* – též nazývané *dynamické*; jedná se o vlastnosti založené na chování osoby. Při autentizačním procesu je vyžadována akce uživatele. Tyto vlastnosti mohou být naučené, natrénované a teoreticky také v průběhu života měnitelné. Typickými příklady mohou být rozpoznávání hlasu, dynamika podpisu, dynamika psaní na klávesnici.

Z určitého úhlu pohledu můžeme říct, že každá biometrika, tedy i ta fyziologická, v sobě zahrnuje behaviorální složku. Způsob, jakým uživatel prezentuje biometriku snímači, je akcí uživatele, kterou se musel naučit, a tedy vyjadřuje chování uživatele. Navíc, získání správných návyků pro práci s biometrickými snímači snižuje obtížnost registrace a zvyšuje míru úspěšných přijetí, což s sebou přináší snížení nákladů a zvýšení pohodlí uživatelů.

Charakteristiky dále dělíme na genotypické a fenotypické.

- *Genotypické* – charakteristiky zděděné od rodičů (barva očí, DNA, atd.); časově neměnné a neovlivnitelné, a tedy vhodné pro identifikaci osoby

- *Fenotypické* – tyto charakteristiky se vytváří v raných stádiích vývoje embrya a jsou pro každého člověka jedinečné (otisk prstu, vzor oční duhovky a další)

Snímání biometrických dat může být prováděno buď přímým kontaktem biometriky se snímačem (např. otisk prstu, geometrie ruky), nebo bez kontaktu se snímačem (např. rozpoznávání tváře). Bezkontaktní biometriky lze tedy snímat i bez vědomí uživatele, což může v krajním případě vést až ke sledování pohybu lidí.

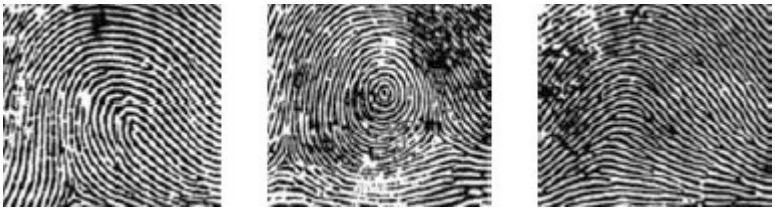
3.6 Biometrické technologie

3.6.1 Otisky prstů

Otisky prstů jsou nejstarší a stále nejrozšířenější biometrikou využívající vzorů papilárních linií na povrchu prstu. Vzory se utvářejí během embryonálního vývoje a obecně jsou uznávány jako jedinečné nejen pro každou osobu, ale i pro každý prst. Otisky prstů jsou celosvětově používanou metodou identifikace v kriminalistice, a proto jsou řadou uživatelů spojována s trestnou činností i v rámci civilních aplikací. [2]

Linie vytvářející různé vzory se také označují pojmem *rýhy*. Jsou to právě rýhy, které jsou využívány pro porovnání dvou otisků. K porovnávání otisků lze využít dvou principů.

Prvním z nich je porovnání otisků jako celku, tzv. *srovnání vzorů*. Vzory vytvářené rýhami se dělí do tří kategorií: *smyčka (Loop), vír (Whorl)* a *oblouk (Arch)*, viz. obr. 3.2. Tyto kategorie tvoří klasifikační systém (*Henry System*) popsaný na počátku 20. století Sirem Edwardem Henrym. [1] Je známo, že 60–70% všech otisků obsahuje smyčky, víry tvoří 25–35% otisků a oblouky asi pouze 5% všech otisků.

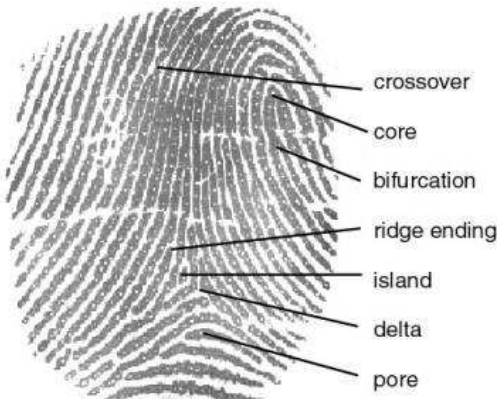


Obr. 3.2: Klasifikační vzory. Po řadě smyčka, vír a oblouk [12]

Druhým principem je srovnání na základě charakteristických detailů rýh, tzv. *markant*. Markanty otisků prstů jsou identifikační body nacházející se v rýhách vzoru, které popisují změny jednotlivých rýh. Mezi základní typy markant patří: [13]

- *Ukončení (ridge ending)* – označuje bod, kde rýha končí
- *Vidlice (bifurcation)* – místo, kde dochází k rozvětvení rýhy
- *Bod (dot)* – velmi krátká rýha
- *Ostrov (island)* – rýha delší než bod nacházející se v uzavřené oblasti mezi dvěma rýhami
- *Oko (lake)* – místo v uzavřené oblasti mezi rozdvojenou a následně spojenou rýhou
- *Most (bridge)* – rýha spojující dvě sousední rýhy

Minutiae	Example	Minutiae	Example
ridge ending		bridge	
bifurcation		double bifurcation	
dot		trifurcation	
island		opposed bifurcations	
lake		ridge crossing	
hook		opposed bifurcation / ridge ending	



Obr. 3.3, 3.4: Markanty otisků prstů [13, 15]

Při porovnávání otisků na základě markant se využívají informace o přítomnosti a typu markantu, jeho umístění v otisku a orientaci (směru). Otisk prstu obsahuje přibližně 75–175 identifikačních bodů, pro potvrzení shody dvou otisků stačí v průměru 10–15 shodných bodů. [9]

Dále mohou být pro srovnávání otisků využívány další dva znaky: *jádro (core)* – střed otisku (např. vrchol oblouku, střed víru) a *delta* – místo, kde se rýhy rozcházejí do tří různých směrů. Tyto znaky nemusí být přítomny na všech otiscích prstů. Některé snímače využívají i informace o umístění kožních pórů nebo šířce a tvaru hran rýh. [2]

Otisk prstu lze získat buďto za použití inkoustu, kdy se prst nejprve potře inkoustem a následně se přiloží na papírovou kartu. Karta se následně převede do digitální podoby prostřednictvím skeneru nebo CCD (Charged Coupled Device) kamery. Druhou možností je snímání otisků bez použití inkoustu prostřednictvím senzoru. Získaná data jsou následně převedena na adekvátní obraz otisku prstu v odstínech šedi, který je dále zpracováván (nalezení markant, vytvoření vzorku pro srovnání).

Při získávání otisku hrají podstatnou roli následující vlastnosti: *rozlišení* (min. 250–300 DPI (bodů na palec), FBI specifikace 500 DPI), *velikost snímané oblasti* (FBI specifikace 1×1 inch^2), *počet pixelů*, *dynamický rozsah* (počet bitů pro zakódování intenzity každého pixelu; černobílému obrazu odpovídá 8 bitů), *geometrická přesnost* (zakřivení způsobené snímacím zařízením), *kvalita obrazu* (vlhkost prstu, přítomnost jizev, nečistoty, apod.). [14]

Snímače otisků prstů se dělí podle použité technologie [2,13,14].

- *Optické* – nejstarším a nejpoužívanějším principem je FTIR (Frustrated Total Internal Reflection). Prst přiložený na skleněnou desku je osvětlován světelným zdrojem (LED (Light Emitting Diode), laser). Odražené světlo je zachycováno CCD prvkem. Hřebeny otisku jsou v kontaktu se snímačem, zatímco údolí mají od povrch snímače odstup. Světlo dopadající na hřebeny se odráží do CCD prvku, údolími je pohlcováno. Výhodou je nízká cena. Nevýhodou jsou problémy s mokrými nebo suchými prsty, nečistotami a latentními otisky.

- *Kapacitní* – snímač je tvořen dvoudimenzionálním polem kondenzátorových desek, které jsou pokryty silikonovou deskou. Druhou část každého kondenzátoru tvoří kůže prstu přiloženého na silikonový povrch snímače. Měří se napětí na jednotlivých kondenzátorech, které závisí na vzdálenosti desek, tedy napětí je pro hřebeny a údolí odlišné. Výhodou je malá velikost snímače a možnost nastavení elektrických parametrů v případě nepříznivých podmínek (např. vlhkost kůže). Nevýhodou je nutnost častého čištění povrchu senzoru od nečistot a závislost na vlhkosti kůže.

- *Tepelné* – senzor je vyroben z pyroelektrického materiálu, který na základě teplotního rozdílu generuje proud. Obraz otisku je vytvářen na základě různých teplot v případě hřebenů, které jsou přímo v kontaktu se snímačem a údolí, které jsou od povrchu snímače vzdáleny. Nevýhodou je nízká kvalita vzorků.

- *Tlakové* – povrch snímače je tvořen pružným, piezoelektrickým materiálem, který se přizpůsobuje tvaru otisku prstu a převádí jej na elektrický signál. Nevýhodou je nízká citlivost používaných materiálů.

- *Ultrazvukové* – využívají ultrazvukové signály, které jsou vysílány směrem k povrchu prstu. Odražený signál je zachycován přijímačem a reprezentuje rozdíly mezi hřebeny a

údolími. Výhodou těchto snímačů je vysoká spolehlivost, protože jsou na rozdíl od ostatních typů odolné vůči nečistotám i vlhkosti. Nevýhodou je vysoká cena a velikost přístroje.

Výhodou otisků prstů je vysoká přesnost (FAR < 0,1% při FRR cca. 5%), nízká cena, malá velikost zařízení a poměrně vysoká přijatelnost mezi uživateli.

3.6.2 Geometrie ruky

Metoda založená na snímání tvaru ruky. Délka, šířka, tloušťka prstů, zakřivení, relativní pozice charakteristických znaků a případně velikost dlaně umožňují rozlišit jednotlivé osoby mezi sebou. Tvar ruky však není pro každou osobu jedinečný, proto jsou tyto systémy vhodné pouze pro verifikaci, pro identifikaci jsou získaná data nedostatečná. Pro účely verifikace se často kombinují s PINem.

Tvar ruky je snímán speciálním skenerem, který se skládá ze CCD kamery s rozlišením 32000 pixelů, infračerveného zdroje světla (LED) a zrcadel. Získává se třídimenzionální obraz tvaru ruky, kdy se za pomoci zrcadel snímá obrys hřbetu a jedné boční strany ruky. Nezaznamenává se žádná informace o barvě, papilárních liniích otisků prstů, jizvách, apod. Roli nehrají časově proměnné vlastnosti jako například nečistoty, pot, poranění pokožky. [2]

Obr. 3.5: Geometrie ruky [6]

Při autentizačním procesu uživatel položí ruku (dlaní dolů) na vysoce reflexní snímací podložku. Pro správné umístění ruky obsahuje podložka několik (typicky 5) kolíků. V krátkém časovém okamžiku (1 sekunda) je provedeno více než 90 měření a získané charakteristiky jsou reprezentovány jako 9-bytový vzorek. Malá velikost vzorku dělá tyto systémy atraktivní pro aplikace s omezenou velikostí paměti.

Registrační proces se obvykle skládá ze tří až pěti opakovaných měření, čímž se dosáhne kvalitnějšího registračního vzorku, a tedy zvýšení přesnosti celého systému. Při verifikaci uživatel předloží tvrzení o své identitě (PIN), následně se provede snímání tvaru ruky a získaný vzorek se srovná se vzorkem svázaným s uvedeným PINem. [1, 2]

Geometrie ruky nachází uplatnění v aplikacích pro řízení přístupu, docházkových systémech nebo při přístupu ke zdrojům (zabraňuje půjčování tokenů).

Výhodou autentizace na základě geometrie ruky je malá velikost vzorku, vysoká rychlost verifikace, přijatelnost u uživatelů a malý vliv okolního prostředí na verifikační proces. Mezi nevýhody patří především malá přesnost, poměrně vysoká chybovost (FAR i FRR kolem 5%), nepoužitelnost pro identifikaci a také se může vyskytnout problém se správným umístěním ruky na snímací podložku u osob s omezeným pohybem dlaně, např. u lidí trpících artrózou.

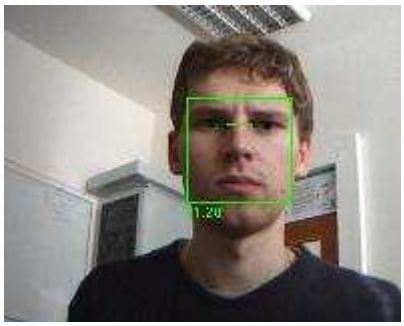
3.6.3 Rozpoznávání tváře

Tvář je jednou z nejpřijatelnějších biometrik, protože se jedná o jednu z nejzákladnějších metod identifikace, kterou lidé běžně využívají v každodenním životě při styku s jinými osobami. Jako lidé máme schopnost rozlišit stovky tváří: rodinu, přátele, spolupracovníky nebo i známé osobnosti.

V oblasti využití tváře jako biometriky se jedná o poměrně mladou technologii. Stále je předmětem zkoumání, zdokonalování a hledání nejvhodnějšího přístupu pro detekci a srovnání tváří. Výzkum se soustředí především na vývoj takové techniky, která umožní srovnání, které bude nezávislé na pozici tváře vzhledem ke kameře, výrazu v obličeji, kosmetických úpravách (účes, vousy, brýle, náušnice) nebo důsledcích stárnutí.

Snímání obrazu tváře je typicky prováděno videokamerou, detekce a srovnání tváře potom příslušnou softwarovou aplikací. Kvalita získaného obrazu má pak vliv na výkon celého systému. Významnou roli při získávání obrazu hraje vliv okolního prostředí, osvětlení a prezentovaná data (vzdálenost od kamery, pozice vzhledem ke kameře, výraz v obličeji). Je rozdíl, pokud chceme porovnávat dva statické obrazy získané za definovaných (standardizovaných) podmínek (čelní pohled, jednobarevné pozadí, atd.) nebo identifikovat osobu nacházející se ve skupině lidí (např. při pohybu na ulici).

Detekce obličeje v obraze probíhá na základě tvarů a rysů v obraze, které jsou podobné lidskému obličeji. Algoritmy obvykle postupují od středu obrazu směrem k okrajům. Výstupem algoritmu je umístění a ohraničení detekovaného obličeje, souřadnice očí, špičky nosu a středu úst. Výkon je velmi dobrý pro obrazy s jednou tváří. Větší problémy se vyskytují u zpracovávání obrazů s více tvářemi, kde hrají významnou roli rozdíly ve vzdálenosti, úhlu snímání, poloha tváře a také okolní prostředí. Proto, aby byl systém dostatečně spolehlivý, je třeba dbát na precizní nastavení systému pro cílové prostředí.



Obr. 3.6: Příklad detekce obličeje

V současnosti existuje mnoho technik pro rozpoznávání tváře. Lze je rozdělit do tří kategorií: *neuronové sítě*, *„eigenfaces“*, *analýza charakteristik tváře*[1]. Analýza charakteristik tváře je nejzákladnějším principem a využívá informace o tvaru obličeje a poloze a velikosti významných míst ve tváři (oči, nos, ústa, obočí, lícní kosti). Uchovávají se například informace o vzdáleností očí, vzdálenosti rtů od nosu, úhlu mezi špičkou nosu a okem, atd.

Využití rozpoznávání tváře nachází v aplikacích řízení přístupu nebo monitorování. Monitorovací systémy snímají tváře na veřejných místech a srovnávají je z databází vyhledávaných osob (zločinci, apod.). [1, 2, 9]

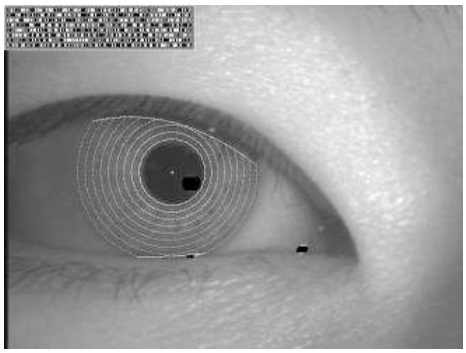
[1] John D. Woodward, Nicholas M. Orlans, Peter T. Higgins: Biometrics. McGraw-Hill Professional, 2003, str. 72–76

Výhodou této technologie je relativně nízká cena a vysoká přijatelnost u uživatelů. Nevýhodou je velká výpočetní náročnost a z toho plynoucí dlouhá doba srovnání (i několik sekund) a nižší přesnost ve srovnání s otisky prstů, duhovkou nebo sítnicí.

3.6.4 Oční duhovka

Lidské oko poskytuje dvě z nejpřesnějších biometrik, duhovku a sítnici. Duhovka je kruhová barevná tkáň kolem panenky, která má bohatě strukturované vzory vytvořené během embryonálního vývoje. Je ovládána dvěma svaly, které mění její velikost a řídí množství světla vstupujícího do oka. Duhovka je jedinečná pro každou osobu a každé oko a zároveň časově neměnná, což jsou klíčové vlastnosti využitelné pro biometriky. V každé oční duhovce může být libovolně kombinováno asi 400 charakteristických znaků (pro srovnání, otisky prstů mohou kombinovat asi 60 různých znaků).

Pro snímání oční duhovky se používá klasická černobílá CCD kamera. Snímání je bezkontaktní a provádí se ze vzdálenosti v řádu desítek centimetrů. Vyžaduje tedy spolupráci uživatele. V obrazu se lokalizuje duhovka a následně se provádí korekce velikosti a kontrastu z důvodu přirozených změn způsobených intenzitou okolního světla. Výstupem je 256-bytový *IrisCode* popisující vzor duhovky.



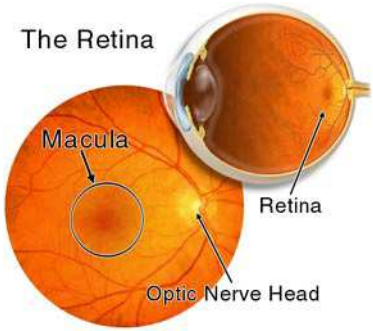
Obr. 3.7: Lokalizace duhovky [15]

Srovnání dvou „IrisCodes“ využívá výkonné nízkoúrovňové operace XOR (Exclusive OR) a umožňuje miliony srovnání za sekundu. Rozdílnost dvou vzorků je pak vyjádřena Hammingovou vzdáleností mezi příslušnými „IrisCodes“, tedy počtem bitů, ve kterých se kódy liší.

Jedná se o technologii s velmi nízkou chybovostí, pravděpodobnost, že by dvě různé duhovky generovaly stejné kódy je asi 1:1200000. [1] Výhodou je tedy vysoká přesnost (FAR téměř nulové při FRR kolem 3 %), rychlost (srovnání trvá asi 4 sekundy, z nichž značnou část zabírá správné umístění oka před kameru). Mrkání, přirozené pohyby oka, kontaktní čočky ani řasy ve většině prostředí nevykazují problémy s lokalizací sítnice v obrazu. Díky vysoké přesnosti je metoda vhodná i pro identifikaci. Nevýhodou jsou vysoké pořizovací náklady a poměrně velká velikost ukládaného kódu.

3.6.5 Oční sítnice

Sítnice je na světlo citlivá tkáň pokrývající zadní stěnu oka. Skládá se z velkého počtu nervových buněk (čípky a tyčinky), které přijímají světelné paprsky a posílají je zrakovým nervem



do zrakových center v mozku. [9]

Obr. 3.8: Oční sítnice [16]

Ověření identity osoby probíhá na základě srovnání jedinečného vzoru cév na oční sítnici v okolí slepé skvrny, tj. místa, kde oční nerv vystupuje z oka. Považuje se za jednu z nejpřesnějších biometrik. Krevní řečiště na sítnici se utváří náhodným biologickým procesem, není jednoduché jej změnit nebo okopírovat. Změna v průběhu života však není nemožná. Podobně jako všechny fyzické charakteristiky osoby může být sítnice poznamenána úrazem, který může poškodit krevní řečiště. Změny mohou být také způsobeny některými chorobami, např. cukrovka, zelený zákal.

Skenování je prováděno jejím osvětlováním infračerveným (IR) světlem s nízkou intenzitou. Získaný obraz se dále zpracovává, výsledkem je záznam o velikosti 96 bytů. Protože sítnice není za normálních okolností viditelná (jedná se o vnitřní orgán), skenování vyžaduje vysokou míru spolupráce uživatele. Uživatel musí nahlédnout do okuláru a zaostřit na pevně daný bod. Samotné snímání pak trvá 1–2 sekundy, kdy snímač osvětlí, zaostří a sejme obraz sítnice. Nepříjemný proces snímání vzorku vede k nízké přijatelnosti technologie ze strany uživatelů.

Jedná se o velmi přesnou technologii, FAR téměř nulové, FRR však relativně vysoké, způsobené především náročným procesem snímání vzorku. Míru bezpečnosti zvyšuje také fakt, že se jedná o vnitřní orgán. Není zanechávána na různých místech jako např. otisky prstů nebo není stále viditelná jako obličej. Navíc je také méně náchylná ke zraněním a změnám během života. Z těchto důvodů technologie nachází uplatnění zejména v prostředích s požadavkem na vysokou úroveň zabezpečení jako např. řízení přístupu do jaderných elektráren, ve vojenském a vládním sektoru. [1]

Výhodou je výše zmíněná vysoká přesnost a spolehlivost. Nevýhodou je uživatelská nepřívětivost a nepříjemnost snímání a také vysoká cena.

3.6.6 Verifikace hlasu

Biometrika kombinující fyziologické a behaviorální vlastnosti. Fyziologickou vlastností je anatomie hlasového ústrojí. To ovlivňuje měřitelné akustické vzory v mluvené řeči, jako například barvu, výšku nebo hlasitost tónu. Za behaviorální charakteristiky lze považovat výslovnost nebo způsob vyjadřování.

Metoda je někdy označována také jako rozpoznání mluvčího. Úkolem verifikace hlasu je ověření identity osoby na základě mluvené řeči. K získání hlasového vzorku (slovo, krátká fráze) se používá mikrofon nebo běžný telefon. Biometrika může být využita pro verifikaci i identifikaci. V závislosti na povaze aplikace lze použít textově závislý nebo textově nezávislý mód.

Textově závislý mód spočívá ve vyslovení předem určeného slova nebo fráze, která byla zaznamenána do systému v průběhu registrace uživatele. Je používanější a vykazuje nižší chybovost. Využívá se především pro verifikaci, kdy uživatel nejprve zadá uživatelské jméno nebo předloží kartu, potom je vyzván k vyslovení určené fráze. K ochraně proti útoku přehráním se často fráze vytváří náhodně z více uživatelem zaregistrovaných slov. Metoda nepatří mezi nejpřesnější, FAR i FRR se pohybují okolo 2 %. Výkon je ovlivněn prostředím a dalšími okolnostmi. Problémy mohou být způsobeny použitím jiného mikrofonu při registraci a při následné verifikaci, okolním hlukem, nekvalitním komunikačním kanálem.

Textově nezávislý mód umožňuje vyslovení libovolné fráze, která zpravidla musí být delší než v případě textově závislého módu, protože je zapotřebí získat větší množství charakteristických akustických znaků. Přesnost je nižší než u textově závislého módu. [1]

Verifikace hlasu probíhá tak, že analogová data (hlas) jsou převedena na digitální reprezentaci metodou vzorkování. Následně jsou ze získaných dat vybrány charakteristické rysy, které jsou seskupeny a takový vzorek je uložen. Výsledný vzorek má velikost 70–80 bytů dat na každou sekundu záznamu. V úvahu je brána kvalita, doba trvání, výška a hlasitost získaného signálu a tyto charakteristiky jsou srovnávány s registračním vzorkem.

Výhodou verifikace hlasu oproti jiným biometrikám je možnost ověření identity vzdáleně (po telefonu). Dalšími výhodami jsou nízká cena, jednoduchost použití a možnost ověření výzva-odpověď (i kontinuálně).

Nevýhodou je malá přesnost a robustnost a vysoká závislost na okolních podmínkách. Příčinou nedostatečné robustnosti je vývoj řeči v průběhu života, změna charakteristik v důsledku nemoci nebo emocí.

3.6.7 Dynamika podpisu

Dynamika podpisu a dynamika psaní na klávesnici patří mezi behaviorální biometriky, tedy zjišťuje se, jak uživatel něco dělá – jak se podepisuje, resp. jak píše na klávesnici.

Pro ověření identity na základě dynamiky podpisu není důležitý jen výsledný podpis, ale i způsob jeho psaní. Podpis samotný poskytuje informace o geometrii, zakřivení a tvaru jednotlivých znaků a slov. Způsob jeho psaní vyjadřuje, jaký je směr a rychlost tahů, tlak pera na podložku, kdy je pero pokládáno na a kdy zvedáno z podložky. [1]

Podpis je snímán pomocí tabletu nebo speciálního pera. Moderní snímače zaznamenávají relevantní informace 100–200krát za sekundu. Analyzují se změny tlaku pera na podložku, celková rychlost, zrychlení v jednotlivých částech podpisu, zarovnání jednotlivých částí, dráha pohybu pera a doba, po kterou se pero pohybuje po a nad podložkou. [9] Registrační vzorek se vytváří ze 3–10 podpisů, jeho velikost je asi 20 kB.

Obr. 3.9: Tablet pro rozpoznávání podpisu [17]

Technologii lze použít všude tam, kde se využívá „klasický“ podpis. Dále také v elektronických aplikacích jako přihlašování k počítačům, přístup k datům nebo při platebních transakcích.

Výhodou biometriky založené na ověření podpisu je vysoká přijatelnost u uživatelů (všichni jsou zvyklí používat klasický podpis pro ověření identity) a nízká cena snímacího zařízení.

Nevýhodou je nízká přesnost, nedostatečná pro většinu aplikací (FAR i FRR v řádu desítek procent). Příčinnou je i to, že se jedná o biometriku založenou na chování a opakovatelnost podpisu může být ovlivněna psychickým stavem uživatele, důležitostí podepisovaného dokumentu. Roli může hrát i rozdílné snímací zařízení. U levnějších zařízení navíc uživatel při psaní nevidí dříve napsané.

3.6.8 Dynamika psaní na klávesnici

Narozdíl od většiny ostatních biometrických technologií nevyžaduje speciální zařízení, pro ověření identity se využívá běžná klávesnice. Předpokládá se, že každá osoba píše na klávesnici charakteristickým způsobem, Toto chování poskytuje dostatečnou informaci pro autentizaci uživatele, přestože se nepovažuje za unikátní pro každou osobu.

Technologie měří dynamiku úhozů, tedy čas stlačení klávesy (*dwell time*) a čas mezi stisky jednotlivých kláves (*flight time*) při psaní textu na klávesnici. Pro měření lze využít hardwarové přerušení generované jak při stisku, tak i při uvolnění kláves.

Obr. 3.10: Měřené charakteristiky dynamiky psaní na klávesnici [18]

Srovnávací algoritmy jsou založeny na principu srovnávání vzorů nebo neuronových sítí. Autentizace probíhá buďto staticky nebo kontinuálně. Statická autentizace analyzuje dynamiku psaní pouze v určitý časový okamžik (např. při přihlašování uživatele do systému). Kontinuální autentizace monitoruje psaní uživatele po celou dobu používání systému. [13] Výhodou kontinuální autentizace je ochrana před neoprávněným užitím neobsazeného terminálu, např. pokud si oprávněný uživatel potřebuje odskočit nebo se zapomene odhlásit.

Dynamika psaní na klávesnici se často využívá k získání složitějších hesel, kdy každý uživatel nejen že musí znát své heslo, ale navíc jej musí napsat odpovídajícím způsobem.

Výhodou je nízká cena (není potřeba žádné speciální zařízení) a vysoká uživatelská přívětivost. Nevýhodou je nízká přesnost. Únava, nemoc, zranění nebo stres, stejně jako faktory ovlivňující prostředí (typ klávesnice) mohou způsobit větší míru nesprávných odmítnutí.

3.6.9 Další biometriky

Existuje celá řada dalších fyziologických charakteristik nebo vlastností chování, na jejichž základě lze ověřit identitu člověka, jsou tedy pro každého člověka jedinečné. Výše popsané biometriky se řadí do skupiny biometrik, které jsou běžně dostupné a komerčně využívané. Následující biometriky jsou stále ve stádiu raného vývoje a experimentů. [1]

- *DNA* – (kyselina deoxyribonukleová); jedná se o dvouvláknovou spirálovitou molekulu, která je obsažena ve všech buňkách každého živého organismu a je nositelkou jeho genetické informace. DNA je jedinečná pro každého jedince, jedinou výjimku tvoří jednovaječná dvojčata. Patří mezi genotypické charakteristiky, které jedinec dědí od rodičů.

  Jedinečnost DNA je známa již od roku 1953 díky výzkumu J. Watsona a F. Cricka. V roce 1985 byla poprvé použita v kriminálním vyšetřování a od té doby je využívána pro identifikaci v kriminalistice a forenzních aplikacích po celém světě, často pod pojmem „DNA profilování“. Identifikace je velice přesná, slabinou mohou být pouze chyby lidského faktoru nebo laboratorní chyby.

  Přesto DNA nelze považovat za biometriku v pravém slova smyslu, protože proces identifikace není automatizovaný.

Výhodami DNA jsou jedinečnost a robustnost (časová stálost v průběhu celého života). Nevýhodou je drahý a časově náročný identifikační proces, dále také dotěrnost (vyžaduje se určitá forma lidské tkáně, krev, sliny, atd.). Navíc, DNA obsahuje citlivé informace o osobě.

- *Vzor žil* – měření vzorů krevního řečiště tvořeného cévami na hřbetu nebo dlani ruky. Vzory se vytvářejí před narozením a jsou odlišné i u jednovaječných dvojčat. Velikost se s věkem mění, avšak vzory zůstávají stejné po celý život.

  Snímání se provádí speciální infračervenou (IR) kamerou. Získaný obraz v odstínech šedi (se zvýrazněnými žílami, které absorbují IR světlo) je digitalizován a převeden na binární vzorek o velikosti 300 bytů. Snímání je nezávislé na časově proměnných parametrech – nečistoty, malá poranění).

  Mezi výhody patří univerzálnost (každý má tuto vlastnost), odolnost proti poranění (žíly jsou chráněny kůží), časová stálost vzorů, nelze je jednoduše změnit a také uživatelská přívětivost (není nutný fyzický kontakt se zařízením). Nevýhodou je vysoká cena zařízení.

- *Termografie obličeje* – založeno na vzorech vyzařování tepla v obličeji určených tokem krve pod kůží. Měření vyzařovaného tepla se provádí IR kamerou a vytváří teplotní vzor. Struktura žil a tkáně pod kůží je stabilní, krevní tok může způsobovat druhotné vzory. Získaná data mohou být ovlivněna okolním prostředím (např. teplota, vítr) nebo působením dalších faktorů (alkohol, drogy). Toto může být i výhodné v případě, kdy kromě ověření identity je požadováno i zjištění fyzického stavu osoby, např. zda není pod vlivem alkoholu.

  Výhodou je použitelnost technologie i při omezeném osvětlení. Nevýhodou je nízká uživatelská přívětivost z důvodu možnosti odhalení informací o zdravotním stavu osoby a vysoká cena zařízení.

- *Potní žlázy* – jsou zodpovědné za latentní otisky prstů, tzn. otisky zanechané na předmětech. Při kontaktu prstu s předmětem je v důsledku stálého vyměšování potu z potních žláz na povrchu prstu zanechána na předmětu tenká vrstva tuku a vlhkosti, tzv. *latentní otisk*.

  Umístění a hustota drobných potních žláz obsahuje informaci použitelnou pro ověření identity osoby. Jedinečnost je však založena pouze na předpokladu a nebyla ověřena na dostatečně velkém vzorku populace.

  Pro měření se využívá senzor, který zaznamenává relativní pozici potních žláz vzhledem k ploše prstu. Měření není uživatelsky nepříjemné. Problémy může způsobit špinavé nebo prašné prostředí. Nutný je senzor s vysokým rozlišením, rozlišení běžných senzorů pro snímání otisků prstů není dostačující.

- *Stisk ruky* – existují dva různé přístupy pro využití stisku ruky jako biometriky. První využívá IR světlo k osvětlení a analýze podkožní tkáně a vzorů krevního řečiště ruky v pozici stisku.

  Druhý přístup využívá jedinečnosti tlaku vyvinutého při stisku objektu. Rozlišení osob pak probíhá na základě neurofyziologického ovládání pohybů prstů, ruky a zápěstí.

Jedinečnost není dosud empiricky prokázaná, prostředí a stav jedince může mít vliv na IR snímače. Stisk může být ovlivněn věkem a zdravotním stavem. Problematika hygieny může způsobit nespokojenost uživatelů.

Využití by technologie mohla nalézt ve zbrojním průmyslu, řízení letadel a vozidel, kde probíhá řada výzkumů.

- *Lůžka nehtů* – technologie založená na snímání struktury kůže pod nehty. Na kůži se nachází paralelní linie tvořící unikátní podélné prostorové uspořádání pokožky. Jedinečnost vzorů opět není dokázaná. Struktura je poměrně jednoduchá, a proto by její zpracování nemělo být výpočetně náročné.

- *Pach těla* – každý člověk má jedinečný pach těla, který je složen z přibližně třiceti chemických látek. Využívá se elektronický „nos“ složený z mnoha senzorů, které generují rozdíly v napětí, pokud je daná chemická látka přítomna. Identifikace probíhá pomocí neuronových sítí. Žádný biometrický systém využívající pach těla zatím nebyl vyroben.

  Tělní zápach je značně ovlivněn některými faktory jako je dieta nebo emocionální stav, používání parfémů, apod. Navíc poskytuje citlivé informace o zdravotním stavu a hygieně jedince.

- *Ucho* – tvar vnější části ucha a struktura chrupavek ušního boltce jsou považovány za jedinečné a v průběhu času se radikálně nemění (zejména po dosažení plnoletosti). Měření je možné provádět dvěma způsoby, buďto bezkontaktně prostřednictvím fotografií (*ear images*) nebo kontaktním otiskem (*ear prints*). Bezkontaktní přístup se jeví výhodnější, protože nezpůsobuje při snímání deformace jako v případě otisku. Porovnávají se vektory vzdáleností výčnělků ušního boltce od pevně daného bodu.

  Otisk ucha je v některých státech považován za dostatečně průkazný k usvědčení zločinců. Přestože jedinečnost biometriky je pouze hypotetická, ucho je někdy považováno za identifikačně bohatší na informace než tvář.

  Pro snímání je nutné správné osvětlení a úhel kamery. Vzhledem k relativně malé velikosti ucha je vyžadována kvalitní kamera, snímání může být díky jednotné barevnosti ucha prováděno v odstínech šedi.

- *Chůze* – metoda založená na rozpoznávání osob podle způsobu jejich chůze. Jedná se o behaviorální biometriku, která se může v rámci dlouhého časového období měnit. Způsob chůze ovlivňuje váha, zranění, nemoc, emoční stav, stejně jako i typ bot, oblečení, prostředí a další faktory. Jedinečnost není dokázaná, metriky jsou stále předmětem výzkumu.

  Snímání není nijak dotěrně, je bezkontaktní a je možné jej provádět i na větší vzdálenosti. Technologie by mohla být využitelná i v oblasti sledování nebo monitorování pohybu.

- *Mozkové vlny* – rozšíření EEG (encephalogram – mozkové vlny), které měří rozdíly v elektrickém potenciálu způsobené mozkovou aktivitou. Subjektu jsou předkládány fotografie nebo slova související s nějakou situací (např. zločin) spolu s irelevantními informacemi. Zároveň se měří aktivita mozku, která se liší v případě, že předložená informace je subjektu známá a v případě, kdy se s ní subjekt setkal poprvé.

- *Otisk chodidla* – existují dva přístupy. První z nich měří statické charakteristiky, podobně jako v případě otisku prstu. Měří se velikost, tvar, geometrie stopy nebo vzory rýh v otisku chodidla. Druhý přístup měří dynamiku kroku při chůzi. Zajímavé jsou především délka kroku, analýza tlaku, časování nebo tření.

  Statické charakteristiky mohou být jedinečné a robustní, dynamické charakteristiky mohou být ovlivněny váhou, typem bot, věkem, zraněním, apod. Měření statických charakteristik je dotěrné, osoba si musí vyzout boty, dynamické charakteristiky lze měřit pasivně. Otisk chodidla může doplňovat biometriku založenou na chůzi.

3.6.10 Kombinované biometriky

Hand geometry + vein pattern
Face recognition + facial thermograph
Fingerprint + sweat pores

3.7 Chybovost

Jak již bylo zmíněno výše, je prakticky nemožné, aby uživatel při autentizaci poskytl systému naprosto stejný vzorek jako během procesu registrace. Proto je nutné povolit určitou variabilitu mezi srovnávanými vzorky, což může vést k chybám rozhodování. Druhou skupinu chyb tvoří chyby způsobené nemožností získat od uživatele adekvátní vzorek. [1]

3.7.1 Chyby rozhodování

- *FAR (False Acceptance Rate)* – pravděpodobnost, že neautorizovaný uživatel získá přístup do systému, tzn. že neautorizovaný uživatel je nesprávně rozpoznán jako autorizovaný uživatel. Tento typ chyby se někdy rovněž označuje jako *chyba typu II* nebo *False Match Rate (FMR)*.

$$FAR = \frac{\text{počet nesprávných přijetí}}{\text{počet všech pokusů}} \cdot 100\,[\%]$$

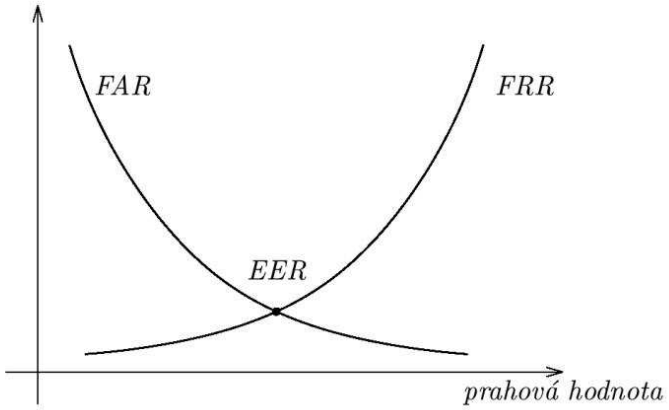
- *FRR (False Rejection Rate)* – pravděpodobnost, že autorizovanému uživateli je zamítnut přístup do systému, tzn. že autorizovaný uživatel není v systému rozpoznán. Označuje se též jako *chyba typu I* nebo *False Non-Match Rate (FNMR)*.

$$FRR = \frac{\text{počet nesprávných odmítnutí}}{\text{počet všech pokusů}} \cdot 100\,[\%]$$

- *ERR (Equal Error Rate)* – tato hodnota odpovídá rovnosti FAR a FRR. Lze říci, že čím nižší je hodnota EER, tím přesnější je biometrický systém, avšak znalost ERR nevypovídá o bezpečnosti systému tolik, jako znalost samotných hodnot FAR a FRR

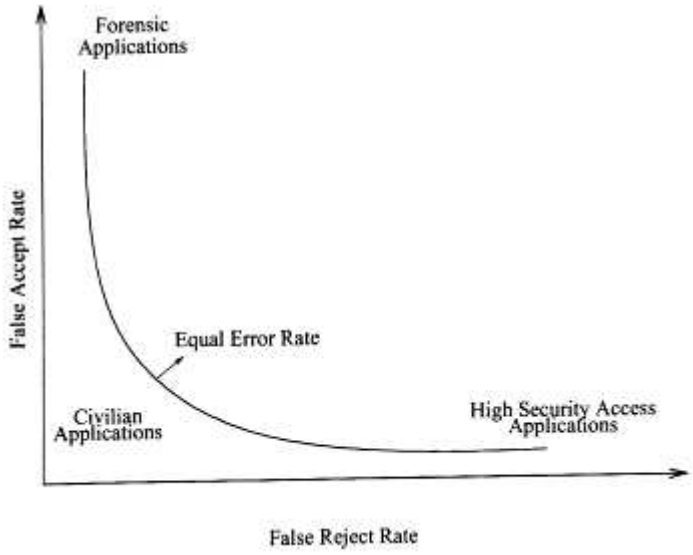
Hodnoty FAR a FRR obvykle závisí na nastavení prahové hodnoty systému. Zvyšováním prahové hodnoty sice získáme bezpečnější systém (snižuje se FAR), ale na druhou stranu dochází ke zvýšení počtu nesprávných přijetí (FRR se zvyšuje), což vede k nespokojenosti uživatelů. Naopak snižováním prahové hodnoty nebudou uživatelé obtěžováni opakovanými pokusy o

autentizaci (FRR se snižuje), ale systém bude vykazovat větší počet přijetí neautorizovaných osob (zvyšuje se FAR). Z výše uvedeného plyne, že FAR a FRR jsou nepřímo úměrné (viz. obr. 3.8). Konkrétní nastavení prahové hodnoty závisí na účelu daného systému, rozhodnutí, které chyby jsou méně kritické a zvážení rizik plynoucích z jednotlivých chyb.



Obr. 3.8: Závislost FAR a FRR na prahové hodnotě [6]

ROC křivka (Receiver Operating Characteristics) – zobrazuje závislost mezi FRR a FAR. Každý bod křivky definuje FAR a FRR pro daný systém operující s určitou prahovou hodnotou. Příklad ROC křivky je uveden na obr. 3.9. ROC křivka slouží k porovnání různých biometrických systémů pracujících za podobných podmínek nebo k porovnání jednoho systému za odlišných podmínek. Čím více se křivka blíží k bodu (0,0), tím menší je chybovost systému. [2, 4]



Obr. 3.9: ROC křivka [2]

3.7.2 Chyby snímání biometrických dat

- *FTE (Failure To Enroll Rate)* – pravděpodobnost, že z jakéhokoliv důvodu se daná osoba nemůže do systému zaregistrovat. Důvodem může být zranění, problémy s kvalitou

vzorku nebo nesprávná poloha měřené biometriky na snímači. Zahrnují se zde také osoby bez požadované biometriky (lidé s chybějícími orgány).

$$FTE = \frac{\text{Počet neúspěšných registrací}}{\text{Počet všech uživatelů pokoušejících se o registraci}} \cdot 100\,[\%]$$

- *FTA (Failure To Acquire Rate)* – pravděpodobnost, že systém není schopen zachytit nebo rozpoznat obraz dostatečné kvality v okamžiku, kdy uživatel předkládá biometriku snímači. Chyba může být způsobena nesprávnou polohou snímané biometriky na snímači, neoptimálním prostředím (např. při rozpoznávání tváře) nebo zraněním.

$$FTA = \frac{\text{Počet neúspěšných prezentovaných biometrických dat snímačem}}{\text{Počet všech prezentací biometrických dat}} \cdot 100\,[\%]$$

3.8 Testování biometrických systémů

Výrobci a prodejci biometrických systémů se snaží své výrobky prodat, proto někdy klamně jmenují všemožné výhody svého produktu, deklarují vysokou výkonnost, jednoduchost použití a možnost použití ve všech možných prostředích.

Informace od různých výrobců často používají odlišnou notaci a i když mohou být informace o produktech objektivní, pro zákazníka, snažícího se porovnat různé produkty, je mnohdy obtížné dobrat se smysluplných závěrů.

Nezávislé testování je základním prostředkem pro posouzení vyspělosti produktů a porozumění funkčnosti v různých podmínkách nebo ve srovnání s ostatními.

Důkladné, opakovatelné testování je drahé. Vyžaduje pečlivé plánování, sběr dat, provedení a zdokumentování. Zpravidla jej provádějí vládní organizace, univerzity nebo vládní laboratoře a výzkumná centra, které mají potřebné finanční prostředky, znalosti a vybavení.

Výsledky testů mají vysokou hodnotu jak pro vládní programy, tak i pro malé průmyslové firmy. Pomáhají vývojářům odhalit a následně odstranit slabiny a nedostatky, integrátorům vhodně rozložit, nastavit a obsluhovat systémy a celkově lépe dosáhnout bezpečnostních požadavků.

Existuje mnoho testovacích a hodnotících metod. Odlišnost metod může mít za následek zdánlivě protichůdné výsledky, které se těžce srovnávají nebo kombinují. Snahou o sjednocení průběhu testování bylo vydání „The Best Practices for Biometrics Testing“ skupinou CESG (Communications-Electronics Security Group) ve Velké Británií. Dokument obsahuje obecný slovník, metody a měření pro prezentaci a srovnání výsledků, což umožňuje sdílet data, metody a výsledky mezi univerzitami, vládními laboratořemi a průmyslem. Dokument zároveň shrnuje typy testování a navrhuje kritéria pro hodnocení biometrických systémů. [1]

3.8.1 Kritéria testování

- *Chybovost* – FAR, FRR, ERR, FTE, FTA

- *Uživatelský výkon* – počet uživatelů, kteří mohou být autentizováni za jednotku času v daném systému. Může být také vyjádřen celkovým časem transakce pro jednoho

uživatele (čas snímání dat, zpracování a případně zadání PINu, identifikačních údajů nebo předložení tokenu)

- *Výkon srovnávacího algoritmu* – počet srovnání proveditelných za jednotku času, resp. čas potřebný pro srovnání určitého počtu vzorků. Důležitou roli hraje především při identifikaci (1:N) v rámci velkých databází

3.8.2 Typy testování

- *Testování algoritmu* – zaměřeno na porozumění a srovnání softwarových technik pro získávání, zpracovávání a srovnávání biometrických dat. Různé techniky jsou srovnávány z hlediska efektivity, rychlosti a výkonnosti.
  Obvykle nezahrnuje lidský faktor, testovací data jsou připravena offline.

- *Testování technologie* – testování kompletního systémového produktu a zařízení. Soustředí se na ustavení operačních charakteristik dané technologie a jsou navrženy pro srovnání jednoho nebo více systémů za specifických podmínek a proti stejné množině vstupů. Testovací data by neměla být předem známá.

- *Testování scénáře* – zájem se soustředí na integraci biometrického systému do reálného prostředí. Testování poskytuje informace o tom, jak úspěšně technologie funguje v cílovém prostředí. Ideálně by mělo zahrnout skutečné uživatele a administrátory. Uživatelé by měli být předem poučeni o technologii. Reakce uživatelů poskytují informace o použitelnosti, lidském faktoru a přijatelnosti.

- *Testování zranitelnosti* – porozumění, jak lze systém prolomit nebo jaké je riziko samotného selhání systému. Nejvíce se soustředí na snímače, které tvoří rozhraní mezi systémem a uživatelem a jsou místem, kde jsou biometrická data prezentována systému. Snaží se nalézt slabá místa v systému a zneužít je k získání přístupu.

3.9 Testování živosti

Biometrické testy živosti jsou automatizované testy prováděné za účelem zjištění, zda biometrický vzorek pochází skutečně od živé osoby. Navíc ne od libovolné osoby, ale od osoby, která je v systému zaregistrována.

Biometrický systém může být prolomen náhradou skutečného vzorku falešným (umělým) vzorkem osoby, která je v systému zaregistrována. Vzorek autorizované osoby nemusí být obtížné získat, protože biometriky nejsou tajné informace, například otisk prstu zanecháváme na všem, čeho se dotkneme. Testování živosti by mělo těmto typům útoků zabránit a zvýšit tak bezpečnost biometrického systému. [1]

3.9.1 Metody testování živosti

Za základní metodu testování živosti lze považovat lidského pozorovatele, který dohlíží na snímání biometrických vzorků. Jednotlivé metody se od sebe navzájem liší, avšak lze je rozdělit do tří následujících kategorií:

- *Vyhledávání přirozených vlastností lidského těla* – fyzické (váha, hustota, pružnost), elektrické (kapacita, odpor, impedance), vizuální (barva, vzhled, tvar), spektrální (odrazivost, absorpce, propustnost), tělní tekutina (kyslík, krevní složky, DNA)

- *Analýza přirozených signálů vytvářených lidským tělem* – tep, krevní tlak, teplota, krevní tok, pocení, tělesný pach, elektrické signály vytvářené srdcem (EKG), mozkové vlny

- *Měření reakcí těla na podněty („výzva-odpověď")* – založené buďto na reakci uživatele na výzvu (hmatové, zrakové nebo sluchové podněty), nebo na reflexivních reakcích (reakce svalů na elektrický impuls (EMG), rozšiřování očních zornic při různých intenzitách osvětlení, reakce kolena na úder, změna barvy kůže při tlaku

Robustnost techniky testování živosti nezávisí takovou měrou na zvolené metodě, ale především na její implementaci. Aby testy živosti byly spolehlivé, měly by být prováděny zároveň se snímáním biometrických dat (ve stejný čas a prostřednictvím stejného snímače). To zajišťuje, že data získaná pro test živosti pochází od stejného zdroje jako primární biometrický vzorek.

Testování živosti s sebou přináší i několik nevýhod. Obvykle má za následek zvětšení snímacího zařízení, delší čas prezentace vzorku (uživatel musí vydržet i několik sekund bez hnutí), vyšší počet nesprávných odmítnutí a také vyšší cenu.

Kapitola 4

Testované systémy

Následující kapitola se věnuje popisu jednotlivých systémů, které byly v mé práci podrobeny testování. Jedná se o systémy dostupné v Laboratoři bezpečnosti a aplikované kryptografie Fakulty informatiky Masarykovy univerzity. Testovány byly dvě různé biometrické technologie, a to otisk prstu a rozpoznávání tváře. U otisku prstu byly k dispozici zařízení od společností Bioscrypt, Cross Match, Microsoft a APC. V rámci rozpoznávání tváře se jednalo o softwarové produkty společností Neurotechnology a Luxand.

4.1 Bioscrypt V-Pass

Čtečka otisků prstů V-Pass od společnosti Bioscrypt patří do produktové řady *Veri-Series*. Produkty jsou využívány k identifikaci nebo verifikaci osob v řadě aplikací, především řízení přístupu, kontrola docházky, přístupu k počítačům a další.

4.1.1 Technické parametry

Model V-Pass umožňuje identifikaci osob (1:N) na základě otisků prstů, kdy vyhledávací algoritmus porovnává získaný vzorek se všemi záznamy v databázi a hledá shodu. Model je určen pro malé databáze uživatelů, dokumentace uvádí do 200 nebo 500 vzorků, v závislosti na firmwaru. Protože zařízení slouží pouze pro identifikaci, uživatelé nemusí disponovat žádnou znalostí (PIN) nebo tokenem. Čtečka automaticky detekuje přiložený prst, následně sejme vzorek otisku, porovná jej s databází uložených vzorků a rozhodne o shodě, případně provede požadovanou akci.

Rozměry zařízení jsou 135 × 70 × 64 mm a konstrukce je uzpůsobená pro upevnění na stěnu do vnitřních prostor budov. Pro připojení napájení a dalších externích zařízení (např. pro řízení přístupu) je použit 15-pinový konektor DB15M. Napájecí napětí musí být stejnosměrné v rozmezí 9–24 V, doporučeno je 12 V. Komunikace s počítačem probíhá prostřednictvím sériového portu RS-232, resp. RS-485. Na straně čtečky je použit port RJ11, případně dříve zmíněný port DB15M.

Samotný snímač otisků prstů je založen na kapacitním principu. Jedná se o snímač AFS2 společnosti AuthenTec. Povrch je tvořen silikonem a jeho rozměry jsou 24 × 24 × 3,5 mm. Snímací plocha má rozměry 13 × 13 mm a rozlišení 250 dpi (bodů na palec). [22]

Signalizace stavu zařízení je prováděna prostřednictvím dvou LED, přičemž první, v přední části zařízení, je zelená a signalizuje přítomnost napájecího napětí. Druhá, nacházející se nad snímačem, je složena ze dvou LED a je schopna poskytovat výstup ve třech barvách (červená, zelená a oranžová). Slouží k signalizaci stavu zařízení a poskytuje uživateli zpětnou vazbu. Význam popisuje tabulka 3.10.

LED indikátor	Význam
Zhasnuto	Snímání otisku dokončeno – probíhá zpracování
Svítí červeně	Identifikace neúspěšná
Svítí zeleně	Identifikace úspěšná; snímání registračního vzorku dokončeno
Svítí oranžově	Zařízení připraveno ke snímání

Tab. 3.10: Signalizace stavu zařízení

Zařízení disponuje energeticky nezávislou pamětí typu flash, která uchovává registrační vzorky a konfigurační data. Během registrace jsou vytvářeny registrační vzorky o velikosti 2488 bytů, kódující charakteristické informace pro daný otisk prstu. Vzorky mohou být následně distribuovány do jiných kompatibilních čteček nebo uloženy do počítače (*.tms).

Pro správné umístění prstu na snímač při registraci i následném používání k identifikaci disponuje čtečka speciální zarážkou, tzv. *Ridge-Lock*. Zarážka by se při snímání měla nacházet na úrovni prvního kloubu prstu. Poté by měl uživatel přiložit prst za působení mírného tlaku na snímač. Zarážka by měla zajistit, že bude snímána právě oblast otisku kolem jádra, která je informačně nejbohatší.

Obr. 3.11: Zařízení Bioscrypt V-Pass [22]

Výkon systému se uvádí v hodnotách FRR a FAR. Model V-Pass neumožňuje nastavovat bezpečnostní úrovně a výrobcem uváděná bezpečnostní úroveň odpovídá FRR = 1 % a FAR = 0,2 %.

4.1.2 Software VeriAdmin

Spolu se čtečkou je dodáván software *VeriAdmin*, který umožňuje konfiguraci zařízení a správu registračních vzorků z prostředí operačního systému Microsoft Windows (98 a vyšší). Software lze využít pro správu většího počtu čteček propojených do sítě, registraci nových uživatelů, úpravu nebo mazání registračních vzorků, distribuci vzorků uložených ve čtečce do počítače nebo jiné čtečky, nastavení parametrů zařízení (komunikace, biometriky, výstup, signalizace a další) a aktualizaci firmwaru.

Seznámení se s čtečkou a příslušným softwarem, možnostmi konfigurace systému a jeho správného používání bylo úvodní pasáží praktické části práce.

Konfigurace zařízení

Po připojení zařízení k počítači je nutné nastavit v aplikaci VeriAdmin parametry připojení. Nastavení se týká zejména výběru sériového nebo Ethernet portu počítače pro připojení zařízení a nastavení přenosových rychlostí. K tomuto slouží nástroj *Network Setup*. Následně je spuštěn

dialog pro nastavení sítě zařízení – *Network Configuration Dialog*. Zde je ve stromové struktuře zobrazena logická struktura sítě zařízení Bioscrypt, připojených na jednotlivé porty. Pomocí tohoto nástroje lze přidávat, odebírat zařízení, přesouvat je mezi jednotlivými porty nebo získat informace o jejich stavu. Každé zařízení je reprezentováno unikátním identifikátorem a pro správu zařízení prostřednictvím počítače musí být přidáno do sítě. Nastavení komunikačních parametrů pro konkrétní zařízení je součástí dokumentace.

Jakmile máme ustavenu komunikaci mezi čtečkou a počítačem, můžeme systém spravovat a konfigurovat prostřednictvím následujících nástrojů:

- *Template Manager* – nástroj pro správu registračních vzorků uživatelů. Umožňuje přidávat, editovat, mazat vzorky, přesouvat vzorky mezi pamětí čtečky a počítačem nebo mezi více čtečkami a provádět verifikaci daného uloženého vzorku s „živým“ vzorkem uživatele. Výstupem je míra shody, tzv. *skóre*.

  Každý vzorek je v databázi identifikován jedinečnou kombinací dvou čísel – *ID* a *Index*. Index je možné využít, pokud chceme uchovávat otisky více prstů pod jedním ID, jinak může být 0. Záznam vzorku v databázi se skládá z matematické reprezentace otisku prstu (obraz otisku se neukládá), identifikace, o který prst se jedná, identifikátoru a jména uživatele. Dále mohou být uchovávány další údaje, které však pro tento model čtečky nejsou využitelné, např. bezpečnostní úroveň pro verifikaci pro jednotlivé vzorky, doplňkové heslo a další.

- *Command Card Manager* – umožňuje přidávat nebo odebírat uživatele ze systému bez použití počítače, pomocí definovaných čipových karet. Využitelné administrátory například pro přidělování dočasného přístupu do systému, především u čteček spolupracujících s čipovými kartami. V mém případě netestováno.

- *Unit Parameters* – nástroj sloužící ke konfiguraci zařízení. Umožňuje změny nastavení komunikačních parametrů. Zde se jedná zejména o identifikační údaje v rámci sítě, výběr komunikačního protokolu a přenosové rychlosti, včetně možnosti ochrany komunikačního portu heslem.

  Další nastavení se týkají rozhraní Wiegand, které bývá využíváno pro připojení čteček čipových karet, resp. karet s magnetickým proužkem.

  Následují nastavení se týkají biometrické autentizace. Konfigurovat lze globální bezpečnostní úroveň pro zařízení. Nastavení lze provést výběrem jedné z pěti úrovní, vztahuje se však pouze na verifikaci. U testovaného modelu V-Pass nastaveno pevně na střední úroveň (FAR i FRR 0,1 %). Dále je možné vypnout biometrickou autentizaci (např. u modelů využívajících kromě biometriky i čipové karty), u modelů určených pro identifikaci lze zapnout/vypnout automatickou detekci prstu, chování systému v případě, kdy je biometrika při verifikaci ignorována (musí/nemusí alespoň přiložit prst na snímač). Pro zvýšení bezpečnosti je možno vyžadovat při autentizaci otisky více prstů (počet lze nastavit), a to buď od jedné osoby, nebo více osob. Systém nabízí možnost registrovat otisk vybraného prstu, který by byl použit při identifikaci v případě nátlaku útočníka na oprávněnou osobu o umožnění přístupu. Systém pak může na takovou situaci reagovat provedením odpovídající akce.

  Další nastavení se týkají konfigurace reakcí systému na úspěšnou autentizaci, konfigurace vstupních a výstupních TTL linek.

- *Broadcast Parameters* – pomocí tohoto nástroje lze modifikovat nastavení na všech zařízeních v síťovém prostředí současně.

- *LED Table Settings* – umožňuje konfigurovat chování signalizačních LED na zařízení v závislosti na provedené operaci. Specifikovat lze, která LED má být rozsvícena, po jakou dobu, případně rychlost blikání nebo použití doplňkové zvukové signalizace.

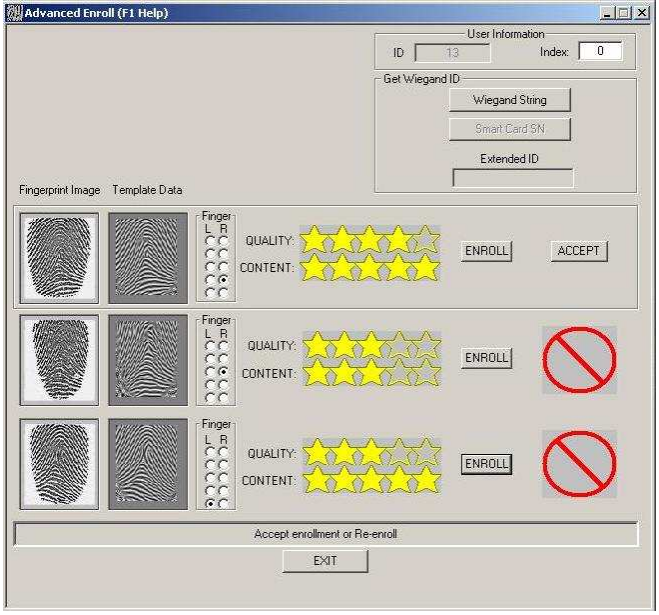
Dalšími nástroji aplikace VeriAdmin jsou *Sensor Configuration* (kalibrace a konfigurace snímače), *Update Firmware* (aktualizace firmwaru procesoru čtečky), *Reset Unit To Factory Default* (obnovení továrního nastavení) a *Template Conversion* (slouží k převodu mezi vzorky určenými pro identifikaci a vzorky pro verifikaci).

Registrace uživatele

Software VeriAdmin nabízí pro registraci uživatele dva nástroje, *Quick Enroll* a *Advanced Enroll*, které se liší v počtu snímaných otisků.

- *Quick Enroll* – při tomto procesu je snímán pouze jeden otisk, ze kterého se vytváří registrační vzorek. V příslušném okně aplikace VeriAdmin je nutné nejprve zadat ID vzorku. Následně klikneme na tlačítko „Enroll“, čímž je zahájeno snímání vzorku. Požadavek na přiložení prstu na snímač je zároveň signalizován oranžovou barvou LED. Prst lze ze snímače uvolnit po zhasnutí oranžové LED. Snímání trvá zhruba 5 sekund. Zelené světlo LED signalizuje úspěšné získání vzorku, v opačném případě se rozsvítí světlo červené. V okně aplikace je zobrazen skutečný obraz sejmutého otisku i jeho matematická reprezentace, která bude uložena do databáze. Zároveň je zobrazena informace o kvalitě otisku, kdy aplikace hodnotí kvalitu snímaného obrazu (*Quality*) a množství získaných charakteristických znaků v otisku (*Content*), obě hodnoty v pěti stupních (1–5 hvězdiček, kde 5 je nejvyšší kvalita). V případě nekvalitního vzorku (minimálně jedno hodnocení nižší než 3) je doporučeno proces opakovat. Pokud jsou získaná data dostatečně kvalitní, následuje vyplnění doplňujících údajů (jméno, apod.) a vzorek je uložen do paměti čtečky nebo do počítače.

- *Advanced Enroll* – proces registrace se skládá ze tří nezávislých snímání otisku prstu. Je možné použít třikrát otisk stejného prstu nebo různých prstů. Aplikace po provedení tří měření určí nejlepší vzorek, který doporučí k uložení. Nicméně uživatel, resp. administrátor se doporučením řídit nemusí, může vybrat vzorek, který uzná za vhodný a ten uložit. Jedná se o doporučený proces pro registraci všech uživatelů. Poskytuje informaci o optimálním umístění prstu na snímač nebo umožňuje znázornit, jak se liší kvalita otisků různých prstů stejné osoby. To umožňuje odhalit optimální umístění prstu na snímač pro konkrétní osobu, resp. vybrat optimální prst, čímž je možné zvýšit přesnost systému.



Obr. 4.1: Okno aplikace Advanced Enrollment

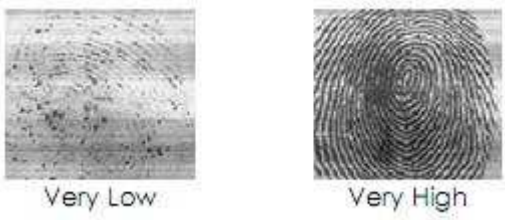
Quality, *Content* a správná pozice prstu na snímači

Maximální výkon systému je podmíněn správným umístěním prstu na snímač během registrace i následné identifikaci. Prst by měl být přikládán tak, aby byly zachyceny charakteristické vzory v otisku. Snímána by měla být část prstu kolem jádra otisku, tedy jádro by mělo být umístěno uprostřed snímaného obrazu a celý prst uprostřed snímače. Pomůckou pro správnou pozici je již dříve zmiňovaná zarážka (*Ridge-Lock*) nacházející se pod snímačem.

Dalším faktorem ovlivňujícím kvalitu snímaného otisku jsou příliš suché, resp. příliš vlhké prsty. Přirozená vlhkost pokožky umožňuje optimální zachycení hřebenů a údolí v otisku. Příliš suché prsty snižují kontrast obrazu, příliš vlhké prsty mají za následek slévání hřebenů.

Zároveň by uživatelé měli pamatovat na to, aby prst při identifikaci přikládali pokud možno stejně jako při registraci.

- *Quality* – specifikuje, jak kvalitní je získaný obraz otisku prstu, tedy jak kvalitně jsou v otisku patrné vzory rýh. Míra kvality je vyjádřena v počtu hvězdiček v rozmezí 1–5, kdy 5 vyjadřuje nejvyšší kvalitu. Čím je kvalita při registraci nižší, tím vyšší je riziko nesprávného odmítnutí. Pro spolehlivou funkci systému výrobce doporučuje minimální kvalitu 3 hvězdičky. Nízká kvalita může být způsobena především suchými prsty nebo znečištěným povrchem senzoru.



Obr. 4.2: Příklad nízké a vysoké kvality otisku [22]

- *Content* – vyjadřuje množství informace použitelné pro identifikaci, tedy množství charakteristických rysů v otisku rozpoznaných systémem ve snímaném obraze. Menší množství informačního obsahu u vzorku může způsobit vyšší náchylnost systému k nesprávnému přijetí. Míra informačního obsahu je opět vyjadřována 1–5 hvězdičkami. Doporučováno je akceptovat při registraci vzorky s mírou alespoň 3 hvězdičky. Zdrojem nízkého hodnocení obsahu může být nesprávná pozice prstu na snímači nebo otisky s výjimečně nízkým počtem markant.

Obr. 4.3: Příklad nízkého a vysokého informačního obsahu [22]

Identifikace uživatele

Čtečka V-Pass disponuje digitálním signálovým procesorem (DSP), který umožňuje automatickou detekci a sejmutí otisku prstu přiloženého na snímač. Připravenost čtečky je signalizována oranžovým světlem LED. Uživatel tedy může přiložit prst na snímač. Prst musí být přiložen na snímači po dobu, kdy svítí oranžové světlo. Čtečka následně provede srovnání vzorku s databází a rozhodnutí o shodě je uživateli prezentováno zeleným/červeným světlem LED. Proces identifikace trvá asi 2–3 sekundy.

4.2 Cross Match Verifier 300 LC 2.0

Čtečka otisků prstů společnosti Cross Match, která ve spojení s počítačem a příslušným programem slouží k registraci, verifikaci a identifikaci osob. Využívaná je především v aplikacích řízení fyzického přístupu, pro kontroly na hraničních přechodech nebo letištích, k přístupu k uživatelským účtům na počítačích apod.

4.2.1 Technické parametry

Zařízení se připojuje k počítači prostřednictvím rozhraní USB 2.0. Rozměry jsou 62 × 162 × 83 mm, váha 0,45 kg. Snímač pracuje na optickém principu, snímací plocha je tvořena skleněnou deskou o rozměrech 30,5 × 30,5 mm, rozlišení snímače je 500 dpi. Otisk je snímán přiložením prstu na snímač, bez jakéhokoliv následného pohybu. Napájení i výstup je řešen prostřednictvím USB kabelu.

Obr. 4.4 Cross Match Verifier 300 LC 2.0 [23]

Zařízení je možné připojit k počítači s operačním systémem Windows 2000 nebo XP. Správná činnost čtečky je podmíněna instalací příslušného ovladače hardwaru. Ovladač lze stáhnout ze stránek výrobce. Je součástí sady nástrojů pro vývojáře (Software Developer's Kit) USB SDK. Konkrétně pro tuto čtečku je vyžadována verze 4.0 a vyšší. USB SDK poskytuje kromě samotného ovladače zařízení i nástroje pro jeho konfiguraci, což se týká zejména úpravy parametrů obrazu (jas, kontrast, velikost, otočení, automatická korekce, apod.) a možností snímání obrazu (funkce AutoCapture). Podporovaná rychlost snímání je 7 snímků za sekundu. Vývojářům je k dispozici podpora pro jazyky Visual C/C++ a Visual Basic. [23]

4.2.2 Software VeriFinger 6.0 Algorithm Demo

Pro účely autentizace uživatelů jsem zvolil aplikaci *VeriFinger 6.0 Algorithm Demo*. Jedná se o aplikaci demonstrující příklad využití možností sady vývojových nástrojů *VeriFinger SDK* pro práci s otisky prstů od společnosti Neurotechnology.

Aplikace může pracovat ve čtyřech režimech:

- *Registrace* – software zpracuje otisk prstu přiloženého na snímač zařízení (detekce přiložení prstu probíhá automaticky) nebo nahraného ze souboru (*.bmp, *.tif), identifikuje charakteristické znaky a vzorek uloží do databáze.

- *Registrace s generalizací znaků* – tento režim vytváří registrační vzorek zpracováním kolekce charakteristických znaků získaných ze tří otisků stejného prstu a jejich následným zkombinováním do jednoho obecného registračního vzorku. Účelem tohoto procesu je zvýšení přesnosti systému rozpoznávání otisků prstů.

- *Verifikace* – umožňuje srovnání 1:1, kdy uživatel prezentuje systému dva otisky prstu, které jsou následně srovnány a je zobrazeno rozhodnutí o shodě, spolu s číselným údajem vyjadřujícím míru podobnosti.

- *Identifikace* – umožňuje srovnání 1:N. Uživatel prezentuje systému otisk prstu, který je následně srovnán se všemi registračními vzorky uloženými v databázi. Pokud je nalezena shoda, je na výstupu zobrazen identifikátor shodného vzorku a míra podobnosti vzorků (pozitivních výsledků může být i více).

Všechny režimy mohou pracovat jak s „živými“ vzorky získanými od uživatele prostřednictvím čtečky v okamžiku provádění dané akce, tak se vzorky získanými dříve a uloženými v obrazovém souboru typu *.bmp nebo *.tif. Aplikace umožňuje i ukládat sejmuté otisky, a to buďto přímo snímaný obraz nebo obraz digitalizovaný se zvýrazněnými rýhami.

V menu *Options* je možné nastavit řadu parametrů aplikace. Lze změnit rozlišení obrazu nahraného ze souboru (implicitně 500 dpi), zapnout nebo vypnout automatické přidělovaní identifikátoru otisku. Rozlišení obrazu snímaného čtečkou je 504 × 480 pixelů. Pro registraci je možné zvolit minimální počet markant v otisku (aplikace běžně rozliší 20–40 markant, pro úspěšnou identifikaci je zapotřebí nejméně 5–7 markant; implicitní hodnota je 10) a vyhledávání duplicit v databázi. Aplikace umožňuje zrychlit proces identifikace tím, že lze identifikační proces ukončit po první nalezené shodě. Vzorky jsou v databázi navíc seřazeny podle základních podobných rysů. Identifikace pak probíhá tak, že se nejprve otisk porovnává s malou skupinou nejpodobnějších otisků. Pokud není nalezena shoda, porovnává se s další skupinou podobných vzorků, atd. Protože je velká pravděpodobnost, že shoda bude nalezena v první skupině otisků, lze nastavit maximální procento databáze, která se má do identifikace zahrnout. Volbu je možno vypnout položkou *Use G* (G vyjadřuje hustotu rýh).

Menu *VeriFinger Options* umožňuje měnit parametry algoritmu zpracování otisků. Lze nastavit míru nesprávného přijetí (0,1 %; 0,01 % (implicitní hodnota); 0,001 %) pro generalizaci a srovnání. Dále lze nastavit maximální rotaci prstu při snímání a počet vzorků vyžadovaných pro zápis s generalizací (implicitně 3 vzorky).

Registrační vzorky lze využít pro výpočet ROC. Pro výpočet je nutné, aby vzorky stejného prstu měly stejný identifikátor, vzorky různých prstů různé identifikátory.

FAR	**Srovnávací práh (minimální míra podobnosti)**

10 %	12
1 %	24
0,1 %	36
0,01 %	48
0,001 %	60
0,0001 %	72
0,00001 %	84
0,000001 %	96

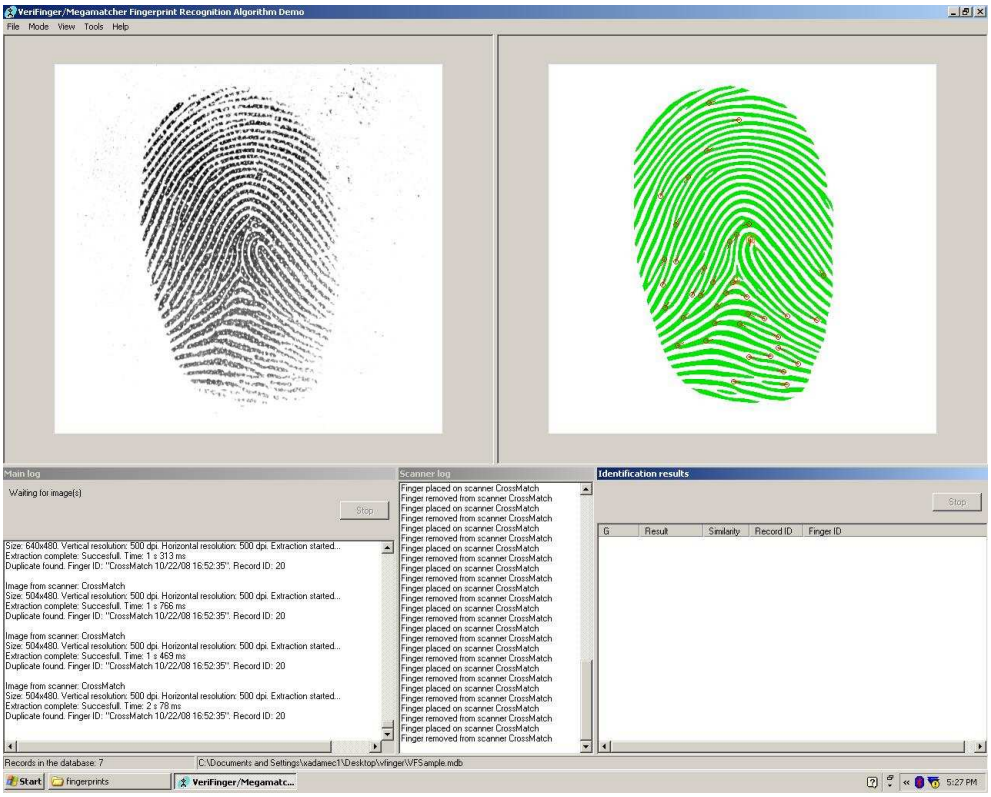
Tab. 4.5: Tabulka prahových hodnot pro různé FAR [24]

Srovnávací práh lze určit podle požadovaného FAR. FAR uvedené v tabulce se vztahuje na srovnání 1:1. Pro identifikaci (1:N) lze odpovídající FAR vypočítat podle následujícího vzorce:

$$FAR_{id} = (1-(1-\frac{FAR_{ver}}{100})^{N}) \cdot 100\,[\%]$$

FAR_{id} …FAR pro identifikaci (1:N)
FAR_{ver} …FAR pro verifikaci (1:1)
N …velikost databáze

Hlavní okno aplikace se skládá z menu pro práci s aplikací a pěti oken. V levém horním okně je zobrazen skutečný obraz sejmutého otisku, vpravo nahoře obraz zpracovaný s identifikátory markant. V dolní části okna aplikace je okno pro zobrazení informací souvisejících s registrací a verifikací/identifikací (časy zpracování a srovnání otisků, počet shodných vzorků, jméno souboru s otiskem, aj.). Dole uprostřed je výpis akcí snímače zařízení a vpravo se zobrazují výsledky identifikace.



Obr. 4.6: Hlavní okno aplikace

Snímání otisku prstu

Prst by měl být na snímač přiložen tak, aby pokrýval co největší plochu snímače a zároveň aby jádro otisku prstu bylo zhruba uprostřed snímaného obrazu. Prst je nutno přiložit na snímač celou plochu současně, uživatel by jej neměl po snímači rolovat. Jinak je možné, že snímač zachytí pouze část otisku prstu, která se jako první dostala do kontaktu s povrchem snímače, což může zvýšit míru nesprávných odmítnutí. Dalším problémem mohou být příliš suché prsty. Prsty bez přirozené vlhkosti mají za následek snížení kontrastu snímaného obrazu, tedy nejasné rozlišení mezi vyvýšeninami a údolími.

Sejmutí otisku a identifikace charakteristických znaků trvá zhruba 1–2 sekundy. Doba závisí především na výkonnosti počítače, na kterém aplikace běží.

4.3 Microsoft Fingerprint Reader

Dalším testovaným zařízením v oblasti otisků prstů je čtečka Microsoft Fingerprint Reader. Jedná se o typ čtečky typicky využitelné uživateli osobních počítačů v domácím prostředí nebo pro přístup k uživatelským účtům v prostředí s malým počtem uživatelů.

Spolu se čtečkou je poskytován program *DigitalPersona Password Manager*. Prostřednictvím tohoto programu lze čtečku využít jako alternativu k autentizaci pomocí hesel. Aplikace je určena pro operační systém Windows a umožňuje uživateli přihlašování pomocí otisku prstu všude tam, kde se používají hesla. Typickým využitím je přihlašování k uživatelským účtům na počítači, přístup k účtům na Internetu nebo k aplikacím, které vyžadují ověření identity uživatele.

4.3.1 Technické parametry

Čtečka se k počítači připojuje prostřednictvím USB kabelu. Rozměry zařízení jsou 82 × 50 × 15,7 mm, hmotnost 107 g. Podporovány jsou operační systémy Windows XP a Windows Vista. Snímač pracuje na optickém principu. Je podsvětlen červenou LED, která také poskytuje zpětnou vazbu uživateli. [25]

Obr. 4.7 Microsoft Fingerprint Reader

4.3.2 Software GrFinger 4.2

Pro praktické testování čtečky Microsoft jsem zvolil ukázkovou aplikaci sady vývojových nástrojů pro snímání, zpracování a srovnání otisků prstů společnosti Griaule *GrFinger 4.2 SDK*.

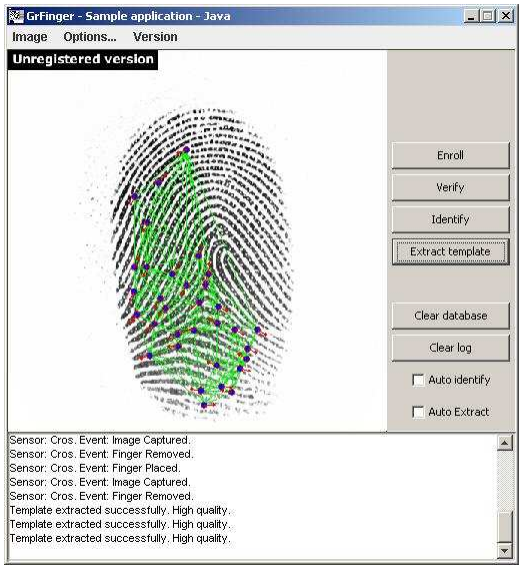
Aplikace vyžaduje pro komunikaci se čtečkou ovladač *FingerCap USB Driver 1.0*. Jakmile je ovladač nainstalován, můžeme připojit čtečku k počítači a začít pracovat s aplikací GrFinger. Okno

aplikace se skládá z plochy, na které se zobrazuje aktuálně sejmutý vzorek otisku prstu. Jeho rozlišení je v případě čtečky Microsoft 355 × 390 pixelů. Pod obrazem je textové pole, ve kterém je uživatel informován o různých událostech (připojení/odpojení čtečky, umístění prstu na snímač a jeho odstranění ze snímače, kvalita sejmutého otisku, míra shody při verifikaci/identifikaci a podobně), tzv. *log*.

Dále se v okně aplikace nacházejí tlačítka pro získání charakteristických znaků z otisku, uložení vzorku do databáze (registrace uživatele), verifikaci, identifikaci a smazání databáze nebo logu. Rovněž lze zvolit možnost automatického zpracování otisku nebo identifikace po získání obrazu otisku. Při verifikaci je navíc nutné zadat identifikátor vzorku, který je vzorku automaticky přidělen při procesu registrace. Výsledek srovnání je zobrazen v logu v hodnotách skóre. Snímání vzorku a jeho zpracování trvá přibližně 1–2 sekundy, v závislosti na výkonu počítače.

Získaný obraz je možné uložit do souboru formátu *.bmp. Aplikace pracuje jak s „živými“ vzorky, tak i s dříve uloženými vzorky, které lze do aplikace opětovně nahrát ze souboru.

V menu *Options* lze nastavit srovnávací práh (minimální skóre) pro verifikaci a identifikaci, toleranci rotace otisku prstu při snímání a možnosti vizualizace charakteristických rysů v otisku. Implicitní srovnávací práh je 25 pro verifikaci a 45 pro identifikaci. Pro tyto hodnoty je udávána hodnota 1 % FRR.



Obr. 4.8: Aplikace GrFinger 4.2

Pro práci se čtečkou platí stejné zásady jako v případě čtečky Cross Match. Kvalita získaného otisku je vyjádřena jedním ze tří stupňů (bad, medium, high) a je po získání charakteristických znaků z otisku zobrazena v logu. Při registraci bychom měli dbát na to, aby získaný otisk měl nejvyšší kvalitu.

4.4 APC Biopod

Poslední testovaná čtečka otisků prstů. Využití je prakticky stejné jako v případě čtečky Microsoft, tedy využívá speciální software pro přístup k heslem chráněným systémům, aplikacím a webovým stránkám s použitím identifikace na základě otisku prstu.

4.4.1 Technické parametry

Rozměry čtečky jsou 51 × 25 × 13 mm,hmotnost 110 g. K počítači se připojuje USB kabelem. Je kompatibilní s operačními systémy Windows 98 a vyššími. Senzor pracuje na kapacitním principu. [26]

Obr. 4.9: APC Biopod

4.4.2 Software Softex Omni Pass 2.0

Se čtečkou je dodáván software *OmniPass 2.0* od společnosti Softex. Software je kompatibilní s operačními systémy Windows a poskytuje funkce pro správu hesel a možnost využít čtečku otisků prstů pro přístup k uživatelským účtům operačního systému, aplikacím a webovým službám, kde autentizace pomocí otisku prstu nahrazuje autentizaci heslem.

Aplikace poskytuje nástroje pro správu uživatelských účtů (přidávání, odebírání, import/export, registraci nového otisku), nastavení chování aplikace v prostředí Windows (přihlašování) a správu přihlašovacích údajů pro aplikace využívající otisk prstu jako alternativu k zadávání hesla. Aplikace je navržena pro maximálně dvacet uživatelských účtů.

Registrace otisku uživatele probíhá za pomoci průvodce, proces vytváření registračního vzorku se skládá z osmi snímání otisku prstu. Následně si uživatel může pod zaregistrovaným otiskem uložit přihlašovací údaje do různých aplikací. Přihlašování k takovým aplikacím je pak možno provést buďto klasickým zadáním přihlašovacích údajů, nebo pouhým sejmutím otisku prstu. V takém případě jsou přihlašovací údaje vyplněny automaticky, pokud je identifikace otisku úspěšná.

Proces registrace trvá zhruba 30 sekund, následné autentizace do 5 sekund.

4.5 VeriLook 3.2 Algorithm Demo

VeriLook 3.2 Algorithm Demo je aplikace demonstrující využití sady vývojových nástrojů a knihoven pro technologii rozpoznávání tváře společnosti Neurotechnology *VeriLook 3.2 Trial SDK*. Aplikace je kompatibilní se systémem Windows 2000/XP, nicméně samotné SDK poskytuje podporu nejen pro Windows, ale i Linux a MacOS.

Aplikace podporuje obrazový vstup z externí kamery nebo ze souboru typu *.bmp, *.tif, *.jpg, *.gif a *.png.

Umožňuje práci ve třech režimech:

- *Registrace* – proces spočívá v získání obrazové informace, detekci tváře a určení charakteristických znaků a uložení záznamu do databáze pod zadaným identifikátorem.

- *Registrace s generalizací znaků* – proces registrace se skládá ze snímání a určení charakteristických znaků více obrazů. Získané informace jsou následně analyzovány a

zkombinovány a výsledná kombinace znaků je uložena do databáze jako registrační vzorek.

- *Identifikace* – obrazová informace je srovnána se všemi záznamy v databázi. Identifikátory nalezených shodných záznamů v databázi jsou zobrazeny v okně aplikace spolu s mírou podobnosti srovnávaného vzorku se vzorkem v databázi.

Technologie rozpoznávání tváře je do značné míry závislá na okolních podmínkách prostředí a pozici a výrazu tváře uživatele během snímání. Z toho vyplývají následující doporučení:

Obličej by měl být snímán z čelního pohledu, maximální povolené natočení hlavy je ± 5° ve všech směrech. Výraz by měl být neutrální (úsměv není žádoucí), s oběma očima otevřenýma a se zavřenými ústy. Pohled směřuje přímo do kamery. Vlasy nebo obroučky brýlí by neměly zakrývat oči.

Výkon systému může být ovlivněn přirozenými změnami v lidské tváři (vousy, účes, apod.).

Osvětlení musí být rozloženo rovnoměrně, ve tváři by neměly být patrné stíny nebo naopak příliš světlá místa.

V případě, kdy uživatel nosí brýle, je vhodné provést registraci s brýlemi i bez nich. Brýle musí být čiré a čisté, aby oči za nimi byly v obraze patrné. Při snímání nesmí být na brýlích viditelné odlesky světla. Příliš tmavé brýle nejsou povoleny. [27]

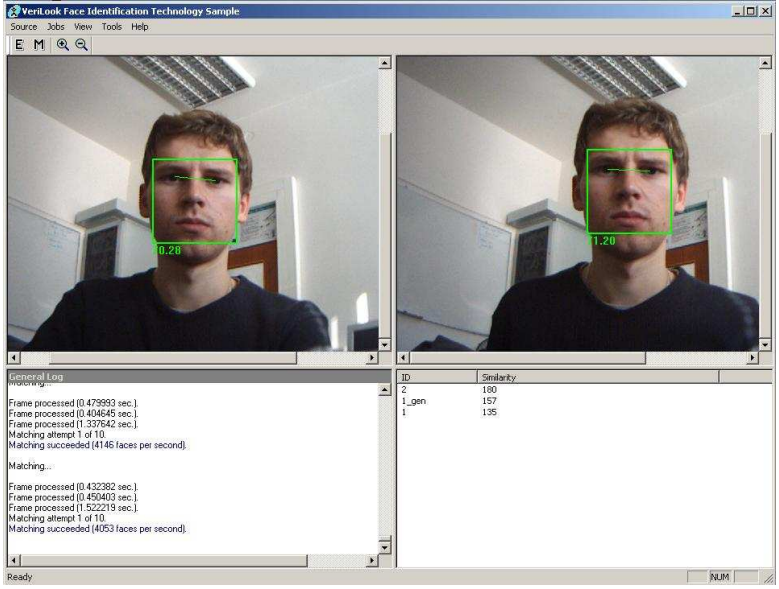
4.5.1 Snímací zařízení

Omezení jsou kladena také na snímací zařízení. V současné době jsou pro rozpoznávání tváře hojně využívány webové kamery. Pro biometrické použití je pro zajištění dostatečné kvality obrazu zapotřebí minimální rozlišení 640 × 480 pixelů. Registrace i následné autentizace by měly být prováděny prostřednictvím stejné kamery, protože každá kamera má své specifické vlastnosti.

Pro praktické testování v rámci této práce byla použita webová kamera od společnosti Creative *Creative WebCam Live! Motion*. Kamera disponuje CCD senzorem o maximálním rozlišení videa 640 × 480 pixelů bez interpolace a s automatickým ostřením. Připojení k počítači je realizováno prostřednictvím rozhraní USB 2.0.

4.5.2 Prostředí aplikace a nastavení

Hlavní okno je rozděleno do čtyř částí. První okno, vlevo nahoře, slouží k zobrazení obrazu ze vstupního zařízení (kamera, soubor) spolu s označením detekované tváře. Okno vpravo zobrazuje obraz, který bude uložen do databáze nebo použit pro srovnání. V dolní části hlavního okna se nachází dvě textové pole (logy). Vlevo se vypisují systémové informace a informace o činnosti aplikace. Vpravo pak výsledky identifikačního procesu, tedy identifikátory shodných záznamů v databázi spolu s hodnotou míry podobnosti. Může zde být zobrazena pouze nejlepší shoda, nebo všechny záznamy vyhodnocené jako shodné (s podobností převyšující srovnávací práh). V horní části hlavní okna je navíc menu sloužící k ovládání a konfiguraci aplikace.



Obr. 4.10 Aplikace VeriLook 3.2 Algorithm Demo

V aplikaci je možné nastavit řadu parametrů týkajících se detekce tváře a určení charakteristických znaků, registrace a identifikace.

Část detekce tváře umožňuje následující nastavení:

- *Face confidence threshold* – číselná hodnota určující požadavky na detekci obličeje. Čím vyšší hodnota, tím vyšší nároky jsou kladeny na správnou pozici a výraz ve tváři. Implicitní hodnota je 55.
- *Minimum/Maximum IOD* – minimální/maximální vzdálenost očí od sebe. Implicitně 40/4000.
- *Face quality threshold* – požadavky na kvalitu snímaného obrazu (ostrost, osvětlení, apod.). Implicitní hodnota je 128.

Pro registraci je možné nastavit:

- *Enroll stream length* – počet snímků zpracovávaných detekčním algoritmem při registraci z kamery. Implicitně 10.
- *Generalization template count* – počet obrazů použitých pro registraci s generalizací. Implicitně jsou snímány 4 obrazy.

Nastavení identifikačních parametrů zahrnuje:

- *FAR* – uvádí se v procentech. Tato hodnota určuje srovnávací práh podle tabulky 4.5 uvedené výše v popisu aplikace VeriFinger. Implicitně 0,01 %.
- *Matching attempts* – maximální počet pokusů o nalezení shody v databázi v rámci identifikačního procesu. Implicitně se provádí 10 pokusů.
- *Use liveness check* – zahrnutí testování živosti do identifikačního procesu. Toto umožňuje odlišit, zda před kamerou stojí živá osoba a zabraňuje tak možnosti vniknutí do systému neoprávněným uživatelem předložením fotografie uživatele, který je v systému zaregistrován. Při testování živosti je požadováno, aby uživatel během identifikačního procesu, který se skládá ze snímání více obrazů, nestál nehybně před kamerou. Doporučeny jsou pohyby hlavy, změny výrazu ve tváři. Pohyby však musí být pouze v takovém rozsahu, aby detekční algoritmus byl stále schopen tvář detekovat.
- *Liveness threshold* – číselná hodnota (0–100) vyjadřující požadavky pro testování živosti. Čím vyšší hodnota, tím větší úsilí o změny výrazu musí uživatelé vynaložit. Implicitně 50.

- *Matching stream length* – počet snímků zpracovávaných detekčním algoritmem při identifikaci z kamery. Implicitně 3 snímky. Pro testování živosti je vyžadováno minimálně 10 snímků.

Doba potřebná pro registraci, registraci s generalizací a identifikaci závisí především na počtu snímků snímaných při daném procesu a také na výkonu počítače. Detekce a srovnání jednoho snímku probíhá v řádu milisekund.

4.6 Luxand FaceSDK 1.7

Druhou aplikací testovanou v rámci rozpoznávání tváře je ukázková aplikace od společnosti Luxand, která demonstruje využití vývojových nástrojů pro detekci a srovnání tváří *Luxand FaceSDK 1.7*. SDK nabízí aplikační programové rozhraní pro detekci tváře a obličejových rysů, verifikaci a identifikaci. Během detekce jsou určeny souřadnice asi čtyřiceti charakteristických rysů, např. oči, oční koutky, obočí, špička nosu, apod., které jsou využity pro další zpracování.

SDK je distribuováno ve formě knihoven DLL (Dynamic Link Library) a je kompatibilní s platformou Win32.

Ukázková aplikace podporuje pouze práci s obrazovými soubory, pro praktické testování byly využity obrazy získané v rámci testování aplikace VeriLook.

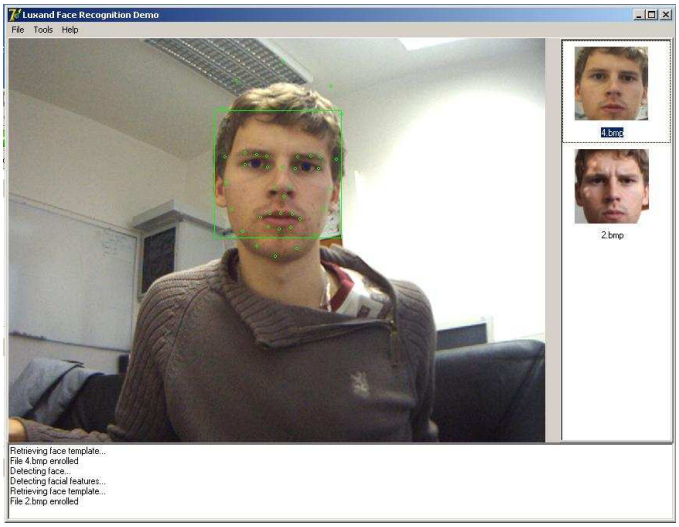
Tvář v obraze by měla být zachycena čelně, nicméně výrobce uvádí možnou odchylku v natočení hlavy až ± 30°. Detekce tváře v obrazové informaci trvá zhruba 1 sekundu. Výstupem detekčního algoritmu jsou souřadnice tváře v obraze (střed, šířka tváře a úhel natočení).

Následně jsou detekovány charakteristické rysy. Výstupem jsou souřadnice čtyřiceti nalezených rysů v obličeji. Proces trvá také zhruba 1 sekundu. Získaná data lze uložit do databáze jako registrační vzorek. [28]

Identifikace probíhá tím způsobem, že je nahrán obrazový soubor, stejně jako v předchozím případě proběhne detekční proces a získaná data jsou srovnána se všemi záznamy v databázi. Srovnání trvá také zhruba 1 sekundu. Výstupem je náhled a identifikátor shodného registračního vzorku v databázi (případně jich může být více), spolu s mírou shody obou vzorků (0 – 100, 100 značí shodu 100 %). Srovnávací práh je možné specifikovat nastavením hodnoty FAR (po jednotkách procent, viz. Tab. 4.11).

FAR	Prahová hodnota
0%	86,00
1%	80,00
2%	79,00
3%	78,00
4%	77,00
5%	76,70
10%	75,70

Tab. 4.11: Nastavení prahové hodnoty



Obr. 4.12: Aplikace Luxand

Kapitola 5

Testování systémů

Testování jednotlivých biometrických systémů bylo rozděleno do několika částí. První částí bylo seznámení se se zařízeními a aplikacemi pro jejich administraci. Tato část měla za úkol seznámení se s možnostmi nastavení systémů a zjištění aspektů ovlivňujících jejich výkon. Na základě zjištěných poznatků bylo upraveno nastavení systémů s ohledem na dané prostředí a navržen postup pro registraci a následnou autentizaci osob.

Následovala hlavní část celé práce, a to testování systémů na dobrovolnících. Testován byl proces registrace a autentizace (identifikace) jednotlivých osob. Cílem bylo především zkoumání chybovosti systémů, uživatelské přívětivosti a náročnosti procesu registrace a identifikace osob, především v kontextu získání správných návyků pro používání biometrických systémů.

Poslední částí práce pak byla identifikace několika z dříve zaregistrovaných osob s časovým odstupem. Tímto postupem byla testována stálost biometrických vzorků a schopnost uživatelů úspěšně se autentizovat po delším časovém období, kdy systém nebyl používán.

5.1 Možnosti systémů a nastavení pro testování

Kapitola zaměřující se na první praktickou část práce, a to seznámení se se systémy, které byly podrobeny testování. Zaměřuje se především na funkcionalitu aplikací a jejich správné nastavení s ohledem na použité snímací zařízení a prostředí, ve kterém je snímání prováděno. Cílem je osvojení si správných návyků pro používání jednotlivých systémů tak, aby administrátor systému byl následně schopen seznámit se správným používáním systému i budoucí nezasvěcené uživatele. Zkoumány byly vlivy správné i nesprávné prezentace biometrického vzorku snímači, použití různých metod registrace uživatele, vlivy různých nastavení aplikací na výkonnost sytému a vlivy okolního prostředí na kvalitu biometrického vzorku. Na základě zjištěných poznatků bylo odvozeno nastavení systémů pro další testování.

5.1.1 Systémy pro snímání otisků prstů

V první fázi bylo nutné pro všechna zařízení nainstalovat na počítače ovladače a příslušné aplikace pro jejich správu. Následovalo seznámení se s možnostmi aplikací a vyzkoušení si práce s nimi. U systémů pro snímání otisků prstů byly následně zkoumány především vlivy nedodržení doporučené pozice prstu na snímači. Rovněž byly zkoumány vlivy přiložení prstu na snímač za působení různého tlaku a s různou vlhkostí pokožky a možnosti registrace a identifikace různých prstů ruky.

Doporučení pro správnou prezentaci biometrických dat snímači jsou pro jednotlivé systémy uvedena v předchozí kapitole v popisu jednotlivých systémů. Následuje shrnutí doporučení vyplývajících z úvodních testů, které je v podstatě pro všechny systémy založené na snímání otisků prstů shodné.

Prst by měl být na snímač přikládán tak, aby byl zaznamenán co největší počet charakteristických znaků v otisku. Měl by pokrývat co největší plochu snímače a snímána by měla být část prstu kolem jádra otisku. Tedy jádro by mělo být umístěno uprostřed snímaného obrazu a

celý prst uprostřed snímače. Nesprávná pozice (natočení prstu v jakémkoliv směru, umístění prstu příliš k okraji snímače, snímání špičky prstu namísto oblasti kolem jádra otisku) má za následek snížení počtu získaných markant v otisku, a tedy snížení výkonnosti celého systému, především zvýšení chybovosti.

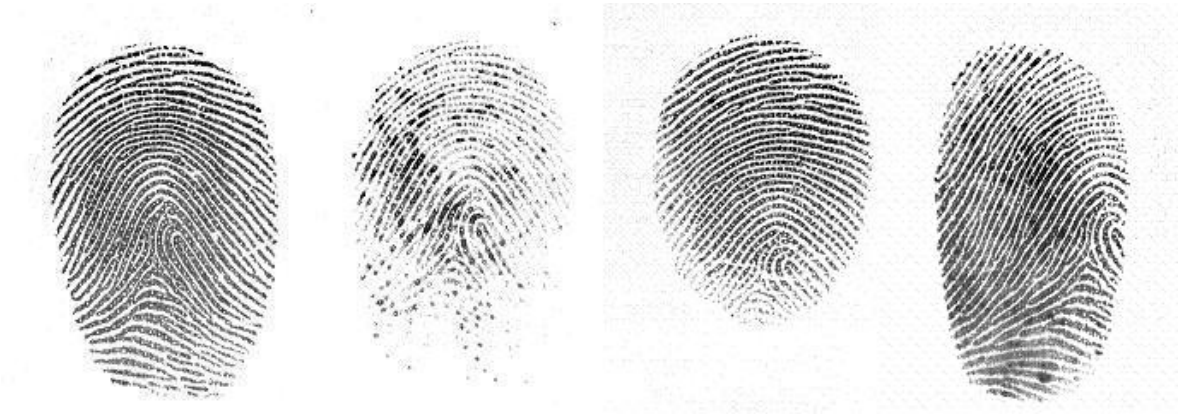
Protože všechna testovaná zařízení disponují snímači, které snímají celý obraz najednou, tedy uživatel pouze přiloží prst na snímač bez jakéhokoliv následného pohybu, celá plocha prstu by měla být na snímač přiložena současně, jinak hrozí nebezpečí, že snímač zachytí pouze část obrazu, která se jako první dostane do kontaktu se snímačem.

Dalšími faktory ovlivňujícím kvalitu snímaného otisku jsou vlhkost pokožky a tlak při prezentaci otisku snímači. Přirozená vlhkost pokožky umožňuje optimální zachycení hřebenů a údolí v otisku. Příliš suché prsty snižují kontrast obrazu, přílišná vlhkost má za následek slévání hřebenů. Tlak při přikládání prstu na snímač by měl být přiměřený. Přílišný nebo naopak nedostatečný tlak má opět za následek sníženou schopnost snímače rozpoznat v otisku dostatečný počet markant.

Správné návyky pro prezentaci otisku prstu biometrickému snímači by měly být budoucímu uživateli vysvětleny před registrací do systému, spolu s možností prakticky si vyzkoušet práci se zařízením se zpětnou vazbou od administrátora nebo odpovědné osoby.

Při registraci je důležité vyžadovat vzorky v co možná nejvyšší kvalitě. Pokud je daný vzorek nekvalitní, měl by být registrační proces proveden znovu. Kvalita registračního vzorku značně ovlivňuje úspěšnost následné autentizace uživatelů. V aplikaci VeriFinger lze požadavky na kvalitu otisku upravit nastavením minimálního počtu nalezených markant v otisku, ostatní aplikace poskytují zpětnou vazbu o dosažené kvalitě. Zároveň by uživatelé měli pamatovat na to, aby prst při identifikaci přikládali pokud možno stejně jako při registraci.

Pro autentizaci pomocí otisků prstů se nejvíce hodí otisky palce nebo ukazováku. Jejich snímání je uživatelsky nejpřívětivější a nejpřirozenější.



Obr. 5.1: Příklady prezentace otisku prstu snímači; zleva: správný otisk, nedostatečná vlhkost pokožky, špatná pozice (špička prstu), špatná pozice (natočení prstu)

5.1.2 Systémy založené na rozpoznávání tváře

Podobně jako v předcházejícím případě bylo prvním krokem seznámení se s aplikací a vyzkoušení si práce s ní v nabízených režimech činnosti. U aplikace VeriLook se jednalo o registraci, registraci s generalizací, verifikaci a identifikaci, a to jak při snímání obrazu pomocí

webové kamery, tak i při nahrávání obrazu ze souboru. Aplikace Luxand umožňuje registraci a identifikaci pouze načtením obrazu ze souboru.

Následně byly zkoumány aspekty mající vliv na celkový výkon systému. Zkoumání se zabývalo různými aspekty, které mohou mít vliv na detekční a identifikační algoritmus. Lze zde zahrnout odchylky natočení hlavy od čelního pohledu, změny výrazu ve tváři, různou vzdálenost uživatele od kamery, nošení brýlí a čepice nebo různé světelné podmínky při snímání tváře.

Úvodní testy potvrdily všechna doporučení pro snímání tváře v rámci technologie rozpoznávání tváře. Tedy tvář by měla být snímána z čelního pohledu. Malé natočení hlavy (cca. do 30° v jakémkoliv směru) sice nevadí, detekční algoritmus tvář v obraze rozpozná, ale identifikace vykazuje nižší míru shody.

Výraz ve tváři by měl být neutrální, obě oči otevřené, pohled směřující přímo do kamery a zavřená ústa. Úsměv se zavřenými ústy nemá na proces identifikace značný vliv, avšak nedoporučuji jej. Nežádoucí jsou otevřená ústa nebo úsměv s otevřenými ústy, zavřené nebo přimhouřené oči, pohled nesměřující do kamery, zvednuté obočí nebo zamračený výraz. Vlasy nebo jiné předměty nesmí zakrývat oči ani jinou část tváře. Stejně tak není přípustné nošení jakékoliv pokrývky hlavy.

V případě, že osoba nosí brýle, je výhodné provést registraci takové osoby jak s brýlemi, tak i bez nich. Výsledkem by mělo být zvýšení pravděpodobnosti úspěšného přijetí, osoba by měla být schopna bezproblémové identifikace s brýlemi i bez nich. Brýle však musí být čiré, aby oči za nimi byly viditelné. Nežádoucí jsou příliš tmavé brýle a brýle s mohutnými obroučkami. Při snímání nesmí obroučky zakrývat oči a na brýlích nesmí být patrné odlesky světla.

Výkon systému může být ovlivněn přirozenými změnami v lidské tváři, například v důsledku stárnutí nebo pokud si uživatel nechá narůst vousy, změní účes, apod.

Osvětlení musí být během snímání rozloženo rovnoměrně, ve tváři by neměly být patrné stíny nebo naopak příliš světlá místa. Pozadí by mělo být co nejjednodušší, nejlépe jednobarevné.

Obr. 5.2: Příklady správné/nesprávné prezentace tváře; nahoře zleva: správné snímání, nesprávná pozice (natočení hlavy v horizontálním směru, naklonění hlavy), nesprávná prezentace vzorku (čepice); dole zleva: nesprávný výraz (úsměv, zavřené oči), nesprávná prezentace vzorku (odlesky na brýlích), nesprávné osvětlení

V případě aplikace **VeriLook** lze dodržování správné prezentace biometriky vynutit úpravou nastavení *Face Confidence Threshold*. Implicitní hodnota je 55. Při této hodnotě vyhovují detekčnímu algoritmu všechny výše uvedené případy správné i nesprávné prezentace tváře. Hodnoty nad 60 již vyžadují striktnější dodržování pravidel, není již detekována tvář s tmavými brýlemi, s nasazenou čepicí, se zavřenýma očima, s odlesky na brýlích nebo pokud pohled

nesměřuje do kamery. Při hodnotách 70 a více je tvář detekována pouze při dodržení všech doporučení (čelní pohled, neutrální výraz, atd.).

Maximální možná vzdálenost, kdy je obličej v obraze detekován lze ovlivnit nastavením *Face Quality Threshold*. Implicitní hodnota je 128 a při této hodnotě je možné snímání zhruba do vzdálenosti 1 metru (závisí také na aktuálních světelných podmínkách a použitém snímacím zařízení). Čím je hodnota vyšší, tím se snižuje možná vzdálenost a zároveň jsou kladeny větší požadavky na správné a dostatečné osvětlení.

Jako ochranu proti podvržení identity předložením tváře z fotografie lze do identifikačního procesu zahrnout testování živosti. Úsilí, které musí uživatel vyvinout při testování živosti lze ovlivnit úpravou hodnoty *Liveness Threshold*. Implicitní nastavení je 50. Při této hodnotě stačí pootočení hlavy při identifikačním procesu, mrkání nebo pootevření úst. Při vyšších hodnotách je třeba kombinovat výše uvedené činnosti. Hodnoty nad 70 již vyžadují nepřirozené aktivity a pro testování nejsou použitelné. Nevýhodou testování živosti je prodloužení identifikačního procesu.

Kvalita registrace je ovlivněna počtem snímků snímaných během registračního procesu (*Enroll Stream Length*). V případě registrace s generalizací navíc počtem vzorků, ze kterých se vytváří registrační vzorek (*Generalization template count*). Vyšší hodnoty umožňují získat registrační vzorek vyšší kvality, ale zároveň se prodlužuje doba registračního procesu, kdy uživatel musí vydržet delší dobu nehybně před kamerou, což může snižovat uživatelskou přívětivost.

Úspěšnost detekce a identifikace obličeje je podobně jako kvalita registrace ovlivněna počtem snímků, které jsou během identifikace snímány (*Matching Stream Length*) a maximálním počtem opakování prohledávání databáze v případě, že během snímání nedojde ke shodě (*Matching Attempts*). Vyšší hodnoty mají za následek zvýšení pravděpodobnosti úspěšného přijetí, ale zároveň také prodloužení identifikačního procesu.

Přínos snímání více snímků, ať již v případě registrace, tak i při identifikaci je patrný při srovnání chybovosti v případě snímání tváře pomocí kamery, kdy se v rámci jednoho procesu registrace/identifikace zpracovává více snímků a při získání obrazu ze souboru, kdy máme k dispozici pouze jeden snímek. Identifikace z obrazového souboru vykazuje vyšší počet nesprávných odmítnutí a obecně nižší hodnoty podobnosti s registračním vzorkem.

5.2 Testování procesu registrace a identifikace osob

Následující kapitola se věnuje hlavní části práce, a to testování systémů na netriviálním počtu osob. Zaměřuje se na chybovost jednotlivých systémů a biometrických technologií, uživatelskou přívětivost a náročnost na administrativu aplikací. Pro účely testování bylo osloveno několik osob, z nichž 42 se testování nakonec zúčastnilo. Testováno bylo celkem 6 systémů, z nichž 4 byly založeny na snímání otisků prstů a 2 využívaly technologii rozpoznávání tváře. V rámci otisků prstů pak 2 čtečky byly založeny na principu kapacitního snímače a zbylé 2 využívaly optický snímač[2]. Testy probíhaly v Laboratoři bezpečnosti a aplikované kryptografie na Fakultě informatiky Masarykovy univerzity a byly rozloženy do několika dní.

V první fázi bylo nutné jednotlivé systémy správně nakonfigurovat. Z předchozích testů vyplynulo, že danému prostředí nejlépe vyhovují implicitní nastavení aplikací. Výchozí nastavení , včetně srovnávacího prahu vyjadřujícího minimální míru shody vzorků pro úspěšnou identifikaci, tedy nebylo měněno.

Každá osoba byla nejprve seznámena s jednotlivými systémy. Následně byl vysvětlen způsob práce se snímacími zařízeními, spolu s praktickou ukázkou správné prezentace biometrických dat

[2] Jednotlivé systémy již byly podrobněji popsány v kapitole 4.

snímači tak, aby byl budoucí uživatel schopen systém sám a správně používat. Po úvodním proškolení prošla každá osoba procesem registrace a několika pokusy o identifikaci na každém z testovaných zařízení.

5.2.1 Otisk prstu

V rámci technologie otisků prstů byly registrovány dva prsty každé osoby, a sice palec a ukazovák pravé ruky. Při registraci bylo dbáno na to, aby byl registrační vzorek dostatečně kvalitní, v opačném případě byla registrace opakována. Autentizace se skládala z pěti pokusů o identifikaci každého zaregistrovaného prstu. Touto cestou bylo testováno nesprávné odmítnutí (FRR). Zároveň byli uživatelé požádáni o předložení jednoho otisku palce a ukazováku levé ruky, za účelem testování nesprávného přijetí (FAR). Počet pokusů o registraci, výsledky identifikace a další poznámky z průběhu testování byly zaznamenávány pro pozdější zpracování. Zároveň u systémů, které umožňovaly uložení obrazu otisku prstu a práci s obrazovými soubory, byly otisky ukládány a využity pro určení chybovosti daného systému při různých nastaveních aplikace, především srovnávacího prahu.

Bioscrypt V-Pass

Čtečka otisků prstů disponující kapacitním snímačem a umožňující práci pouze s „živými“ vzorky, tedy aktuálně sejmutými otisky snímacím zařízením při pokusu o identifikaci. Identifikace byla prováděna pouze pro jedno nastavení srovnávacího prahu, protože aplikace neumožňuje změnit srovnávací práh pokud čtečka pracuje v režimu identifikace.

V rámci **registrace** bylo do databáze uloženo 82 registračních vzorků z 84 možných a pro registraci byly využity oba nabízené režimy – palec byl registrován metodou *Quick Enroll*, ukazovák pak v režimu *Advanced Enroll*. Registrace palce proběhla asi v polovině případů na první pokus, ve většině ostatních případů byly pro dosažení požadované kvality vzorku nutné 2–3 pokusy. Ve dvou případech bylo zapotřebí 5 a více pokusů, otisk jedné osoby nebylo možné do systému zaregistrovat.

Ukazovák byl ve většině případů zaregistrován na první pokus. Výjimkou byly tři případy, kdy bylo nutné registrační proces jednou opakovat a jeden případ, kdy otisk nebylo možné zaregistrovat vůbec. Jednalo se o stejnou osobu jako v případě registrace palce. Snímač v obou případech ani nereagoval na přiložení prstu na snímač. Příčinou neúspěšné registrace byla pravděpodobně manuální práce, při které osoba pracovala s louhem.

Co se týče kvality obrazu otisku (*Quality*), v 80 % případů bylo dosaženo počtu 4 hvězdiček z 5, zbylé vzorky byly akceptovány s počtem 3 hvězdiček. Množství charakteristických znaků v otisku (*Content*) bylo v 95 % případů ohodnoceno plným počtem 5 hvězdiček, ostatní počtem 4 hvězdiček.

Pro registraci bych doporučil využívat režim *Advanced Enroll*, který se skládá ze tří nezávislých snímání otisků prstů. Výhody vidím v tom, že díky většímu počtu snímání lze získat kvalitnější registrační vzorek a zároveň ve většině případů se registrace povede napoprvé. Nevýhodou se může zdát větší časová náročnost registračního procesu, avšak pokud vezmeme v úvahu, že v režimu *Quick Enroll* bylo v mnoha případech nutné registrační proces vícekrát opakovat, pak režim *Advanced Enroll* může být výhodnější i z hlediska časové náročnosti.

Autentizace zahrnovala 5 pokusů o identifikaci každého zaregistrovaného prstu. Celkem tedy testování zahrnovalo 410 pokusů o úspěšnou autentizaci. Nesprávně bylo odmítnuto 11 pokusů o autentizaci palce a 9 autentizačních pokusů s využitím ukazováku.

Následoval test nesprávných přijetí, pro který bylo k dispozici 82 otisků (palec a ukazovák levé ruky každé ze 41 osob). Nesprávně nebyl identifikován ani jeden otisk prstu.

Chybovost systému lze tedy vyjádřit následovně:

$$FAR = \frac{\text{počet nesprávných přijet}}{\text{počet všech pokusů o nesprávné přijet}} \cdot 100 = \frac{0}{82} \cdot 100 = 0\%$$

$$FRR_{celkem} = \frac{\text{počet nesprávných odmítnutí libovolného prstu}}{\text{počet všech pokusů o identifikaci libovolného prstu}} \cdot 100 = \frac{20}{410} \cdot 100 = 4{,}878\%$$

$$FRR_{palec} = \frac{\text{počet nesprávných odmítnutí palce}}{\text{počet všech pokusů o identifikaci palce}} \cdot 100 = \frac{11}{205} \cdot 100 = 5{,}366\%$$

$$FRR_{ukazovák} = \frac{\text{počet nesprávných odmítnutí ukazováku}}{\text{počet všech pokusů o identifikaci ukazováku}} \cdot 100 = \frac{9}{205} \cdot 100 = 4{,}390\%$$

$$FTE = \frac{\text{počet neúspěšných registrací}}{\text{počet všech otisků pokoušejících se o registraci}} \cdot 100 = \frac{2}{84} \cdot 100 = 2{,}381\%$$

$$FTA = \frac{\text{počet neúspěšných prezentovaných otisků snímačem}}{\text{počet všech prezentovaných otisků}} \cdot 100 = \frac{0}{410 + 82} \cdot 100 = 0\%$$

Z výsledků vyplývá, že pro tento systém je rozdíl mezi mírou nesprávných odmítnutí palce a ukazováku minimální. Může být způsoben rozdílným způsobem registrace, popsaným výše. Roli může hrát také to, že otisk ukazováku byl pro uživatele snadněji prezentovatelný snímači ve správné poloze, zatímco otisk palce, vzhledem k jeho velikosti, poskytoval značnou variabilitu přiložení prstu na relativně malou plochu snímače. Zároveň velikost palce neumožňovala využit pro správnou pozici prstu pomocnou zarážku (*Ridge-Lock*) a musela být prováděna korekce vzhledem k tomu, aby byla snímána oblast kolem jádra otisku.

Nulové FAR při FRR kolem 5 % značí dostatečně spolehlivý a použitelný systém pro použití v aplikacích řízení přístupu nebo kontroly docházky, pro které je určen. Problémem může být nemožnost registrace některých osob, například z důvodu manuální práce, kterou by bylo třeba řešit jinou autentizační metodou.

V průběhu celého měření bylo třeba několikrát očistit povrch snímače, na kterém zůstával latentní otisk.

Na základě výše uvedeného bych pro tento systém doporučil využívat otisk ukazováku.

APC Biopod

Čtečka otisků prstů s kapacitním snímačem, využitelná především jako náhrada hesel v počítačových aplikacích. Podobně jako čtečka Bioscrypt umožňuje pouze práci s „živými“ otisky. Srovnávací práh v aplikaci nastavovat nelze.

Do systému bylo zaregistrováno 60 otisků prstů od 31 osob. Otisk palce a ukazováku jedné osoby nebylo možné do systému zaregistrovat, v získaném obrazu nebyla aplikace schopna nalézt markanty. Jednalo se o stejného uživatele jako v případě čtečky Bioscrypt.

Pro testování míry nesprávných odmítnutí uživatelů bylo provedeno 285 pokusů o autentizaci (29 × 5 palců + 28 × 5 ukazováků). Nesprávně bylo odmítnuto 12 otisků palce a 8 otisků ukazováku. 15 pokusů o autentizaci (5 palců a 10 ukazováků) nebylo možné provést z důvodu „pádu“ aplikace vždy při prezentaci biometrických dat snímači. Tyto případy byly klasifikovány

jako neúspěšně prezentované otisky snímači a zahrnuty do FTA. Pravděpodobnou příčinou je skutečnost, že aplikace je navržena pro maximálně 20 uživatelských účtů. Právě při dosažení tohoto počtu začala aplikace vykazovat nestabilitu.

Pro test nesprávných přijetí byly opět k dispozici 2 vzorky od každé osoby. Celkem 56 vzorků ze 60, 4 vzorky nebylo možné získat a byly rovněž započítány do FTA.

Z důvodu výměny počítačů v laboratoři během testování a nutnosti opětovné instalace aplikace, bylo posledních 11 osob registrováno a autentizováno v rámci nové databáze, nicméně výsledky byly vyhodnocovány souhrnně.

Výsledky testů jsou následující:

$$FAR = 0\%$$
$$FRR_{celkem} = 7{,}018\%$$
$$FRR_{palec} = 8{,}276\%$$
$$FRR_{ukazovák} = 5{,}714\%$$
$$FTE = 3{,}226\%$$
$$FTA = 5{,}278\%$$

Rozdíl mezi mírou nesprávných přijetí palce a ukazováku je vetší než v předchozím případě. Příčinou je malá plocha snímače, která v kombinaci s relativně velkou plochou palce dává uživateli prostor pro značně variabilní přiložení prstu na snímač. Výkon systému je tak degradován, protože různá měření mohou snímat různé části otisku prstu.

Celkově, ačkoliv se jedná o stejnou technologii, je chybovost větší než v případě čtečky Bioscrypt. Je to dáno výše zmíněnou malou plochou snímače, která je schopna snímat jen malou část otisku. Vyšší míra nesprávných odmítnutí může vést k nespokojenosti uživatelů. Pozitivem je nulový počet nesprávných přijetí a menší náchylnost ke znečištění senzoru ve srovnání s předchozím snímačem.

Cross Match Verifier 300 LC 2.0

Čtečka pracující na principu optického snímání otisků prstů. Aplikace VeriFinger umožňuje jak práci s „živými“ otisky, tak i s obrazovými soubory otisků prstů. Všechny obrazy otisků, jak registračních, tak i identifikačních, byly ukládány a následně využity pro testování chybovosti systému při různých hodnotách srovnávacího prahu.

Databáze registračních vzorků čítala opět vzorky palce a ukazováku pravé ruky 42 osob. Nebyl zaznamenán žádný případ, kdy by uživatele nebylo možné do systému zaregistrovat. **Registrace** probíhala ve dvou režimech. Prvním byla standardní registrace, kdy bylo prováděno jedno snímání otisku prstu, druhým pak registrace s generalizací, při kterém byly prováděny tři snímání stejného otisku a kolekce získaných charakteristických znaků byla algoritmicky zpracována a použita pro vytvoření registračního vzorku. Databáze tedy ve výsledku obsahovala celkem 168 vzorků, rozdílných však bylo 84 (palec a ukazovák každé osoby). Cílem využití obou režimů bylo jejich vzájemné porovnání s ohledem na kvalitu výsledného registračního vzorku a její vliv na chybovost systému.

Proces registrace se ukázal být náročnější než u ostatních systémů, a to v obou režimech. Při klasické registraci (pouze jeden otisk) byly ve většině případů nutné 2–4 pokusy, než byl získán vzorek dostatečné kvality. Jeden pokus stačil asi ve 25 % případů, výjimečně se vyskytly i hodnoty

přesahující 5 pokusů. Ještě větší nároky na uživatele by měl klást proces registrace s generalizací, kde je zapotřebí tří otisků prstů ve vysoké kvalitě. Paradoxně však v 50 % případů stačil k úspěšné registraci jeden pokus. Ve zbylých případech byly nutné 2–4 pokusy.

Problémy s kvalitou otisku byly z velké části zapříčiněny nedostatečnou vlhkostí pokožky, uživatelé měli často tendenci prsty před snímáním otisku utírat. Druhým, avšak méně častým problémem, byl nesprávný způsob přikládání prstu na snímač, kdy uživatelé nepokládali prst na snímač celou plochou současně, ale postupně směrem od prvního kloubu ke špičce. Často byl zachycen neúplný obraz.

Velikost palce již nehrála takovou roli jako u předchozích zařízení, snímač byl dostatečně velký na to, aby zachytil celou plochu palce. Přesto u některých osob, s dlouhými prsty, nebylo možné dosáhnout toho, aby se jádro otisku nacházelo uprostřed obrazu. Jádro tak bylo situováno v dolní části snímače, na úkor snímání informačně méně bohaté oblasti v okolí špičky prstu.

Pokud srovnám oba režimy registrace, tak pro klasickou registraci hovoří menší časová náročnost a větší uživatelská přívětivost (při nekvalitním vzorku stačí opakovat pouze jedno snímání). Na druhou stranu, registrace s generalizací by měla produkovat kvalitnější registrační vzorky a snížit tak chybovost systému, ovšem na úkor složitějšího registračního procesu. Otázkou zůstává, zda rozdíl v kvalitě registračních vzorků je opravdu takový, aby se vyplatilo registraci s generalizací používat?

Pro účely **autentizace** bylo sejmuto a uloženo celkem 416 obrazů otisků prstů pro testování míry nesprávných přijetí, z nichž bylo 209 otisků palce a 207 otisků ukazováku. Obrazové soubory 4 otisků nebyly správně uloženy, proto nebyly ani zahrnuty do testování. Pro testování míry nesprávných přijetí bylo získáno dalších 84 otisků. Aplikace VeriFinger umožňuje ve výsledcích identifikace zobrazit všechny registrační záznamy, jejichž míra shody s prezentovaným vzorkem je vyšší než prahová hodnota a jsou tak systémem považovány za shodné. Toho lze s výhodou využít při testování míry nesprávných přijetí, protože do testů tak můžeme zahrnout i vzorky původně určené pro testování míry nesprávných odmítnutí. Celkem tak máme k dispozici 416 + 84 otisků.

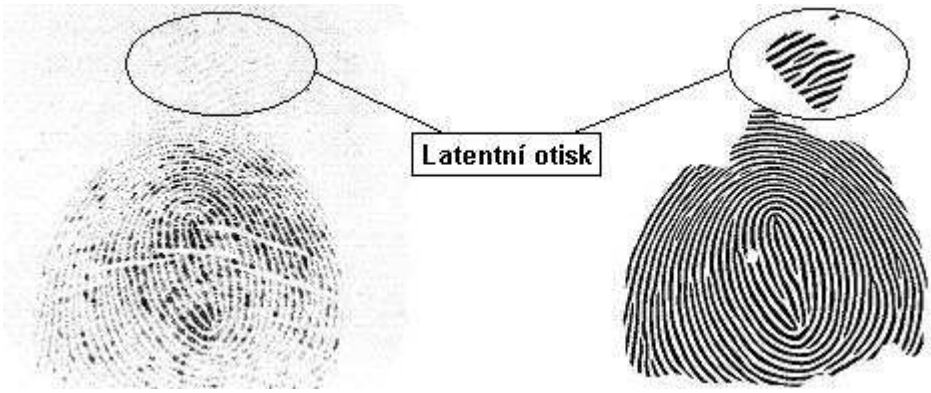
Snímání otisků prostřednictvím čtečky bylo prováděno při výchozí prahové hodnotě, která činí 48 (minimální míra podobnosti, kdy jsou dva vzorky považovány za shodné). Tomuto nastavení odpovídají následující hodnoty chybovosti:

$$FRR = 0\%$$
$$FAR_{klasická\_reg.} = 0\%$$
$$FAR_{gen.,celkem} = 0{,}200\%$$
$$FAR_{gen,palec} = 0\%$$
$$FAR_{gen,ukazovák} = 0{,}402\%$$
$$FTE = 0\%$$
$$FTA = 0\%$$

Výsledky ukazují, že systém při daném nastavení nevykazoval ani jeden případ nesprávného odmítnutí, což platí jak pro klasickou registraci, tak pro registraci s generalizací. Během testování se vyskytnul jeden případ nesprávného přijetí, kdy vzorek ukazováku byl nesprávně identifikován jako shodný s jedním s registračních vzorků pořízených registrací s generalizací. Celkové FAR vyjadřuje míru nesprávných přijetí v případě, kdy nerozlišujeme mezi palcem a ukazovákem. FAR palce, resp. ukazováku vyjadřuje FAR v případě, kdy srovnáváme chybovost jednotlivých prstů.

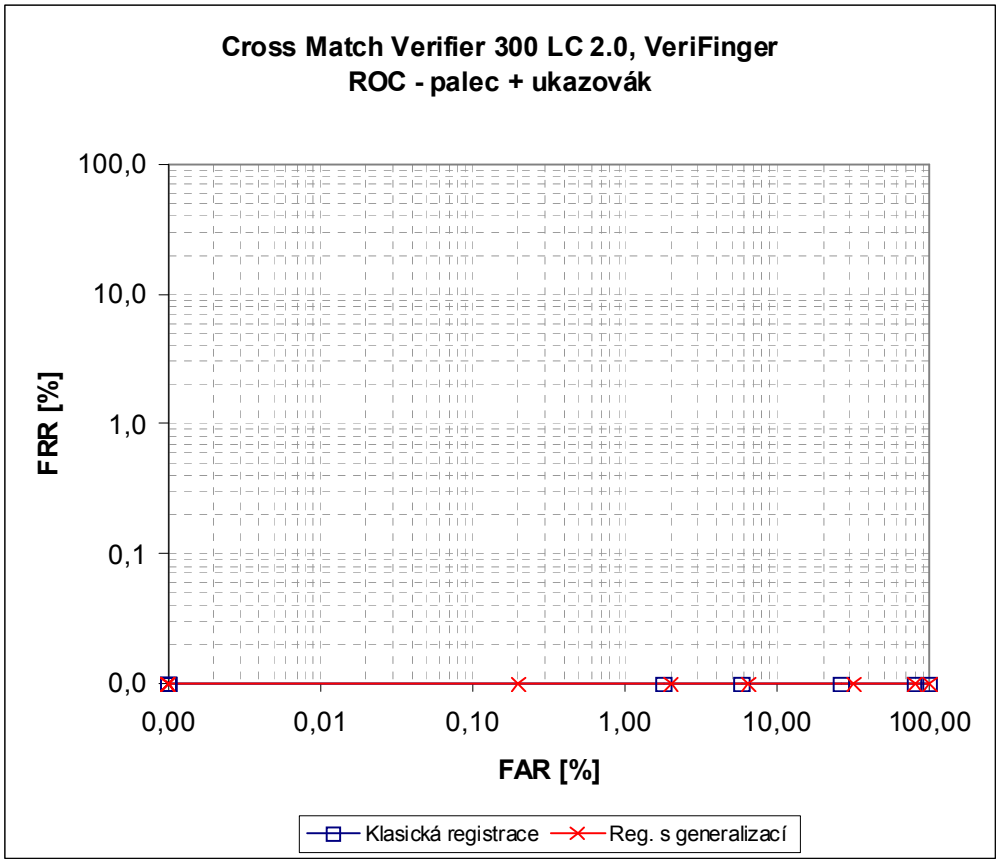
V případě klasické registrace k nesprávnému přijetí nedošlo. Rovněž nebyl zaznamenán žádný případ neúspěšné registrace (FTE), ani neúspěšné prezentace biometriky snímači (FTA).

Během testování bylo nutné průběžně čistit povrch snímače, protože se na něm usazovaly nečistoty v podobě latentního otisku (viz. Obr. 5.3).



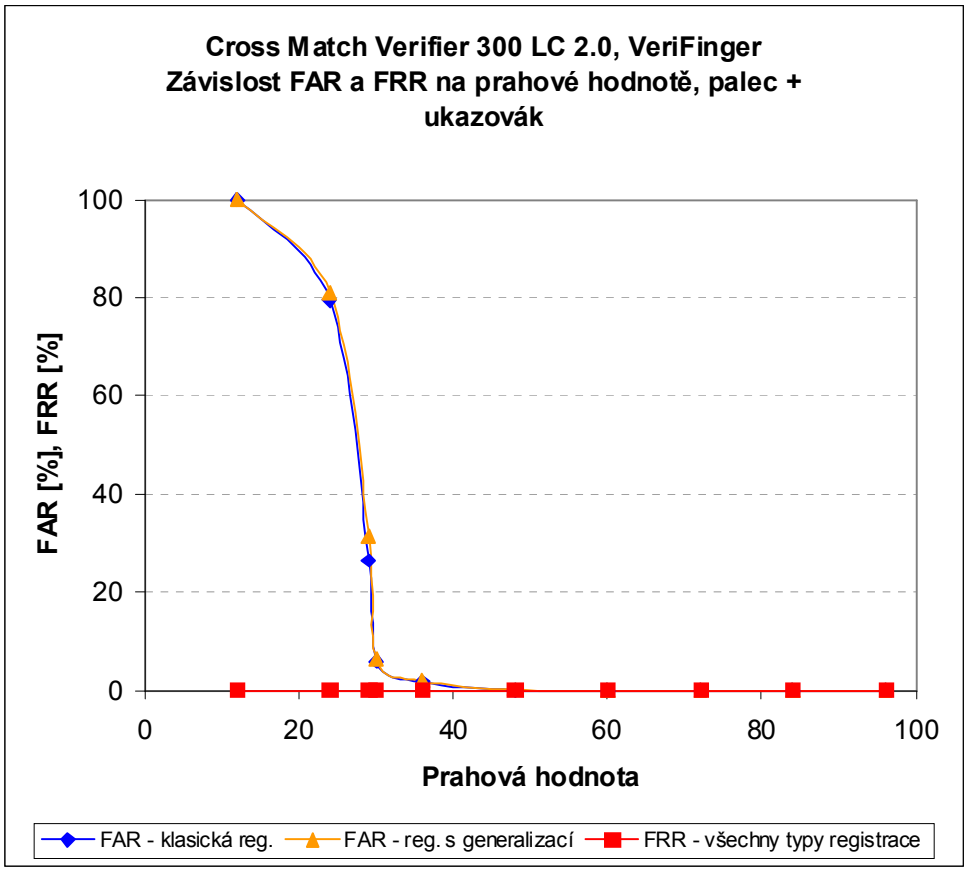
Obr. 5.3: Latentní otisk; vlevo – obraz sejmutý snímačem, vpravo – obraz zpracovaný aplikací VeriFinger

S využitím získaných snímků otisků prstů byl následně proces identifikace opakován pro různá nastavení srovnávacího prahu. Měření bylo provedeno pro všechna nastavení, která aplikace VeriFinger podporovala (viz. Tab. 4.5). Získané výsledky byly zpracovány do grafů vyjadřujících závislost FAR a FRR na prahové hodnotě a byly vytvořeny operační charakteristiky (ROC křivky) systému vyjadřující závislost mezi FAR a FRR. Vše pro různé režimy registrace i pro jednotlivé prsty za účelem srovnání.



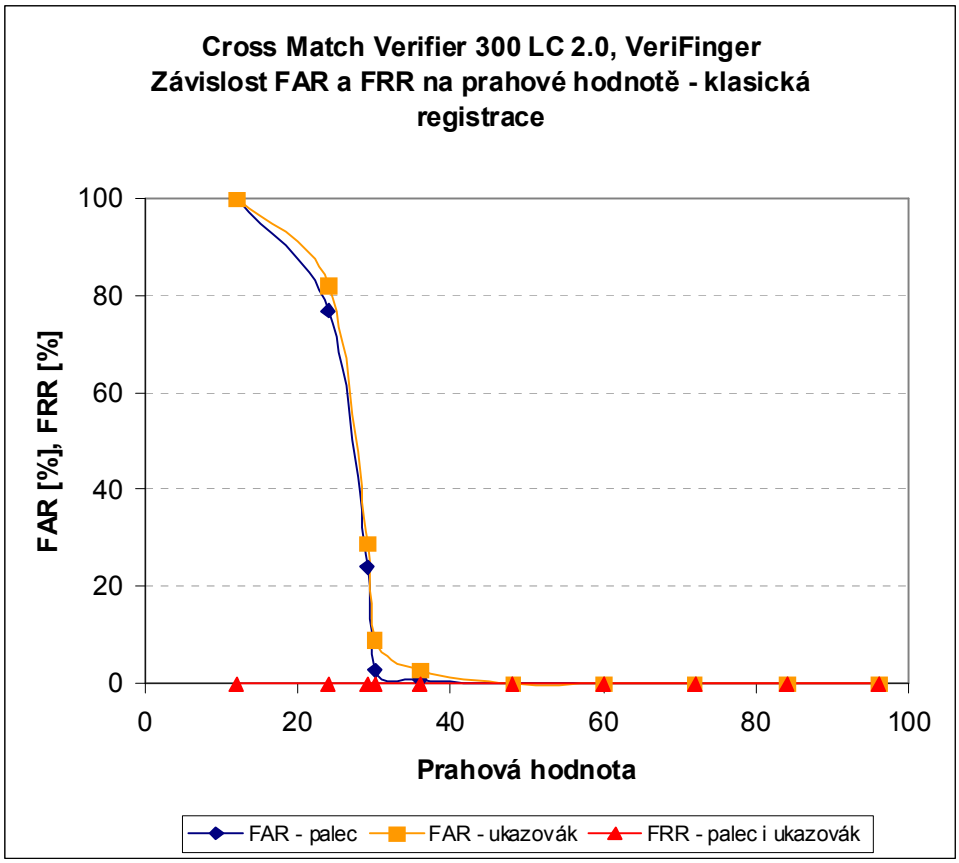
Graf 5.1: ROC – srovnání registračních režimů

Z grafu 5.1 je patrné, že míra nesprávných odmítnutí (FRR) obou prstů je nulová pro všechny hodnoty srovnávacího prahu, a to jak v případě klasické registrace, tak i při registraci s generalizací. Míra nesprávných přijetí (FAR) u obou registračních metod roste se snižujícím se srovnávacím prahem. Protože křivka prochází bodem [0; 0], lze pro určitou prahovou hodnotu dosáhnout nulové chybovosti a jedná se tak z hlediska bezpečnosti o ideální systém. Nulovou chybovost systém vykazoval pro prahovou hodnotu 60 a vyšší. Závislost FAR a FRR na hodnotě srovnávacího prahu je znázorněna v grafech 5.2 a 5.3.



Graf 5.2: Srovnání závislost FAR a FRR na prahové hodnotě pro různé metody registrace

Graf 5.2 vypovídá o tom, že hodnoty FAR jsou pro obě metody registrace téměř shodné. Z hlediska chybovosti jsou registrační metody za daných podmínek, při kterých testování probíhalo, srovnatelné. Nepotvrdil se tedy předpoklad, že proces registrace s generalizací produkuje registrační vzorky vyšší kvality a snižuje tak chybovost systému. Jako kritérium pro výběr jedné z metod bych za daných okolností vzal v úvahu časovou náročnost, uživatelskou přívětivost a komplikovanost celého procesu. Z tohoto pohledu se jeví jako přijatelnější klasická registrace.



Graf 5.3: Srovnání závislost FAR a FRR na prahové hodnotě pro různé prsty

Graf 5.3 znázorňuje srovnání chybovosti v rámci jednotlivých prstů. Ačkoliv rozdíly v hodnotách FAR nejsou nijak markantní, vyšší míru nesprávných přijetí produkují otisky ukazováku. Rozdíly jsou však pouze v jednotkách procent, nedá se tedy říct, že ukazovák by byl ve srovnání s palcem nepoužitelný. Příčinu rozdílu v chybovosti bych přisoudil počtu markant v otisku prstu, kdy palec je obecně považován za informačně bohatší ve srovnání s ostatními prsty, což se projevuje i v obtížnějším dosažení pro systém dostatečné podobnosti s jiným otiskem.

Nulové FRR ve všech případech navíc dokazuje, že systém je schopen identifikovat při registraci dostatečné množství charakteristické informace, takže oprávněný uživatel je při následné identifikaci vždy správně rozpoznán.

Graf 5.3 znázorňuje chybovost jednotlivých prstů při klasické registraci. Stejných výsledků bylo dosaženo i při registraci s generalizací.

Hodnota EER byla stanovena na 0 %, což jen dokazuje vysokou spolehlivost systému.

Další grafy a tabulky se všemi zjištěnými údaji jsou k dispozici v příloze A.

Microsoft Fingerprint Reader

Stejně jako čtečka Cross Match i čtečka Microsoft využívá ke snímání otisků prstů optický snímač. Ke snímání otisků byla využita aplikace **GrFinger**, která umožňuje jak práci s živými otisky, tak i uložení obrazu otisku prstu a práci s obrazovými soubory. Proto i zde byly všechny sejmuté otisky ukládány pro účely testování chybovosti při různých prahových hodnotách.

Do databáze bylo zaregistrováno celkem 84 otisků od 42 osob, otisky všech osob se podařilo úspěšně zaregistrovat. **Registrace** proběhla zhruba v 50 % případů na první pokus, u většiny zbylých případů bylo nutné registrační proces 2–3krát opakovat. V pěti případech bylo nutné pro úspěšnou registraci provést 8 a více pokusů, protože se nedařilo získat vzorek vysoké kvality. Kritériem pro hodnocení kvality otisku byla informace o kvalitě poskytovaná samotnou aplikací po zpracování získaného otisku. Kvalita byla hodnocena jedním ze tří stupňů – vysoká, střední a špatná. Úspěšná registrace byla podmíněna získáním vzorku vysoké kvality. Ve čtyřech případech z 5, kdy bylo nutné proces registrace opakovat více než osmkrát, byly nakonec přijaty vzorky střední kvality.

Proces registrace nebyl uživatelsky příliš náročný a klasifikoval bych jej jako vůbec nejjednodušší a časově nejméně náročný ve srovnání s ostatními systémy. Co se týče palce a problémům s jeho velikostí, u této čtečky byla také v některých případech nutná korekce umístění prstu na snímač. Důvodem byla zejména menší šířka povrchu snímače, která v kombinaci s nevhodným natočením prstu způsobovala, že jádro otisku se nacházelo příliš u okraje snímané oblasti.

Následná **autentizace** zahrnovala 5 pokusů o úspěšnou identifikaci každého zaregistrovaného prstu. Pro testování FRR tak bylo sejmuto a uloženo 420 otisků. FAR bylo zjišťováno na základě prezentace dvou otisků, které nebyly v systému zaregistrovány. Od 42 osob tak bylo využito 84 otisků.

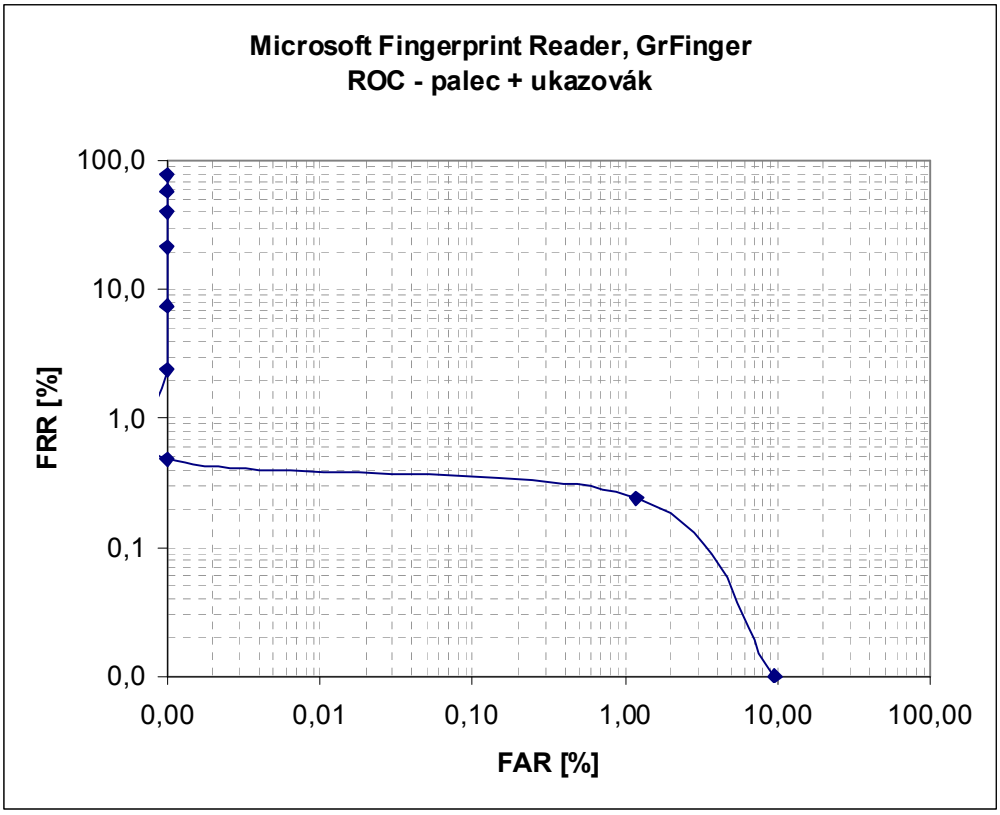
Snímání otisků bylo prováděno při výchozí prahové hodnotě, která činila 45. Pro toto nastavení byly zjištěny následující výsledky:

$$FAR = 0\%$$
$$FRR_{celkem} = 2{,}410\%$$
$$FRR_{palec} = 1{,}914\%$$
$$FRR_{ukazovák} = 2{,}913\%$$
$$FTE = 0\%$$
$$FTA = 0{,}992\%$$

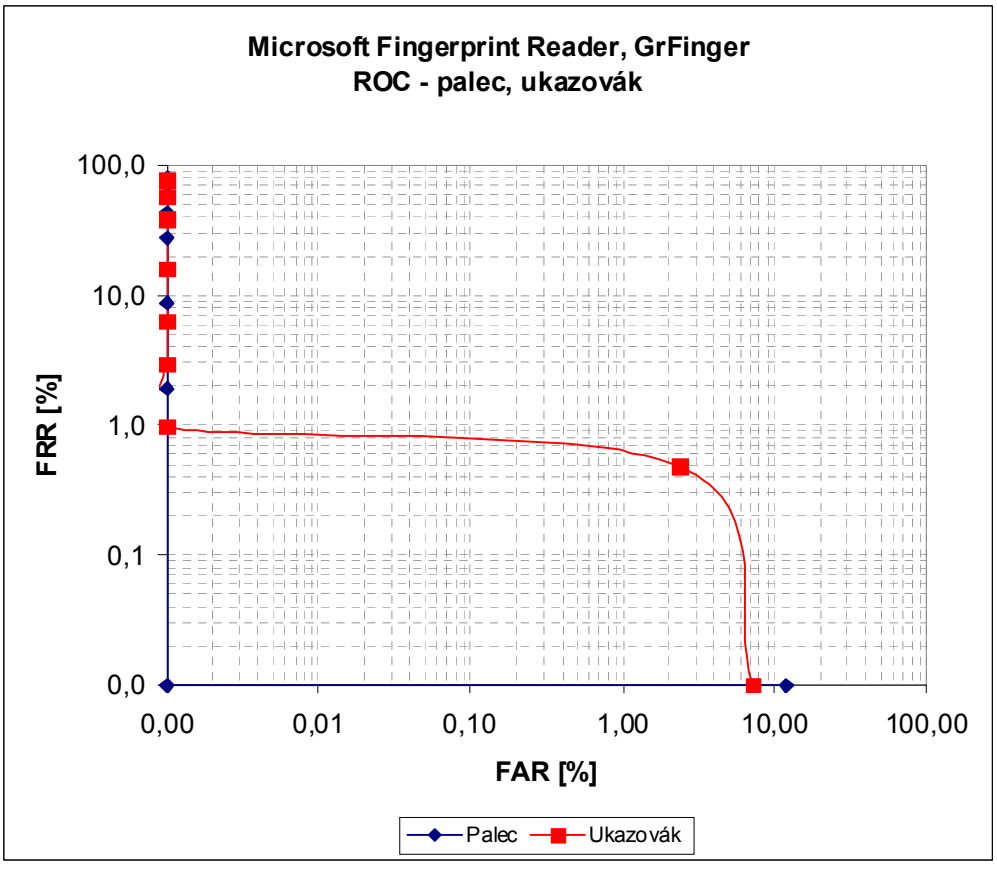
Z výsledků je patrné, že systém při dané prahové hodnotě nevykazoval žádný případ nesprávného přijetí. Pokud nerozlišujeme mezi jednotlivými prsty, bylo zaznamenáno 10 případů nesprávného odmítnutí. 4 případy se pak týkaly identifikace palce a 6 případů ukazováku. 5 otisků (1 palec (FTA = 0,397 %) a 4 ukazováky (FTA = 1,587 %)) aplikace nebyla schopna správně zpracovat a tyto byly zahrnuty do FTA. Registrace ve všech případech proběhla úspěšně, což vyplývá z nulové hodnoty FTE.

S latentním otiskem nebyly v průběhu snímání žádné problémy, což je velká výhoda tohoto systému oproti ostatním testovaným systémům, kdy bylo nutné pravidelně povrch snímače čistit.

Získané otisky byly dále využity pro testování chybovosti při různých prahových hodnotách. Hodnota byla nastavována v rozmezí 10–180.



Graf 5.4: ROC; aplikace GrFinger

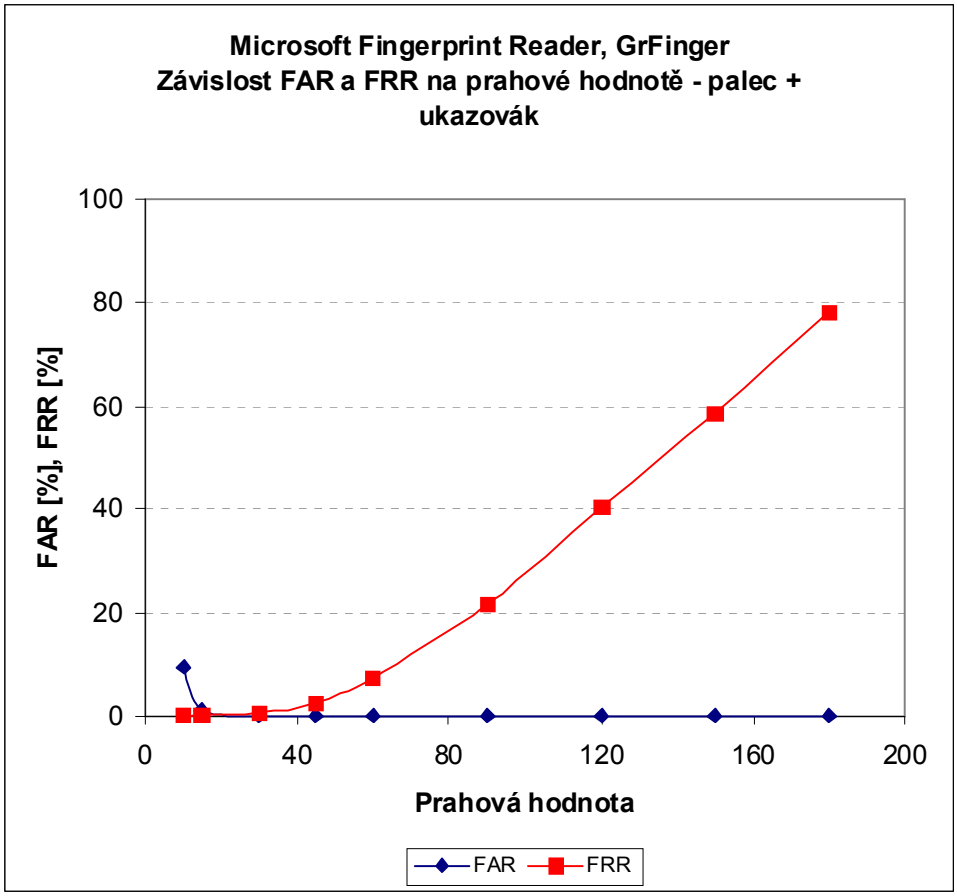


Graf 5.5: Srovnání ROC pro různé prsty; aplikace GrFinger

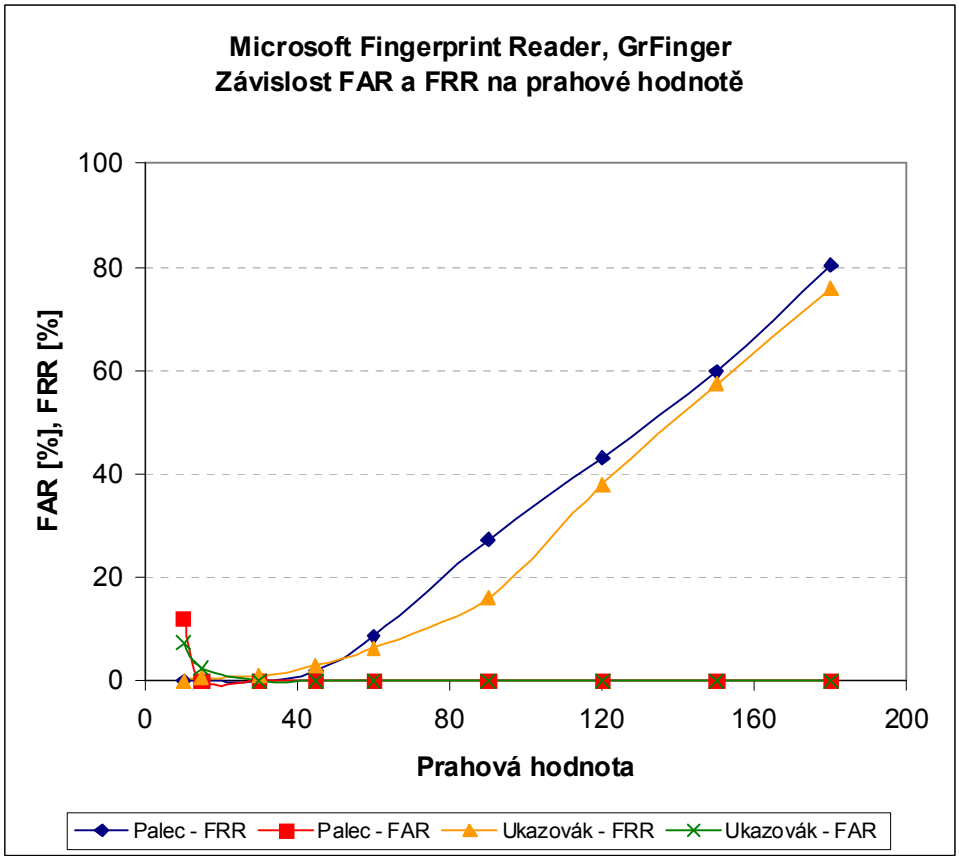
Grafy 5.4 a 5.5 znázorňují závislosti mezi FAR a FRR při různých prahových hodnotách. Graf 5.4 vyjadřuje tuto závislost pro případ, kdy nerozlišujeme mezi jednotlivými prsty. Lze vidět, že při

FRR přibližně 0,5 % a vyšším systém vykazuje nulové FAR. Při FAR asi 10 % lze naopak dosáhnout nulové FRR.

Graf 5.5 představuje porovnání jednotlivých prstů. Z grafu 5.5 vyplývá, že v případě palce je systém spolehlivější než v případě ukazováku. ROC křivka pro palec prochází bodem o souřadnicích [0; 0], což znamená, že pro určitou prahovou hodnotu lze dosáhnout nulové chybovosti systému. Konkrétně se jednalo o prahové hodnoty v rozmezí 15–30.



Graf 5.6 Závislost FAR a FRR na prahové hodnotě v aplikaci GrFinger



Graf 5.7: Srovnání závislosti FAR a FRR na prahové hodnotě pro jednotlivé prsty; aplikace GrFinger

Graf 5.6 znázorňuje závislost FAR a FRR na prahové hodnotě opět v případě, kdy nerozlišujeme mezi jednotlivými prsty. Vidíme, že FRR postupně roste se zvyšující se prahovou hodnotou až k hodnotě 80 %, zatímco FAR se i při velmi nízkých prahových hodnotách pohybuje na hranici maximálně 10 % a při prahových hodnotách 30 a vyšších je již nulová. Hodnota EER systému byla stanovena na přibližně 0,33 %, což značí dostatečně kvalitní systém, zejména pro oblast nasazení, pro kterou je čtečka primárně určena, a kterou je autentizace v počítačových aplikacích, zejména v domácím prostředí.

V grafu 5.7 je zachyceno srovnání chybovosti jednotlivých prstů. Z měření vyplývá, že FRR pro palec je při nižších prahových hodnotách nižší než v případě ukazováku. To platí do prahové hodnoty 45, dále palec vykazuje vyšší FRR než je tomu u ukazováku, což je vidět i v grafu 5.7. Rozdíly se vždy pohybují v řádu jednotek procent. Vyšší FRR palce při vyšších prahových hodnotách přisuzuji větší ploše palce a variabilitě umístění palce na snímač, kdy může být snímána vždy trochu jiná oblast prstu, což ve výsledku produkuje nižší míru podobnosti s registračním vzorkem. FAR je u palce od prahové hodnoty 15 nulové, v případě ukazováku je nulové od hodnoty 30.

EER bylo v případě palce stanoveno na 0 %, u ukazováku pak na 0,66 %.

Jelikož aplikace GrFinger ve výsledcích identifikace zobrazuje pouze záznam s nejvyšší mírou podobnosti, nebylo možné využít pro testování FAR všech získaných vzorků, jako tomu bylo v případě aplikace VeriFinger využité pro čtečku Cross Match, ale pouze dva vzorky od každé

osoby, které byly k tomuto účelu získány. Pro relevantní srovnání čtečky Cross Match a Microsoft byly tedy otisky získané prostřednictvím čtečky Microsoft zpracovány i v aplikaci **VeriFinger**.

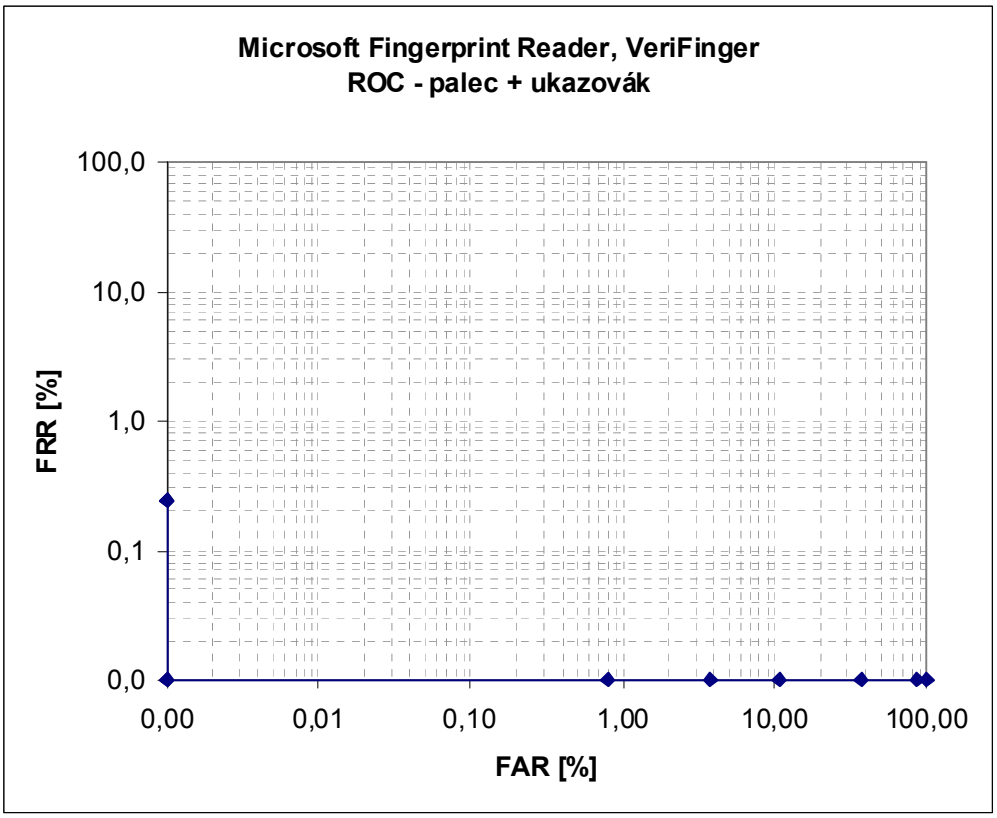
Registrace i následné autentizační pokusy byly prováděny pouze s využitím obrazových souborů otisků prstů, získaných prostřednictvím aplikace GrFinger. Registrace s generalizací prováděna nebyla, protože k tomuto účelu nebyly získány obrazové soubory.

Pro výchozí prahovou hodnotu byly zjištěny následující hodnoty chybovosti:

$$FRR = 0\%$$
$$FAR_{celkem} = 0{,}802\%$$
$$FAR_{palec} = 0\%$$
$$FAR_{ukazovák} = 1{,}619\%$$
$$FTE = 0\%$$
$$FTA = 0{,}992\%$$

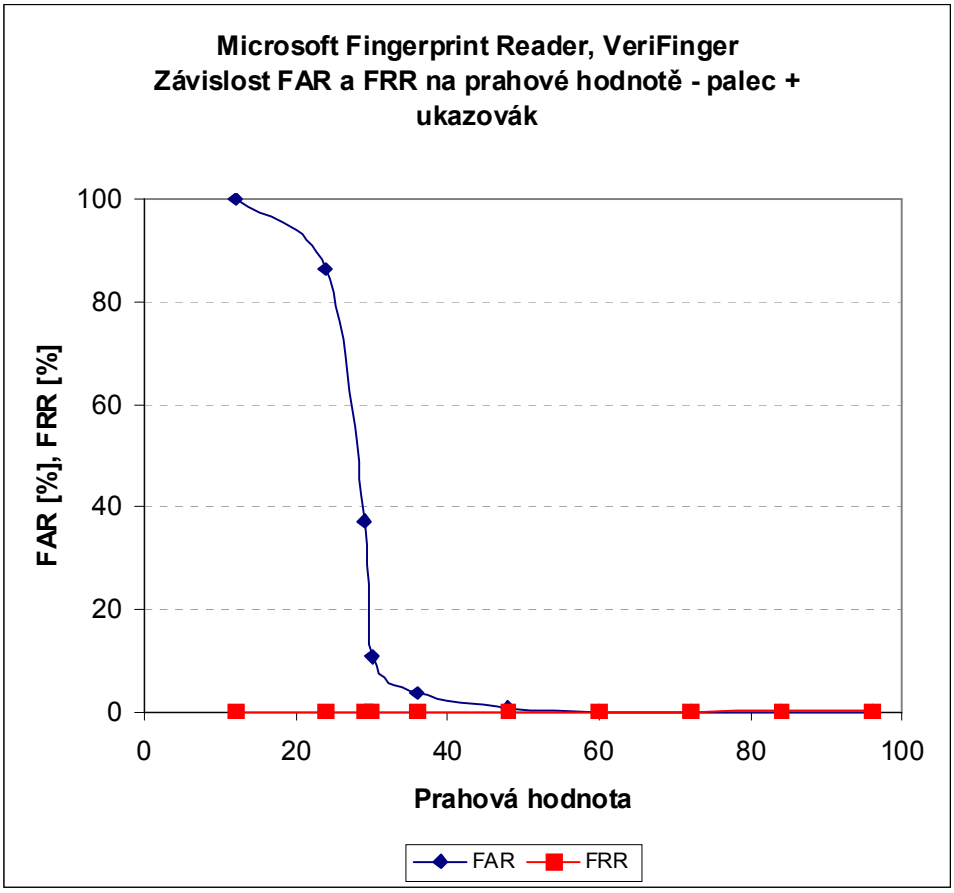
Pro danou prahovou hodnotu nebyl zaznamenán žádný případ nesprávného odmítnutí. Naopak byly zaznamenány 4 případy nesprávného přijetí, všechny se navíc týkaly pouze ukazováku. Všechny otisky se podařilo bez problémů zaregistrovat, což dokazuje nulové FTE. 5 vzorků aplikace nedokázala správně zpracovat, což se odráží v téměř 1 % FTA. Všechny tyto vzorky navíc pocházely ze stejného prstu jedné osoby a nejednalo se o stejné vzorky jako v případě aplikace GrFinger.

Různé hodnoty chybovosti dokazují různé metody zpracování otisků prstů různými aplikacemi. Rozdíly v FAR jsou navíc dány počtem otisků, které byly k tomuto účelu využity (pouhých 84 otisků v aplikaci GrFinger, zatímco v aplikaci VeriFinger bylo využito 84 + 415 otisků)



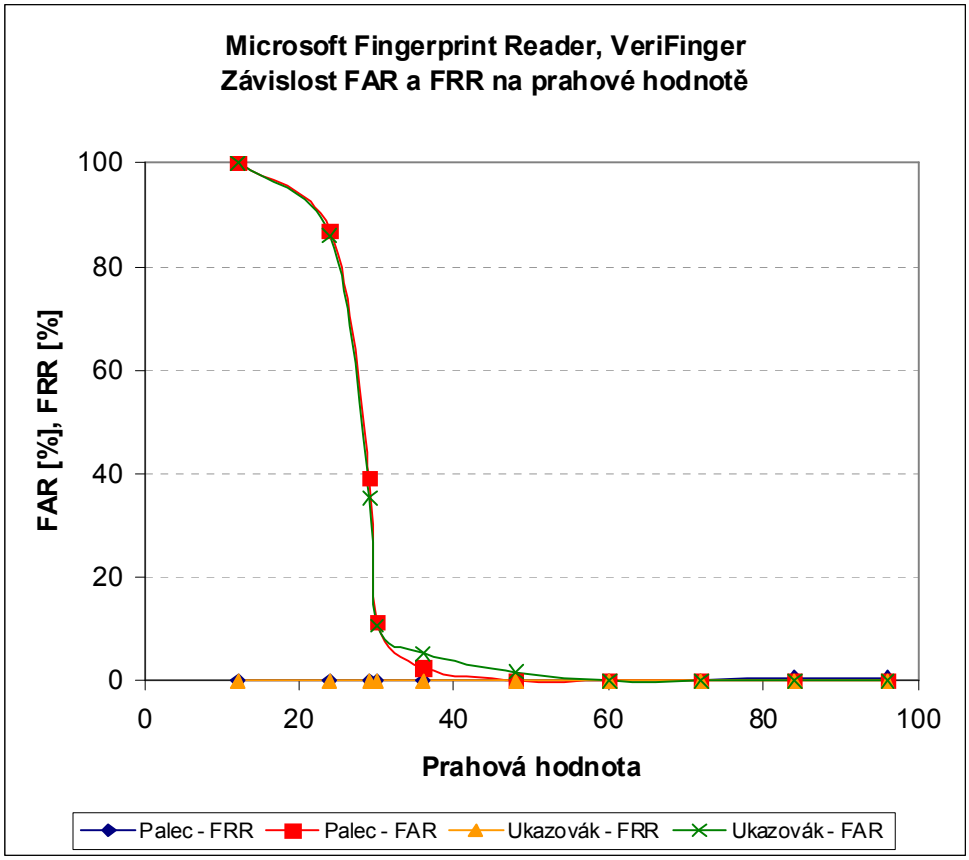
Graf 5.8: ROC; aplikace VeriFinger

ROC křivka pro aplikaci VeriFinger (graf 5.8) ukazuje, že ačkoliv byly pro měření využity stejné otisky prstů, v aplikaci VeriFinger bylo dosaženo lepších výsledků než tomu bylo při použití aplikace GrFinger. Křivka opět prochází bodem o souřadnicích [0; 0], což umožňuje dosáhnout nulové chybovosti při určité prahové hodnotě. Nulová chybovost byla dosažena pro prahové hodnoty v rozmezí 60–84.



Graf 5.9: Závislost FAR a FRR na prahové hodnotě pro aplikaci VeriFinger

Graf závislosti FAR a FRR na prahové hodnotě vyjadřuje nulovou míru nesprávných odmítnutí pro jakoukoliv prahovou hodnotu. FAR pro velmi nízkou prahovou hodnotu dosahuje i 100 %, ale se zvyšující se prahovou hodnotou klesá a pro hodnoty 60 a výše je již nulová.



Graf 5.10: Srovnání závislosti FAR a FRR na prahové hodnotě pro různé prsty; aplikace VeriFinger

Srovnání chybovosti pro autentizaci pomocí otisku palce a ukazováku odhalilo, že rozdíly jsou v aplikaci VeriFinger minimální. Během celého měření byl zaznamenán pouze jeden případ nesprávného odmítnutí, jednalo se o jeden z otisků palce a při prahové hodnotě 84 a vyšší. Co se týče FAR, rozdíly mezi palcem a ukazovákem byly maximálně asi 3 %.

Hodnota EER byla při zpracování otisků aplikací VeriFinger nulová.

Pokud bych měl zhodnotit obě aplikace, tak z hlediska míry nesprávných odmítnutí je aplikace VeriFinger jednoznačně spolehlivější, protože FRR je nulová, resp. téměř nulová pro všechny prahové hodnoty. Aplikace VeriFinger tak dokáže s větší pravděpodobností správně rozpoznat identitu osoby. Z hlediska FAR vykazuje při nízkých prahových hodnotách lepší výsledky aplikace GrFinger s nižším počtem nesprávných přijetí. Pokud však prahovou hodnotu zvyšujeme, FAR klesá a od výchozí prahové hodnoty aplikací je v obou případech téměř shodná. Srovnání z hlediska míry nesprávných přijetí není příliš objektivní, jelikož byly pro její výpočet použity rozdílné množiny otisků. Pokud bychom však provedli srovnání na stejné množině otisků, výsledky by dopadly téměř shodně jako je popsáno výše. Srovnání na základě ROC křivek vychází také nepatrně lépe pro aplikaci VeriFinger, kde lze pro určitou prahovou hodnotu dosáhnout nulové chybovosti systému. Aplikace GrFinger však v tomto ohledu dosahuje také velice dobrých výsledků, kdy při FRR kolem 0,5 % dosahuje nulové hodnoty FAR. Dobré výsledky obou aplikací dokazuje také hodnota EER dosahující 0 % v aplikaci VeriFinger a 0,33 % v aplikaci GrFinger.

Další grafy a tabulky se všemi zjištěnými údaji v obou aplikacích jsou k dispozici v příloze A.

5.2.2 Rozpoznávání tváře

U technologie rozpoznávání tváře registrace obnášela prezentaci biometriky aplikaci prostřednictvím webové kamery. Podobně jako v případě otisků prstů bylo vyžadováno dodržení všech doporučení (pozice, výraz, atd.). Pokud osoba nosí brýle, byla provedena registrace s brýlemi i bez nich. Zaregistrovaná osoba poté absolvovala pět pokusů o identifikaci. Všechny relevantní údaje byly opět zaznamenávány a obrazy ukládány pro pozdější použití.

VeriLook 3.2 Algorithm Demo

Aplikace pro rozpoznávání tváře VeriLook umožňuje práci jak s „živým“ obrazem získaným prostřednictvím webové kamery nebo jiného zařízení schopného snímat obraz v reálném čase, tak i s obrazovými soubory uloženými na paměťovém médiu.

Pro snímání obrazu byla využita webová kamera Creative WebCam Live! Motion. Během **registrace** bylo do systému průběžně zaregistrováno celkem 42 osob. Registrace probíhala dvěma metodami. První byla klasická registrace, kdy byl registrační vzorek vytvořen na základě jediné sekvence snímaných obrazů (počet snímaných obrazů závisel na nastavení hodnoty *Enroll Stream Length*, která byla ponechána na výchozí hodnotě 10). Druhou metodou byla registrace s generalizací, u které bylo k vytvoření registračního vzorku zapotřebí více vzorků, tedy sekvence byla několikrát opakována (*Generalization Template Count*). Nastavení bylo rovněž výchozí, takže zapotřebí byly čtyři vzorky. Navíc, pokud daná osoba nosila brýle, byl navíc pořízen klasickou cestou registrační vzorek bez brýlí. Takových osob bylo během testování 9. Obě metody byly využity za účelem porovnání s ohledem na kvalitu registračního vzorku a její vliv na chybovost systému.

S výjimkou 7 případů z 93 registrací proběhla registrace úspěšně na první pokus. Ve zbylých 7 případech bylo nutné proces opakovat. Nejčastější příčinou byl nesprávný výraz, nebo nedostatečná kvalita obrazu.

V rámci procesu **autentizace** bylo provedeno 5 pokusů o identifikaci tváře každé osoby, z toho 2 pokusy zahrnovaly testování živosti, kdy osoba musela vyvinout dodatečné úsilí, aby vzorek byl klasifikován jako vzorek od živé osoby.

Touto cestou bylo provedeno celkem 210 autentizačních pokusů. Vzorky byly využity jak ke zjištění míry nesprávných odmítnutí, tak míry nesprávných přijetí, protože aplikace ve výsledcích identifikace uváděla všechny registrační záznamy, které byly vyhodnoceny jako shodné s aktuálním vzorkem.

Každý autentizační pokus se skládal ze získání několika snímků (*Matching Stream Length*) a zároveň z několika opakovaných pokusů o nalezení shody v databázi (*Matching Attempts*). Hodnoty byly ponechány na výchozích – *Matching Stream Length* = 3, *Matching Attempts* = 10. Test živosti však vyžadoval vetší počet snímků, aby bylo možné detekovat v obraze změny, proto byla hodnota položky *Matching Stream Length* nastavena na 15. Z toho plyne, že testování živosti prodlužuje dobu identifikačního procesu.

V průběhu testování byly několikrát zaznamenány problémy s kvalitou obrazu, kdy kamera nedokázala za daných okolních podmínek snímat obraz v dostatečné kvalitě. Největší vliv na kvalitu obrazu mělo osvětlení v místnosti, nedostatečná kvalita byla nejčastěji spojena se špatnými světelnými podmínkami ve večerních hodinách, kdy bylo k dispozici pouze umělé osvětlení. Řešením byla úprava osvětlení nebo snížení požadavků na kvalitu obrazu.

Snímky byly průběžně ukládány a využity k získaní informací o chybovosti systému při různých prahových hodnotách.

Snímání pomocí kamery bylo prováděno při výchozí prahové hodnotě, která byla 48. Pro tuto hodnotu byly získány následující výsledky:

$FRR_{klasická\_reg.} = 4{,}286\%$
$FRR_{generalizace} = 4{,}286\%$
$FRR_{klasická+bez\_brýlí} = 3{,}333\%$
$FRR_{gen.+bez\_brýlí} = 2{,}857\%$
$FRR_{klasická+gen.} = 2{,}381\%$
$FRR_{klasická+gen.+bez\_brýlí} = 1{,}905\%$
$FTE = 0\%$
$FTA = 0\%$

$FAR_{klasická\_reg.} = 6{,}190\%$
$FAR_{generalizace} = 2{,}857\%$
$FAR_{klasická+bez\_brýlí} = 7{,}143\%$
$FAR_{gen+bez\_brýlí} = 4{,}286\%$
$FAR_{klasická+gen.} = 7{,}619\%$
$FAR_{klasická+gen.+bez\_brýlí} = 8{,}571\%$

Rozdíl mezi klasickou registrací a registrací s generalizací není v případě FRR při dané prahové hodnotě žádný, v obou případech byla 9krát identifikace neúspěšná. Rozdíl je patrný v hodnotách FAR, která je v případě klasické registrace přibližně dvojnásobná, což může být důsledkem kvalitnějších registračních vzorků při registraci s generalizací.

Pokud provedeme navíc u osob s brýlemi i registraci bez brýlí, lze pozorovat snížení míry nesprávných přijetí, a to i přesto, že brýle nosila jen zhruba pětina ze všech zaregistrovaných osob. Zároveň však dochází ke zvýšení FAR, protože více registračních vzorků v databázi zvyšuje pravděpodobnost, že neoprávněný uživatel bude chybně spojen s některým registračním vzorkem.

Dalšího snížení FRR lze dosáhnout, pokud bude mít v databázi každá osoba více registračních vzorků (např. jeden získaný klasickou cestou a druhý metodou s generalizací). V tomto případě se počet nesprávných přijetí snížil zhruba na polovinu. Negativním důsledkem může být opět zvýšení FAR.

Výběr vhodné strategie pro registraci uživatelů závisí na požadavcích konkrétní oblasti nasazení. Jako výhodné se jeví provést u osob, které nosí brýle registraci s brýlemi i bez nich. Registrace s generalizací nepřináší oproti klasické metodě markantní snížení chybovosti, navíc negativně může působit prodloužení registračního procesu, kdy osoba musí déle vydržet nehybně před kamerou. Zapomínat bychom neměli ani na možné zvýšení FAR, pokud bude mít každá osoba v databázi více vzorků.

Během testování nebyl zaznamenán žádný případ neúspěšné registrace, ani neúspěšného snímání biometrických dat (FTE i FTA nulová).

Získané obrazy byly následně využity pro měření chybovosti při různých nastaveních prahové hodnoty. Do testování již nebyla zařazena registrace s generalizací, protože během registračního procesu s využitím kamery nebylo možné uložit jednotlivé obrazy, ze kterých se vytvářel generalizovaný registrační vzorek. Prahová hodnota byla nastavována po stejných krocích jako v aplikaci VeriFinger, v rozmezí 12–96.

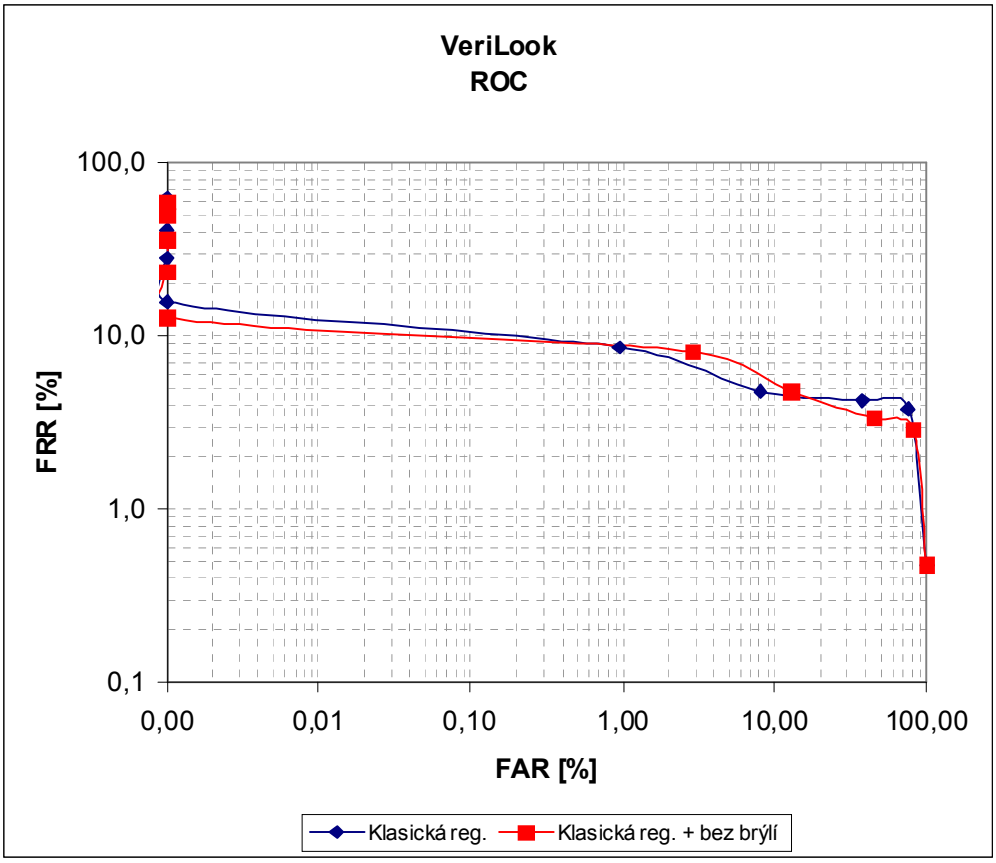
Výchozí nastavení bylo 48 a pro tuto hodnotu byly zjištěny následující výsledky:

$FRR_{klasická\_reg.} = 15{,}714\%$
$FRR_{klasická+bez\_brýlí} = 12{,}857\%$
$FAR_{klasická} = 0\%$
$FAR_{klasická+bez\_brýlí} = 0\%$
$FTE = 0\%$
$FTA = 0\%$

V porovnání se snímáním „živého“ obrazu z kamery, při využití obrazových souborů je patrné značné zvýšení FRR (z 9 případů na 33). Podobně pokud provedeme navíc registraci bez brýlí u osob, které nosí brýle (ze 7 případů na 27). Během testování nebyl zaznamenán žádný případ nesprávného přijetí, což je ve srovnání s obrazy z kamery, kdy bylo zjištěno 13, resp. 15 případů nesprávného přijetí, pozitivní výsledek.

Opět nebyl zaznamenán ani jeden případ neúspěšné registrace (FTE), ani neúspěšného zpracování vzorku při autentizaci (FTA). Muselo však být změněno nastavení požadavků na kvalitu obrazu (*Face Quality Threshold*) z hodnoty 128 na hodnotu 100, protože v některých případech hlásila aplikace při načtení obrazového souboru nedostatečnou kvalitu obrazu, a to i přesto, že při získávání obrazu z kamery nebyl s kvalitou problém.

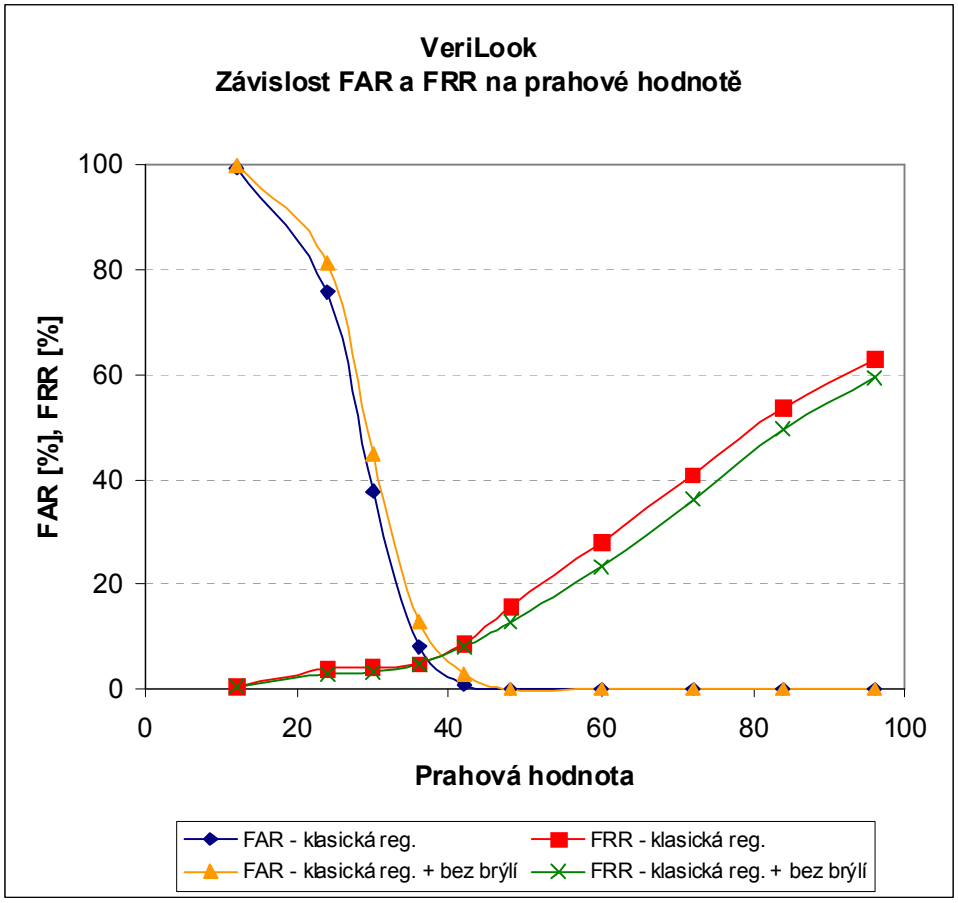
Příčinu rozdílných výsledků přisuzuji rozdílnému procesu získávání obrazové informace aplikací pro následnou registraci, resp. identifikaci. Při snímání obrazu z kamery se při registračním i autentizačním procesu získává více snímků v rychlém sledu za sebou, zatímco při použití dříve uloženého obrazového souboru je k dispozici pouze jeden snímek. Vyústěním je pak snížení kvality vzorků, které způsobuje zvýšení FRR. Nižší kvalita však paradoxně může vést ke snížení FAR, protože vzorky nižší kvality obsahují méně charakteristických rysů, a tedy je nižší pravděpodobnost, že vzorek od neoprávněné osoby bude chybně označen za shodný s nějakým vzorkem v databázi.



Graf 5.11: ROC – srovnání registračních strategií

Graf 5.11 znázorňuje porovnání chybovosti systému pro dvě registrační strategie. První strategií je případ, kdy má každá osoba v databázi pouze jeden registrační vzorek (klasická reg.), druhou pak

případ, kdy u osob, které nosí brýle, je do databáze uložen navíc kromě vzorku s brýlemi i vzorek bez brýlí. Z grafu je patrné, že volbou první či druhé strategie není chybovost systému nijak výrazně ovlivněna. Nulové FAR lze v obou případech dosáhnout při FRR kolem 15 %. Naopak nulové FRR nebylo během testování dosaženo, při 100 % FAR byla FRR 0,5 %. Relativně vysoké FRR (při FAR kolem 1 % je FRR nad 8 %) může vést k nespokojenosti uživatelů, kteří jsou obtěžování častými nesprávnými odmítnutími.



Graf 5.12: Porovnání závislosti FAR a FRR na prahové hodnotě pro různé registrační strategie

Hodnota EER systému byla pro případ, kdy má každá osoba v databázi pouze jeden registrační vzorek (osoby s brýlemi pouze vzorek s brýlemi), stanovena na 5 %. V případě, kdy byl u osob s brýlemi uložen do databáze navíc vzorek bez brýlí, hodnota EER vzrostla na 6 %. Rozdíly v hodnotách FAR a FRR se v obou případech pohybují v jednotkách procent. Více registračních vzorků v databázi sice vede ke snížení FRR, zároveň je však nutno počítat s tím, že dojde ke zvýšení FAR, což se odráží i ve vyšší hodnotě EER.

Během testování byly zaznamenány případy, kdy, ačkoliv osoba měla na očích brýle, míra podobnosti s registračním vzorkem bez brýlí byla vyšší než se vzorkem s brýlemi. Registrace dvou vzorků tak může snížit FRR nejen v případě, kdy se uživatel občas pokouší o autentizaci s brýlemi a jindy bez nich, ale také v případě, kdy se ve většině případů autentizuje s brýlemi na očích.

Tabulky se všemi zjištěnými údaji jsou k dispozici v příloze A.

Luxand FaceSDK 1.7

Aplikace Luxand umožňovala pouze práci s obrazovými soubory. Proto byly pro registraci osob i následnou autentizaci využity snímky získané při testování systému VeriLook.

Do systému bylo zaregistrováno 42 osob, u 9 z nich, které nosily brýle, byla provedena i registrace bez brýlí.

Proces autentizace opět zahrnoval 5 pokusů o identifikaci každé osoby, celkem tedy 210 pokusů o úspěšnou autentizaci. Aplikace ve výsledcích identifikace prezentovala všechny záznamy v databázi, které byly vyhodnoceny jako shodné s daným vzorkem, proto bylo možné měřit zároveň s mírou nesprávných odmítnutí i míru nesprávných přijetí.

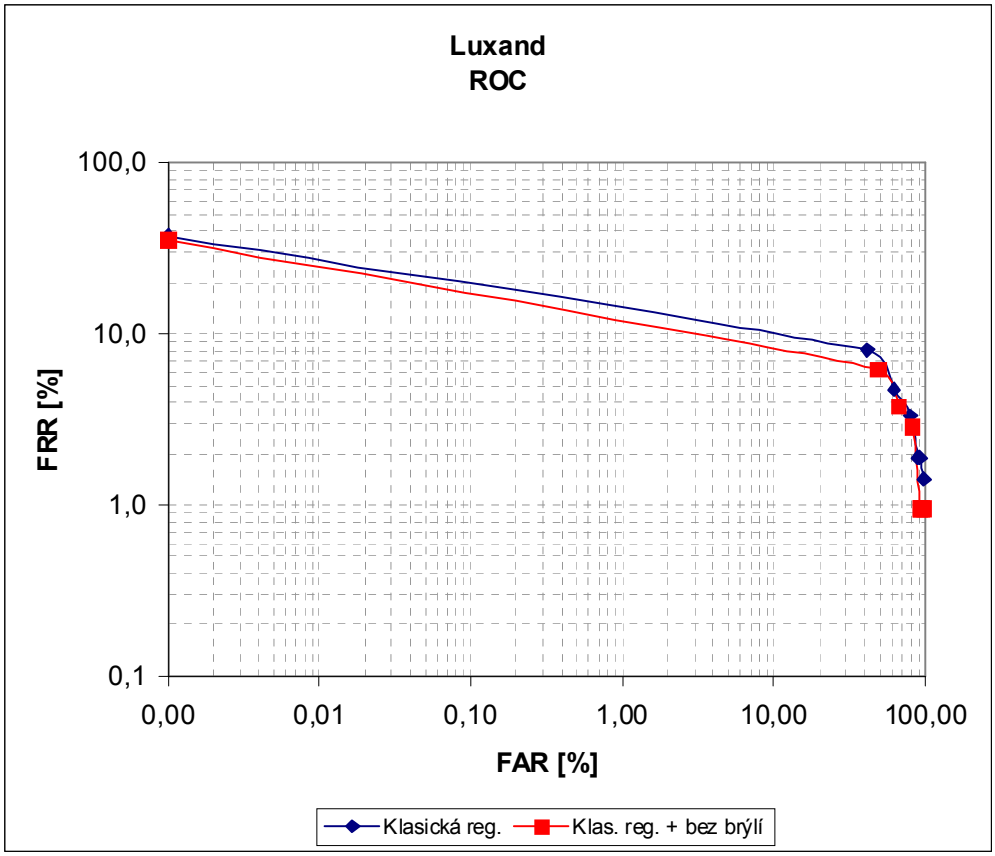
Pro výchozí prahovou hodnotu (80,00) byla chybovost systému následující:

$$FRR_{klasická\_reg.} = 8{,}095\%$$
$$FRR_{klasická+bez\_brýlí} = 6{,}190\%$$
$$FAR_{klasická\_reg.} = 40{,}952\%$$
$$FAR_{klasická+bez\_brýlí} = 48{,}095\%$$
$$FTE = 0\%$$
$$FTA = 0\%$$

Lze pozorovat podobné chování jako v případě aplikace VeriLook. Pokud osoba, která nosí brýle má v databázi uložen jak vzorek s brýlemi, tak i bez brýlí, dojde ke snížení FRR. Naopak FAR s více vzorky v databázi roste. Při výchozí prahové hodnotě je chybovost systému značně vysoká. Z 210 pokusů o autentizaci bylo 17, resp. 13 v případě, kdy databáze obsahuje i vzorky bez brýlí, neúspěšných. Ještě hůře systém dopadl v případě míry nesprávných přijetí, kdy bylo nesprávně přijato 86, resp. 101 osob z 210, což je téměř každá druhá osoba.

Během testování se nevyskytl žádný případ nemožné registrace osoby (FTE = 0 %), ani neúspěšného zpracování obrazové informace (FTA = 0 %).

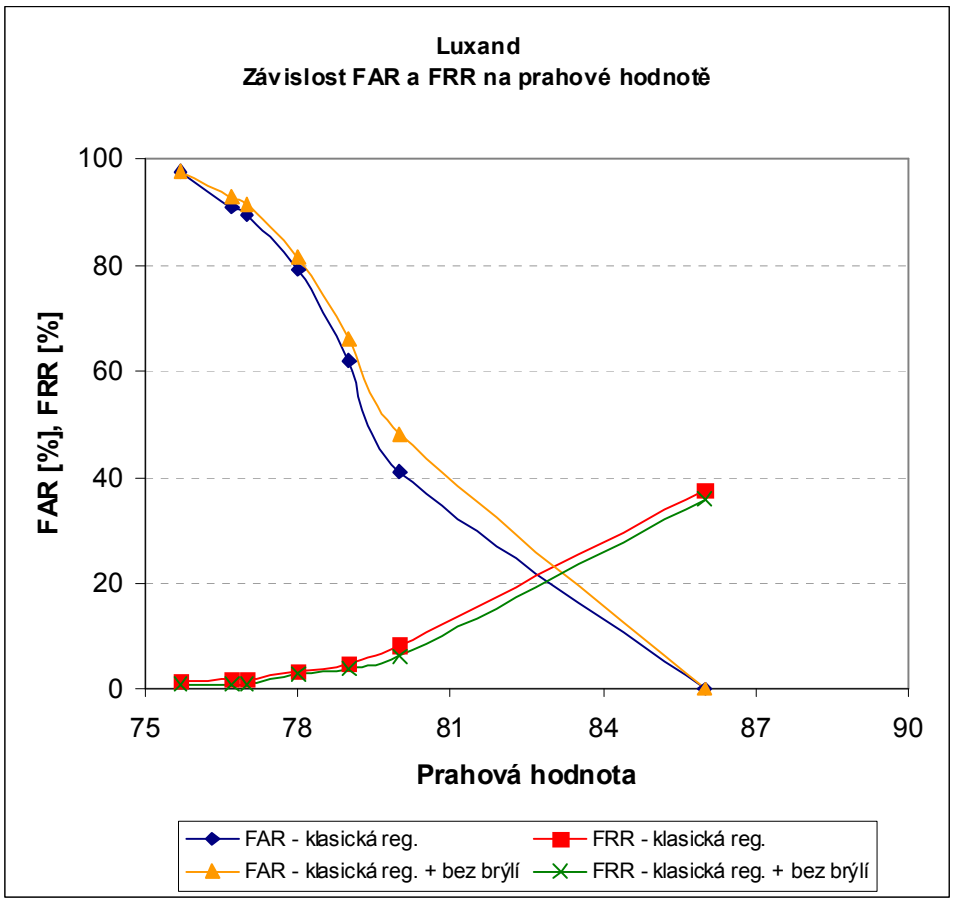
Prahová hodnota byla dále nastavována v rozmezí 75,70–86,00 (viz. Tab. 4.11).



Graf 5.13: ROC – srovnání registračních strategií

Pokud provedeme kromě klasické registrace i registraci vzorků bez brýlí, dosáhneme mírného snížení chybovosti systému, což plyne z ROC křivek. Při FAR 1 % by to znamenalo snížení FRR z přibližně 15 % na 12 %, což ovšem neznamená žádné výrazné zlepšení. Nulové FAR odpovídá FRR kolem 36 %. Při FAR 100 % bylo dosaženo hodnoty FRR přibližně 1 %.

Chybovost systému je vysoká, pokud bychom chtěli zajistit FAR v řádu jednotek procent, uživatelé by byli obtěžováni nutností, často podstupovat více pokusů, něž budou systémem rozpoznáni.



Graf 5.14: Porovnání závislosti FAR a FRR na prahové hodnotě pro různé registrační strategie

Hodnota EER byla v případě pouze jednoho vzorku v databázi pro každého uživatele stanovena na 21,5 %. V případě, kdy do databáze zahrneme i vzorky bez brýlí, EER bude asi 22 %. Vysoká hodnota EER v obou případech jen potvrzuje vysokou chybovost systému.

Podobně jako v aplikaci VeriLook jsou rozdíly v FRR, resp. v FAR pro jednotlivé registrační strategie v řádu jednotek procent, přičemž FRR při více vzorcích v databázi klesla a FAR naopak vzrostla.

Tabulky se všemi zjištěnými údaji jsou k dispozici v příloze A.

5.3 Testování identifikace osob s časovým odstupem

Součástí testování biometrických systémů bylo také testování úspěšnosti autentizace uživatelů s časovým odstupem od registrace biometrického vzorku do databáze. Takto byla autentizace otestována na 11 osobách z celkového počtu 42 osob, které byly dříve do systému zaregistrovány. Časový odstup od registrace činil zhruba 3 měsíce.

Cílem bylo zjistit, jak časový odstup ovlivní výkonnost systému, především, zda jsou biometrické vzorky časově dostatečně stálé a jak si uživatelé poradí s prezentací biometrických dat systému po delším období jeho nepoužívání. Závěrem je porovnání chybovosti s případem, kdy byla autentizace prováděna bezprostředně po registraci.

5.3.1 Otisky prstů

V rámci otisků prstů bylo stejně jako v případě autentizace ihned po registraci provedeno 5 pokusů o identifikaci obou zaregistrovaných prstů (palec a ukazovák pravé ruky). Celkem tak bylo provedeno 110 pokusů o úspěšnou autentizaci, čímž bylo zjišťována FRR. Dále bylo sejmuto po jednom vzorku palce a ukazováku levé ruky (celkem 22 vzorků) pro zjištění FAR. Navíc v aplikaci VeriFinger (čtečky Cross Match a Microsoft) bylo možné pro test FAR využít všechny sejmuté otisky (110 + 22 = 132 otisků).

Testování probíhalo při výchozích nastaveních prahové hodnoty aplikací, u zařízení Cross Match a Microsoft, kde byla možnost uložit snímky otisků bylo měření provedeno pro tři různé prahové hodnoty. Srovnání chybovostí je uvedeno pouze pro prahové hodnoty aplikací, další zjištěné výsledky jsou součástí příloh.

Bioscrypt V-Pass

Z testování vyplynuly problémy uživatelů se správným umístěním prstu na snímač po delším časovém období nepoužívání systému. U palce, kde bylo při registraci často nutné z důvodu velikosti prstu upravit pozici prstu na snímači a nemohla tak být využita pomocná zarážka pro jeho správné umístění, bylo u několika osob nezbytné nejprve zjistit správnou polohu prstu na snímači a až posléze provést pokusy o autentizaci, v opačném případě by se uživatel nebyl schopen autentizovat. Ukazovák byl z tohoto hlediska použitelnější.

Chybovost byla následující:

$$FAR = 0\%$$
$$FRR_{celkem} = 10\%$$
$$FRR_{palec} = 9{,}091\%$$
$$FRR_{ukazovák} = 10{,}910\%$$
$$FTA = 0\%$$

Stejně jako při autentizaci ihned po registraci, i v tomto případě nebyl zaznamenán žádný případ nesprávného přijetí. Míra nesprávných odmítnutí je však pro autentizaci s časovým odstupem dvojnásobná, a to pro všechny případy – palec samostatně, ukazovák samostatně i v rámci obou prstů dohromady (FRR_{celkem}). FRR kolem 10 % je pro technologii otisků prstů nebývale vysoká a pravděpodobně by vedla k nespokojenosti uživatelů.

Příčinu vidím ve výše zmíněných problémech se správným umístěním prstu na snímač.

Cross Match Verifier 300 LC 2.0

U tohoto systému nebyly ze strany uživatelů zaznamenány žádné problémy s prezentací biometrických dat pro autentizaci jako v předchozím případě. Pro výchozí prahovou hodnotu jsou výsledky následující:

$$FRR = 0\%$$
$$FAR = 0\%$$
$$FTA = 0\%$$

Chybovost byla nulová pro všechny zkoumané případy, tedy v rámci klasické registrace i registrace s generalizací, a také pokud srovnáváme jednotlivé prsty. Zároveň vidíme, že výsledky jsou srovnatelné s chybovostí zjištěnou ihned po registraci, kde byl zaznamenán pouze jeden případ nesprávného přijetí, počet nesprávných odmítnutí byl také nulový.

Výsledky pro zbylé prahové hodnoty jsou k dispozici v příloze A. Chybovost byla také srovnatelná s případem, kdy byla autentizace prováděna bezprostředně po registraci.

Microsoft Fingerprint Reader

Rovněž u tohoto systému nebyly zaznamenány žádné potíže s prezentací otisků prstů biometrické čtečce. Zařízení bylo opět testováno ve dvou aplikacích – GrFinger a VeriFinger.

Pro výchozí nastavení aplikací bylo dosaženo následujících výsledků:

GrFinger :

$$FAR = 0\%$$
$$FRR_{celkem} = 0{,}909\%$$
$$FRR_{palec} = 1{,}818\%$$
$$FRR_{ukazovák} = 0\%$$
$$FTA = 0\%$$

VeriFinger :

$$FAR_{celkem} = 0{,}758\%$$
$$FAR_{palec} = 1{,}515\%$$
$$FAR_{ukazovák} = 0\%$$
$$FRR = 0\%$$
$$FTA = 0\%$$

V rámci aplikace GrFinger je FAR nulové, stejně jako při dřívějším testování. FRR palce je srovnatelné s případem autentizace ihned po registraci, v případě ukazováku byla dokonce chybovost nulová (ve srovnání s 3 % FRR v předchozích testech). Nulová chybovost ukazováku se pak projevila i v celkovém snížení FRR, kdy nerozlišujeme mezi jednotlivými prsty (FRR_{celkem}). Snížení FRR však může být pouze v důsledku nižšího počtu testovaných osob. Důležité je zejména zjištění, že časový odstup nezpůsobuje znatelné zvýšení chybovosti systému.

Podobně v aplikaci VeriFinger bylo také dosaženo srovnatelných výsledků jako při předchozím testování. Nedošlo k žádnému zvýšení chybovosti systému.

Srovnatelných výsledků bylo u obou aplikací dosaženo i pro další dvě nastavení prahových hodnot. Výsledky chybovosti jsou k dispozici v příloze A.

5.3.2 Rozpoznávání tváře

Prováděno bylo stejně jako v předchozích testech 5 pokusů o identifikaci každé osoby, celkem tedy 55 pokusů. Z měření bylo zjišťováno FRR i FAR. Snímky byly v aplikaci VeriFinger ukládány, aby bylo možné porovnání chybovosti v rámci různých zdrojů obrazových dat (kamera,

soubor) a při různých prahových hodnotách. Zároveň obrazové soubory byly nutné pro aplikaci Luxand, která vstup z kamery nepodporovala.

Srovnání chybovostí je uvedeno pro výchozí prahové hodnoty aplikací, další výsledky jsou součástí příloh.

VeriLook 3.2 Algorithm Demo

Pro výchozí prahovou hodnotu bylo dosaženo následujících výsledků:

Zdroj obrazu : kamera	Zdroj obrazu : soubor
$FRR_{klasická\_reg.} = 5{,}455\%$	$FRR_{klasická\_reg.} = 34{,}545\%$
$FRR_{klasická+bez\_brýlí} = 5{,}455\%$	$FRR_{klasická+bez\_brýlí} = 34{,}545\%$
$FAR_{klasická\_reg.} = 0\%$	$FAR_{klasická\_reg.} = 0\%$
$FAR_{klasická+bez\_brýlí} = 0\%$	$FAR_{klasická+bez\_brýlí} = 0\%$
$FTA = 0\%$	$FTA = 0\%$

Z výsledků jsou opět patrné značné rozdíly v chybovosti v případě různých obrazových zdrojů. V obou případech nebyla chybovost ovlivněna, pokud byly do databáze registračních vzorků zahrnuty i vzorky osob bez brýlí (u osob, které nosily brýle). Příčinou je, že testování s časovým odstupem se zúčastnila pouze jedna osoba, která nosila brýle.

V případě, kdy zdrojem dat byla kamera, došlo pouze k mírnému nárůstu FRR (zhruba o 1 %), což je výborný výsledek, pokud vezmeme v potaz proměnlivost lidské tváře (vlasy, vousy, apod.). Dobrých výsledků bylo dosaženo i v rámci FAR, kdy z 55 pokusů nebyl zaznamenán žádný případ nesprávného přijetí.

Znatelně vyšší chybovost, co se týče FRR byla zaznamenána v porovnání výsledků, kdy vstupem byl obrazový soubor. FRR vzrostla oproti identifikaci ihned po registraci dvojnásobně. FAR je v obou případech nulová. Markantní zvýšení míry nesprávných odmítnutí přisuzuji proměnlivosti lidské tváře v čase v kombinaci s horší schopností identifikace v případě vstupu z obrazového souboru.

Při snímání z kamery nehrála proměnlivost tváře takovou roli, protože aplikace byla schopna z delší sekvence snímaných obrazů získat kvalitnější vzorek, a tedy míra shody s registračním vzorkem byla stále dostačující pro úspěšnou autentizaci.

V rámci FAR bylo dosaženo stejných výsledků jako v předchozím testování.

Podobných výsledků v rámci vstupu dat ze souboru bylo dosaženo i pro další prahové hodnoty, tedy znatelné zvýšení FRR a srovnatelné FAR. Výsledky jsou k dispozici v příloze A.

Luxand FaceSDK 1.7

Výsledky pro výchozí prahovou hodnotu:

$$FRR_{klasická\_reg.} = 21{,}818\%$$

$$FRR_{klasická+bez\_brýlí} = 20\%$$

$$FAR_{klasická\_reg.} = 34{,}545\%$$

$$FAR_{klasická+bez\_brýlí} = 34{,}545\%$$

$$FTA = 0\%$$

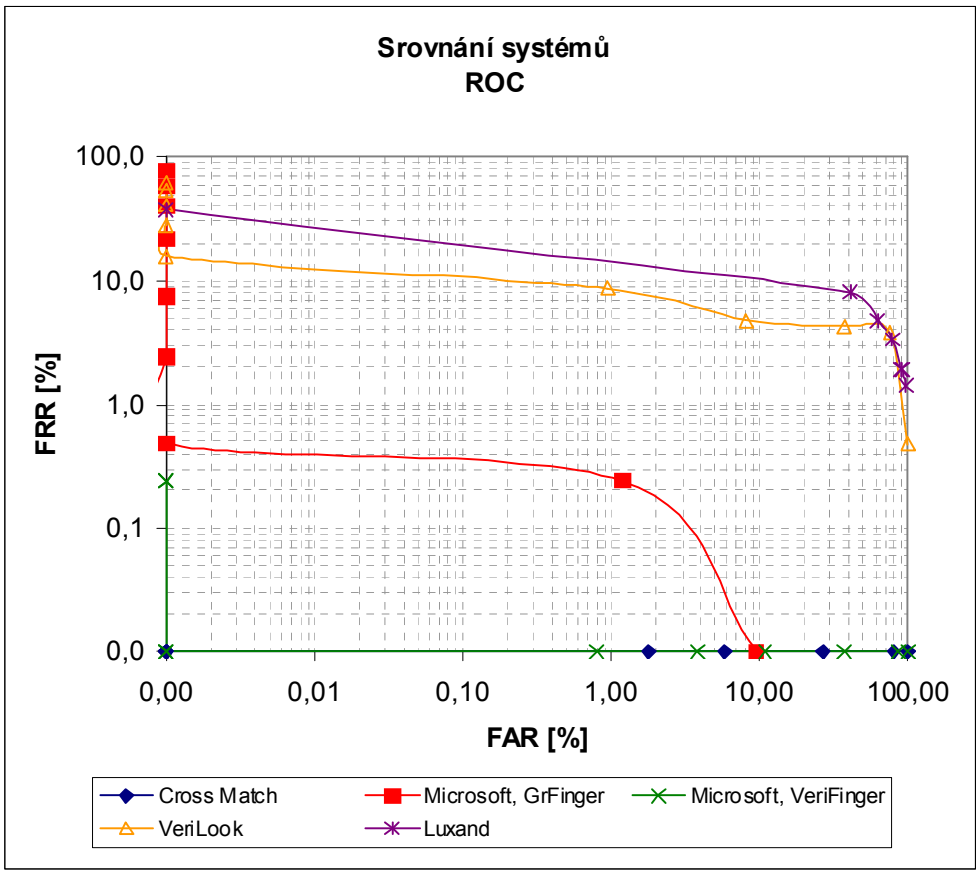
Podobně jako v aplikaci VeriLook při vstupu z obrazového souboru, i zde došlo v porovnání s autentizací bezprostředně po registraci ke dvojnásobnému zvýšení FRR. Příčina je pravděpodobně stejná jako v předchozím případě, a to proměnlivost lidské tváře.

FAR bylo nižší než v předchozích testech, zhruba o 6 % při jednom registračním vzorku v databázi pro každého uživatele a o 13 % pokud jsou do databáze zahrnuty vzorky bez brýlí osob, které nosí brýle.

Obdobných výsledků porovnání bylo dosaženo i při jiné prahové hodnotě. Výsledky jsou uvedeny v příloze A.

5.4 Srovnání testovaných systémů

Závěrem kapitoly o testování systémů uvádím srovnání všech systémů z hlediska chybovosti (viz. Graf 5.15). V grafu nejsou zahrnuty čtečky otisků prstů Bioscrypt V-Pass a APC Biopod, protože u těchto zařízení nebylo možné měnit nastavení prahové hodnoty a chybovost tak byla měřena pouze pro jedno nastavení.



Graf 5.15: ROC – srovnání systémů

Z grafu vyplývá, že nejlepších výsledků dosáhly čtečky otisků prstů s optickým snímačem otisku a spolupracující s aplikací VeriFinger. Tato konfigurace byla reprezentována čtečkami Cross Match Verifier 300 LC 2.0 a Microsoft Fingerprint Reader. U obou zařízení bylo pro specifickou prahovou hodnotu dosaženo nulové chybovosti systému. V případě čtečky Cross Match nebyl během celého testování zaznamenán ani jeden případ nesprávného odmítnutí uživatele, u čtečky Microsoft byl zaznamenán pouze 1 případ z 415, a to při nejvyšší prahové hodnotě. Registrace byla úspěšná u všech osob a až na 5 případů z 420 u čtečky Microsoft nebyly problémy ani se zpracováním sejmutého otisku aplikací. Autentizace s časovým odstupem od registrace nezpůsobila žádné významné změny v chybovosti systémů. Jediným problémem byla nutnost pravidelného čištění povrchu snímače čtečky Cross Match.

Mírně horších výsledků dosáhla čtečka Microsoft ve spojení s aplikací GrFinger. Zde již nebylo dosaženo nulové chybovosti systému, nejlepším výsledkem bylo 0,5 % FRR při 0 % FAR, což je však také výborný výsledek. Registrace otisků prstů proběhla u všech osob úspěšně, i když v některých případech bylo nutné přistoupit na nižší kvalitu vzorku. Podobně jako u aplikace VerFinger bylo zaznamenáno 5 neúspěšně zpracovaných otisků prstů, kdy si aplikace nebyla schopna poradit s nedostatečnou kvalitou otisku. Rovněž autentizace s časovým odstupem nezpůsobila změny v chybovosti systému.

Technologie rozpoznávání tváře, kterou v testování reprezentovaly aplikace VeriLook 3.2 Algorithm Demo a Luxand FaceSDK 1.7, dopadla z hlediska chybovosti podstatně hůře. V aplikaci VeriLook bylo při 0 % FAR dosaženo FRR kolem 15 %, při 1 % FAR bylo FRR stále kolem 8 %, což značí docela vysokou míru nesprávných odmítnutí, které v praxi mohou uživatele obtěžovat.

Ještě horších výsledků dosáhla aplikace Luxand. Pro 0 % FAR bylo FRR nad 30 %. Snížení FRR mělo za následek vysoký nárůst FAR, abychom dosáhli FRR do 5 %, FAR by bylo nad 60 %, což je pro praktické použití neúnosné.

Značné zvýšení chybovosti bylo u obou aplikací zaznamenáno při autentizaci s časovým odstupem, kdy míra nesprávných odmítnutí vzrostla zhruba dvojnásobně.

Horší výsledky technologie rozpoznávání tváře jsou patrné i ze zjištěných hodnot EER, kdy u aplikace VeriLook bylo EER asi 5 %, u aplikace Luxand dokonce až 21 %, zatímco v případě otisků prstů se u všech systémů pohybovala hodnota EER pod 1 %.

Přínosem technologie rozpoznávání tváře může být vyšší uživatelská přívětivost, protože během snímání není nutný kontakt se snímacím zařízením.

Do testování byly zařazeny ještě dvě čtečky otisků prstů využívající pro snímání kapacitní snímač. Jednalo se o čtečky Bioscrypt V-Pass a APC Biopod. Jak již bylo zmíněno, tyto čtečky byly podrobeny testování pouze při jedné prahové hodnotě. Co se týče chybovosti, čtečka Bioscrypt vykazovala asi 5 % FRR při 0 % FAR. Autentizace s časovým odstupem měla za následek téměř dvojnásobné zvýšení FRR. Nutností bylo pravidelné čištění povrchu snímače.

Čtečka APC vykazovala chybovost asi 7 % FRR při 0 % FAR, což je srovnatelné se čtečkou Bioscrypt.

Je nutné vzít v potaz, že hodnoty FAR nevychází ze všech autentizačních pokusů, jak tomu bylo u předchozích systémů, ale pouze ze dvou vzorků každé osoby, k tomuto účelu určených.

Kapacitní snímač si navíc nedokázal poradit s nižší kvalitou některých otisků. Výsledkem byla nemožnost registrace jedné osoby do systému u obou zařízení.

V rámci technologií využívající k autentizaci otisky prstů bych na základě zjištěných výsledků zvolil jako spolehlivější technologii využívající optické snímače otisků.

Kapitola 6

Závěr

Použité zdroje

[1] John D. Woodward, Nicholas M. Orlans, Peter T. Higgins: Biometrics. McGraw-Hill Professional, 2003, 432 str.

[2] Anil Jain, Ruud Bolle, Sharath Pankanti: Biometrics: Personal Identification in Networked Society. Kluwer Academic Publishers, 1999, 411 str.

[3] http://en.wikipedia.org/wiki/Authentication (říjen 2008)

[4] Jaromír Plhák: Testování chybovosti biometrických systémů, [bakalářská práce], Fakulta informatiky Masarykovy univerzity, Brno, 2005

[5] Jindřich Juhász: Identifikace žáka při provozu školy, [diplomová práce], Pedagogická fakulta Masarykovy univerzity, Brno, 2007

[6] Václav Matyáš, Zdeněk Říha: studijní materiály předmětu PV157 – Autentizace a řízení přístupu

[7] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone: Handbook of applied cryptography, chapter 10 – Identification and entity authentication. CRC Press, 1996, 41 str.; URL: http://www.cacr.math.uwaterloo.ca/hac/about/chap10.pdf (leden 2009)

[8] Václav Matyáš, Jan Krhovják a kolektiv: Autorizace elektronických transakcí a autentizace dat i uživatelů. Masarykova univerzita, 1. vydání, 2008, 125 str.

[9] Tomáš Janeček: Biometrika. URL: http://www.nula.wz.cz/biometrika/ (leden 2009)

[10] Mark Dermot Ryan: Authentication.
URL: http://www.cs.bham.ac.uk/~mdr/teaching/modules/security/lectures/biometric.html (únor 2009)

[11] Václav Matyáš, Zdeněk Říha: Biometric Authentication – Security and Usability. Fakulta informatiky Masarykovy univerzity, Brno, 13 str.;
URL: http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf (únor 2009)

[12] Ondřej Bitto: Biometriky nejen v pasech (1.).
URL: http://www.lupa.cz/clanky/biometriky-nejen-v-pasech-1/ (únor 2009)

[13] Ondřej Bitto: User Authentication Based On Hands, [bakalářská práce], Fakulta informatiky Masarykovy univerzity, Brno, 2005

[14] Petr Bouška: Biometrické systémy: Zpracování otisku prstu včetně možnosti rekonstrukce otisku z biometrické šablony, [diplomová práce], Fakulta informatiky Masarykovy univerzity, Brno, 2007

[15] http://www.biometricsinfo.org/ (únor 2009)

[16] http://www.bioconsulting.com/Bio_Tech_Assessment.html#_Toc513626726 (únor 2009)

[17] Gait, signature recognition, URL:
http://www.biometricvisions.com/technology/technology.htm (březen 2009)

[18] http://www.keystrokesecurity.com/Science-Keystroke-Dynamics.asp (březen 2009)

[19] Vein pattern,
URL: http://www.fujitsu.com/th/en/news/archives/2008/news_fujitsu_palm_08en.html (březen 2009)

[20] Face thermogram, Footprint, Nailbed, DNA,
URL: http://pagesperso-orange.fr/fingerchip/biometrics/biometrics.htm (březen 2009)

[21] Sweat pores, URL: http://www.policensw.com/info/fingerprints/finger04.html (březen 2009)

[22] Veri-Series Operations Manual.

URL: http://www.l1id.com/pages/450-product-manuals#vpass (březen 2009)

http://www.authentec.com/products-accesscontrol-afs2-spec.cfm (březen 2009)
[23] http://www.crossmatch.com/Verifier_300_LC.html (Cross Match, březen 2009)
[24] http://www.neurotechnology.com/verifinger.html (VeriFinger, březen 2009)
[25] http://www.microsoft.com/products/info/product.aspx?view=4&pcid=1df805b1-7a19-47f5-9001-337bb76d8688&type=ovr (Microsoft, březen 2009)
http://www.grfinger.com/ (GrFinger, březen 2009)
[27] http://www.neurotechnology.com/verilook.html (VeriLook, březen 2009)
[28] http://www.luxand.com/facesdk/ (Luxand, březen 2009)
[26] http://www.apc.com/products/family/index.cfm?id=246 (APC, březen 2009)

Seznam příloh

- Příloha A: Doplňující grafy a tabulky chybovostí systémů

Příloha A