

Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu

Sulovská Kateřina · Informačné technológie

07.09.2011



Biometrické systémy jsou v současné době velmi populární prostředky ke zvýšení bezpečnosti střežených prostor. Ve většině případů slouží jako kontrola vstupu. V této oblasti se můžeme setkat s několika základními systémy, které dominují na trhu. Především jsou to systémy pro rozpoznávání otisků prstů. V dnešní době, kdy je stále větší nebezpečí, že samotný otisk bude nahrazen falešným, nebo bude systém obcházen různými padělkami, byla vyvinuta technologie na kontrolu živosti této části těla, což je technologie poměrně nová, ale zároveň také velmi drahá, což ji odsouvá lehce do pozadí a u uživatelů stále hraje velkou roli identifikace podle otisků prstů bez této kontroly.

1. Úvod

Novinkou v oblasti snímání otisků prstů je využití tzv. fotonických krystalů na bázi křemíku umožňující snímání otisků prstů v barevné škále, která odpovídá tlaku působenému na detektor různými částmi snímané oblasti – jsou tedy detekovány papilární linie, navíc je detekována i hloubka linie, tvar prstu a také vlastnosti kůže [21]. Dalším, ve světě velmi často používaným systémem, je rozpoznávání osob podle duhovky. Tyto systémy jsou velmi spolehlivé, ale zároveň patří i do vyšší cenové třídy. Co se duhovky týče, jsou rozdílné i pro jednovaječná dvojčata, a dokonce i každý jedinec má duhovky rozdílné. Výhodou tohoto systému je jeho bezkontaktnost.

Existuje i kombinace pro vysoce střežené subjekty kdy byla navržena kombinace snímání duhovky se snímáním sítnice. Mezi další nejvíce užívané systémy patří dále biometrie obličeje. Tyto systémy v současnosti dosahují uspokojivých výsledků, ačkoli nejsou natolik spolehlivé, jak je tomu u otisků prstů. Uživatelsky jsou však velmi přívětivé a proto jsou poměrně často nasazovány. V neposlední řadě bych na tomto místě zmínila biometrii založenou na geometrii ruky. Tyto systémy jsou v dnešní době nejčastěji kombinovány ještě s dalšími přístupovými systémy (karty, PIN, atd.), jelikož jejich přesnost nedosahuje přesnosti systému otisku prstu.

Geometrie ruky však podléhá častým změnám a proto je vhodnější spíše jako docházkový systém pro menší počet zaměstnanců. Poměrně novou technologií je poté rozpoznávání osob podle krevního řečiště. I v tomto případě jde o metodu relativně novou, ve vyšších cenových hladinách. Její předností je však velká spolehlivost, jelikož

použité charakteristiky se vlivem času nemění. Opomenout však nesmíme ani řadu biometrických charakteristik integrovaných do tzv. e-pasů, které jsou podmínkou pro vstup do některých zemí světa (např. USA).

2. Historie biometrických systémů

Identifikace osob podle jejich fyziologických znaků je stará jako lidstvo samo. Biometrická identifikace/verifikace je využití jedinečných, měřitelných, fyzikálních nebo fyziologických znaků nebo projevů (behaviorální charakteristiky) člověka k jednoznačnému zjištění (identifikaci) nebo ověření (verifikaci) jeho identity. První dochované písemné zmínky o identifikaci osob jsou datovány do starověkého Egypta, kde byly používány i ke „komerční identifikaci“ farmářů a dělníků v povodí řeky Nil. Producenti obilí zde byly identifikovány na základě jejich unikátního vzhledu (jizev, viditelných zranění, charakteristikou pleti, barvou očí, váhou a antropometrickými měřeními) a řádně vyplaceni za prodané zboží státu, případně byly zaznamenány jejich platby za zakoupené zboží (obilí) od státu.

Tímto způsobem staří Egypťané předcházeli dvojímu nebo neoprávněnému vyplácení měsíčních mezd, neboť záznamy o vzhledu jedinců byly velmi detailní. Moderní základy biometrických systémů, tak jak je známe dnes, položil francouzský vědec Alphonse Bertillon koncem 19. století svojí antropometrickou metodou. Touto metodou přeměřil, popsal a vyfotografoval každého odsouzeného zločince, který pak mohl být jednoznačně identifikován při dalším zadržení. Tuto metodu po několika málo desetiletích nahradila daktyloskopie. [1, 2, 12, 18, 19, 20, 22]

K masivnímu rozvoji biometrických systémů však došlo teprve v posledních čtyřiceti letech. Biometrická identifikaci byla vždy nejdříve využívána bezpečnostními a policejně-soudními složkami/aplikacemi. Teprve další rozvoj technologií umožnil využití těchto systémů i pro komerční a civilní sféru. Prudký růst obliby biometrických systémů výrazně podpořila událost z 11. září 2001, kdy nároky na bezpečnost výrazně stouply a důkladněji chránit své hodnoty začali nejen soukromé firmy, ale i jednotlivci. [1, 2, 12, 18, 19, 20, 22]

Pro identifikační účely se používají charakteristiky, které jsou pro každého jedince unikátními, a předpokládá se, že jsou časově neměnné. Pro identifikační účely využíváme poznatky z různých vědních oborů a zaměření, jako jsou lékařství, antropologie, počítačové vidění, robotika, umělá inteligence, matematika, fyzika, biologie. Vytvoření identifikačních metod pro civilní využití (tzn. vytvoření softwaru) je proto nadmíru obtížná záležitost, vzhledem ke složitosti zpracovávaných dat a použitých algoritmů, které musí být kombinovány a dále vyvíjeny k dosažení co nejlepších výsledků. [1, 2, 12, 18, 19, 20, 22]

Anatomicko-fyziologické biometrické charakteristiky k členění biometrických systémů [1]

- Oční duhovka
- Oční sítnice
- Tvář
- Tvar vnějšího ucha

- Rty
- Rentgen chrupu
- Daktyloskopické otisky prstů, dlaní a chodidel
- Geometrie prstů a ruky
- Topografie žil zápěstí, cévní řečiště
- RFID nehtu, nehtové lůžko
- Pach lidského těla
- Obsah soli v lidském těle
- Rozměry a váhy lidského těla
- Krev, srdeční pulz
- DNA

Behaviorální biometrické charakteristiky k členění biometrických systémů [1]

- Hlas
- Lokomoce
- Písmo
- Podpis
- Dynamika psaní na klávesnici
- Dynamika pohybu myši

3. Identifikace vs. Verifikace

V praxi se mezi laiky velmi často zaměňují následující dva pojmy (procesy), jež jsou výchozími pro náročnost a požadavky na zvolené aplikace. Tyto procesy je nezbytně nutné důsledně rozlišovat:

- Identifikace – jinak též porovnávání typu one-to-many. Existuje-li již vytvořená databáze zkoumaných dat a pokusíme-li se jakýmkoliv prvkem této databáze porovnat neznámý nový prvek, hledáme případnou shodu, ale ne nezbytně ji systém očekává, jedná se o proces identifikace. Slouží ke snaze pojmenovat a zařadit neznámý vzorek. Pokud ke shodě nedojde ani v jednom z případů porovnání, prvek je stále označen jako neznámý. Identifikace je typická využitím u policejné-soudních aplikací.
- Verifikace – porovnání typu one-to-one. Ke shodě může dojít pouze v případě, kdy je systému předložen jediný konkrétní vzorek, totožný s jedinou uloženou šablonou. Nový prvek se nesnažíme zařadit, ale ověřit, zda-li se skutečně jedná o vzorek s oprávněním k autentizaci. Verifikace je typická v bezpečnostně-komerční sféře.

4. Možnosti nasazení biometrických systémů

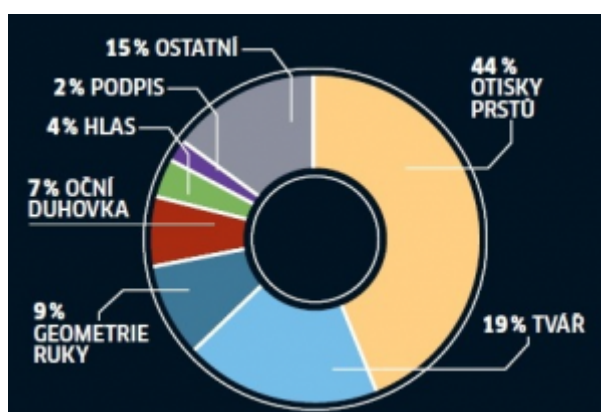
Biometrické systémy (viz tabulka 1, obrázek 1) jsou využitelné v mnoha aplikacích, mezi něž můžeme zařadit autentizaci: spojenou s kreditními kartami, pasy, řidičskými průkazy a ostatními doklady, s přístupem k výpočetním a telekomunikačním systémům. Bezpečnostní systémy založené na biometrii také slouží pro kontrolu a regulaci přístupů osob do objektu a mohou zároveň být i docházkovými aplikacemi pro: hraniční, celní a imigrační kontroly, ochranu věznic a dalších objektů s režimovými opatřeními, automatizovanou ochranu vládních objektů, bank, finančních institucí, hotelů a kasin, komerčních a společenských objektů a klubů, politických, zdravotnických a sociálních zařízení, škol a školek, domova, a najde si samozřejmě i

mnoho dalších aplikací. Nesmíme samozřejmě ani opominout policejně-forenzní a další bezpečnostní aplikace, na které jsou kladeny vyšší nároky než na zařízení pro civilní sféru [1].

Za biometrické systémy však můžeme považovat i SW zpracovávající obrazové informace z vytvořených záznamů, kdy provádíme např. dálkové pozorování, identifikaci osoby v davu, identifikaci sejmutých otisků prstů, apod. Těmito projekty se zabývají výzkumné týmy po celém světě, jelikož jejich přesnost je stěžejní a používají je převážně policejně-forenzní a bezpečnostní složky.



Obrázek 1 – Různé druhy biometrických systémů s využitím v civilní sféře [1]



Obrázek 2 – Podíl biometrických aplikací na trhu [Zdroj: časopis CHIP 08/2010, str. 32 – 33]

Tabulka 1 – Srovnání biometrických metod [10]

Biometrie	jedinečnost	univerzálnost	stálost	dostupnost	přesnost
DNA	V	V	V	N	V
Otisk prstu	V	V	V	S	S
Geometrie ruky	V	S	S	S	N
Duhovka	V	V	V	S	V
Sítnice	V	V	V	N	V
Obličej	S	V	S	V	S-V*
Geometrie žil	V	V	V	S	S
Podpis	N	N	N	V	N
Stisk kláves	N	N	N	S	N
Hlas	N	S	N	S	N

Biometrie	přijatelnost	odolnost	rychlost	cena
DNA	N	V	N	V
Otisk prstu	S	S	V	N
Geometrie ruky	N	N	V	S
Duhovka	N	V	S	S
Sítnice	N	V	S	S
Obličej	V	S	S	S-V*
Geometrie žil	S	V	V	S
Podpis	V	N	S	N
Stisk kláves	V	S	V	N
Hlas	V	N	S	N

Vysvětlivky k tabulce: V - vysoká (zelená - považováno za kladné), S - střední (oranžová - považováno za neutrální), N - nízká (červená - považováno za nepříznivé) , * - ovlivněno aplikací, pro kterou je určeno a také je důležité přihlídnutí k použité technologii.

Pokud se zaměříme na samotné rozpoznávání tváří, můžeme zjistit, že počet jeho nasazení vzrůstá, ať už jde o celé systémy kontroly vstupu, monitorování vnitřních a venkovních prostor, vyhledávání obrázků nebo jejich označování ve webových aplikacích, přihlašování do aplikací nebo jiných systémů (přihlašování do Windows) a vyhledávání tváří mobilními telefony nebo fotoaparáty (i se zaměřením na rozpoznávání úsměvu). Rozpoznávání se samozřejmě také stále zdokonaluje pro účely policejně-forenzní a soudní, kdy je důležité, aby software s co možná největší procentuální úspěšností identifikoval danou osobu i přes různé výrazy jejího obličeje.

V současnosti můžeme nalézt také velké množství nových nebo vylepšených algoritmů pro samotné nalezení obličeje a jeho následné porovnávání. Většina dřívějších aplikací pracovala v režimu odstínů šedi (v černobílém režimu). Dnes se již používají i aplikace/algoritmy pracující se škálou odstínů pleti, kdy je tato lépe detekována a rozlišena od okolního prostředí. Tyto systémy jsou teprve ve vývojovém stupni, jejich výpočetní náročnost je poměrně velká, avšak jejich úspěšnost přesahuje 83%. Toto číslo je však vyšší než u klasické kriminalistické portrétní identifikace, která dosahuje přibližně 70%, což je uspokojující.

5. Ceny biometrických systémů

Ceny biometrických systémů se samozřejmě liší v závislosti na použité technologii. Zásadním rozdílem je, zda si kupujeme pouze biometrický prvek (např. pouze zařízení na snímání duhovky), nebo zda si kupujeme celý systém „se vším všudy“, kde je potom cena i mnohonásobně vyšší, zvláště pak pokud jde o implementaci několika biometrických systémů dohromady (např. duhovka a sítnice). Některá zařízení jsou v České republice hůře dostupné a jejich dosažitelnost je výrazně lepší v západní Evropě nebo ve Spojených státech amerických. V následujícím odstavci jsou uvedeny ceny základních zařízení, případně postupů, které je možno využít k identifikaci/verifikaci osoby:

- Analýza DNA – nejzákladnější „testy“ DNA mají základní cenu začínající na cca 2000 Kč, přičemž bezpečnostně komerční aplikace v současnosti není k dispozici (díky technickým a technologickým otázkám a otázce zcizení biologického vzorku – např. krádež vlasu), analýza probíhá pouze ve forenzních laboratořích.
- Snímač otisku prstu – základní zařízení cca 2500 Kč.
- Kliky s integrovaným snímačem otisku prstu – od 10000 Kč.
- Snímání geometrie ruky – od 11000 Kč.
- Snímač duhovky – od 28000 Kč.
- Snímač sítnice – od 30000 Kč.
- Rozpoznávání obličeje – od 3600 Kč.
- Snímání topografie žil (krevní řečiště) – od 20000 Kč.
- Analýza podpisu – od 3000 Kč.
- Analýza dynamiky stisku kláves – od 6500 Kč.
- Analýza hlasu – od 6500 Kč.

6. Hodnocení biometrických systémů

Biometrické systémy jsou vyráběny na základě požadavků na úroveň bezpečnosti, spolehlivost, praktičnost, přijatelnost a samozřejmě také uživatelskou přívětivost a cenu investice. Na základě dosavadních zkušeností nejen z civilního sektoru se tedy dá říct, že ne každý biometrický systém je vhodný pro každé prostředí: vysoce střežené prostory s přítomností utajovaných informací, případně přítomností technologie/výzkumu, který má být utajen před konkurencí budou s největší pravděpodobností střeženy skenem sítnice, který poskytuje maximální stupeň zabezpečení; oproti tomu, vstup do kanceláře účetní může být zajištěn pouze zámkem s instalovanou čtečkou otisku prstu, která je v tomto případě dostačujícím ochranným prvkem a sken sítnice by byl příliš nákladnou investicí a z pohledu bezpečnosti i zbytečným prvkem na tak vysoké úrovni.

Tabulka 2 – Základní kritéria pro hodnocení biometrických systémů [1]

Kritéria hodnocení	
Operační	• jedinečnost • neměnnost • měřitelnost • uchovatelnost • spolehlivost • exkluzivita • praktičnost • přijatelnost • lidskost
Metodologická, algoritmická a bezpečnostní	• správnost teorie • správnost algoritmů • bezpečnost algoritmů • správné markanty • kódování • databáze • protokoly • distribuované prostředí

Finanční	• pořizovací cena • cena instalace • školení, trénink • upgrade • návazné systémy • logistická podpora a provoz • inovace • obsluha
Výrobní	kvalita • podpora • záruky • perspektiva • reference
Technická	• čas zpracování • chybovost • flexibilita • odolnost • efektivnost • výkonnost • standardizace • skladovatelnost • charakteristiky šablony • přesnost • jednoduchost • rychlost • nezávislost

Jelikož biometrická zařízení jsou systémy především bezpečnostní, je hlavní kritériem správné rozpoznání oprávněného uživatele a správné odmítnutí neznámé osoby. Mohou nastat případy, kdy systém nerozpozná osobu, která má oprávnění pro vstup do daného objektu, nebo naopak je systémem vpuštěna do objektu neoprávněná osoba. V praxi poté pracujeme s pravděpodobností obou zmíněných negativních a tedy nežádoucích jevů. V průběhu let byly zavedeny základní pojmy uvedené v následujících podkapitolách [1, 11, 12, 17, 23].

6.1 Senzitivita a specifita

Termín senzitivita vyjadřuje pravděpodobnost, že osoba s oprávněním k přístupu (je uložena v databázi), bude identifikačním algoritmem vyhodnocena jako pokus o identifikaci osobou s pozitivním povolením k přístupu. Vyhodnocuje se ze vztahu:

$$TPR = \frac{TP}{TP+FN} \quad (1)$$

kde: TPR (True Positive Rate) - pravděpodobnost přijetí oprávněné osoby, TP (True Positive) - počet přístupů s povolením vyhodnocených jako oprávněné, FN (False Negative) - počet přístupů s povolením vyhodnocených jako neoprávněné. Termín specifita vyjadřuje pravděpodobnost, že osoba bez oprávnění k přístupu (není uložena v databázi), bude identifikačním algoritmem vyhodnocena jako pokus o identifikaci osobou s negativním povolením k přístupu. Vyhodnocuje se ze vztahu:

$$TNR = \frac{TN}{TN+FP} \quad (2)$$

kde: TNR (True Negative Rate) - pravděpodobnost odmítnutí neoprávněné osoby, TN

(True Negative) – počet přístupů bez povolení vyhodnocených jako neoprávněné, FP (False Positive) – počet přístupů bez povolení vyhodnocených jako oprávněné.

6.2 Pravděpodobnost chybného odmítnutí (False rejection rate - FRR)

FRR bývá také označováno za Chybu I. druhu je jedním z bezpečnostních kritérií biometrických systémů. Udává pravděpodobnost, s jakou bude zařízení chybovat a neidentifikuje/neverifikuje oprávněného uživatele, přestože uživatel má v aplikaci již uloženou svou biometrickou šablonu. Z tohoto důvodu je uživatel nucen opakovaně se identifikovat/verifikovat.

$$FRR = \frac{N_{FR}}{N_{EIA}} = \frac{N_{FR}}{N_{EVA}} \quad (3)$$

kde: N_{FR} – počet chybných odmítnutí, N_{EIA} – počet pokusů oprávněných osob o identifikaci, N_{EVA} – počet pokusů oprávněných osob o verifikaci.

6.3 Pravděpodobnost chybného přijetí (False Acceptance Rate - FAR)

FAR můžeme označit také Chybou II. druhu. Jestliže FRR nemá na bezpečnost v komerčním sektoru veliký význam, tak u FAR je to právě naopak. Jedná se o situaci, kdy biometrické zařízení nesprávně vyhodnotí cizí osobu jako registrovanou v systému a vpustí ji do objektu, nebo aplikace, přestože tato k tomu nemá oprávnění. Pravděpodobnost chybného přijetí je závažným nedostatkem, který může mít nedozírné následky, ať už finančního, společenského nebo jiného charakteru.

$$FAR = \frac{N_{FA}}{N_{IIA}} = \frac{N_{FA}}{N_{IVA}} \quad (4)$$

kde: N_{FA} – počet chybných přijetí, N_{IIA} – počet pokusů neoprávněných osob o identifikaci, N_{IVA} – počet pokusů neoprávněných osob o verifikaci.

6.4 Uživatel nemůže být zaregistrován do biometrického systému (Failure to Enroll Rate - FTE nebo FER)

Tento fakt se týká lidí s určitým deficitem, jako je například chybějící prst, slepota atd. FER udává poměr osob, u kterých selhal proces sejmutí vlastnosti. Jedná se o pohyblivou veličinu, která má vztah nejen k osobě, ale i ke konkrétní biometrické vlastnosti, která se snímá. Lze poté určit i tzn. osobní FER (Personál FER) udávající vztah konkrétní osoby a jejích biometrických vlastností k procesu snímání. V případě, že byla uživateli správně sejmuta biometrická vlastnost, avšak systém ho chybně odmítl i po mnoha identifikačních/verifikačních pokusech, mluvíme o tzv. Koeficientu selhání přístupu FTA (Failure To Acquire). Abychom získali spolehlivé statistické údaje, je nutno provést velké množství pokusů o sejmutí biometrické vlastnosti.

6.5 Pravděpodobnost nesprávného přiřazení biometrické vlastnosti referenčnímu vzorku (FIR)

Pravděpodobnost, že při procesu identifikace je biometrická veličina (vlastnost) nesprávně přiřazena k některému referenčnímu vzorku (False Identification Rate - FIR) kde přesná definice závisí na principu, kterým se přiřazuje pořízený vzorek k

referenčnímu, jelikož se často stává, že po srovnávacím procesu vyhovuje více než jeden referenční vzorek, tzn., překračuje rozhodovací práh.

6.6 False Match rate (FMR).

Koeficient FIR udává poměr neoprávněných osob, které jsou nesprávně rozpoznány jako akreditované během srovnávacího procesu. Porovnáme-li ho s koeficientem FAR, liší se v tom, že na rozdíl od FAR se do FMR nezapočítává odmítnutí z důvodu špatné kvality snímaného obrazu. Znamená to tedy, že koeficienty FAR a FRR jsou více závislé na způsobu používání biometrického zařízení, tzn., nesprávně rozpoznané biometrické vlastnosti tyto koeficienty zhoršují.

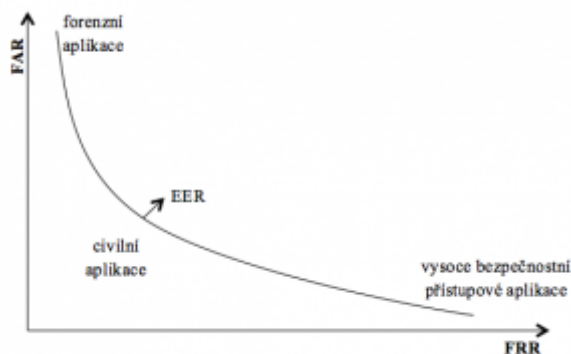
6.7 Chyby snímání biometrických dat

- 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. Zahrnují se zde také osoby bez požadované biometrie (lidé s chybějícími orgány).
- FTA (Failure to Acquire Rate) – pravděpodobnost, že systém není schopen sejmout vzorek dostatečné kvality v okamžiku, kdy uživatel předkládá biometriku snímači. Chyba může být způsobena nesprávnou polohou snímané biometrie na snímači, neoptimálním prostředím (např. osvětlení, pozadí při rozpoznávání tváře) nebo zraněním.

6.8 Receiver Operating Characteristics (ROC křivka)

Výše uvedené pravděpodobnostní charakteristiky zvyšují svůj statut hodnotících kritérií spolehlivosti při vzájemném porovnání vynesemím do tzv. ROC křivky. Věrněji vyjadřuje neoklamatelnou závislost těchto jednotlivých kritériálních parametrů na svém významovém protějšku (FRR na FAR a opačně, senzitivity na specificitě a opačně). Pokud se budeme změnou hodnoty prahu citlivosti snažit minimalizovat chybu jednoho z těchto parametrů, chyba druhého se bude naopak adekvátně zvyšovat.

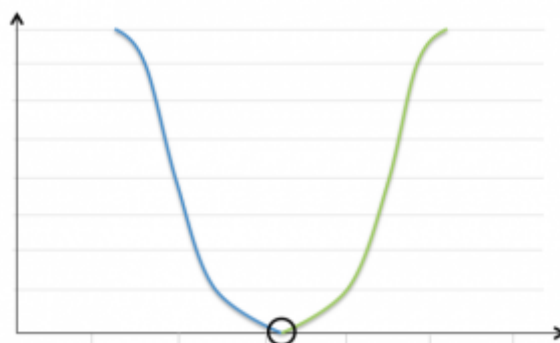
Míra růstu chyby druhého parametru je odvislá od robustnosti diskutovaného biometrického systému a u každého takového produktu se liší. Hodnota prahu citlivosti tak nefiguruje v grafu přímo, ale je zohledněna v zobrazovaných funkčních hodnotách tvořících křivku grafu, neboť na ní závisí chyba každého uvažovaného parametru zvlášť. ROC křivka slouží také 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.



Obrázek 3 - ROC křivka

6.9 Ideální aplikace

Pravděpodobnost chybného vyhodnocení shody nebo neshody biometrického vzoru a šablony nelze teoreticky vypočítat. Veškeré biometrické metody jsou založeny na statistickém vyhodnocení míry shody porovnávaných obrazů (skóre). Skóre dvou po sobě sejmutých šablon stejného otisku při porovnání vůči vzoru se vždy bude lišit. Biometrické systémy nikdy nezaznamenají stejnou informaci při několikanásobném předložení snímaného objektu a jeho charakteristik. Rozhodovací práh algoritmu se nastavuje dle požadavků uživatele podle toho, jak velká chyba je pro aplikaci a uživatele ještě přijatelná. Posouváním prahové hodnoty se pravděpodobnost obou chyb závisle na sobě mění. Pokud jedna z nich klesá, druhá vzrůstá a naopak. Můžeme si tak sami vytvořit vlastní, pro nás ideální aplikaci.



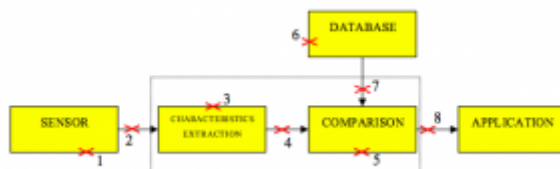
Obrázek 4 - Ideální biometrická aplikace [1, 20] - Bod protnutí křivek FRR a FAR se nazývá Equal Error Rate (EER), slouží k orientačnímu porovnání dvou aplikací, kdy pro stejný práh citlivosti vykazují oba dva parametry stejnou hodnotu chyby. Jinak nemá bod EER žádný fyzikální význam.

Pro ideální aplikaci platí, že křivky FAR a FRR se navzájem neprotínají a vhodným zvolením prahu citlivosti je lze bezchybně oddělit a současně dosáhnout nulové chybovosti jak chyby prvního, tak druhého druhu. Všechny osoby podstupující identifikační proces jsou tak 100% rozpoznány.

7. Možnosti napadení biometrických systémů

Stejně jako ostatní přístupové a bezpečnostní systémy, tak i biometrické, lze překonat. Je potřeba vynaložit určité úsilí a mít určité dovednosti a znalosti těchto systémů. Celý systém je tak silný a odolný vůči pokusu o prolomení, jako je odolné jeho nejslabší místo. V následujícím obrázku je znázorněno několik slabých míst biometrických

systémů [20].



Obrázek 5 - Možnosti napadení biometrických systémů [18, 19, 20]

kde [18, 19, 20]:

1. Podvrh biometrické vlastnosti – na místo přiložení biometrické vlastnosti může útočník podstrčit falešná data v podobě např. falešného otisku prstu, makety dlaně, umělé duhovky, repliky tváře a tím zmást senzor systému.
2. Replikace starých dat – útočník může odpozorovat uživatelské číslo a PIN a po přistoupení pak může obnovit latentní biometrickou vlastnost na snímači. Reálné ohrožení v tomto případě hrozí zejména u otisku prstů.
3. Modifikace extraktoru – tato situace může nastat za určitých specifických podmínek, kdy modifikovaný extraktor bude generovat předem připravený vektor rysů. Tento způsob útoku se nazývá „Trojský kůň“.
4. Syntetický vektor rysů – útok založený na vytvoření vlastní umělé šablony obsahující konkrétní markanty otisků prstů nebo kód duhovky, apod.
5. Změna porovnávání – útoku je vystaveno klíčové místo pro všechny biometrické systémy a to práh porovnávání, na základě kterého je pak vygenerován výsledek porovnání. Pokud je nastaven extrémně nízký práh u verifikace je útočníkovi potvrzena libovolná identita. V opačném případě může být narušena plynulá činnost systému velkým počtem nesprávně odmítnutých uživatelů.
6. Modifikace šablony – zásah do databáze, kdy je pozměněna uložená šablona v databázi. Původnímu uživateli tak není povolen přístup, ale tento je umožněn cizí osobě, které přísluší změněná data v šabloně.
7. Blokování kanálu – bez přístupu k databázi šablon není schopen systém provádět porovnávání. Všem osobám je tak odepřen přístup. Jde o útok typu „Denial of Service“ (DoS). Nefunkční systém pak musí být nahrazen jiným verifikačním/identifikačním prvkem, který může být pro útočníka lehce oklamatelný.
8. Změna výsledku – zaslání předem vybraného výsledku řídicí aplikaci, která na jeho základě povolí přístup neautorizované osobě.

Mimo těchto osm míst bývá v některé literatuře ještě naznačena devátá možnost, a to obejítí celého systému, tedy modifikace aplikace. Biometrická data pak nemusí být vůbec vložena, nedochází k extrakci rysů a jejich porovnání – uživatel napojený přímo na aplikaci si povolí přístup sám.

8. Metodika rozpoznávání tváří

Počítačové identifikace osob podle jejich tváří se dá rozdělit do dvou základních částí: detekce a lokalizace tváře v dané scéně a rozpoznání tváře. Náročnost celého procesu závisí především na typu scény – reálná scéna je pro detekci a lokalizaci obličeje velmi problematická, vzhledem k okolním rušivým obrazcům, oproti tomu za ideální se dá považovat scéna „logovací“ (laboratorní, interiérové prostředí), kde je pozadí

jednoduché, stejnorodé a neměnné pro všechny jedince, s přesně vymezenou vzdáleností od snímací kamery. Velmi podrobně je tato problematika popsána v [1, 2], odkud je také čerpán následující text.

8.1.1 Detekce a lokalizace tváře

Základním předpokladem nalezení zvolené tváře v reálné scéně je vytvoření počítačového modelu této tváře (2D, 3D, černobílý, barevný, infračervený a další typy modelů) a její následné srovnání s každým objektem na scéně, jehož podobnost je vypočítána. Na základě tohoto srovnání je konstatováno, zda na scéně je objekt představující lidskou tvář, či nikoliv. Zároveň je vypočítána pozice případné tváře na scéně. Z hlediska matematického modelování můžeme detekci a lokalizaci tváře rozdělit na dva základní typy [1]:

- statisticky orientované metody:
 - metoda podprostoru,
 - metoda neuronových sítí,
- znalostní metody:
 - metody založené na rozložení odstínů šedi v obraze,
 - metody založené na rozpoznávání obličejových obrysů,
 - metody založené na informaci o barvách,
 - metody založené na informaci o pohybu na scéně,
 - metody založené na symetrii.

8.1.2 Rozpoznávání tváře

Cílem rozpoznávání tváře je nalezení rozdílů v každém obličejí na dané scéně. Právě tyto rozdíly jsou použity k verifikaci nebo identifikaci osoby. Rozpoznávání tváří začíná extrahováním identifikačních markantů (charakteristik) a jejich efektivní porovnání s charakteristikami známé osoby uložené v databázi. K rozpoznávání tváří můžeme použít tyto metody (některé z níže uvedených metod jsou totožné s metodami pro detekci a lokalizaci tváří) [1]:

- metody založené na rozložení odstínů šedi v obraze,
- metody založené na geometrických tvarech a identifikačních markantech,
- metoda optických toků,
- metoda deformačních modelů,
- metody neuronových sítí,
- metoda „Eigenhead“.

Mimo výše uvedené metody, které jsou velmi dobře popsány v [1], samozřejmě ještě existuje velké množství algoritmů [4], které se dají pro jednotlivé metodologické postupy využít. Mezi nejznámější algoritmy používané pro rozpoznávání tváří můžeme zařadit zejména: Principal Component Analysis (PCA) navržená autory Turk a Pentland, Independent Component Analysis (ICA), Linear Discriminant Analysis (LDA), Evolutionary Pursuit (EP), Elastic Bunch Graph Matching (EBGM), Active Appearance Model (AAM), Support Vector Machine (SVM), Hidden Markov Model (HMM), algoritmy pro 3D rozpoznávání a mnoho dalších.

9. Závěr

V současné době je velmi dobře řešena problematika většiny civilních aplikací biometrických systémů. Ačkoli je výzkum zaměřený na tyto systémy velmi pokročilý a jeho dosavadní výsledky jsou velmi uspokojivé a v mnoha případech bylo dosaženo velkých úspěchů, stále se nedá říci, že by všechny systémy byly dokonalé a definitivně vytvořené. Je tak stále možno objevit nové možnosti, přístupy a také postupy, jak tyto systémy zdokonalit, zpřesnit a zrychlit a zajistit tak jejich lepší funkčnost a integritu ve smyslu nemožnosti obejítí/napadení jednotlivých částí systémů (např. detekce živosti u snímání otisku prstu).

Zajímavou skutečností je fakt, že Česká republika či vyspělé státy Evropské unie v zavádění biometrie do praxe výrazně zaostávají oproti na první pohled technologicky mnohem méně vyspělým zemím rozvojovým. Příkladem může být např. Indie (registr obyvatelstva založený na snímání otisků prstů, duhovky a rozpoznávání tváře), Afghánistán, a další státy. V České republice i v Evropě se používají všechny typy biometrických senzorů, samozřejmě v různém procentuálním zastoupení. Nejčastěji se můžeme setkat se senzory otisků prstů, často také vidíme zařízení založená na rozpoznávání obličejů nebo geometrie ruky. Méně často jsou pak používána zařízení na snímání duhovky či sítnice.

Použitá literatura a zdroje

1. RAK, R.; MATYÁŠ, V.; ŘÍHA, Z., A KOL. Biometrie a identita člověka ve forenzních a komerčních aplikacích. Praha: GRADA, 2008, ISBN 978-80-247-2365-5
2. LI, S. Z.; JAIN, A. K. Handbook of face recognition. New York: Springer Science+Business Media, Inc., 2005, ISBN 0-387-40595-X
3. KOTEK, Z., MAŘÍK, V. A KOL. Metody rozpoznávání a jejich aplikace, Praha: Academia, 1993, ISBN 80-200-0297-9
4. FACE RECOGNITION HOMEPAGE [online]. 1.3.2005, 14.2.2011 [cit. 2011-03-07]. Face recognition. Dostupné z WWW: <http://www.face-rec.org/general-info/>
5. NORMAN, T. Integrated security systems design: Concepts, design, and implementation. Oxford: Elsevier Inc., 2007, ISBN 978-0-7506-7909-1
6. CIPOLLA, R.; BATTIATO, S.; FARINELLA, G. M. Computer Vision: Detection, recognition and reconstruction. Berlin Heidelberg: Springer-Verlag, 2010, ISBN 978--642-12847-9
7. WAYMAN, J., et al. Biometric Systems: Technology, design and performance evaluation. London: Springer-Verlag, 2005, ISBN 1-85233-596-3
8. MOU, D. Machine based intelligent face recognition. Berlin Heidelberg: Springer-Verlag, 2010, ISBN 978-3-642-00750-7
9. TISTARELLI, M.; BIGUN, J. Advanced studies in biometrics. Summer School in Biometrics. Alghero, Italy, June 2003, Revised selected lectures and papers. Berlin Heidelberg: Springer-Verlag, 2005, ISBN 3-540-26204-0
10. JAIN, A.; ROSS, A.; PRABHAKAR, S. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 2004, vol. 14, no. 1.
11. SVOZIL, L. Aspekty biometrického rozpoznávání osob s využitím rozpoznávání tváře. Bakalářská práce, UTB ve Zlíně, Fakulta aplikované informatiky, Zlín, 2009, vedoucí bakalářské práce Ing. Rudolf Drga
12. ŠČUREK, R. Biometrické metody identifikace osob v bezpečnostní praxi. VŠB TU Ostrava, Fakulta bezpečnostního inženýrství, Katedra bezpečnostního managementu,

- Oddělení bezpečnosti osob a majetku [online]. 2008 [cit. 2011-03-08]. Dostupný z WWW:
http://www.fbi.vsb.cz/shared/uploadedfiles/fbi/biometricke_metody.pdf
13. DUBSKÝ, M. Simulace biometrických zabezpečovacích systémů pracujících na základě rozpoznávání tváře. Diplomová práce, VUT v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, Brno, 2007, vedoucí diplomové práce Ing. Hicham Atassi
 14. MICHALÍK, M. Algoritmy pro rozpoznání obličeje. Bakalářská práce, UTB ve Zlíně, Fakulta aplikované informatiky, Zlín, 2008, vedoucí bakalářské práce doc. RNDr. Petr Ponížil, Ph.D.
 15. FLÁŠKOVÁ, Z. Biometrické systémy založené na rozpoznávání tváře. Masarykova Univerzita, Fakulta informatiky, Brno 2009, vedoucí bakalářské práce Ing. Mgr. Zdeněk Říha, Ph.D.
 16. MOŽNÝ, D. Extrakce charakteristických vlastností pro systém rozpoznávání obličejů. Masarykova Univerzita, Fakulta informatiky, Brno, 2009, vedoucí bakalářské práce RNDr. Stanislav Bartoň, Ph.D.
 17. BS ISO/IEC 19795-1:2006 - British Standard: Information technology - Biometric performance testing and reporting: Part 1: Principles and framework . Online, [cit. 7.3.2011], dostupné z www:
<http://www.scribd.com/doc/28132066/BS-ISO-IEC-19795-1-2006-Information-Technology-Biometric-p>
 18. KOVÁČ, P., SULOVSÁ, K. Biometrical systems and their usage in IT and data protection. In XII. Ročník mezinárodní konference Internet, bezpečnost a konkurenceschopnost organizací: Řízení procesů a využití moderních terminálových technologií, Kraków - Zlín: EAS, Tomas Bata University, Zlín, 2009, s. 232 - 240, ISBN 978-83-61645-16-0
 19. NAVRÁTIL, P. Podpora výuky biometrických přístupových systémů. Diplomová práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, vedoucí práce doc. Ing. Karel Burda, CSc.
 20. KOVÁČ, P. Návrh biometrického identifikačního systému pro malou organizaci. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, vedoucí práce Ing. Stanislav Goňa, Ph.D.
 21. BENEŠ, R. Autentizační metody založené na biometrických informacích. Online, [cit. 11.3.2011], dostupné z www:
<http://access.feld.cvut.cz/view.php?cisloclanku=2010110002>
 22. SULOVSÁ, K., ADÁMEK, M., JAŠEK, R.: Identification of an individual via gait recognition as a tool for protection of assets. In Knowledge for Economic Use 2010, Olomouc, Univerzita Palackého v Olomouci, Filozofická fakulta, s. 128 - 137, ISBN 978-80-904477-5-2
 23. JAIN, L. C., et al. Intelligent biometric techniques in Fingerprint and Face recognition. 1. vydání, CRC press, New York, 1999, ISBN 0-8493-2055-0

Ústav bezpečnostního inženýrství, Fakulta aplikované informatiky, Univerzita Tomáše Bati ve Zlíně
