Česká zemědělská univerzita v Praze

Technická fakulta

Identifikace uživatele na základě rozpoznání jeho tváře

Bakalářská práce

Vedoucí bakalářské práce: Ing. Veronika Hartová, Ph.D.

Autor bakalářské práce: Marek Veselý

Praha 2016

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Marek Veselý

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Identifikace uživatele na základě rozpoznání jeho tváře

Název anglicky

Identification of the user based on recognition of his face

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku identifikace uživatele na základě rozpoznání jeho tváře. Rozebírá jednotlivé možnosti této identifikace a její výhody a nedostatky. Dále poukazuje na spolehlivost těchto systémů.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýzách odborných informačních zdrojů. Vlastní řešení je realizováno formou hodnocení prvků této identifikace. Na základě rozboru teoretických poznatků a výsledků hodnocení budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

30-40 str.

Klíčová slova

tvář, sken, identifikace, biometrie, spolehlivost

Doporučené zdroje informací

HEŘMAN, J., et al.: Elektrotechnické a telekomunikační instalace. Praha: Verlag Dashöfer, 2008. ISSN 1803-0475.

JAIN, A.; BOLLE, R.; PANKANTI, S. „Biometrics. Personal Identification in Networked Society." Norwell, Massachusetts, USA, Kluwer Academic Publisher, 1999, ISBN 0-7923-8345-1.

RAK, R.; MATYÁŠ, V.; ŘÍHA, Z. a kolektiv. „Biometrie a identita člověka ve forenzních a komerčních aplikacích." Praha, Nakladatelství Grada, 2012

Předběžný termín obhajoby

2016/17 LS – TF

Vedoucí práce

Ing. Veronika Hartová, Ph.D.

Garantující pracoviště

Katedra elektrotechniky a automatizace

Elektronicky schváleno dne 12. 1. 2016

prof. Ing. Jaromír Volf, DrSc.

Vedoucí katedry

Elektronicky schváleno dne 2. 3. 2016

prof. Ing. Vladimír Jurča, CSc.

Děkan

V Praze dne 26. 03. 2017

Prohlášení:

„Prohlašuji, že jsem bakalářskou práci na téma: Identifikace uživatele na základě rozpoznání jeho tváře vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů. Jsem si vědom, že odevzdáním bakalářské práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby. Jsem si vědom, že moje bakalářská práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí. Jsem si vědom že, na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla."

V Praze dne 30.3. 2017

……

Marek Veselý

Poděkování

Rád bych poděkoval vedoucí mé bakalářské práce Ing. Veronice Hartové, Ph.D. za cenné rady, věcné připomínky, konzultace a pomoc při tvorbě této bakalářské práce. Chtěl bych také poděkovat své rodině za podporu při studiu.

Abstrakt: Bakalářská práce se zabývá biometrickou identifikací uživatele na základě jeho tváře. První část bakalářské práce je zaměřena na vysvětlení základních pojmů v biometrii, jako je identifikace a verifikace, aby nedocházelo k jejich záměně. Další část bakalářské práce se věnuje měření výkonnosti biometrických systémů. Popsány jsou především základní výpočty chybovosti a pravděpodobnost chybného přijetí nebo odmítnutí. Dále jsou v bakalářské práci popsány jednotlivé metody pro identifikaci a lokalizaci tváře. Při popisu metod je poukázáno na jejich výhody, nedostatky a na jakém principu fungují. V další části jsou popsány příklady využití biometrické identifikace na základě tváře v praxi. Praktická část je věnována popisu jednotlivých biometrických čteček a jejich vzájemnému porovnání. Následně je na těchto zařízeních provedeno měření rychlosti identifikace uživatele, kde časový limit pro identifikaci je stanoven na 3 sekundy.

Klíčová slova: tvář, sken, identifikace, biometrie, spolehlivost

Identification of the user based on recognition of his face

Summary: This bachelor thesis deals with Identification of the user based on recognition of his face. The firs part of the bachelor thesis is focused on explanation of basic concepts of identification and verification, to avoid confusion. The next part of bachelor thesis deals with performance measurement of biometrics systems. Primarily are described False Rejection Rate and False Acceptance Rate. Next are described metods for identification and localization of the face. In description of this methods refer their benefits and weaknesses. In the next part of bachelor thesis are described examples application in practice. In practical part were chosen specific individual readers of biometrics systems. Based on their parameters and financial individual readers compared to each other. On this biometrics readers is realize measurement of speed identification user. Time limits for identification is three seconds.

Key words: face, sken, identification, biometrics, reliability

Obsah

1 Úvod

V dnešní době patří otázka bezpečnosti určitě mezi nejvíce probírané. Zvyšuje se snaha co nejlépe zabezpečit nejen svůj majetek. Velmi vysoká poptávka po zabezpečujících službách je i v státní nebo komerční sféře. Velký důraz je kladen na zabezpečení finančních budov, komplexů podniků a státních budov. Vzhledem ke zvyšující poptávce letecké dopravy lze očekávat i vyšší nároky na zabezpečení při celních kontrolách na letištích a dopravních uzlech. [3]

Na poli bezpečnosti sehrávají biometrické systémy velmi důležitou roli. Mezi nejčastěji používané systémy lze označit otisk prstů, rozpoznání tváře a také rozpoznání oční duhovky. Rozpoznávání podle tváře je lidstvem využíváno odnepaměti. Na začátku se samozřejmě nejednalo o automatizované počítačově řešené metody, ale o přirozené smyslové rozeznávání lidí a blízkých osob. Počátky počítačově automatizovaného rozpoznání tváře přišli v 60. letech 20. století. Vývoj této technologie byl závislý na pokroku ve vývoji snímací a výpočetní techniky. Největších pokroků bylo dosaženo za posledních 20 let. [1; 10]

Identifikace uživatele podle jeho tváře má v praxi velmi široké využití. Například celní kontroly, biometrické pasy, monitorování veřejných prostorů, kde systém může upozornit na zájmovou osobu, kontroly vstupů do veřejných budov atd. Praktické využití systémů je závislé kvalitě použitého zařízení a algoritmu pro rozpoznání tváře. Většina těchto aplikací je stále ve zkušebním provozu a ve fázi vývoje. [17]

2 Cíl práce

Bakalářská práce bude tematicky zaměřena na problematiku identifikace uživatele na základě rozpoznání jeho tváře. Hlavním cílem bude rozebrat jednotlivé možnosti této identifikace a její výhody a nedostatky a následně poukázat na spolehlivost těchto systémů.

Dílčí cíle bakalářské práce budou:

- Udělat charakteristiku základních pojmů v biometrii
- Popsat jednotlivé metody identifikace tváře
- Porovnat jednotlivé biometrické systémy
- Zhodnotit spolehlivost vybraných zařízení

3 Metodika

Tato práce se bude zabývat právě zmíněnou biometrickou metodou rozpoznání tváře. V teoretické části budou nejprve rozebrány základní pojmy v biometrii a výpočty chybovosti biometrických systémů.

Další část práce bude věnována popisu jednotlivých metod pro lokalizaci a rozpoznání tváře. Lokalizace a rozpoznání lidské tváře jsou důležitá pro specifikaci a určení kde přesně se daná tvář na snímku nachází. K lokalizaci a rozpoznání tváře jsou určeny porovnávací metody, které jsou založeny na vlastnostech prostředí, barvě pleti nebo pohybu tváře. Popsány budou jejich výhody, nedostatky a spolehlivost. Pro rozpoznání tváře budou dále rozebrány dosud nejvíce prozkoumané algoritmy PCA, LDA a EBMG.

Praktická část bude věnována popisu jednotlivých zařízení pro biometrickou identifikaci IFace 302, Multibio 700 a Aktion AFT 500. Jednotlivá zařízení budou porovnána a zhodnocena podle technických parametrů, které udává výrobce systémů a také podle výsledků měření. Na zařízeních bude provedeno měření rychlosti ověření uživatelů. Stanovený čas doby ověření jsou tři sekundy. Měření bude provedeno u deseti vybraných osob.

4 Přehled řešené problematiky

Pojem biometrie představuje metody měření určitých charakteristických vlastností osob. Díky těmto metodám měření je možné osoby s určitou přesností identifikovat nebo autorizovat. Mezi nejpoužívanější metody identifikace patří například: skenování otisku prstu, obraz krevního řečiště, lidský obličej, oční sítnice nebo duhovka. Biometrie při identifikaci využívá i různé vlastnosti chování. Například vlastnosti chůze, stisk kláves nebo dynamiku podpisu. [8]

Mezi nejpoužívanější metody dnes patří použití hesla nebo identifikačního čísla (PIN). Tyto metody sebou nesou riziko autorizace neoprávněnou osobou. Vzhledem k nižší bezpečnosti těchto metod, dnes dochází k implementaci silnějších nástrojů a technologií. Mezi ty bezesporu patří biometrie. [11; 8]

4.1 Historie biometrie

Podstatu biometrie využívají lidé od nepaměti. V pravěku žili lidé v malých komunitách a společenství, kde se vzájemně rozeznávali podle fyziologických rysů. Například podle vzhledu tváře nebo podle hlasu. [8; 22]

Mezi nejstarší metodu patří otisk prstu ruky. Obyvatelé Babylonu a Persie používali otisk prsu do hliněné destičky. [22]

Moderní historie biometrie se datuje až od 70. let 20. století s příchodem výpočetní techniky. Tyto technologie byly nejprve využívány pouze v kriminalistice a pro soudní praxi, avšak později se začala uplatňovat v různých kontrolních systémech u vstupů do objektů nebo budov. Byly to zejména technologie otisku prstu a identifikace struktury sítnice. Další metody jako je například identifikace pomocí DNA, duhovky nebo geometrie ruky přišli později. Metoda rozpoznání uživatele pomocí tváře patří mezi „mladší“ používané metody. [8; 22]

S obrovským vývojem a rozšiřováním výpočetní techniky v 90. letech 20. století přišel i velký rozvoj biometrických metod ověřování. V dnešní době už si lze jen těžko představit biometrickou identifikaci bez výpočetní techniky. [22]

4.2 Základní pojmy biometrie

V problematice biometrie je nezbytné vysvětlení jednotlivých základních pojmů, jelikož mají původ v anglickém jazyce a do češtiny bývají občas špatně překládány.

Verifikace - ověření

Z anglického slova verification. Při tomto procesu ověřování biometrický systém srovnává vzorek, který sejme s dříve zapsaným vzorkem tzv. šablonou neboli template. Jedná se o princip one-to-one. [2]

Rekognoskace – rozpoznávání

Z anglického slova recognition. Tímto termínem se nemusí nutně označovat identifikace ani verifikace. Při tomto procesu se rozpoznává vlastnost člověka za použití vhodné tělesné vlastnosti. [2]

Identifikace

Z anglického slova identification. Při tomto procesu se biometrický systém určuje totožnost neznámého jedince. V momentě kdy je sejmuta biometrická informace tak je porovnávána se všemi uloženými vzorky (šablonami). Jedná se o princip one-to-many. [2]

Autentizace

Z anglického slova authentication. Autentizace je pojem, který je možné sloučit s termínem rozpoznávání. Rozdíl je v tom, že při autentizaci získá uživatel určitý status např. oprávněný/neoprávněný. [2]

4.3 Měření výkonosti biometrických systémů

Momentálně se na trhu nachází velké množství zařízení pro biometrickou identifikaci, které se od sebe na první pohled neliší. Před výběrem určitého zařízení je třeba zhodnotit faktory, které nám mohou pomoci při výběru. Kritéria, podle kterých lze porovnávat jednotlivá

zařízení se mohou rozdělit na hlavní a vedlejší. Mezi vedlejší kritéria patří rychlost zpracování samotného porovnání, kapacita (počet realizovaných identifikací/verifikací za určitý časový interval), uživatelská přijatelnost, cena, spolehlivost zařízení atd. [1; 3]

Biometrická zařízení jsou především bezpečnostní systémy, proto je hlavním kritériem správné rozpoznání oprávněného uživatele a správné odmítnutí neznámé osoby. Nastávají případy, kdy může dojít k nerozpoznání osoby, která má oprávnění pro vstup. Nebo v opačném případě, kdy systém umožní přístup neznámé osobě. [1]

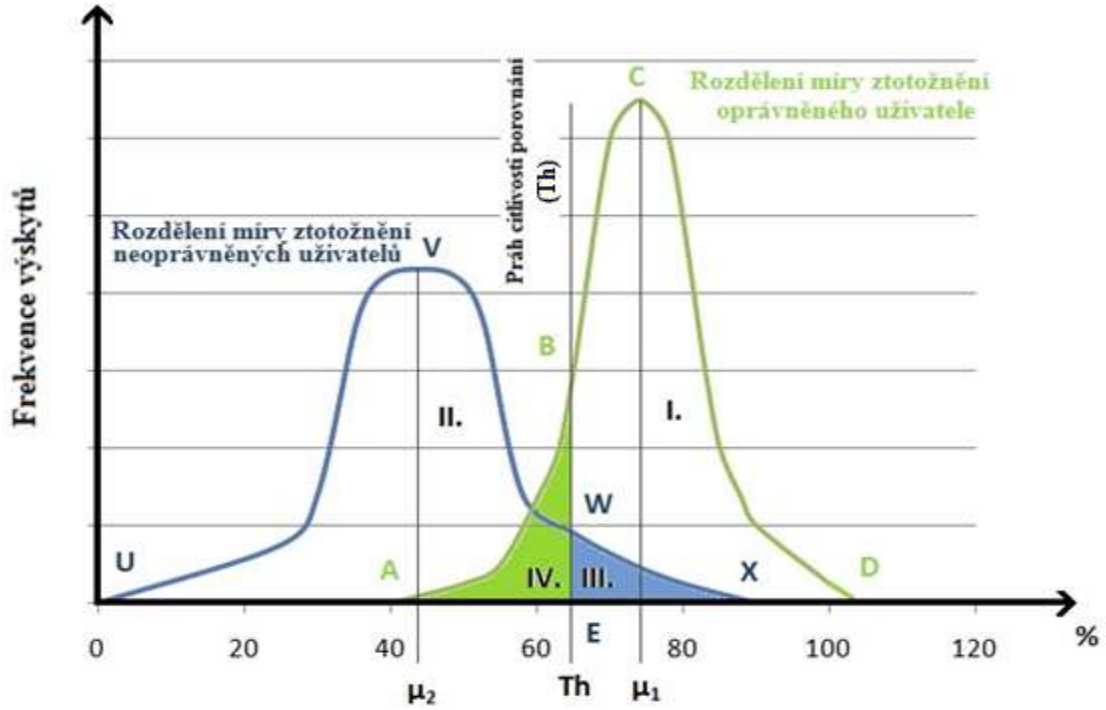
V praxi se následně pracuje s pravděpodobností těchto negativních a nežádoucích jevů. Během let byly zavedeny dva základní pojmy: [3]

- **Pravděpodobnost chybného odmítnutí** (autorizované osoby) biometrickým zařízením, v anglickém překladu **False Rejection Rate (FRR).** Lze se setkat i s pojmem **Type I Error Rate** (**chyba 1. typu**). [1]
- **Pravděpodobnost chybného přijetí** (neoprávněné osoby), v anglické literatuře označovaná jako **False Acceptance Rate (FAR)** nebo **Type II Error Rate** (**chyba 2. typu**). [1]

Biometrické metody identifikace/verifikace se statisticky vyhodnocují pomocí podobnosti biometrického vzoru a biometrické šablony. Když se snímá biometrický vzor, nejsou zaznamenány absolutně stejné hodnoty pořizovacích charakteristik. V konečném porovnání se pak obě šablony od sebe liší. [1; 2]

V praxi se postupuje tak, že pro každé zařízení je graficky zaznamenána závislost četnosti míry ztotožnění osob, u kterých je zrovna prováděna identifikace nebo verifikace. Závislosti jsou následně zaznamenány graficky (viz Obr 1.) pro dvě skupiny osob, pro které platí dvě křivky zobrazení. [1]

Obrázek 1. Výsledek porovnání - míra ztotožnění [3]



První křivka, která prochází body A, B, C, D je rozdělení četnosti výsledků porovnání jednoho uživatele, který se několikrát podrobil identifikačnímu nebo verifikačnímu procesu. Druhá křivka, která prochází body U, V, W, X značí rozdělení pokusů uživatelů, kteří nemají oprávnění a pokoušejí se dostat přes biometrickou aplikaci. [1]

V aplikaci je nastavený určitý práh citlivosti (přímka EB, kolmá na osu x), který společně s oběma křivkami rozděluje plochu do čtyř oblastí, označených I. Až IV. Když má uživatel výsledek porovnání vyšší než práh citlivosti, je aplikací přijatý a je označen jako oprávněný uživatel. V opačném případě je aplikací odmítnut a označen jako neoprávněný uživatel. [1]

- Oblast $P_{E, B, C, D, E}$ představuje korektní akceptaci oprávněného uživatele tzn. uživatel je s aplikací spokojen, protože byl rozpoznán. [1]
- Oblast $P_{U, V, W, E, U}$ představuje korektní odmítnutí neoprávněného uživatele. Uživatel je s aplikací nespokojen, protože se mu do ní nepodařilo proniknout. [1]

- $P_{W, X, E, W}$ představuje oblast nekorektního přijetí neoprávněného uživatele. Uživatel je spokojený, protože se dostal přes aplikaci. Správce aplikace je však nespokojený, protože vznikl bezpečnostní incident. [1]
- $P_{A, B, E, A}$ označuje oblast nekorektního odmítnutí oprávněného uživatele. V tomto případě se dá aplikace označit jako nespolehlivá, protože nerozpoznala uživatele. Odmítnut byl uživatel, který měl oprávnění. [1]

Míra ztotožnění biometrických vzorků rozhoduje o tom, zda je uživatel oprávněný nebo neoprávněný. [1]

4.3.1 Pravděpodobnost chybného odmítnutí (False Acceptance Rate-FAR)

FAR koeficient určuje pravděpodobnost toho, že osoba, která nemá oprávnění je přijata jako oprávněná. Velice často vznikají škody nesprávným přijetím. FAR je tedy koeficient, který nám udává míru bezpečnosti. Je označován jako chyba II. druhu. Jedná se přijetí neoprávněné osoby, která nemá za normálních podmínek přístupové oprávnění. Tato chyba se dá považovat za velmi závažnou, a to hlavně z bezpečnostního, ale i marketingového hlediska. [1; 2]

FAR je dán vztahem:

$$FAR = \frac{N_{FA}}{N_{IIA}} \times 100[\%] \quad [2]$$

N_{FA} – Počet chybných přijetí

N_{IIA} – Počet všech pokusů neoprávněných osob při identifikaci

Nesprávné přijetí může mít závažný důsledek např. v policejně-soudních aplikacích, kdy identita pachatele je chybně ztotožněna s jinou osobou. V praxi tedy může dojít k tomu, že vyšetřování se odkloní zcela jiným směrem, protože identita hledané osoby byla chybně zaměněna s jinou identitou, která vůbec nesouvisí s případem. [1]

4.3.2 Pravděpodobnost chybného odmítnutí (False Rejection Rate-FRR)

FRR koeficient určuje pravděpodobnost toho, že uživatel s oprávněním bude systémem odmítnut. Pro uživatele je nesprávné odmítnutí nepříjemné. FRR koeficient tedy vyjadřuje komfort pro uživatele. Je označován jako chyba I. druhu. Dochází k nerozpoznání registrovaného uživatele, který má za normálních okolností oprávnění k přístupu. Z hlediska bezpečnosti, není tato chyba příliš významná. Jde spíše o marketingovou nevýhodu, protože uživatel musí opakovat pokus o přístup, a to pro něj může být důvod k nespokojenosti. [2]

FRR je dán vztahem:

$$FRR = \frac{N_{FR}}{N_{EIA}} \times 100[\%] \quad [2]$$

N_{FR}- Počet chybných odmítnutí

N_{EIA}- Počet všech pokusů oprávněných osob o identifikaci

Chyby FRR a FAR mohou být vyjadřovány i poměrem např. FAR 0,01% by odpovídal poměru 1: 10 000. To znamená, že do systému by mohl být připuštěn 1 z 10 000 neoprávněných uživatelů. [2]

4.3.3 Výpočty chybovosti

Metody výpočtu FAR a FRR je možné aplikovat pouze v případech, že počty chyb se rovnají počtům pokusů. V případě, že se počty pokusů a chyb nerovnají je zapotřebí spočítat u každé osoby její osobní chybovost. Pro přesnější výpočty chyb se uvádějí další metody. [2]

Failure to Enroll Rate (FTE nebo FER)

Jedná se o případ, kdy se nedaří uživatele zaregistrovat do biometrického systému. Uživatel nemůže být zaregistrován, pokud má tělesné (chybějící prsty) nebo smyslové postižení. Tato veličina je pohyblivá a vztahuje se jak k osobě, tak i ke snímané biometrické

vlastnosti. Poté můžeme určit i tzv. FER (Personal FER), který udává vztah uživatele a jeho biometrické vlastnosti ve snímacím procesu. V momentě, kdy je uživateli správně sejmuta jeho biometrická vlastnost, ale systém ho chybně vyhodnotí i po mnoha verifikačních nebo identifikačních pokusech, jedná se o tzv. Koeficient selhání přístupu FTA (Failure to Acquire). [2; 3]

Abychom zajistili správné statistické hodnoty, je zapotřebí provést mnoho pokusů sejmutí biometrické vlastnosti. Vzorec pro výpočet pravděpodobnosti nesprávného sejmutí vlastnosti konkrétní osoby je následující:

$$FER(n) = \frac{počet\ neúspěšných\ pokusů\ o\ zápis\ u\ 1\ osoby\ n}{celkový\ počet\ pokusů o\ zápis\ u\ 1\ osoby\ n}$$ [2]

Lepší hodnoty budou vycházet, když bude provedeno víc pokusů. Vzorec je pak definován jako průměr z FER(n) následně:

$$FER = \frac{1}{N} \times \sum_{n=1}^{N} FER(n)$$ [2]

False Identification Rate (FIR)

Pomocí FIR koeficientu můžeme určit, jaká je pravděpodobnost špatného přiřazení biometrické vlastnosti k vzorku při procesu identifikace. [2]

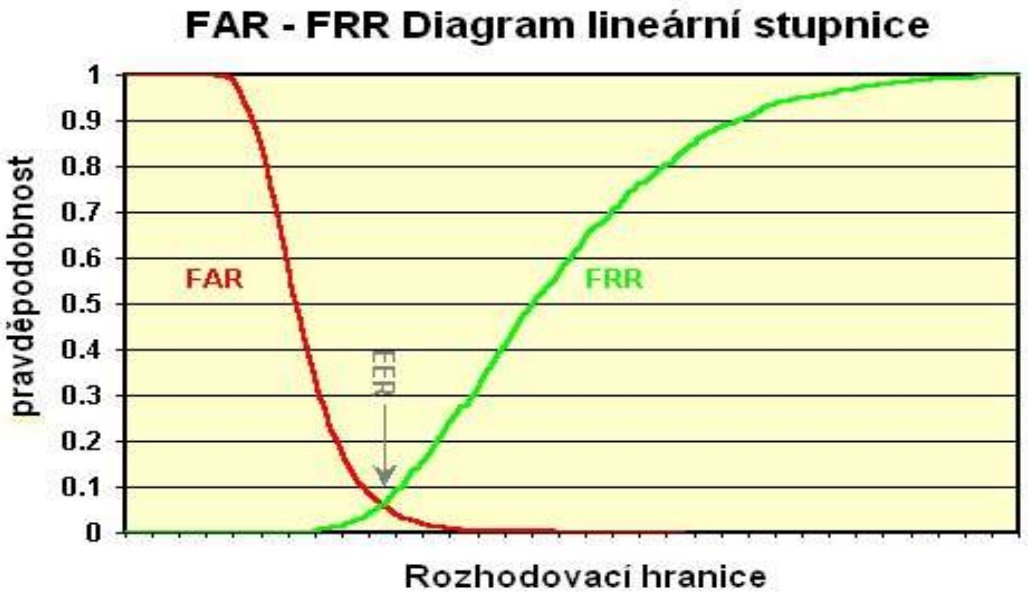
False Match Rate (FMR)

Koeficient FIR určuje poměr osob, které jsou nesprávně rozpoznány. Tedy neoprávněné jsou systémem rozpoznány jako osoby s oprávněním. Rozdíl mezi koeficientem FAR a FMR je v tom, že do FMR se nezahrnuje odmítnutí kvůli horší kvalitě snímaného obrazu. Koeficienty FAR a FRR tedy zhoršují nesprávně rozpoznané biometrické vlastnosti. [2]

Křížový koeficient ERR

Důležitý koeficient, který určuje pravděpodobnost, při jakém nastavení rozhodovací hranice nastane jev FFR a FAR současně (FFR=FAR). Tento koeficient je také velmi důležitý při nastavování citlivosti systému. V momentě kdy je v rovnováze FRR a FAR koeficient je v rovnováze i nastavení systému. Z diagramu vyplývá, že posunutím hranice doleva nebo doprava lze činit systém více bezpečný nebo více uživatelsky komfortní (viz Obr. 2). [2;3]

Obrázek 2. FAR-FRR Diagram [3]



4.3.4 Zvyšování bezpečnosti biometrických systémů

Vzhledem k tomu, že biometrické aplikace pracují s určitou chybovostí, je zapotřebí zvyšovat jejich bezpečnost. V dnešní době se navíc pachatelé trestných činů pokouší napadat jak přístupové systémy (PIN), tak i biometrické systémy. [2; 3]

Jsou známy pokusy překonání biometrických systémů např. plastickými operacemi obličeje, což může být velmi nebezpečné pro bezpečnostní přístupové systémy tak i pro forenzní identifikace. [2]

Bezpečnost biometrických systémů lze zvýšit tzv. Multiple Biometric, neboli vícenásobnou biometrií. Jedná se o kombinaci nejméně dvou biometrických technologií v jednom systému. Nejčastěji se můžeme setkat s kombinací identifikace podle geometrie

obličeje (2D, 3D) a otisků prstů. Od roku 2008 jsou všechny členské státy EU povinny zadávat biometrické prvky (identifikace obličeje a otisk prstu) do všech nově vydaných cestovních pasů. [7; 14]

4.4 Rozpoznání tváře

V dnešní době je verifikace tváře velmi zkoumanou metodou, protože problematika této technologie je velmi rozsáhlá. Metoda je založena na porovnání obrazu, který je sejmut kamerou s uloženým obrazem v centrální databázi. V obličeji se vyhledávají v jednotlivých krocích detekce hlavní rysy (poloha nosu, úst a očí). Následně se detekuje poloha obočí, uší, rtů atd. Porovnání se realizuje na základě vzdáleností mezi jednotlivými body, přičemž jsou využívány toleranční limity. Modelů rozpoznávání však existuje mnoho. [8; 23]

Tvář představuje jednu z mnoha biometrií, kterou je možné použít k rozpoznání osob. Poskytuje vysokou škálovatelnost a také je výborně akceptována uživateli. Jedním z důvodů této široké akceptace může být přirozenost rozpoznání na základě tváře, případně nízký strach z možného zneužití. Také je důležitá skutečnost, že při skenování nedochází k přímému kontaktu s osobou ani jiným nežádoucím jevem. Porovnání vlastností jednotlivých biometrií je zobrazeno v tabulce 1.1. [5; 25]

Tabulka 1. Porovnání vlastností jednotlivých biometrií [8]

	Tvář (3D)	**Otisk prstu**	**Duhovka**
Univerzálnost	vysoká	střední	vysoká
Jedinečnost	střední	vysoká	vysoká
Výkonost	nízká	vysoká	vysoká
Akceptace	vysoká	střední	nízká
Bezpečnost	střední	vysoká	vysoká
Konstantnost	střední	vysoká	vysoká

4.4.1 Metody detekce a lokalizace tváře

Pro nalezení zvolené tváře v reálné scéně je zapotřebí vytvořit počítačový model této tváře a následně ho porovnat s každým objektem na scéně, u kterého je vypočítána jeho podobnost. Po srovnání počítačového modelu tváře s objektem na scéně je vyhodnoceno, zda se jedná o objekt představující lidskou tvář. Zároveň je vypočítávána pozice tváře na scéně. Detekce a lokalizace tváře lze z matematického modelování rozdělit na dva základní typy: [4; 23]

- **Statisticky orientované metody**
  - Metoda podprostoru
  - Metoda neuronových sítí

- **Znalostní metody**
  - Metody založené na rozložení odstínu šedi v obraze
  - Metody založené na rozpoznání obličejových kontur
  - Metody založené na informaci o barvách
  - Metody založené na symetrii

Metoda podprostoru

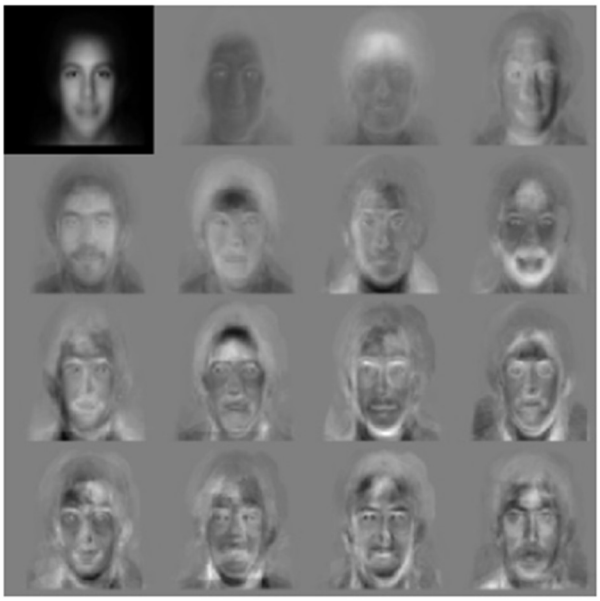
Pomocí této metody je možné nalézt v obrazu tváře obecné a zároveň výrazné charakteristiky (nos, ústa, oči atd.) typické pro lidský obličej. V případě, že v obraze nalezneme tyto charakteristiky, můžeme prohlásit, že vyhodnocený obraz je obrazem tváře. [1]

U této metody se v praxi využívá Karhumen-Ločve transformace, která je známější pod pojmem eigenface neboli normalizovaný obraz tváře. Obraz je normalizován, pokud je změněno měřítko a jsou nalezeny a nastaveny specifické body, které určují prostorovou orientaci tváře (např. oči). Normalizace zahrnuje i šedé odstíny obrazu. Normalizované

rozdělení šedých odstínů obrazů je prováděno globálně (v celém obrazu), i lokálně. Normalizaci podléhá i standardizované nastavení jasu. [1; 9]

Počítačová aplikace tedy využívá normalizované tváře jako množinu identifikačních charakteristik pro identifikaci nebo verifikaci osob na základě jejich tváří. Jedna osoba má v databázi zpravidla uloženo více normalizovaných tváří, které odrážejí její momentální stavy (viz. Obr 3). [1]

Obrázek 3. Rozložení normalizovaných tváří [1]



Metoda založená na rozpoznání obličejových kontur

Rozpoznání pomocí kontur obličeje je další metodou, která využívá charakteristické znaky lidské tváře. Kontury (obrysy) hlavy tedy slouží detekování hranic obličeje. V častých případech, ale není zajištěna korektní detekce hran tváře, protože algoritmy, které jsou v současné době využívány jsou do jisté míry omezené. Proto dochází ke kombinaci s jinými přístupy lokalizace tváře. K detekci kontur lze využít metodu energetických křivek. V odborné literatuře známá jako metoda snakes neboli „hady“. [1; 9]

Proces detekce probíhá tak, že se křivky (hady) přikládají na jednotlivé snímky. Vlivem vnitřních a vnějších sil obrazu se křivky deformují. Vnitřní síly obrazu se tvoří při počátečním přiložení křivek. Křivka se při procesu tvaruje k hranám objektu, tedy do pozic kde je nejmenší celková energie. [3]

Metoda založená na rozložení odstínů šedi v obraze

I když ve skutečnosti existují velké rozdíly vzhledů tváří různých osob, je možné stanovit určitá pravidla pro rozložení šedých odstínů v obraze za normálních světelných podmínek. Například v oblasti, kde se nachází oči, jsou odstíny vždy tmavší než v oblasti čela. Tato metoda je poměrně efektivní a v praxi často využívána. [3]

Ze skupiny metod je nejznámější mozaiková metoda, protože je dostatečně spolehlivá, i když je oblast obličeje málo výrazná. Metoda funguje na principu přirozeného rozpoznání obličeje lidským mozkem. Oblast, která je zpracována se dělí do obrazových bloků ve čtvercové síti 4×4 (viz Obr. 4). Do těchto bloků jsou pak rozděleny oči, ústa, líce, nos atd. Jestliže se ve zpracovaném obraze nachází tvář, potom lze nalézt identifikační charakteristiky obličeje (ústa, oči, nos, líce), které by měly odpovídat pravidlům rozložení šedých odstínů. Jednotlivé bloky jsou postupně zkoumány, jestli se v nich nachází hledané charakteristiky. Obrazové bloky, které nevyhovují těmto pravidlům, jsou vyřazeny a nejsou dále zpracovány. Bloky, které vyhovují, se dělí stejným způsobem do detailnějších bloků v rozlišení 8×8. Konečná pozice charakteristik (očí, úst, nosu, atd.) se určuje pomocí metod detekce hran. [3; 8]

Obrázek 4. Mozaiková metoda [1]

Nevýhodou této metody je pomalé zpracování obrazu, a proto se kombinuje s jinými metodami, které připravují obraz před aplikací mozaikové metody. [1]

Metoda založená na informaci o barvách

Lokalizace tváře pomocí této metody je další často využívanou metodou nejen díky své rychlosti rozpoznávání. Ačkoliv je na světě několik etnických ras a každý lidský jedinec má rozdílnou barvu kůže, lze definovat určitou podobnost z hlediska počítačového vidění (viz Obr. 5). Tato podobnost umožnuje detekovat všechny skupiny. [3]

Obrázek 5. Detekce tváře pomocí barvy kůže [3]

U této metody je velmi důležité pozadí při verifikaci. V případě využití této metody například u celních kontrol nebo při vstupu do budovy kde jsou statické kamery, lze připravit ideální pozadí pro verifikaci obličeje. Problém nastává při špatných světelných podmínkách, což je případ dynamického snímání nejen venkovních prostorů. Proto se tato metoda kombinuje s jinými algoritmy. Výhodou této metody je nezávislost na natočení hlavy vůči kameře. [1; 3]

4.4.2 Kombinace metod pro lokalizaci a detekci tváře

Lokalizace a detekce tváře pouze jednou metodou je celkově složitou úlohou a málokdy získáme uspokojivý výsledek. Proto v praxi dochází ke kombinaci různých metod pro lokalizaci tváře. Kombinací metod je možné eliminovat nedostatky, které se projevují pomalým časem lokalizace nebo falešnou detekcí. Účelný způsob, jak zajistit vyšší efektivnost detekce a lokalizace tváře i celkovou produktivitu je vytvoření ideálního pozadí scény při snímání tváře. [1]

4.4.3 Metody rozpoznání tváře

Při procesu rozpoznání tváře je cílem nelézt rozdílnost v každém obličeji na scéně. K verifikaci nebo identifikaci jsou právě tyto rozdílnosti používány. Rozpoznání tváře se provádí získáním identifikačních charakteristik a jejich následným porovnáním s charakteristikami známé osoby, která je uložena v databázi. K rozpoznání tváře je možné použití těchto metod: [4]

- Metoda odstínů šedi v obraze
- Metoda geometrických tvarů a identifikačních charakteristik
- Metoda optických toků
- Metoda deformačních modelů
- Metoda neuronových sítí

Metoda odstínů šedi v obraze

Tato metoda je kromě lokalizace tváře využívána i při jejím rozpoznání. Princip spočívá v rozložení obrazu neznámé osoby do jednotlivých segmentů (geometrických bloků) mozaiky. U záznamu známé tváře v databázi se provede stejný proces. V další fázi dochází k porovnání segmentů obrazu známé a neznámé tváře. Následně je zkoumáno bezprostřední okolí mezi dvojicí porovnávaných segmentů. V konečné fázi následuje proces rozhodování, zda obraz neznámé a známé tváře patří jedné osobě. Dochází tedy k postupnému vyhodnocování všech obrazů, které jsou uloženy v databázi, dokud není nalezena shoda mezi záznamy obrazů. V okamžiku, kdy je shoda nalezena je osoba identifikovaná nebo verifikovaná. [1; 3]

Vzhledem k tomu, že se porovnávají jednotlivé segmenty neznámého obrazu se segmenty velkého množství obrazů, je tato metoda výpočetně velmi náročná. Při tomto porovnání je navíc zkoumáno i okolí segmentů. Úspěšnost identifikace nebo verifikace u této metody je závislá na počtu registrovaných tváří v databázi. [1]

Metoda geometrických tvarů a identifikačních charakteristik

Metoda vychází z definovaných geometrických charakteristik, které byly určeny člověkem. Tyto charakteristiky vycházejí z antropologických poznatků a následné detekci geometrických rysů v obličeji. Jedná se o charakteristiky určené úhly a vzdáleností mezi identifikačními markanty. Jedná se o vnější horizontální body rtů, bod spodní hrany nosu, přechodový bod nosu a čela a vnější koutky očí. [1; 3]

V odborné literatuře se lze setkat s různými metodami pro konkrétní charakteristiky lidské tváře. Někteří specialisté na umělou inteligenci nebo matematici se zabývají například jenom obrysem tváře, případně ústy, nosem nebo jenom očima. Avšak všechny metody mají v automatizované praxi několik problémů: [1]

- Při nízké kvalitě obrazu, nízkém stupni rozlišení nebo při špatných světelných podmínkách se velmi snižuje spolehlivost automatické detekce
- Při natočení tváře nemusí být viděny všechny identifikační body a pro počítačové zpracování je jich nedostatek
- Složité vyjádření spolehlivosti a přesnosti měření těchto antropologických charakteristik

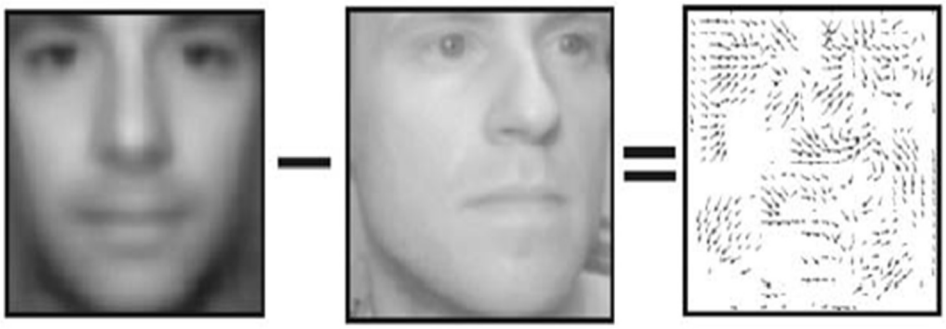
Metoda optických toků

Princip této metody je založen na postupném snímání sekvence snímků pohybu hlavy jedné osoby. Při analýze dvojic sekvenčních snímků, se pozoruje, zda dochází k dynamickým změnám. Jedná se o změny světelné intenzity mezi body a zároveň se analyzuje pohyb těchto bodů. Všechny body mají svůj směr pohybu, a proto je lze vyjádřit vektorově. Jednotlivé snímky tedy podléhají změnám: [1; 16]

- Texturálním (změny intenzity)
- Strukturálním (prostorové změny)

Mezi dvojicí snímků je možné definovat rozdíly, které jsou vyjádřeny za pomoci optických toků neboli optic flow (viz Obr. 6). Optickými toky lze také určit výraz a charakter tváře. Typické využití této metody se uplatňuje pro rozpoznání emocí. V současné době toto automatizované využití intenzivně testuje. [1; 16]

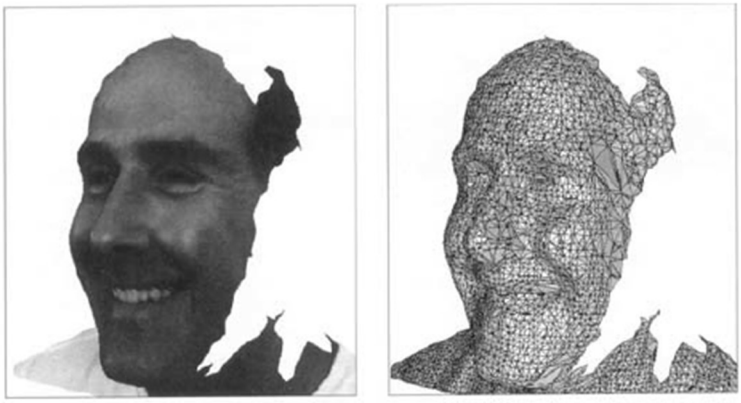
Obrázek 6. Dvojice snímků a výsledný optický tok [1]



Metoda deformačních modelů

Tuto metodu si lze představit jako 3D model tváře, který je pokrytý rovnoměrnou sítí s určitou elasticitou. Síť je tvořena horizontálními a vertikálními čarami. Když je síť přiložena na povrch tváře, dochází k jejímu zakřivení. Podle hustoty čar je možné rozpoznat určité charakteristiky a rysy tváře. Reálnou tvář lze tedy vyjádřit síťovým modelem, který obepíná povrch tváře (viz obr. 7). V momentě kdy se mění výraz tváře, začnou se zakřivovat síťové čáry. [4; 16]

Obrázek 7. Tvář vyjádřena síťovým modelem [1]



Identifikace nebo verifikace obrazu tváří je tedy prováděna porovnáním dvou 3D zakřivených síťových povrchů. V důsledku změny tváře například vyvoláním různých emocí, se zároveň mění i povrch tváře. Ke změnám tedy dochází i u grafického modelu. [17]

Pro každého jedince jsou tedy definovány určité změny 3D modelu, které ho charakterizují. Všechny změny na grafickém modelu, je třeba postupně analyzovat a vyhodnotit, aby v průběhu identifikace nebo verifikace nedošlo k chybnému určení osoby. [1]

Metoda neuronových sítí

V odborné literatuře se můžeme také setkat s názvem Artifacial Neural Networks – ANN. Díky vlastnostem, které neuronové sítě využívají je tato metoda oproti ostatním značně zvýhodněna. Základní vlastnost neuronových sítí je „učit se“. Většina metod funguje podle přesně stanoveného algoritmu. V praxi, ale nastává velké množství různých situací, kdy je zapotřebí zvolit vždy jiný algoritmus, který bude v dané chvíli nejvíce efektivní. V některých situacích nastává problém, že programy pracují s nekvalitními nebo neúplnými daty, které jsou v daný moment jedinou dostupnou informací. Jako správné řešení těchto problémů by mohlo být právě použití metod neuronových sítí. [13; 15]

V umělé inteligenci je neuronová síť jedním z výpočetních modelů. Jako vzor slouží chování biologických neuronů v lidském mozku. Neurony jsou navzájem propojeny a vzájemně si předávají signály a pomocí přenosových funkcí dochází k jejich transformaci. Každý neuron má pouze jeden výstup a libovolný počet vstupů. [10; 15]

Neuron je jednotka, kterou lze ohodnotit a vynásobit všechny vstupy jejich vahami. Váhy neuronu se během učení mění, tedy dokáže se adaptovat. Neuron poté všechny získané jednotky sečte. Konečná hodnota se dosazuje do přenosové funkce neuronu, kde výstup funkce je zároveň výstup neuronu, který plní funkci vstupu do dalších neuronů. [10]

4.4.4 Další techniky rozpoznání tváře

Mimo metody, které jsou uvedeny a popsány v předchozí kapitole, existují ještě algoritmy, které se dají pro jednotlivé postupy využít. Mezi nejvíce studované a prozkoumané algoritmy pro rozpoznání tváře patří zejména: [4]

- PCA (Analýza hlavních částí)
- LDA (Lineární diskriminační analýza)
- EBGM (Elastický srovnávací diagram)

Analýza hlavních částí – PCA

Tento algoritmus byl poprvé popsán v roce 1991 matematiky Matthew Turkem a Alexem Pentlandem. Metoda PCA se stala základem pro ostatní metody. Mnoho metod používá tento algoritmus v kombinaci s jinými algoritmy pro dosažení lepších výsledků. Vzhledem k tomu, že tento algoritmus využívá automatizovanou extrakci základních rysů, je možné využití u velkých datových kolekcí. [3]

Jedná se o algoritmus, který prezentuje lidskou tvář lineární transformací z průměrné nebo původní tváře. Všechny snímky tváře v databázi jsou zprůměrovány v jeden obličej. Zprůměrovaný obličej je následně převeden na normalizovanou tvář neboli eigenface. [3]

Lineární diskriminační analýza – LDA

Podobně jako metoda PCA pracuje ve vektorové oblasti. Zaměřuje se na body ve vektorovém prostoru, které rozděluje do více skupin. Členění se uskutečňuje za pomoci diskriminačních funkcí. Kategorie zvolených bodů se od sebe musí lišit a zároveň by měli být rozdíly co největší. V každé kategorii jsou naopak rozdíly co nejmenší. Prakticky tedy vznikají třídy různých typů obličejů a v každé třídě jsou si obličeje velmi podobné (viz obr. 8). [2; 5]

Lineární diskriminační funkce je jedna z nejprozkoumanějších a nejpřesnějších lineárních metod. Algoritmus pracuje s charakteristickými znaky skupin, z kterých statisticky vyčleňuje obrazy v souladu do jednotlivých tříd. [3; 5]

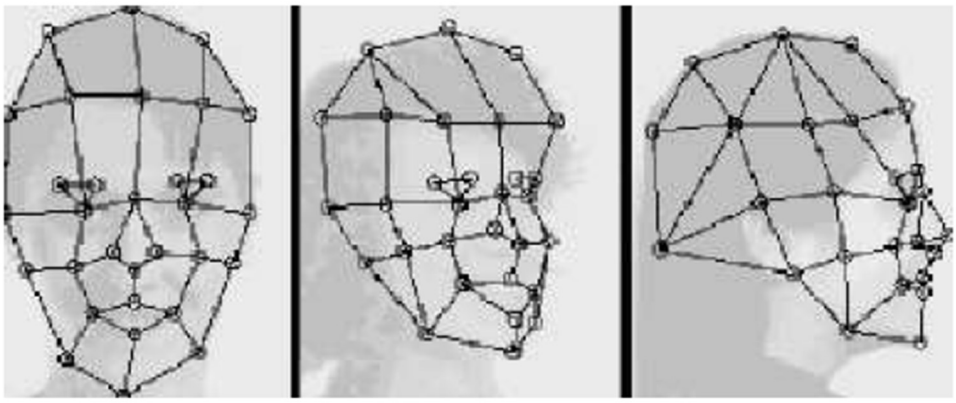
Obrázek 8. Metoda LDA [3]

Elastický srovnávací diagram – EBGM

Zatímco dva předchozí algoritmy využívají lineární charakteristiky, EBGM může reagovat na nelineární podněty. Nelineárními podněty jsou například natočení hlavy, výrazy ve tváři nebo osvětlení tváře. Princip této metody je založen na definování uzlových bodů na obličeji a jejich spojením, které vytvoří elastickou síť (viz obr. 9). Po přiložení na model obličeje, se síť začne deformovat. [17]

Při každé změně výrazu tváře, nejčastěji v oblasti úst, dochází ke změně odstínů šedi a mění se geometrie sítě. Síť, ale nadále kopíruje tvary a křivky obličeje. U této metody se může vyskytovat problém s definováním významných markantů obličeje jako je nos, oči a ústa. Tyto problémy naopak eliminují metody PCA a LDA, které se s metodou EBGM kombinují. [2]

Obrázek 9. Síť vytvořena elastickým mapováním [10]



4.5 Využití v praxi

Jak již bylo řečeno v předchozí kapitole, identifikace pomocí rozpoznání tváře se řadí mezi mladší metody. Velkým zlomem v poptávce a vývoji verifikaci tváře byl teroristický útok ze dne 11.9. 2001. Hlavním důvodem tedy bylo zvýšit bezpečnost hlavně v letecké dopravě a také celní kontroly, které jsou s leteckým provozem úzce spjaté. Dále také zlepšení bezpečnosti státních i soukromých budov a mapování veřejných prostor před vandalismem nebo zločinci. V těchto bezpečnostních opatřeních by metoda rozpoznání obličeje mohla hrát velmi významnou roli. V porovnání s ostatními metodami má rozpoznání obličeje několik výhod, ale zatím i nedostatků. Hlavním nedostatkem je úspěšnost nebo neúspěšnost verifikace. Přestože někteří výrobci udávají úspěšnost i 90 %.V konečném součtu všech systémů není zdaleka tak vysoká. Ukazuje se, že vhodným řešením by mohlo být skloubení této technologie s jinými bezpečnostními prvky jako například použití čipových karet nebo hesel. [3; 4]

Hlavním aspektem, podle kterého by se v budoucnosti měla upřednostňovat verifikace tváře je jednoznačně pasivní charakter sytému. V dnešní době je velmi oblíbené bezkontaktní a rychlé snímání, což tato technologie umožňuje. Otisk prstu má mnoho lidí spojený s kriminální policií (zanechání otisku a jeho zneužití). Mnoho lidí má strach z metody oční sítnice (poškození zraku při snímání sítnice). Z hlediska akceptovatelnosti tedy metoda rozpoznání obličeje vychází velice dobře. [3; 24]

4.5.1 Celní kontroly

V současné době je svět vystaven stálým hrozbám teroristickým útokům a nelegální migrace osob po celém světě. Je to spojeno převážně s leteckou dopravou a současnou globalizací. Pro zamezení páchání trestné činnosti jsou hlavním preventivním opatřením celní kontroly. Požadavkům na vyšší bezpečnost, spolehlivou identifikaci a rychlost odbavení může velkou mírou přispět právě biometrická identifikace tváře. [3]

Biometrické metody pro bezpečnostní kontroly na letištích jsou zatím převážně využívány menšími skupinami osob. Identifikaci využívají hlavně zaměstnanci leteckých společností nebo cestující (prominentní klienti, diplomaté atd.) pro urychlení odbavovacího procesu (viz obr. 10). [1]

Obrázek 10. Kontrola pasů na letišti [21]

Mnoho letišť po celém světě využívá identifikaci podle tváře při kontrole zaměstnanců nebo leteckého personálu. Systém tzv. „SmartGate“ využívá od roku 2003 letiště v Sydney pro bezpečnost palubního provozu a letiště na Novém Zélandu pro migrační kontroly. Od roku 2002 kdy byl poprvé použit automatický biometrický systém, došlo k dalšímu rozmachu této technologie. Letiště v Lyonu poprvé použilo metodu 3D rozpoznání tváře v roce 2006 pro identifikaci pilotů a zaměstnanců s přístupem na přistávací dráhu. Tuto technologii využívá id roku 2010 i letiště v Moskvě. [4; 13]

Rozpoznání tváří pomáhá řešit i problém s odcizováním zavazadel. Při odkládání zavazadel jsou pořizovány snímky majitelů. Tváře majitelů jsou pak porovnány s těmi, co zavazadlo vyzvednou. Spolehlivě lze takto identifikovat i početnější skupiny se zavazadly. Podobným způsobem je možné zabezpečit přístup do velkokapacitních garáží proti odcizení vozidla v době, kdy majitel odcestoval. Do garáží mají povolení vstupu pouze řidičům vozidel, jejich rodinným příslušníkům a personálu garáží. Zabezpečení letištních prostor tedy může být velmi komplexní (viz obr. 11). [4; 13]

Obrázek 11. Komplexní pohled na zabezpečení letištních prostorů [1]

4.5.2 Bezpečnostní aplikace

Biometrická identifikace tváře přinesla do policejně – forenzní a bezpečnostní praxe zcela nový způsob, který velmi ovlivnil způsob práce. Ke zpracování obrazu dochází ve dvou rovinách:

- Zpracování statického obrazu
- Dynamické monitorování scény

Zpracování statického obrazu

V minulosti probíhalo vyhledání snímku, podoby, portrétu či skici dané osoby manuálně. Zpracování bylo realizováno experty, kteří prohledávali jeden záznam za druhým. V současnosti je toto vyhledávání plně automatizováno. [1]

Pokročilé technologie vyhodnocování podle tváře v principu a nelze je proto prezentovat triviálním způsobem. Algoritmicky složité aplikace jsou pro policisty nebo soudní znalce

v podstatě černou skříňkou. V důsledku toho dochází k nedůvěře k těmto technologiím nebo k jejich systematickému odmítání. Řešením těchto problémů by mohlo být prokázání spolehlivosti ve velkém množství správně vyřešených případů. Velmi významnou roli má i certifikace a standardizace. Softwarové řešení vyhledávání v databázích zrychluje a zefektivňuje manuální postupy. [6]

Lze předpokládat, že využití rozpoznání tváře v budoucnu pomohou prvky umělé inteligence. [14]

Dynamické monitorování scény

V bezpečnostní a policejně – soudní praxi je dynamické monitorování scény běžným řešením. Ve většině měst jsou instalovány tyto kamerové systémy, které slouží především k udržení pořádku před výtržníky nebo například k monitorování dopravních situací. Vyhodnocování a sledování situace na kamerách provádí personál na dispečinku. Kamerový systém v kombinaci se softwarovými prostředky na rozpoznání tváře se ovšem stává zcela novým nástrojem. Aplikace pro dynamické monitorování scén je velmi se vyvíjející se oblastí. [3; 6]

Kombinace aplikací pro rozpoznání tváře s kamerovými systémy mají široké spektrum využití. Jednou z možností využití je monitorování dopravních uzlů, jako jsou letiště, nádraží atd. Větší efektivnosti monitorování lze docílit vhodným umístěním například na místa, jako jsou schodiště, turnikety nebo eskalátory (viz obr. 11). [12]

Obrázek 12. Monitorování veřejných prostorů [3]

Další možností využití aplikace rozpoznání tváře při dynamicky snímané scéně je monitorování davu při sportovních zápasech nebo jiných hromadných shromážděních jako jsou například demonstrace. Tyto akce jsou velmi často spojeny s problémovými osobami, které často porušují zákon. Pro zamezení páchání další trestné činnosti je třeba problémové osoby identifikovat. Anglický fotbalový klub PSC Eindhoven již využívá identifikaci problémových fanoušků pomocí kamery několik let. [14]

4.5.3 Ochrana veřejných a komerčních budov

Jedná se zejména o instituce, které kladou vysoké nároky na bezpečnost. Mezi takové patří například banky, pojišťovny, finanční instituce nebo kasina a hotely. Bezpečnost se řeší jak k zaměstnancům a klientům tak i k návštěvníkům. Zaměstnanci mohou být prověřováni pro povolení vstupu na místa pracoviště jako jsou například trezorové místnosti, pokladny, archivy, kanceláře (viz obr. 13). Mohou být prověřováni i klienti a zákazníci. [3; 12]

Obrázek 13. Kontrola vstupů na pracoviště [16]

Typickým příkladem je kontrola v kasinech a hernách. Kamerový systém s propojením aplikace pro rozpoznání tváře okamžitě informuje personál na výskyt falešných hráčů. Většina kasin spolu vzájemně spolupracují a předávají si tedy i informace o nežádoucích klientech. Navštíví-li osoba jiný podnik, personál je automaticky upozorněn systémem. [16]

Dalším příkladem jsou hotely, které tyto systémy využívají nejen pro bezpečnostní opatření. Dalším využitím je rozpoznání tváře například stálého nebo prominentního zákazníka a upozornění personálu na recepci. Aplikace tedy upozorní personál na recepci, že vstupuje

pravidelný host. Obsluze se zobrazí veškeré potřebné informace o zákazníkovi a jeho nejčastější požadavky. Aby byl host zaveden do databáze, musí být seznámen s tímto systémem a následně k tomu potvrdit souhlas. V tomto případě se nejedná o bezpečnostní aplikaci, ale o další využití, které může být užitečné z hlediska komfortu zákazníků. [16]

U těchto výše zmíněných oblastí použití verifikace obličeje je možné v budoucnu očekávat velký nárůst nasazení. Plnému nasazení momentálně brání fakt, že systémy nejsou propracované k plné spolehlivosti. V minulosti se vyskytli případy, kdy byla přes bezpečnostní systém vpuštěna osoba bez oprávnění vstupu. V některých případech tyto chyby nemusí způsobit větší ohrožení, ale pro spolehlivost a vnímání veřejností jsou tyto incidenty zcela nepřijatelné. [3]

4.5.4 Platební karty a doklady

V mikročipu platebních karet je uložena biometrická předloha majitele. V bankomatu je umístěna kamera, která snímá tvář. Sejmutá tvář je následně porovnána se vzorem tváře (biometrickou předlohou v mikročipu). K porovnání dochází přímo mezi kartou a bankomatem, zatímco se uživatel přihlašuje do systému. Tato aplikace zatím není plně zavedena, protože se stále analyzuje, zda by splnila všechny bezpečnostní kritéria. [1]

V případě vydání nového dokladu se například v USA využívá identifikace totožnosti osob podle rozpoznání tváře. Důvodem je zamezení ilegálnímu vydání dokladů. Tvář osoby, které je vydáván doklad se porovnává se snímky v databázi. Dochází k porovnání všech šablon tváří a zjišťuje se, zda má být této osobě doklad vydán. [3]

Fotografie řidičského průkazu se v současné době využívá pro přezkoumání rychlostních přestupků, které jsou zaznamenány kamerovým systémem. Systém využívá dvou kamer, kdy jedna kamera vyfotí vozidlo a SPZ a druhá pořizuje snímky obličeje řidiče. Dle snímku, lze potom dopátrat, kdo automobil řídil. [3]

4.5.5 Autentizace přístupu do výpočetní techniky

Do podvědomí uživatelů se tato aplikace dostala hlavně díky bezpečnostnímu přihlašování do notebooků. Dříve se k přihlašování využívala hesla nebo piny a později přišla biometrická identifikace otisku prstu. Nyní se rozšiřuje i již zmíněná aplikace verifikace obličeje. Webovou kamerou v notebooku při přihlašování porovnává šablonu uložené tváře

s osobou před monitorem. Tato možnost přihlašování do výpočetní techniky, ale nevzbudila příliš pozitivní ohlasy. [16]

U většiny případů nebyl instalovaný software příliš spolehlivý. Problémová byla především změna osvětlení při přihlašování, kdy byl uživatel s oprávněním vyhodnocen jako osoba neznámá. V některých případech bylo možné přihlášení i pomocí kvalitní fotografie. Z bezpečnostního hlediska tedy tyto systémy přihlašování nesplnily očekávání. [14; 24]

5 Praktická část práce

Praktická část se bude zabývat popisem a porovnáním třech biometrických čteček. Na čtečkách bude provedeno měření rychlosti identifikace u deseti osob. Následně budou provedeny výpočty pravděpodobnosti chybného přijetí.

5.1 Popis čtečky IFace 302

Jedná se o systém kontroly a evidence docházky (viz obr. 14), kde identifikace probíhá zadáním vlastního PIN kódu, přiložením čipové karty, skenem biometrických údajů nebo kombinací těchto metod. [20]

Zařízení obsahuje procesor o frekvenci 630 MHz a infračervenou kameru, která slouží k identifikaci uživatele i v mírně tmavém prostředí. K ovládání zařízení slouží 4,3“ TFT dotyková obrazovka. Zařízení je vybaveno komunikačním rozhraním RS232/485, TCP/IP, WiFi nebo GPRS. Je tedy možné i bezdrátové připojení. Pro přechodnou dobu výpadku proudu je vestavěna baterie s kapacitou 2000 mAh pro udržení zařízení v chodu. Do čtečky je integrován infračervený optický systém pro rozpoznání uživatele v tmavém prostředí. [20]

Toto zařízení disponuje i funkcí webserver, díky které je možné vzdálená správa systému pomocí internetového prohlížeče. Zařízení má maximální kapacitu 10000 záznamů. Z toho je možné zaznamenat 400 skenů obličeje a 5000 otisků prstů. Na čtečku lze připojit elektrický zámek, dveřní senzor, alarm a odchodové tlačítko. Zařízení je tedy vhodné použít při způsobu kdy je do zařízení narolováno velké množství uživatelů, kteří se potom identifikují podle nalezených shod. Výrobce udává rychlost verifikace nižší než dvě sekundy. Je zde použit algoritmus ZKFace 5.0, tedy starší verze než u čtečky Multibio 700. [18]

Obrázek 14. Čtečka IFace 302 [19]

5.2 Popis čtečky Multibio 700

Tato čtečka (viz obr. 15) umožňuje identifikaci uživatele na základě jednotlivých biometrických charakteristik, jako je otisk prstu nebo tvář. Pro identifikaci vyžívá základní rysy tváře (velikost očí a jejich umístění na obličeji, tvar nosu, úst, čelistí, popřípadě lícních kostí). Tyto rysy jsou dále použity pro vytvoření předlohové šablony, pomocí které dochází k určení nebo ověření uživatele. U tohoto zařízení je také možnost použít PIN kód nebo identifikační kartu. PIN a ID karta uživatele je načtena a poté se porovnávají biometrické charakteristiky a předlohou, která je uložena v systému zařízení. Dochází tedy k porovnání 1:1. Je možné zaznamenat 2000 otisků prstů a 400 tváří. Pro rozpoznání tváří je použit algoritmus VX7.0. U tohoto algoritmu je větší rychlost verifikace než u čtečky IFace 320. Stejně jako čtečka IFace 320 je vybavena komunikací přes rozhraní RS232/485, TCP/IP, WiFi nebo GPRS. Stejně tak i napájecí napětí 12V DC, které je přiváděno pomocí PoE. Tato čtečka je vhodná i pro venkovní použití. Lze na ní připojit zamykání, alarm, magnetický kontakt dveří pro vstup a výstup, odchodové tlačítko nebo zvonek. [18; 19]

Obrázek 15. Čtečka Multibio 700 [19]

5.3 EFG Aktion AFT – 500

Terminál AFT – 500 je od české firmy EFG CZ spol. s.r.o. a mimo systému pro rozpoznání obličejů má i integrovaný snímač RFID karet (viz obr. 16). V zařízení je procesor TI DM CPU 600 MHz. Na předním panelu se nachází 3,5´´ TFT displej s rozlišením 240x320 DPI. Displej není dotykový a je vedle něj umístěna klávesnice. Paměť SD karty je 4GB a její maximální kapacita je 70000 snímků. Na čtečku je možné připojit elektrický zámek, alarm, odchodové tlačítko a dveřní snímač. U AFT – 500 je možné kombinovat metody přístupu. Uživatel může být autentizován i jednotlivými metodami nebo jejich kombinacemi: [20]

Obrázek 16. Terminál EFG Aktion-500 [20]

- Biometrií tváře
- RFID karty
- Biometrií tváře a PINU
- Biometrií tváře a RFID karty

Každá metoda nebo kombinace vytváří určité podmínky pro správnou identifikaci, které se liší svojí rychlostí. Je vhodné volit kompromis mezi bezpečností a rychlostí podle použití. Kapacita zařízení je 500 osob, ale kapacitu je možné navýšit na 1400 osob. Detekci a identifikaci tváře je možné provádět do 80 cm vzdálenosti od kamery. Jako výstup terminálu je relé 1x NC/NO/N. Pro komunikaci slouží rozhraní USB, Ethernet a Wiegand 26bit/34bit. Konstrukce zařízení má krytí IP54, je tedy možné i venkovní umístění. [10]

5.4 Porovnání jednotlivých zařízení

Pro porovnání byly vybrány tři biometrické zařízení, kterými ústav disponuje. Jedná se čtečky IFace 302, Multibio 700 a EFG Aktion AFT-500. Při porovnání byl kladen důraz na technické parametry jako je kapacita obličejů a rychlost identifikace. Dále jsem se zaměřil na kombinace biometrických metod, které zařízení umožňují. Pro větší přehlednost budou parametry jednotlivých zařízení zobrazeny do tabulky (viz tabulka 2.).

Tabulka 2. Porovnání parametrů biometrických zařízení [vlastní zpracování]

	IFace 302	**Multibio 700**	**EFG Aktion AFT-500**
Kapacita obličejů	400	1500	500/1400
Doba ověřování [s]	<= 2	<= 2	<= 1
Možnosti identifikace	Obličej/ RFID/ otisk prstu/ heslo	Obličej/ Otisk prstu/ Obličej/ Heslo	Obličej/ Pin a obličej/ Karta a obličej
Displej [´´]	4,3	3	3,5
Procesor	Multibio CPU 630MHz	32bit Multibio Microprocessor 630 MHz	TI DM CPU 600MHz
Napájecí napětí [U]	12	12	12
Proudový odběr [I]	3	3	0,5
Provozní teplota [°C]	0 – 45	0 – 45	0 – 40
Rozměry [mm]	194 x 165 x 86	275 x 100 x 195	200 x 115 x 95

Při výběru autonomních vstupních terminálů je důležitou vlastností kapacita obličejů, které zařízení může rozeznat. Nejvyšší kapacitu nabízí zařízení Multibio 700. Nejnižší kapacita je udávána u zařízení IFace 302. Zařízení EFG Aktion AFT – 500 má kapacitu 500 obličejů, ale jak již bylo zmíněno, lze tuto kapacitu navýšit na 1400 obličejů. U podniků s větším počtem zaměstnanců nemusí ani navýšení kapacity stačit. Dalším neméně důležitým parametrem je rychlost autentizace. U čteček IFace 302 a Multibio 700 je rychlost srovnatelná. U EFG Aktion – 500 vychází rychlost nejlépe a to do 1 sekundy. Srovnatelné jsou i výkony procesorů. S lepšími technickými parametry se ukazuje zařízení EFG Aktion AFT – 500. S ohledem na jeho IP krytí je vhodné pro použití ve venkovních prostor, navíc umožnuje kombinování autentizačních metod. Uspokojivou variantou se jeví i zařízení Multibio 700 s kapacitou 1500 obličejů. Výhodou tohoto zařízení může být i wifi modul a vzdálená správa přes internetový prohlížeč.

5.5 Měření

Měření bylo prováděno na třech výše uvedených zařízení. Pro měření bylo vybráno celkem deset osob. Nejprve byla každé osobě uložena její biometrická šablona tváře do všech zařízení. Poté každý uživatel provedl 10 identifikačních pokusů. Jak již bylo uvedeno, prováděno bylo měření rychlosti identifikace uživatele do tří sekund. Výsledky měření jsou uvedeny níže (viz Tab. 3,4,5.). Do spodního řádku jsou zaznamenány celkové součty všech pokusů, kterých bylo provedeno 100 na každé čtečce, dále součet všech přijetí do tří sekund a počet chybných přijetí.

Tabulka 3. Měření na systému IFace 302 [vlastní zpracování]

IFace 302			
Uživatel	Počet pokusů	Počet přijetí do 3 s	Počet chybných přijetí
1	10	3	0
2	10	2	0
3	10	1	0
4	10	1	0
5	10	2	0
6	10	4	0
7	10	3	0
8	10	0	0
9	10	4	0
10	10	2	4
Celkem	100	22	4

Tabulka 4. Měření na systému Multibio 700 [vlastní zpracování]

Multibio 700			
Uživatel	Počet pokusů	Počet přijetí do 3 s	Počet chybných přijetí
1	10	1	0
2	10	2	0
3	10	0	0
4	10	4	0
5	10	2	0
6	10	0	0
7	10	1	0
8	10	2	0
9	10	1	0
10	10	0	2
Celkem	100	13	2

Tabulka 5. Měření na systému EFG Aktion-500 [vlastní zpracování]

EFG Aktion-500			
Uživatel	Počet pokusů	Počet přijetí do 3 s	Počet chybných přijetí
1	10	10	0
2	10	8	0
3	10	10	0
4	10	10	0
5	10	10	0
6	10	9	0
7	10	9	0
8	10	10	0
9	10	10	0
10	10	9	0
Celkem	100	95	0

5.5.1 Výpočet pravděpodobnosti chybného přijetí-FAR

Při měření rychlosti identifikace se objevili případy, u kterých byly zaměněni uživatelé. Tyto případy nastali pouze u systémů IFace 302 a Multibio 700. Výpočet tedy bude zaměřen na pravděpodobnost chybného přijetí, který je dán vztahem:

$$FAR = \frac{NFA}{NIIA} \times 100\ [\%]$$

N_{FA} - počet chybných přijetí

N_{IIA} – celkový počet pokusů

FAR – pravděpodobnost chybného přijetí

Pravděpodobnost u chybného přijetí u IFace 302:

$$FAR = \frac{4}{100} \times 100\ [\%]$$

$$FAR = 4\ \%$$

Pravděpodobnost chybného přijetí u Multibio 700:

$$FAR = \frac{2}{100} \times 100\ [\%]$$

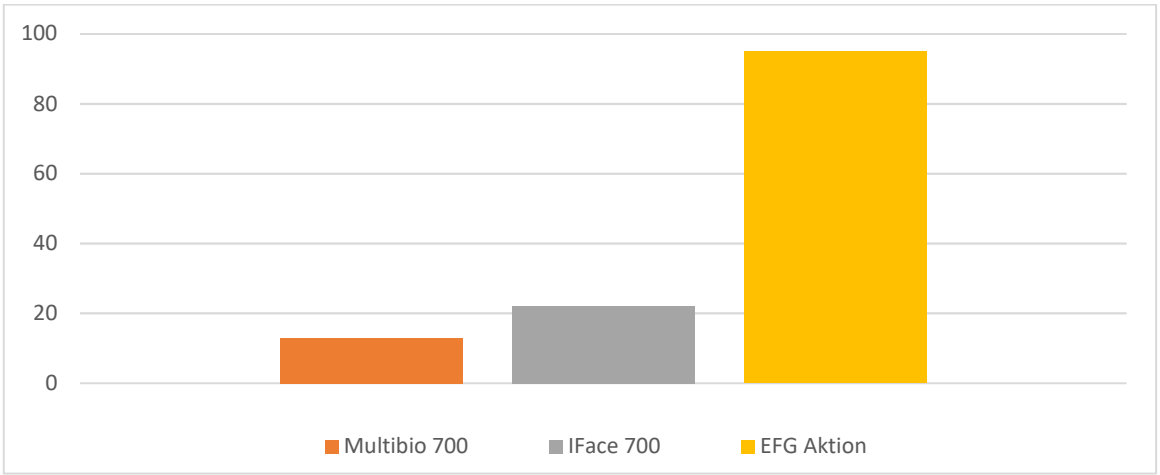
$$FAR = 2\ \%$$

6 Zhodnocení výsledků

Výsledky měření byly jednoznačně příznivější pro systém EFG Aktion-500, kde rychlost identifikace do 3 sekund byla dodržena téměř u všech pokusů identifikace. K chybnému přijetí u tohoto systému nedošlo. Naproti tomu výsledky měření u systémů IFace 302 a Multibio 700 nebyly zdaleka tak příznivé jako u předchozího systému. Problémy nastávaly hlavně při nedodržení vzdálenosti od ověřovací jednotky. Měření u těchto dvou systémů bylo náročnější i z hlediska zavádění biometrické šablony. V případě, že se nepodaří správně sejmout podobu tváře, mohou nastat problémy při rozpoznávacím procesu. U systému IFace 302 navíc došlo u čtyř pokusů k záměně uživatelů 5 a 10. U systému Multibio 700 došlo k chybnému přijetí ve dvou případech také u uživatele 5 a 10. Tyto chybná přijetí uživatelů jsou z bezpečnostního hlediska nepřijatelné. Pro systémy, u kterých došlo k chybnému přijetí uživatelů byly provedeny výpočty FAR koeficientu. Pro zařízení IFace 302 vyšel FAR koeficient 4 % a pro zařízení Multibio 700 vyšel FAR koeficient 2 %. Výrobce udává hodnoty FAR <0,0001 %. V porovnání s vypočtenými hodnotami se výsledky neshodují. Čtečky Multibio 700 a IFace jsou tedy bezpečnostně nevyhovující.

Z měření je patrné, že nejlepší výsledky rychlosti identifikace vykazovala čtečka EFG Aktion (viz obr. 17). Úspěšnost přijetído tří sekund u čtečky EFG Aktion-500 byla 95 přijetí ze 100 pokusů. U čtečky Multibio 700 byla úspěšnost pouze 13 přijetí ze 100 pokusů a u čtečky IFace 302 byla úspěšnost 22 přijetí ze 100 pokusů. Z uživatelského hlediska je tedy přijatelná pouze čtečka EFG Aktion – 500.

Obrázek 17. Pokusy do 3 [s] – celkové porovnání [vlastní zpracování]



7 Závěr

V rámci teoretické části byly nejprve popsány základní pojmy v biometrii jako je identifikace a verifikace a následně i chybové koeficienty pro určování spolehlivosti biometrických systémů. I když je verifikace tváře poměrně mladou metodou, přesto je již celkem často využívána. Jedná převážně o zkušební a testovací provozy. Potenciál využití této metody je velmi široký. Jedná se například o systémy kontroly vstupu, celní kontroly v rámci letištní prevence, dále dynamické snímání vnitřních i venkovních prostorů jako jsou kasina, obchodní centra atd.

V současné době je největším omezením funkčnost systému. V případě použití čipových karet, hesel a tokenů je zajištěna 100% úspěšnost. Metoda rozpoznání podle obličeje však takových výsledků nedosahuje. I když jsou některé systémy velmi kvalitní, vždy existuje určitá míra chybovosti. Jsou tím myšleny především koeficienty FAR a FRR.

Výhoda metody spočívá v uživatelské přijatelnosti. Uplatnění nachází například na letištích jako rychlejší možnost odbavení. Dále by metoda mohla najít uplatnění při dynamickém snímání veřejných prostor, kdy může dojít k upozornění na zájmové osoby. Oproti tomu, při použitích pro kontroly vstupu do budov je zapotřebí zvýšené opatrnosti při výběru systému. Může totiž docházet k chybnému přijetí (FAR). Možnost, jak zavádět metodu rozpoznání tváře jako kontrolu vstupu by mohla být kombinací s jinou metodou jako je například využití hesla nebo identifikační karty.

V praktické části byly popsány a zhodnoceny systémy pro rozpoznání tváře IFace 302, Multibio 700 a EFG Aktion-500. Dále bylo na těchto zařízeních provedeno měření rychlosti identifikace uživatele. Výsledek vyzněl nejlépe pro systém EFG Aktion-500. Byly provedeny výpočty pravděpodobnosti chybného přijetí (FAR) pro systémy IFace a Multibio, u kterých došlo k záměně uživatelů. U čtečky Multibio 700 vyšla hodnota FAR 2 % a pro čtečku IFace 4 %. Vypočtené hodnoty FAR se s hodnotami udávanými výrobcem čteček neshodovali. Takto vysoké hodnoty FAR naznačují, že není vhodné čtečky používat pro vstupní terminály do zabezpečených objektů. U těchto dvou systémů nastávaly problémy a také zpomalení rychlosti identifikace při nedodržení předepsané vzdálenosti od ověřovací jednotky. To je uživatelsky nekonformní. Vzhledem k tomu, že na oblast rozpoznání tváře je zaměřena velká pozornost a provádí se intenzivní výzkumy lze předpokládat, že dojde ke zdokonalení metod a k odstranění některých problémů.

8 Seznam použité literatury

[1] RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. Praha: Grada, 2008. Profesionál. ISBN 978-80-247-2365-5.

[2] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi* [online]. In: . VŠB TU Ostrava, 2008 [cit. 2017-02-13]. Dostupné z: http://www.fbi.vsb.cz/export/sites/fbi/040/.content/syscs/resource/PDF/biometricke_metody.pdf

[3] SVOZIL, Lukáš. *Aspekty biometrické identifikace osob s využitím rozpoznání tváře* [online]. Univerzita Tomáše Bati ve Zlíně, 2009 [cit. 2017-02-15]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/7953/svozil_2009_bp.pdf?sequence=1

[4] SLUKOVSKÁ, Kateřina. Biometrické systémy zaměřené na rozpoznávání tváře, jejich spolehlivost a základní metody pro jejich tvorbu. *Posterus* [online]. 2011

[cit. 2017-02-20]. Dostupné z: http://www.posterus.sk/?p=11511

[5] MICHÁLEK, Martin. *Biometrické rozpoznávání 3D modelů obličeje* [online]. VUT Brno, 2014 [cit. 2017-03-22]. Dostupné z: https://dspace.vutbr.cz/xmlui/bitstream/handle/11012/53352/16514.pdf?sequence=2&isAllowed=y

[6] HORÁK, Rudolf a Rudolf SCHWARZ, ed. *Bezpečnost světa a domoviny: sborník 6. mezinárodní konference CM - Crisis Management : 16. a 17. června 2010*.

Brno: Univerzita obrany, 2010. ISBN 978-80-7231-728-8.

[7] *Cestovní doklady s biometrickými prvky (CDBP)* [online]. 2014 [cit. 2017-02-25]. DOI: mvcr. Dostupné z: http://www.mvcr.cz/clanek/cestovni-doklady-s-biometrickymi-prvky-cdbp.aspx

[8] DRAHANSKÝ, Martin. *Biometrické systémy v praxi* [online]. In: . VUT Brno, 2014 [cit. 2017-02-18]. Dostupné z: http://www.smartworld-konference.cz/prezentace14/blok1/SW2014_Biometrie_a_bezpecnost_Drahansky.pdf

[9] ASHBOURN, Julian. *Practical biometrics: from aspiration to implementation*. New York: Springer, 2004. ISBN 18-523-3774-5.

[10] GÁBRLÍK, Jiří. *Návrh systému na rozpoznání osob prostřednictvím biometrie obličeje* [online]. Univerzita Tomáše Bati ve Zlíně, 2011 [cit. 2017-02-15]. Dostupné z: http://digilib.k.utb.cz/bitstream/handle/10563/17464/g%C3%A1brl%C3%ADk_2011_bp.pdf?sequence=1

[11] BENEŠ, Radek. *Autentizační metody založené na biometrických informacích* [online]. In: . VUT Brno, 2010 [cit. 2017-03-22]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2010110002

[12] POSPÍŠIL, Lukáš. *Detekce obličeje v obraze* [online]. VUT Brno, 2014 [cit. 2017-03-22]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=85175

[13] MODI, Shimon K. *Biometrics in identity management: concepts to applications*. Boston: Artech House, c2011. Artech House information security and privacy series. ISBN 978-1-60807-017-6.

[14] PUŽMANOVÁ, Rita. *Biometrické systémy v praxi* [online]. 2004

[cit. 2017-03-22]. Dostupné z: https://www.systemonline.cz/clanky/biometricke-systemy-v-praxi.htm

[15] NOVÁK, Mirko. *Neuronové sítě*. Praha: C.H. Beck, 1998. ISBN 80-717-9132-6.

[16] MANSSON, Jenny. Automatizované rozpoznávání obličejů - trend nejen v oblasti bezpečnosti. *Security magazín* [online]. 2016, (1) [cit. 2017-03-07]. Dostupné z: http://www.securitymagazin.cz/technologie/-1404049865.html

[17] DRAHANSKÝ, Martin a Filip ORSÁG. *Biometrie*. [Brno: M. Drahanský], 2011. ISBN 978-80-254-8979-6.

[18] HARTOVÁ, Veronika. *Biometrické identifikační systémy*. ČZU Praha, 2014. Disertační práce.

[19] *ACS solutions* [online]. [cit. 2017-03-12]. Dostupné z: http://www.acssolution.cz/?page_id=129

[20] *Aktion* [online]. [cit. 2017-03-19]. Dostupné z: https://www.aktion.cz/aktion_cs/download/katalogove-listy/AFT-500.pdf

[21] BONSON, Kevin a Ryan JOHNSON. *How Facial Recognition Systems Work* [online]. 2014 [cit. 2017-03-21]. Dostupné z: http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm

[22] VACH, Martin. *Historie biometrik a jejich využití ve výpočetní technice* [online]. 2003 [cit. 2017-03-18]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xvach_biometriky.htm

[23] BITTO, Ondřej. *Šifrování a biometrika, aneb, Tajemné bity a dotyky*. Kralice na Hané: Computer Media, 2005. ISBN 80-866-8648-5.

[24] BAZALA, Lukáš. *Využití biometrických údajů obličeje při identifikaci osob* [online]. VUT Brno, 2012 [cit. 2017-03-15]. Dostupné z: https://core.ac.uk/download/pdf/30281678.pdf. Bakalářská práce.

[25] PŘIBYL, Tomáš. *Výhody a nevýhody biometrických systémů* [online]. [cit. 2017-03-09]. Dostupné z: http://www.scienceworld.cz/biologie/vyhody-a-nevyhody-biometrickych-systemu-1-515/?switch_theme=mobile

9 Seznam obrázků

10 Seznam tabulek