Anonymita ve světě bezpečnostních technologií

Jan Rössner

Bakalářská práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Rössner**
Osobní číslo:	**A14616**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Anonymita ve světě bezpečnostních technologií**
Téma anglicky:	**Anonymity in the Security Technologies World**

Zásady pro vypracování:

1. **Proveďte literární rešerši zaměřenou na identifikaci osob pomocí lidské tváře.**
2. **V rámci bakalářské práce se zaměřte na technologii brýlí PrivacyVisor, popište jejich vlastnosti a princip činnosti.**
3. **Popište možnosti identifikace osob vybavených brýlemi PrivacyVisor pomocí kamerového systému.**
4. **Navrhněte způsob identifikace osob vybavených brýlemi PrivacyVisor.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **RAK, Roman, Vašek MATYÁŠ a Zdeněk ŘÍHA. Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha: Grada, 2008, 631 s., 32 s. obr. příl. Profesionál. ISBN 978-80-247-2365-5.**
2. **ŠIMÍČEK, Michal. Právo na soukromí. 1. vyd. Brno: Masarykova univerzita, Mezinárodní politologický ústav, 2011, 212 s. ISBN 978-80-210-5449-3.**
3. **LI, Jun-Bao, Shu-Chuan CHU a Jeng-Shyang PAN. Kernel learning algorithms for face recognition [online]. 2013, xv, 225 pages.**
4. **MELIN, Patricia. Modular neural networks and type-2 fuzzy systems for pattern recognition [online]. Berlin: Springer-Verlag, c2012, x, 214 p. Studies in computational intelligence, v. 389. ISBN 9783642241390.**
5. **BITTO, Ondřej. Šifrování a biometrika aneb tajemné bity a dotyky. Vyd. 1. Kralice na Hané: Computer Media, 2005, 168 s. ISBN 80-86686-48-5.**
6. **DRAHANSKÝ, Martin a Filip ORSÁG. Biometrie. Vyd. 1. [Brno: M. Drahanský], 2011, 294 s. ISBN 978-80-254-8979-6.**

Vedoucí bakalářské práce: **doc. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **23. února 2016**

Termín odevzdání bakalářské práce: **30. května 2016**

Ve Zlíně dne 16. února 2016

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Jan Valouch, Ph.D.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 25. 5. 2016

.....
podpis diplomanta

I hereby declare that:

- I understand that by submitting my Diploma thesis, I agree to the publication of my work according to Law No. 111/1998, Coll., On Universities and on changes and amendments to other acts (e.g. the Universities Act), as amended by subsequent legislation, without regard to the results of the defence of the thesis.
- I understand that my Diploma Thesis will be stored electronically in the university information system and be made available for on-site inspection, and that a copy of the Diploma/Thesis will be stored in the Reference Library of the Faculty of Applied Informatics, Tomas Bata University in Zlin, and that a copy shall be deposited with my Supervisor.
- I am aware of the fact that my Diploma Thesis is fully covered by Act No. 121/2000 Coll. On Copyright, and Rights Related to Copyright, as amended by some other laws (e.g. the Copyright Act), as amended by subsequent legislation; and especially, by §35, Para. 3.
- I understand that, according to §60, Para. 1 of the Copyright Act, TBU in Zlin has the right to conclude licensing agreements relating to the use of scholastic work within the full extent of §12, Para. 4, of the Copyright Act.
- I understand that, according to §60, Para. 2, and Para. 3, of the Copyright Act, I may use my work - Diploma Thesis, or grant a license for its use, only if permitted by the licensing agreement concluded between myself and Tomas Bata University in Zlin with a view to the fact that Tomas Bata University in Zlín must be compensated for any reasonable contribution to covering such expenses/costs as invested by them in the creation of the thesis (up until the full actual amount) shall also be a subject of this licensing agreement.
- I understand that, should the elaboration of the Diploma Thesis include the use of software provided by Tomas Bata University in Zlin or other such entities strictly for study and research purposes (i.e. only for non-commercial use), the results of my Diploma Thesis cannot be used for commercial purposes.
- I understand that, if the output of my Diploma Thesis is any software product(s), this/these shall equally be considered as part of the thesis, as well as any source codes, or files from which the project is composed. Not submitting any part of this/these component(s) may be a reason for the non-defence of my thesis.

I herewith declare that:

- I have worked on my thesis alone and duly cited any literature I have used. In the case of the publication of the results of my thesis, I shall be listed as co-author.
- That the submitted version of the thesis and its electronic version uploaded to IS/STAG are both identical.

In Zlin; dated: 25.5.2016

.....
Student´s Signature

ABSTRAKT

V rámci této bakalářské práce je pozornost věnována biometrii a identifikaci osob dle lidské tváře. První kapitola je věnována pojmu biometrie a tématům, které jsou s tímto termínem úzce spojeny. V druhé kapitole je pozornost zaměřena na dva typy metod identifikace podle tváře, které byly uplatňovány v rámci forenzních činností v minulém století. Tématem třetí kapitoly jsou metody identifikace dle lidské tváře v kamerových záznamech, přičemž pozornost je věnována především metodě eigenface, metodě optických toků a umělým neuronovým sítím. Ve čtvrté kapitole je proveden rozbor právního rámce, týkajícího se soukromí a citlivých údajů, který je uplatňován na území České republiky a pátá kapitola popisuje technologii brýlí PrivacyVisor, které znemožňují identifikaci kamerovými systémy.

Klíčová slova: biometrie, tvář, identifikace, soukromí, privacyvisor

ABSTRACT

In this bachelor thesis, attention is paid to biometrics and identification via human face. The first chapter is aimed to the term of biometrics and themes that are closely linked with this term. The second chapter is focused on two types of facial identification methods that have been applied in the context of forensic activities in the last century. The theme of chapter three are facial identification methods used in the camera records analysis, particular attention is paid to eigenface method, optical flow method and artificial neural networks. The fourth chapter is an analysis of the law related to privacy and personal information, which is applied in the Czech Republic and the fifth chapter describes the technology PrivacyVisor glasses that circumvent the identification by CCTV systems.

Keywords: biometrics, face, identification, privacy, privacyvisor

Tímto bych chtěl poděkovat svému vedoucímu práce, doc. Mgr. Milanu Adámkovi, Ph.D. za čas a veškerou pomoc s vypracováním této práce v podobě cenných odborných rad a konzultací. Dále bych chtěl poděkovat mým nejbližším za veškerou podporu během doby mého studia.

OBSAH

ÚVOD

Je možné si v dnešním světě zachovat anonymitu a oddělit svůj soukromý život od veřejného? Éra digitalizovaného života prostřednictvím sociálních sítí dává pouze iluzi soukromí a člověku nezbývá než si svou diskrétní zónu chránit. Toto bylo hlavním popudem, proč japonští vědci investovali čas a energii na výrobu brýlí, se kterými nebude možné být identifikován smartphonem či dokonce kamerovým systémem. Vyvstává ovšem otázka, zda takové brýle nebudou ve dnech sebevražedných atentátníků, skrytých v davu při demonstracích, hrozbou, která by mohla narušit veřejné bezpečí a ohrozit lidské životy. Je proto nutné znát právní rámec země, ve které žijeme a vidět do jaké míry je možno našemu soukromí ukrátit na kvalitě ve prospěch veřejné bezpečnosti a prevenci protiprávní činnosti.

Tato bakalářská práce popisuje principy biometrických metod a následně je zkoumán z prozatím dostupných zdrojů princip technologie brýlí PrivacyVisor. Rovněž zmiňuje některé ze zákonů, souvisejících s ochranou soukromí, ale nejzásadnějším je dát slovu biometrie správný význam, a tím celá tato práce začíná.

I. TEORETICKÁ ČÁST

1 BIOMETRIE

Tato kapitola je věnována, jak už z názvu vyplývá, biometrii a pojmům s ní blízce sdruženým. V první části je pozornost zaměřena na biometrii a rovněž je zpracován stručný přehled historických milníků, dále je zpracován přehled základních biometrických znaků a v neposlední řadě je tato kapitola zaměřena na definování klíčových termínů, které souvisí s procesem identifikace.

1.1 Pojem biometrie a její stručná historie

Pojem biometrie má původ v řečtině a skládá se ze slov „bios“ s významem „život“ a slova „metron“, které znamená v překladu „měřit“ či „měření“ [1]. Bylo by asi pomýlené překládat tento pojem doslova, ovšem v nepřímém překladu můžeme biometrii dát význam jako věda, která se zabývá měřením charakteristických rysů živých organismů, respektive lidských jedinců.

První zmínky v souvislosti s biometrií se datují až do období okolo roku 2000 před naším letopočtem, kdy byly do kamene, jenž byl nalezen v oblasti dnešního státu Indiana, vyryty grafiky zobrazující papilární linie [2].

Prvním zásadním průkopníkem v metodologii biometrie byl ovšem Louis Alphonse Bertillon [3], který položil základy moderní kriminalistiky svou metodou zvanou „Bertillonáž“. Tato metoda byla Bertillonem vytvořena na popud vysoké kriminality a nemožnost prokázat recidivitu pachatelů [4]. V rámci této metody je měřeno jedenáct lidských markantů, mezi které patří velikost ucha a délka se šířkou hlavy [5]. Tato metoda byla postupem času nahrazena daktyloskopií, která je značně důslednější, a to ve smyslu prokazování viny pachatele na základě zanechaných otisků na místě činu a porovnáváním s otisky podezřelých osob.

Obr. č. 1 – *Louis Alphonse Bertillon* [3]

K enormnímu rozvoji biometrických metod a aplikaci biometrických systémů došlo až na počátku 70. let 20. století a stále tyto systémy expandují, přičemž veškeré technologie jsou primárně směřovány k soudním či detektivním činnostem a do komerčního sektoru se zpravidla dostávají až po aplikování ve zmíněných oblastech [6]. Prudký vzestup integrování biometrických systémů byl zaznamenán v návaznosti na události spojené s útokem 11. září 2001 na budovy World Trade Center, kdy se zpřísnila bezpečnostní politika Spojených Států a následovalo například vyžadování otisků prstů a fotografie každého cizince, žádajícího o vízum pro pobyt v USA [7].

1.2 Základní biometrické znaky

Pokud máme hovořit o konkrétních biometrických znacích, je třeba si nejprve vyjasnit a definovat pojem biometrický znak. Po první části této kapitoly můžeme z poznatků o biometrii vyvodit i to, co je považováno za biometrický znak. Biometrickým znakem se rozumí charakteristický rys lidského jedince, kterým je možné ho jednoznačně identifikovat. Biometrické znaky se dělí na anatomicko-fyziologické znaky, které vznikly růstem a formováním těla člověka v průběhu času a dospívání, a na znaky behaviorální, které získávají svoji charakterističnost až naučením a osvojením určitého typu chování. Mezi nejpoužívanější anatomicko-fyziologické znaky patří:

- Oční duhovka ;

- Oční sítnice;
- Tvář;
- Otisky prstů;
- Tvar chrupavky vnějšího ucha;
- Krevní řečiště v oblasti zápěstí;
- Struktura chrupu;
- Tvar prstů a ruky;
- Pach;
- DNA.

Jako behaviorální znaky pak označujeme:

- Dynamika stisku kláves na PC;
- Dynamika pohybu myši na PC
- Styl ručního psaní;
- Styl podpisu;
- Dynamika chůze;
- Hlas[8].

U všech typů biometrických znaků jsou zkoumány různé vlastnosti, mezi základní čtyři patří tyto:

- Univerzálnost – vlastnost znaku, která udává, do jaké míry je znak přítomný u všech lidských jedinců;
- Unikátnost – vlastnost, která specifikuje, že znak je pro každého člověka jedinečný;
- Trvalost – vlastnost, která zaručuje možnost měření znaku na jedinci i v delších časových intervalech;
- Měřitelnost – vlastnost, zaručující možnost znak na člověku měřit dostupnými technologiemi [9].

Každá z těchto vlastností se projevuje u různých biometrických znaků do určité míry. Pro přehlednost a představu jsou jednotlivé znaky a míry jejich vlastností uspořádány do Tab. č. 1.

Tab. č. 1 - *Základní vlastnosti biometrických znaků* [9]

Biometrický znak	Univerzálnost	Unikátnost	Trvalost	Měřitelnost
DNA	Vysoká	Vysoká	Vysoká	Slabá
Tvar ucha	Střední	Střední	Vysoká	Střední
Obličej	Vysoká	Slabá	Střední	Vysoká
Termosnímek obličeje	Vysoká	Vysoká	Slabá	Střední
Otisky prstů	Střední	Vysoká	Vysoká	Střední
Chůze	Střední	Slabá	Slabá	Vysoká
Tvar dlaně	Střední	Střední	Střední	Vysoká
Krevní řečiště na dlani	Střední	Střední	Střední	Střední
Oční duhovka	Vysoká	Vysoká	Vysoká	Střední
Dynamika stisku kláves	Slabá	Slabá	Slabá	Střední
Pach	Vysoká	Vysoká	Vysoká	Slabá
Otisk dlaně	Střední	Vysoká	Vysoká	Střední
Oční sítnice	Vysoká	Vysoká	Střední	Slabá
Styl podpisu	Slabá	Slabá	Slabá	Vysoká
Hlas	Střední	Slabá	Slabá	Střední

Pro aplikování v rámci bezpečnostních systémů a technologií jsou ovšem potřeba zkoumat další přidané vlastnosti jako například:

- Rychlost – vlastnost, kterou je myšleno výkonové zpracování znaku biometrickým systémem v závislosti na složitosti znaku a množství informací, potřebných pro přesný a jednoznačný popis charakteristického rysu;
- Přijatelnost – vlastnost znaku, kterou ovlivňují faktory jako je veřejné mínění a ochotnost společnosti používat danou biometrickou metodu v každodenním životě;
- Prolomitelnost – vlastnost, specifikující, jak snadné je danou biometrickou metodu obelstít.

Stejně jako u základních vlastností jsou sledovány i míry a kvality přidaných vlastností. Konkrétnější míry vlastností jsou pro představu zpracovány v Tab. č. 2.

Tab. č. 2 – *Přidané vlastnosti biometrických znaků* [9]

Biometrický znak	Rychlost	Přijatelnost	Prolomitelnost
DNA	Vysoká	Slabá	Slabá
Tvar ucha	Střední	Vysoká	Střední
Obličej	Slabá	Vysoká	Vysoká
Termosnímek obličeje	Střední	Vysoká	Slabá
Otisky prstů	Vysoká	Střední	Střední
Chůze	Slabá	Vysoká	Střední
Tvar dlaně	Střední	Střední	Střední
Krevní řečiště na dlani	Střední	Střední	Slabá
Oční duhovka	Vysoká	Slabá	Slabá
Dynamika stisku kláves	Slabá	Střední	Střední
Pach	Slabá	Střední	Slabá
Otisk dlaně	Vysoká	Střední	Střední
Oční sítnice	Vysoká	Slabá	Slabá
Styl podpisu	Slabá	Vysoká	Vysoká
Hlas	Slabá	Vysoká	Vysoká

Kvalitní a aplikovatelný biometrický systém by měl být navržen a založen na biometrickém znaku, jehož průnik výše zmíněnými vlastnostmi by zaručil rychlou, jednoznačnou a neprolomitelnou technologii, která by byla rovněž přijatelná i lidskou společností, protože právě názor společnosti bývá ve většině případů u volby systému rozhodujícím faktorem.

1.3 Základní terminologie

Proces rozpoznání tváře je dvojího zaměření a jednotlivé typy se používají zpravidla v rozdílných odvětvích bezpečnostního průmyslu. Jedním je zmíněná identifikace, která slouží k přiřazení neznámého obličeje za účelem určení identity jedince. Identifikace je aplikována v detektivních činnostech, kdežto druhý typ rozpoznání, jímž je verifikace se uplatňuje především v rámci režimových opatření objektů, kdy systém porovnává snímaný vzorek biometrickým přístrojem s množinou vzorků uložených v paměti systému a vyhodnocuje, zda má osoba patřičná přístupová oprávnění. Nejprve si je třeba vyjasnit zmíněnou identifikaci, verifikaci, detekci a autorizaci.

- **Detekce**

V procesu rozpoznání je detekce obličeje v obrazu klíčovým faktorem pro další zpracování informací. Jedná se o vyhledání množiny vizuálních bodů obrazu se zkoumaným parametrem, kterým je v tomto případě přítomný obličej.

- **Identifikace**

V případě, že byla v obraze detekována tvář, se za pomocí počítačových algoritmů porovnává jeden vzorek s množinou vzorků v databázi a určuje se přesná identita osoby, zaznamenané v obraze. V anglické literatuře můžeme najít tento pojem nahrazen souslovím „One-To-One Matching“ [8].

- **Verifikace či autentizace**

Verifikaci bychom jinými slovy mohli nazvat jako ověření, že dotyčná osoba z naskenovaného modelu z obrazu má patřičná oprávnění, či je to osoba, kterou hledáme. Jinak by se dalo říci, že je to metoda, kdy systém nepotřebuje identitu člověka, ale ověřuje, zda skenovaný vzorek souhlasí alespoň s jedním vzorkem v množině modelů databáze systému. Tímto procesem se tedy ověřuje, zda je skenovaný člověk opravdu tím, za koho se vydává. Stejně jako identifikace i verifikace má svůj název v cizích jazycích a tím je zejména „One-To-Many Matching“. Pro malé soukromé objekty se ještě řídce používá výrazu „One-To-Few Matching“ (česky jeden z několika), kdy kupříkladu objekt není rozdělen do více zón s různými úrovněmi přístupového oprávnění, ale pouze jedna úroveň, kdy mají všichni uživatelé stejná privilegia [8].

- **Autorizace**

Posledním termínem, který by bylo na místě zmínit je autorizace. Autorizace je posledním klíčovým prvkem a synonymicky se dá nazvat jako udělení přístupového oprávnění. Poté, co je osoba v rámci přístupového systému verifikována, jsou dané osobě udělena přístupová oprávnění nebo je v opačném případě přístup zamítnut [10].

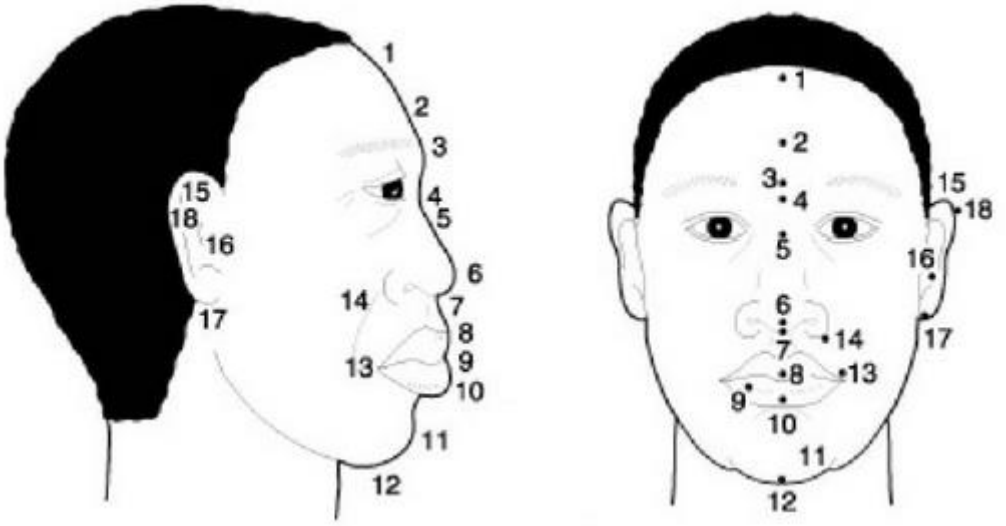
Obr. č. 2 – *Software Luxand Blink! v prostředí Windows Vista* [11]

V dnešní době se biometrické technologie uplatňují v čím dál větší míře i v komerční oblasti, a to například v přístupu do operačních systémů osobních počítačů a za zmínku můžeme dát například software Luxand Blink!, který rozpozná tvář pomocí webkamery a následně po vyhodnocení přijatých dat udělí patřičná přístupová oprávnění [11].

2 GEOMETRIE TVÁŘE

Aby byla tvář přesně a jednoznačně identifikována, je třeba mít obličej jako charakteristický biometrický rys dobře zmapován. K co nejpřesnějšímu vytvoření modelu obličeje slouží jako jeho hlavní rysy jeho tvar a poloha specifických markantů, jako jsou například oči, obočí, nos či ústa. Obraz se zpracovává v menším množství případů jako matice jasových úrovní, ale ve většině případů je aplikována funkce, která zamezí ukládání irelevantních a redundantních dat. Tím je myšlen princip, kdy jednotlivé markanty nejsou ukládány s jejich přesnou pozicí v souřadnicovém systému, ale jsou zaznamenány vzdálenosti mezi nimi. Tento princip vychází z analyticko-statistických metod, které se uplatňovaly v druhé polovině minulého století. [8], [12].

Modernímu počítačovému zpracování obličeje tedy předcházely techniky portrétních identifikací na základě výrazných antropologických bodů.



Obr. č. 3 – *Obecné antropologické body tváře* [8]

Na Obr. č. 3 je vyznačeno hlavních 18 bodů, které jsou řadou kriminalistických škol, zaměřujících se na identifikaci, obecně považovány za základní prvky pro přesné určení identity. V anglické literatuře se body nazývají:

- 1 – trichion,
- 2 – metopion,
- 3 – glabela,
- 4 – nasion,

- 5 – midnasal,
- 6 – pronasale,
- 7 – subnasal,
- 8 – superior labiale,
- 9 – stomition,
- 10 – inferior,
- 11 – pogonion,
- 12 – gnathion,
- 13 – cheilion,
- 14 – alare,
- 15 – superaurale,
- 16 – tragion,
- 17 – subaurale,
- 18 – postaurale [8].

Toto mapování lidské tváře bylo postupem času nedostačující při aplikování ve forenzní portrétní identifikaci, a proto byly zavedeny a zkoumány nové metody, jenž se od této metody mírně diferencovaly.

V 60. letech 20. století byla celá identifikace omezena na dvě metody a těmi byly:

- metody analyticko-statistické,
- metody grafické[8].

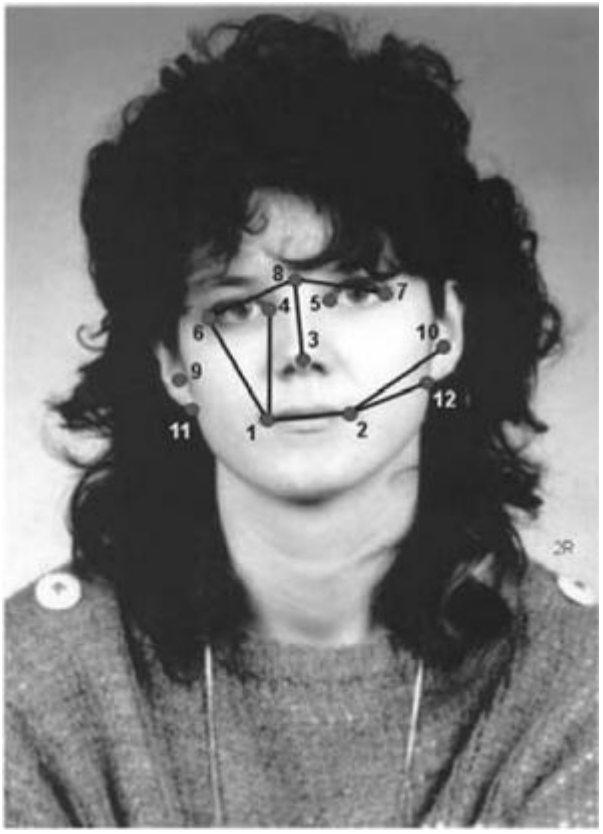
2.1 Analyticko-statistická metoda portrétní identifikace

Jak bylo zmíněno v prvních řádcích tohoto oddílu, tato metoda byla jedním ze základních kamenů moderní identifikace podle lidské tváře.

V této metodě se kombinují informace získané ze zkoumání prostorové i lineární struktury tváře a je založena na vzdálenostech významných bodů. Při experimentálním aplikování

této metody bylo zjištěno, že k přesné identifikaci osoby naplno dostačuje zmapování dvanácti význačných antropologických bodů lidské tváře a těmi jsou:

- vnitřní a vnější koutky oka (body 4, 5, 6, 7 na Obr. č. 4),
- koutky rtů (body 1, 2 na Obr. č. 4),
- místo, kde nos přechází v čelo a špička nosu (body 3, 8 na Obr. č. 4),
- body na chrupavkách uší, chránící vnější zvukovod (body 9, 10 na Obr. č. 4),
- místa přechodu ušního lalůčku do tváře (body 11, 12 na Obr. č. 4) [8].



Obr. č. 4 – *Markantní body analyticko-statistické metody spojeny každý s každým úsečkou* [8]

Na Obr. č. 4 jsou vyznačeny jen některé spojnice, avšak propojením všech bodů mezi sebou získáme 66 spojnic a ty dostačují pro vytvoření lineárního i prostorového modelu obličeje, který lze účinně použít pro co nejpřesnější identifikaci osoby. Pokud porovnáváme dva portréty snímané pod stejným úhlem natočení hlavy a poměry všech vzájemně si odpovídajících spojnic markantů budou konstantní, můžeme pak hovořit o přesné geometric-

ké a proporcionální shodě. V případě snímání dvou různých tváří či natočení hlavy se ovšem poměry spojnic budou lišit a přesná shoda nebude zaručena [8].

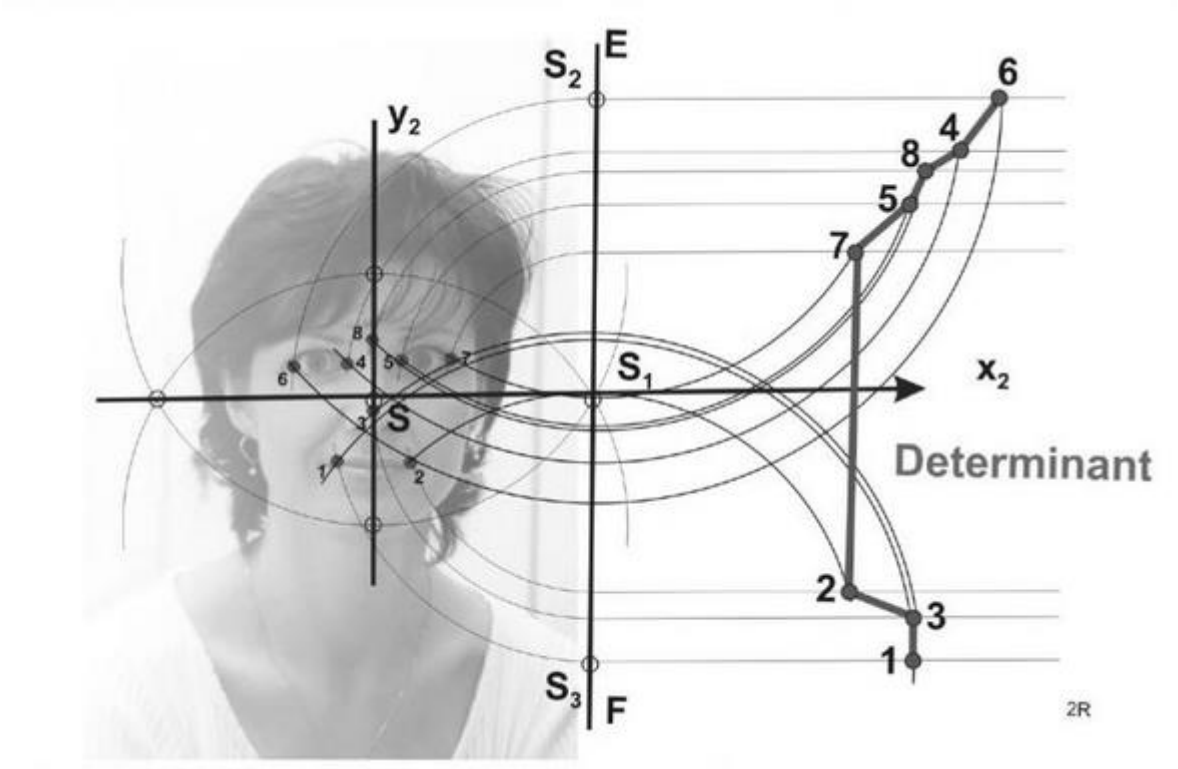
Pro aplikování této metody v praxi a zaručení vyhovujících výsledků je tedy bezpodmínečně nutné, aby byl ošetřen vliv natočení hlavy ve snímku. Touto problematikou se zabýval v 70. letech 20. století Nikolaj Stepanovič Polevoj ve své publikaci zaměřené na automatizované systémy v kriminalistické praxi [13]. Bylo tedy zkoumáno, jaký vliv má natočení hlavy na délky spojnic mezi markantními body. V rámci této studie, při které byl použit jediný fotoaparát, bylo pořízeno na 700 fotografií jedné osoby, kdy fotoaparát byl staticky upevněn a tvář se natáčela úhel o 10° podél tří os standartního kartézského souřadnicového systému. Každá fotografie tak byla doplněna mimo délek spojnic o informace tří úhlů natočení tváře. Výchozímu stavu polohy obličeje se ve studii nazývalo „en face“, kdy všechny tři úhly vyosení měly nulovou hodnotu. Celkový počet matematických operací se pak pohyboval v řádu několika stovek příkazů[8].

Cílem této metody nebylo aplikovat moderní metody, nýbrž zaměřit se na přesný popis vztahu jednotlivých spojnic markantů tváře s co největším procentem shody. Analyticko-statistická metoda se tedy stala výborným odrazovým můstkem pro mapování třídimenzových modelů tváří.

2.2 Grafická metoda

Tato metoda si oproti analyticko-statistické metodě zakládala na principech deskriptivní geometrie a zákonů perspektivy. Jinými slovy v souvislosti s portrétní identifikací též lze říci, že za předpokladu, kdy mezi sounáležícími markanty na dvou fotografiích existuje vztah vycházející ze zákonů perspektivy, jsou objekty zkoumání totožné.

Pokud chceme celou metodu stručně popsat, tak princip této techniky je založen na promítnutí snímků do pravoúhlé soustavy, zkonstruované a definované na základě markantních bodů a průnicích pomocných vynášecích přímek a kružnic. Průniky těchto přímek a kružnic pak tvoří spojitá křivka, která je označována jako grafický determinant markantních bodů lidské tváře. Pro lepší představu slouží grafické zpracování na Obr. č. 5 [8].



Obr. č. 5 – *Sestrojení determinantu markantních bodů lidské tváře* [8]

Pro úspěšnou identifikaci osoby v obraze zpracovanou strojem je ovšem nezbytným krokem detekce a lokalizace obličeje počítačem v rámci snímané oblasti, jelikož bez tohoto úspěšně a jednoznačně provedeného kroku je strojová identifikace zhola nemožná.

3 METODY ROZPOZNÁNÍ TVÁŘE V OBRAZE

Základním principem, na kterém pracuje každá moderní identifikační technologie, zpracovávající obraz, je najít určitý matematický vzorec pro obličej tak, aby počítačový algoritmus pochopil, co má konkrétně v rámci obrazu hledat. Po přesně definovaných instrukcích a popsaných parametrech vlastností obličeje by měl být počítač nejen schopen tvář detekovat, ale zároveň i lokalizovat v rámci obrazu a předzpracovat data pro další operace. Mezi základní metody rozpoznání tváře v obraze patří:

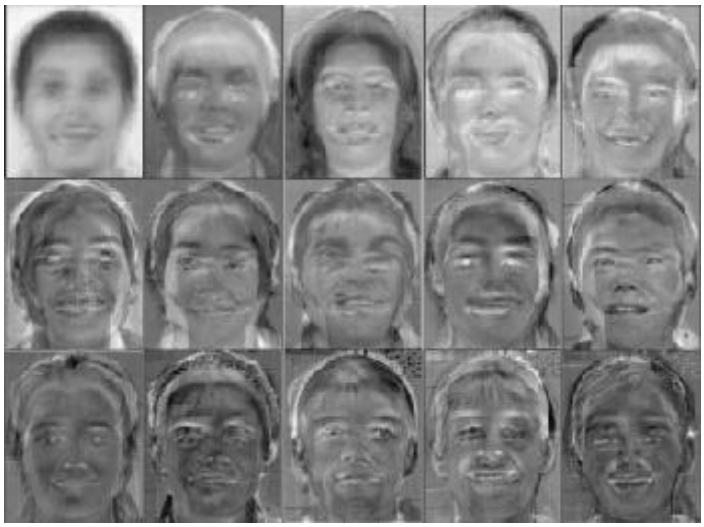
- Metoda podprostoru;
- Metoda aplikace umělých neuronových sítí;
- Metoda optických toků;
- Metody založené na rozložení odstínu šedi v obraze;
- Metody založené na rozpoznávání obličejových rysů;
- Metody založené na informaci o barvách;
- Metody založené na symetrii.

V rámci bakalářské práce je hlavní pozornost věnována metodě podprostoru, metodě aplikace neuronových sítí a metodě optických toků. Ostatní ze zmíněných metod jsou zmíněny s popisem základních principů.

3.1 Metoda podprostoru, eigenface, eigenhead

Celá filozofie této metody je založena na tezi, že každý obraz tváře může být vnímán jako vícerozměrný vektor a jednotlivé základní segmenty obrazu, čímž je míněno pixely zaujímají v obraze místo v určité hladině jednoho z podprostorů. Detekcí tváře je pak hledání podprostoru odpovídajícího lidské tváři. V reálné aplikaci je tato metoda reprezentována Karhumen-Loeve transformací, která dala základ pro metodu detekce a normalizace tváře zvanou „eigenface“ či „eigenhead“, pokud hovoříme o třírozměrném modelu. Eigenface metodou se každý skenovaný obličej zprůměruje na normalizované míry a jsou hledány a ukládány pozice významných markantů v obraze [8], [14], [15].

Obr. č. 6 – *Původní skenované tváře* [16]

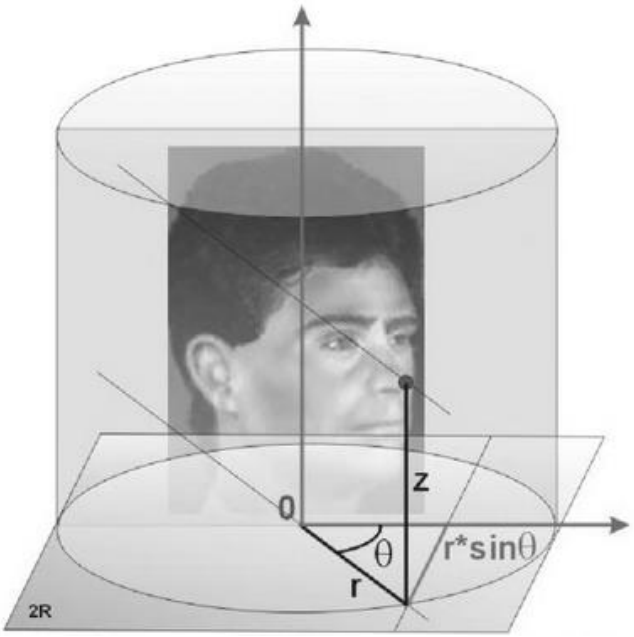


Obr. č. 7 – *Normalizované tváře dle algoritmu eigenface* [16]

Cílem této metody je tedy vytvoření standardizovaného modelu pro přesnou charakteristiku a popis lidské tváře.

Pokud hovoříme o třírozměrné alternativě „eigenhead“, existují dva nejvhodnější způsoby, jak obličej modelovat, a to buďto pořízením série obrazů tváře s různou intenzitou osvětlení a nebo získáním jednoho snímku tváře, na kterém budeme schopni demonstrovat charakteristické vlastnosti lidské tváře, jako stíny v různých částech obličeje a odraz světla od lidského obličeje. V rámci této metody bylo dosaženo vytvoření počítačových grafik, které dokáží předpokládat chování a pohyb mimických svalů obličeje, čímž je ošetřena problematika proměnlivosti výrazů tváře [8].

Pro aplikovatelnost této metody se využívá zápis nikoliv v třírozměrném kartézském systému souřadnic, nýbrž definování lidské hlavy v systému cylindrickém, kdy jedna z os není vyjádřena prostorovou délkou, ale značí úhel natočení hlavy [8].



Obr. č. 8 – *Popis markantu špičky nosu v cylindrické soustavě pro „eigenhead“* [8]

Celá ideologie této metody je postavena na myšlence definování unifikujícího vztahu pro jakoukoliv lidskou tvář, charakterizovaného za použití rysů, znázorněných na Obr. č. 8:

$$r = f_0(\theta, z) \tag{1}$$

a přičítání k tomuto vztahu konkrétních hodnot charakteristik hlavy lidského jedince. Každou lidskou hlavu lze pak vyjádřit vztahem:

$$r = f_0(\theta, z) + \sum_i \alpha_i \Psi_i(\theta, z), \tag{2}$$

kde $\{\alpha_i\}$ jsou koeficienty konkrétní lidské hlavy. Dále je pak tento vztah obohacen o aplikování Lambertova zákona, který definuje intenzitu a absorpci světla, přičemž v této problematice se využívá k určení poměru mezi odráženým a dopadajícím světlem a určení světelného toku v obraze [8].

Pokud se tedy přesně naprogramuje pomocí této metody soubor algoritmů pro lidskou tvář či hlavu a počítač bude schopen zanalyzovat světelný tok v obraze, pak můžeme označit

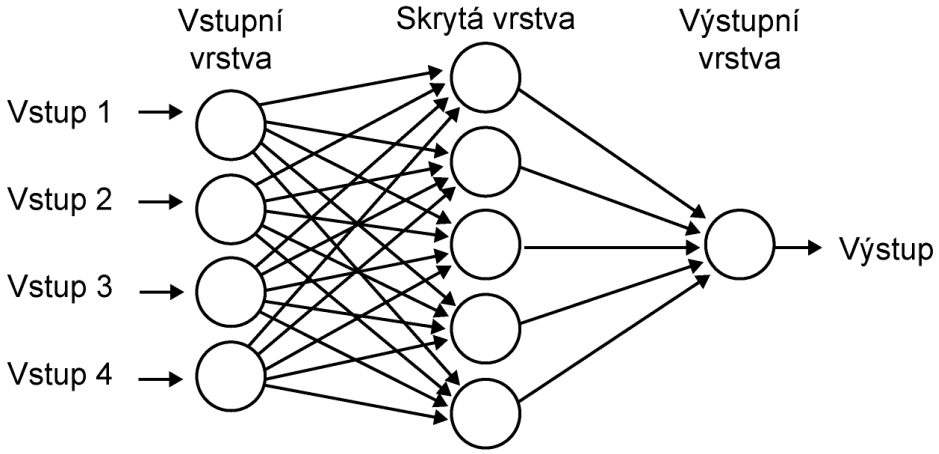
identifikaci lidské tváře pomocí této metody za velmi účinnou při standartních podmínkách.

3.2 Metoda neuronových sítí

O neuronových sítích můžeme hovořit jako o algoritmech na bázi umělé inteligence, které jsou schopny adaptabilního učení. Počítačové neuronové sítě pracují na stejném principu jako lidský mozek. Základní složkou celého nervového systému člověka je nervová buňka, která je nazývána neuron. Pokud si dokážeme představit jednotlivé nervové uzliny lidského mozku a nervové sítě jako komplex mnoha vzájemně propojených informačních center, získáme i představu o tom, jak pracují umělé neuronové sítě, aplikované v počítačových technologiích. Stejně jako lidský mozek se umělé neuronové sítě učí na základě kognitivních procesů a zkušeností s tím rozdílem, že umělým neuronovým sítím, za předpokladu adekvátní hardwareové podpory, odpadá proces zapomínání a s každým dalším přísunem informací se stávají inteligentnějšími.

Umělé neuronové sítě mohou být použity v situacích, kdy získané informace určené k analýze jsou nekompletní či porušené. Lineárně řešené algoritmy směřující přesně určeným postupem k výsledku mohou být v těchto případech neefektivní a v krajních situacích neúčinné [8].

Původně byly všechny umělé neuronové sítě navrženy pouze jako simulace fungování lidského mozku, ale posléze se projevily, jako účinný nástroj sám o sobě. První umělou neuronovou sítí byla síť Perceptron, kterou vymyslel v padesátých letech minulého století americký psycholog Frank Rosenblatt. Síť byla zkonstruována pro rozeznávání obyčejných objektů na základě zpracování obrazu, stejně jako tomu je u dětí, které se učí vnímat okolní svět [8].



Obr. č. 9 – Schéma zpracování informace neuronem [17]

Umělá neuronová síť pracuje tak, že každému prvku v síti je vysláno velké množství informací ke zpracování, přičemž analýza a postupné vyhodnocování dat je zpracováno v několika skrytých vrstvách, takže se nedá vysledovat, co se během zpracování děje, a následně pracující prvek vytvoří jeden sjednocený výstup, který slouží jako vstupní informace pro jiný neuron. Každá umělá neuronová síť je vytvářena implicitně s náhodnými informacemi obsažených v každém z neuronů, které se postupem času mění vzhledem k účelnosti konkrétní umělé neuronové sítě v rámci jejího učení [8].

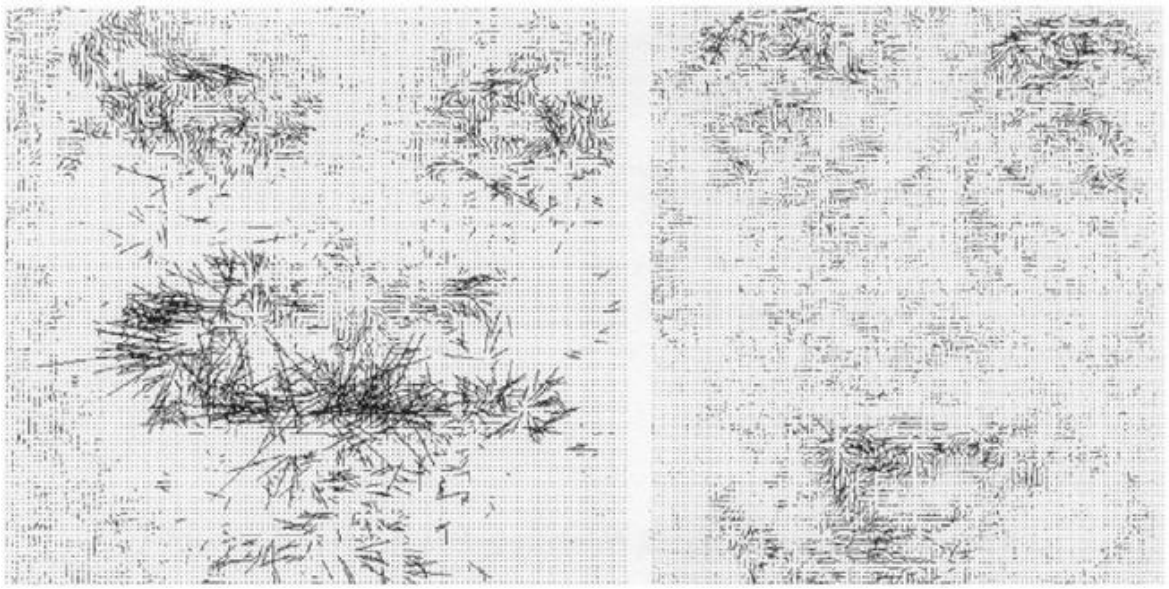
U problematiky, týkající se identifikace, algoritmy umělých neuronových sítí, určených k rozpoznání lidské tváře, klasifikují obrazy do dvou tříd a to do obrazů, které obsahují tvář, a do obrazů, v nichž se tvář nevyskytuje. Práce neuronových sítí je značně ztížena tím, že ve druhé třídě je příliš mnoho dat, nezahrnujících v sobě prvky specifické lidskému obličeji. Do systémů s neuronovými sítěmi se, pro větší efektivitu a úroveň inteligence systémů, integrují speciální knihovny s obrazy obou tříd [8].

3.3 Metody založené na informaci o pohybu na scéně, optické toky

Jak už z nadpisu vyplývá, u těchto metod je potřeba více než jeden snímek a zkoumají se rozdíly v obraze v rámci časové posloupnosti. Pokud je v určité oblasti zaznamenán pohyb, zkoumá se tato část obrazu dál pro hledání markantů, specifikujících lidskou tvář. Jedna z hojně používaných metod se nazývá „optic flow“ a je určena mimo lokalizaci tváře i k rozpoznání [8].

„Optic flow“ můžeme z angličtiny přeložit jako „optický tok“, čímž je myšlena právě změna strukturální podoby celého obrazu a zároveň změna intenzity světla v jednotlivých obrazových segmentech. Pohyb v obraze i s intenzitou světla se dá při zohlednění rychlosti

pohybu na scéně zapsat vektorově, a tak optickým tokem může být určen charakter i výraz tváře. Díky těmto poznatkům nacházejí tyto metody uplatnění zejména v oblasti rozpoznávání emocí, jak můžeme vidět na Obr. č. 10, kdy v levé části je optickými toky zobrazena tvář vyjadřující úsměv a pravá část zobrazuje grafické zpracování optických toků pro údiv. Můžeme vidět, že největší změny se projeví zejména v oblastech mimických svalů úst a v okolí obočí [8], [19].



Obr. č. 10 – *Ukázka optických toků* [8]

3.4 Ostatní metody

Metody založené na rozložení odstínu šedi v obraze

Technologie pracující na tomto principu využívají faktu, že poměr odstínů šedi částí tváře je i na zcela rozdílných osobách za normálních světelných podmínek přibližně stejný. Vytváří se tak výborné podmínky pro detekci lidského obličeje v obraze. Za nejznámější z těchto metod je považována metoda mozaiky. Tato metoda spočívá v rozdělení obrazu na čtvercovou síť o velikosti 4x4 polí (či 3x3 polí u alternativních zpracování této metody) a v jednotlivých polích jsou pak hledány markanty tváře, které by měly odpovídat pravidlům týkajících se poměrů odstínu šedé u lidské tváře. Bloky, které vyhovují těmto pravidlům, podstoupí podobně jako na principu geometrických fraktálů další segmentování do detailnějších čtvercových sítí s tím rozdílem, že velikost sítí nižší úrovně je 8x8 polí. Takto se opět vyřadí čtvercová pole, která neobsahují část tváře a pomocí metody detekování hran se určuje i přesná pozice jednotlivých charakteristických bodů jako jsou oči, ústa a další [8], [18].

Metody založené na rozpoznávání obličejových obrysů

Princip této metody spočívá v transformaci obrazu do konturových linií, avšak kolizní situace nastává v případě, že stroj není schopen přesně určit, které obrysy připadají křivkám obličeje. Absolutní efektivity dosáhneme jen v případě kombinace s jinými metodami a právě tehdy se stává tato metoda jednou z nejefektivnějších [8]

Metody založené na informaci o barvách

Tyto metody jsou založeny na myšlence, že lidská kůže (ať už jde o jakoukoliv rasu) vyzařuje specifické barevné spektrum, oproti ostatním objektům v obraze. Problémy nastávají při malé viditelnosti nebo naopak při přesvětlení scény, kdy obraz ztrácí na barevnosti a pravděpodobnost úspěšné detekce tváře klesá [8].

Algoritmy založené na těchto metodách jsou tedy vhodné jen do vnitřních prostor s adekvátním osvícením, a proto jsou bezpečně aplikovatelné spíše u přístupových systémů.

Metody založené na symetrii

Jeden z faktů, na kterém se dá zakládat je ten, že lidská tvář bez vnějších defektních vlivů od narození do určité míry osově souměrná dle vertikální přímky procházející špičkou nosu a středem úst. Touto metodou se zabývalo mnoho výzkumníků, ač každý výzkumný tým využíval odlišné principy symetrie v obraze. Tým vědců Zabrodsky, Peleg a Avnir se zaměřil na zkoumání symetrie v kruhových oblastech obrazu a matematicky mělo být rozhodnuto, zda oblast odpovídá charakteristikám tváře [20]. Dalším možným přístupem je metoda týmu Reinsfield, Wolfson a Yshurun, jenž se zaobíral se symetrickou transformací, která v rámci obrazu hledá osově sdružené body, odpovídající markantům tváře, které slouží k definování obličeje v obraze [8], [21].

4 PRÁVO A ANONYMITA

Jedno z témat, zaměřených na stanovení rovnováhy mezi opatřeními pro zajištění bezpečnosti veřejné společnosti a ochranou základních lidských práv a svobod, je otázka stanovení možné přípustné míry anonymity jedince ve společnosti tak, aby nezpůsobovala rizika, vznikající při nedohledatelnosti identity potencionálního pachatele jakékoliv protiprávní činnosti. V České republice se na vymezení právního rámce soukromí člověka uplatňují v praxi zejména dokumenty, jako jsou:

- Listina základních práv a svobod, která je od roku 1992 součástí ústavního pořádku České republiky, když byla přijata jako ústavního zákon č. 2/1992 Sb. [22];
- Zákon č. 89/2012 Sb. [23] neboli nový občanský zákoník, který vyšel v platnost 1. ledna 2015;
- Zákon č. 101/2000 Sb. [24] o ochraně osobních údajů a změně některých zákonů, který byl rovněž aktualizován v návaznosti na zavedení zákona č. 89/2012 Sb..

4.1 Ústavní zákon č. 2/1993 Sb. – Listina základních práv a svobod

Tento dokument je rozdělen do šesti hlav, které specifikují konkrétní lidská práva a svobody. Jednotlivými hlavami jsou:

- Hlava první – Obecná ustanovení;
- Hlava druhá – Lidská práva a základní svobody;
- Hlava třetí – Práva národnostních a etnických menšin;
- Hlava čtvrtá – Hospodářská, sociální a kulturní práva;
- Hlava pátá – Právo na soudní a jinou právní ochranu;
- Hlava šestá – Ustanovení společná.

V rámci hlavy první o obecných ustanoveních, v článku 1, je stanoveno, že veškerá základní práva jsou nezadatelná, nezcizitelná, nepromlčitelná a nezrušitelná pro jakéhokoliv člověka, za nutnosti dodržení podmínky, která udává, že všichni lidé jsou si rovni a svobodni vzhledem k lidské důstojnosti a základním lidským právům. Jinak řečeno člověk má nárok na tato práva a svobody již od narození a není možno, aby mu bylo na jednotlivých právech a svobodách upíráno, či dokonce, aby byla jeho práva zrušena. Jednotlivá lidská práva a základní svobody jsou stanovena v hlavě druhé, která je rozdělena na dva oddíly, a těmi jsou Základní lidská práva a svobody a Politická práva. Pokud se máme zaměřit na právní ustanovení zaměřená na soukromí v rámci této práce, týkají se jich tyto paragrafy:

- Článek 7, odstavec 1 – *„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem.“* [22];
- Článek 10, odstavec 2 – *„Každý má právo na ochranu před neoprávněným zasahováním do soukromého a rodinného života.“* [22];
- Článek 10, odstavec 3 – *„Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“* [22].

Listina základních práv a svobod tedy umožňuje bez výhrad každému člověku mít právo na soukromí, což je ve výsledku i právo na volný a nesledovaný pohyb, protože neoprávněný sběr informací o pohybu jakékoliv osoby se dá považovat jako zásah do soukromí a jinak by nedotknutelnost soukromí nemohla být označena zaručenou.

4.2 Zákon č. 89/2012 Sb. – Občanský zákoník

Občanský zákoník je rozdělen do pěti částí a oproti Listině základních práv a svobod je velmi rozsáhlý, což je způsobeno snahou zákonodárné moci České republiky o pokrytí veškerých krajních právních situací, které by mohly být místem vzniku konfliktů, a proto jsou jednotlivé právní aspekty popsány podrobně a co nejvíce jednoznačně. Pro účel této práce je potřeba znát některé oblasti z druhé části hlavy druhé, první části tohoto zákona, která je věnována fyzickým osobám. Zde jsou předmětem zájmu tyto teze:

- §81, odstavec 2 – *„Ochrany požívají zejména život a důstojnost člověka, jeho zdraví a právo žít v příznivém životním prostředí, jeho vážnost, čest, soukromí a jeho projevy osobní povahy.“* [23];
- §84 – *„Zachytit jakýmkoli způsobem podobu člověka tak, aby podle zobrazení bylo možné určit jeho totožnost, je možné jen s jeho svolením.“* [23];
- §85, odstavec 1 – *„Rozšiřovat podobu člověka je možné jen s jeho svolením.“* [23];
- §86 – *„Nikdo nesmí zasáhnout do soukromí jiného, nemá-li k tomu zákonný důvod. Zejména nelze bez svolení člověka narušit jeho soukromé prostory, sledovat jeho soukromý život nebo pořizovat o tom zvukový nebo obrazový záznam, využívat takové či jiné záznamy pořízené o soukromém životě člověka třetí osobou, nebo takové záznamy o jeho soukromém životě šířit. Ve stejném rozsahu jsou chráněny i soukromé písemnosti osobní povahy.“* [23];

- §88, odstavec 1 – *„Svolení není třeba, pokud se podobizna nebo zvukový či obrazový záznam pořídí nebo použijí k výkonu nebo ochraně jiných práv nebo právem chráněných zájmů jiných osob.“* [23];
- §89 – *„Podobizna nebo zvukový či obrazový záznam se mohou bez svolení člověka také pořídit nebo použít přiměřeným způsobem též k vědeckému nebo uměleckému účelu a pro tiskové, rozhlasové, televizní nebo obdobné zpravodajství.“* [23];
- §90 – *„Zákonný důvod k zásahu do soukromí jiného nebo k použití jeho podobizny, písemnosti osobní povahy nebo zvukového či obrazového záznamu nesmí být využit nepřiměřeným způsobem v rozporu s oprávněnými zájmy člověka.“* [23].

Ve shrnutí občanský zákoník upravuje právo na soukromí tak, že nenarušuje koncept o základních lidských právech, ale umožňuje v některých situacích tato práva omezit či v krajních případech porušit. Je neakceptovatelné, aby byl pořizován záznam o podobě lidského člověka bez jeho svolení. Jsou ovšem případy, které specifikuje §89 a těmi je možné integritu práva na soukromí do určité meze oslabit. Vzhledem k informacím o lidské tváři, které popisují předchozí kapitoly, by mohla být brána lidská tvář jako osobní údaj, se kterým je třeba nakládat tak, aby byla zachována základní práva a svobody.

4.3 Zákon č. 101/2000 Sb. – Zákon o ochraně osobních údajů

V předchozí podkapitole, týkající se nového občanského zákoníku byl zmíněn termín osobní údaj. Pokud bereme v úvahu jakékoliv údaje o osobách, mluvíme o třech typech, kterými podle zákona č. 101/2000 Sb. jsou:

- Osobní údaj, za který se považuje jakákoliv informace, sloužící k přímé či nepřímé identifikaci člověka na základě jemu přiřazeného čísla, kódu nebo množiny prvků, které mají původ identity na fyzické, fyziologické, psychické, ekonomické, kulturní nebo sociální úrovni. Jedná se o údaj, který je ze všech třech zmiňovaných údajů nejvíce uplatňován ve veřejném životě, ale přesto musí být zajištěna bezpečnost nakládání s těmito údaji;
- Citlivý údaj, za který se považuje jakákoliv informace, obsahující data o národnosti, rasovém či etnickém původu, víře, kriminální minulosti, sexuálním životě, politickém přesvědčení, zdravotním stavu, genetických údajích a rovněž jsou citlivým údajem veškeré biometrické informace jakékoliv osoby;
- Anonymní údaj, který je údajem, kterým nelze nijak určit identitu osoby, na níž se údaj vztahuje.

Pokud hovoříme o biometrických metodách, bereme v potaz především citlivé údaje, se kterými není možno manipulovat bez vědomého souhlasu osoby, ke které se údaje vztahují. Výjimkou jsou situace stanovené zákonem, kterými jsou v rámci tohoto zákona například situace, kdy:

- §9, odstavec b) – *„je to nezbytné v zájmu zachování života nebo zdraví subjektu údajů nebo jiné osoby nebo odvrácení bezprostředního závažného nebezpečí hrozícího jejich majetku, pokud není možno jeho souhlas získat zejména z důvodů fyzické, duševní či právní nezpůsobilosti, v případě, že je nezvěstný nebo z jiných podobných důvodů.“* [24];
- §9, odstavec c) – *„se jedná o zpracování při poskytování zdravotních služeb, ochrany veřejného zdraví, zdravotního pojištění a výkon státní správy v oblasti zdravotnictví“* [24];
- §9, odstavec i) – *„se jedná o zpracování podle zvláštních zákonů při předcházení, vyhledávání, odhalování trestné činnosti, stíhání trestných činů a pátrání po osobách.“* [24].

S citlivými údaji je tedy pro bezpečnostní účely možno nakládat jen s cílem ochrany zdraví a majetku osob, zajištění veřejného zdraví a dosažení maximální efektivnosti při dodržování veřejného pořádku a řešení situací, týkajících se trestní činnosti.

II. PRAKTICKÁ ČÁST

5 PRIVACYVISOR

V roce 2013 tým vědců tokijského Japonského Národního Institutu Informačních Technologií ve spolupráci s Univerzitou Kogakuin pod vedením Isao Echizena a Seiichi Goschiho vynalezl technologii brýlí, nazvaných PrivacyVisor, které značně zhoršují podmínky pro úspěšnou strojovou identifikaci dle tváře. Isao Echizen konstatoval, že lidská tvář je citlivým údajem, který by měl být chráněn. Naráží tím na fakt, že je dnes pomocí sdílení fotek v rámci sociálních sítí do velké míry narušováno soukromí. Technologie smart telefonů společně s algoritmy pro rozpoznání obličejů, integrovaných do systémů zmiňovaných sociálních sítí, umožňují narušování soukromí v důsledku ledabylosti nahrávání osobních fotografií jednotlivými uživateli, ač v mnoha případech nebylo zveřejňování fotek schváleno osobou, která se na snímcích vyskytuje schváleno. Vědci Echizen a Goschi proto navrhli brýle, které byly opatřeny jedenácti LED diodami, vyzařující světlo blízké svým světelným spektrem infračervenému záření, které je patrné vidět pouze na kamerových snímcích. Celý princip brýlí spočívá ve zvýšení intenzity světla v oblasti tváře do té míry, aby kamerový systém nebyl schopen detekovat charakteristické rysy lidské tváře a nebyl schopen identifikovat člověka.

Obr. č. 11 – *První prototyp PrivacyVisor* [25]

Na Obr. č. 11 můžeme v levé části vidět tvář člověka vybaveného těmito brýlemi v neaktivním režimu a v pravé části stejného člověka se zapnutými brýlemi. Kamerové systémy při neaktivitě LED diod dokáží bez problému detekovat tvář, ale při použití brýlí

v aktivním režimu je tato schopnost kamerových systémů omezena. Podle vědců tyto brýle nemají vliv na vidění uživatele, který má tyto brýle nasazeny, což je považováno za pozitivní aspekt, ale byla zřetelná určitá negativa, která cílovou veřejnost od užívání brýlí demotivovala. Brýle jsou napájeny lithiovou baterií, což bylo zhodnoceno jako nepraktické, kvůli výměně zdroje energie, a zároveň svým vzezřením přitahují pozornost, tak se vědci rozhodli pro hledání alternativy, pro použitelnost v běžném životě [25], [26], [27].

5.1 Aktuální verze brýlí PrivacyVisor

Od června 2016 bude veřejně distribuován korporací Nissey nový prototyp brýlí PrivacyVisor, který oproti předchozímu prototypu nevyžaduje žádné napájení a rovněž svým vzhledem nepůsobí tak nepřirozeně, jako původní verze brýlí využívající LED diod. Podle oficiálního prohlášení budou brýle prodávány za 240$.

Obr. č. 12 – *Nový prototyp brýlí PrivacyVisor* [28]

Brýle jsou zkonstruovány z titanové mřížky s mapovými vzory o různých provedeních, připevněné na obroučky z bílého plastu. Korporace Nissey uvádí, že není vhodné používat brýle při všech každodenních činnostech, například při řízení auta či jízdy na kole, protože brýle do jisté míry omezují schopnost vidění uživatele.

Celý princip brýlí spočívá v odrážení světla ze zdroje osvětlení do čočky kamery. Brýle mají určitý sklon vůči vertikální ose lidské hlavy, a pokud vezmeme v úvahu předpoklad, že osvětlení snímané scény je shora člověka, ať už uvažujeme sluneční světlo či světlo pouličních lamp, světlo je odráženo do čočky snímacího zařízení, respektive v rámci snímaného obrazu je v okolí očí zvýšená intenzita jasu s doplněním faktu, že několik z významných markantů tváře je brýlemi zakryto, jak je vidět na Obr. č. 13.

Obr. č. 13 – *Osoba s brýlemi PrivacyVisor* [29]

Na Obr. č. 13 je rovněž vidět, jak se chovají snímané brýle při odrazu světla. V levé části hlavy odrážené světlo kontinuálně přechází z čela do oblasti obličeje bez změny intenzity, a tím se oblast očí i oblast čela může kamerovému systému jevit jako jedna a tatáž a rovněž je eliminována viditelnost vodících linek, ohraničujících tyto oblasti.

Profesor Echizen tvrdí, že při pořízení obrazového záznamu pro účely vyšetřování protiprávní činnosti, bude záznam kontrolován i lidským okem, které tyto brýle neobelstí. Jsou ovšem situace, kdy je při shromáždění velkého počtu osob spoléháno na rychlost kamerových systémů při zpracování informací o osobách v obraze, a pokud vezmeme v potaz

možné riziko nebezpečných osob, pohybujících se v davu při demonstracích, tak se tyto brýle můžou stát bezpečnostním rizikem [28], [29].

Pokud bychom chtěli tyto brýle porovnat s vnímáním kamerového systému brýlí slunečních či dioptrických, je už z Obr. č. 14 patrné, že pro kamerový systém nebudou dioptrické brýle problémem pro rozpoznání tváře. Skrze dioptrické brýle je snadno vidět markanty v oblasti očí, a proto pro kamerové systémy není problém obličej ani detekovat, ani identifikovat.

Pokud se zaměříme na brýle sluneční, možnosti kamerových systémů se trochu omezují, ale přesto je identifikace možná. Slunečními brýlemi sice jsou zakryty některé markanty, ale metody pro rozpoznání tváře pracují, jak bylo zmíněno v třetí kapitole, s faktem, že lidská tvář má obecně pro všechny jedince společnou charakteristickou vlastnost, jakou je poměr odstínů šedé. Například oblasti okolo očí jsou tmavší, než je oblast čela či nosu. U typických slunečních brýlí se zakrývá především oblast očí, a to v podstatě způsobí, že je oblast očí na kamerovém záznamu jiného odstínu, ale pořád si zachovává tato oblast určitý rozdíl vůči oblastem čela a nosu. Kamerový systém je pak schopen obličej podle těchto charakteristik detekovat a následně je možné i člověka identifikovat podle zbývajících markantů.

Obr. č. 14 – *Porovnání s dioptrickými a slunečními brýlemi* [30]

Pokud se ovšem vyskytne na snímané scéně člověk vybavený těmito brýlemi, působí to pro kamerový systém značné komplikace. Na Obr. č. 14 si můžeme všimnout, že mřížka brýlí je konstruována tak, že z jedné oblasti očí přechází téměř plynule do oblasti druhé bez

změny výšky mřížky brýlí a zakrývá tak i část nosu. Kamerovému systému takto chybí nejen několik z charakteristických markantů pro detekci obličeje, ale navíc je charakteristika tváře z hlediska analýzy odstínu šedi změněna tak, že tvář neodpovídá univerzálnímu popisu obličeje a lineární algoritmy nejsou schopny rozpoznání.

5.2 Alternativní metody identifikace

Za předpokladu, že brýle PrivacyVisor budou omezovat činnost kamerových systémů do té míry, že nebude možná identifikace dle tváře, zbývají pouze dva typy protiopatření. Jedním možným způsobem je aplikovat biometrické metody pro identifikaci, které nejsou založeny na zpracování tváře nebo aplikovat metody, které nebudou činností brýlí ovlivněny. Jedna z možností je rozšířit databáze obrazů tváří, ze kterých se učí umělé neuronové sítě, o snímky, které budou obsahovat obličeje vybavené brýlemi PrivacyVisor. Umělá neuronová síť by si pak mohla vytvořit svou vlastní charakteristiku lidské tváře s těmito brýlemi navzdory zhoršeným podmínkám, které neumožňují úspěšnou identifikaci lineárně založeným algoritmům. Aplikovatelnost jednotlivých biometrických metod identifikace, využívajících lidskou tvář, bude určena až po podrobnějším prozkoumání brýlí při zahájení prodeje v červnu 2016. V rámci kamerových systémů se dají použít jiné biometrické metody, které nevyužívají principiálně lidské tváře, a těmi jsou identifikace podle dynamiky chůze či identifikace podle tvaru ucha.

ZÁVĚR

Tato práce pojednávala o tématech, které se vzájemně potkávají v oblasti ochrany soukromí a zároveň ochrany veřejného bezpečí. Jakou šanci má tedy anonymita v dnešním světě bezpečnostních technologií?

V první kapitole této práce bylo popsáno, co to je biometrie, a bylo poukázáno na fakt, že každý člověk je identifikovatelný podle některého z biometrických znaků. Pro každý typ identifikace či verifikace, stanovený okolními podmínkami, je vhodné používat jiného biometrického znaku. Pro identifikaci na dálku je nejvhodnějším kandidátem lidská tvář.

Proto byla druhá kapitola věnována lidské tváři z hlediska historie její analýzy pro forenzní a soudní účely. V této kapitole byly popsány metody analyticko-statistická a grafická. Tyto metody byly stavebním kamenem pro metody rozpoznání a identifikace strojem.

Ve třetí kapitole byly cílem zkoumání zmíněné metody rozpoznání strojem. Pozornost byla věnována především metodě eigenface, metodě optických toků a metodě aplikace umělých neuronových sítí, ale byly popsány i ostatní metody kterými jsou metody založené na rozložení odstínu šedi v obraze, metody založené na rozpoznávání kontur obličeje, metody založené na informaci o barvách či metody založené na symetrii tváře.

Náplní čtvrté kapitoly bylo pojednání o legislativě České republiky, zaměřující se na oblast soukromí a oblast práce s osobními či citlivými údaji. V souvislosti s těmito oblastmi se v České republice uplatňují prameny, kterými jsou Listina základních práv a svobod, Občanský zákoník a Zákon o ochraně osobních údajů. Z analýzy těchto pramenů vyplývá, že výše zmíněná tvář může být považována za citlivý údaj, jelikož je to biometrický znak, avšak existují v rámci zákona podmínky, kdy není potřeba souhlas pro práci s obrazovým záznamem obličeje určitého jedince. Jednou z těchto situací je stíhání trestné činnosti.

Pátá kapitola byla věnována technologii brýlí PrivacyVisor. Byl popsán princip těchto brýlí, které znemožňují identifikaci lidské tváře již v prvopočátku tohoto procesu a tím je detekce obličeje v obraze. Byly hledány způsoby jak tuto technologii obejít, aby byla identifikace dle tváře účinná, ale vzhledem ke konstrukci brýlí a jejich funkcím nelze aplikovat běžné metody rozpoznání kamerovým systémem. Jedním z možných způsobů by mohlo být naučení umělých neuronových sítí rozpoznání tváře s těmito brýlemi, ale tento proces je možné uskutečnit, až v době, kdy bude technologie PrivacyVisor na trhu k dostání. Jinou

možností je aplikace jiných biometrických metod pro identifikaci, které jsou uplatňovány v kamerových systémech.

Anonymita jedince a zachování jeho soukromí není v dnešním světě prioritou. Prioritou by mělo být bezpečné prostředí, které vyžaduje určité narušení soukromí. V ideální společnosti by tyto dva protipóly rovnoměrně vyvažovány, ovšem kde leží střed této rovnováhy nelze určit s jistotou, protože názor na tato dvě témata a jejich vnímání bude vždy subjektivní.

SEZNAM POUŽITÉ LITERATURY

[1] Výhody a nevýhody biometrických systémů. *Scienceworld* [online]. Praha: F - solutions, 2008 [cit. 2016-04-01]. Dostupné z: http://www.scienceworld.cz/biologie/vyhody-a-nevyhody-biometrickych-systemu-1-515/

[2] VACH, Martin. Historie biometrik a její využití ve výpočetní technice. *Fakulta Informatiky Masarykovy Univerzity* [online]. Brno: Masarykova univerzita, 2003, aktualizováno 12. 4. 2003 [cit. 2016-04-01]. Dostupné z: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xvach_biometriky.htm

[3] Alphonse Bertillon. *Encyclopaedia Britannica* [online]. Chicago, Illinois: En cyclopædia Britannica®, 1997 [cit. 2016-04-07]. Dostupné z: http://www.britannica.com/biography/Alphonse-Bertillon

[4] JEDLIČKA, Miloslav. Louis Alphonse Bertillon: francouzský kriminalista. *Kriminalistika a příbuzné obory* [online]. JuDr. Miloslav Jedlička, 2013, aktualizováno 27. 2. 2016 [cit. 2016-04-01]. Dostupné z: http://kriminalistika.eu/muzeumzla/bertilon/bertilon.html

[5] Alphonse BERTILLON. Signaletic Instructions, Including the Theory and Practice of Anthropometrical Identification. 1896 [cit. 2016-04-01]. ISBN 10.2307/2842360. Dostupné z: http://goo.gl/7oNGzj

[6] SULOVSKÁ, Kateřina. Biometrické systémy zaměřené na rozpoznávání tváře, je jich spolehlivost a základní metody pro jejich tvorbu. *Posterus* [online]. 2011, **4**(9), 14 [cit. 2016-04-01]. ISSN 1338-0087. Dostupné z: http://www.posterus.sk/?p=11511

[7] HESELTINE, Thomas a Nick WHITEHEAD. Facial Recognition. *Ingenia* [online]. 2011, **2011**(48), 6 [cit. 2016-04-01]. Dostupné z: http://www.ingenia.org.uk/Ingenia/Articles/727

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

[9] JAIN, A.K., A. ROSS a S. PRABHAKAR. An Introduction to Biometric Reco gnition. *IEEE Transactions on Circuits and Systems for Video Technology* [online].

2004, **14**(1), 4-20 [cit. 2016-05-11]. DOI: 10.1109/TCSVT.2003.818349. ISSN 1051-8215. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=1262027

[10] Autorizace (oprávnění). *ManagementMania.com* [online]. Wilmington, USA: MANAGEMENTMANIA.COM LLC, 2011 [cit. 2016-04-07]. Dostupné z: https://managementmania.com/cs/autorizace

[11] Luxand - Blink!. *Luxand - Face Recognition, Face Detection and Facial Feature Detection Technologies* [online]. Alexandria, USA: Luxand Inc., 2005 [cit. 2016-04-07]. Dostupné z: https://www.luxand.com/blink/

[12] ŠČUREK, Radomír. *Biometrické metody identifikace osob v bezpečnostní praxi: Studijní text, VŠB TU Ostrava*. Ostrava, 2008. Dostupné také z: https://www.fbi.vsb.cz/export/sites/fbi/040/.content/sys-cs/resource/PDF/biometricke_metody.pdf

[13] POLEVOJ, Nikolaj Stepanovič. *Kriminalističeskaja kibernetika: teorija i praktika matematizacii i avtomatizacii informacionnych processov i sistem v kriminalistike*. Izd. 2., pererabotannoje i dopolnennoje. Moskva: Izdatel'stvo Moskovskogo uni versiteta, 1989. ISBN 5-211-00253-9.

[14] BHABATOSH CHANDA AND DWIJESH DUTTA MAJUMDER. *Digital image processing and analysis*. Eastern economy ed. New Delhi: Prentice Hall of India, 2005. ISBN 81-203-1618-5.

[15] ZHUJIE a Y.L. YU. Face recognition with eigenfaces. *Proceedings of 1994 IEEE International Conference on Industrial Technology - ICIT '94* [online]. IEEE, 1994, , 434-438 [cit. 2016-04-08]. DOI: 10.1109/ICIT.1994.467155. ISBN 0-7803-1978-8. Dostupné z: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=467155

[16] ULRYCH, T. CDSST: Eigenfaces. *University of British Columbia* [online]. Van couver: UBC, 2007 [cit. 2016-04-08]. Dostupné z: https://www.eoas.ubc.ca/research/cdsst/Tad_home/eigenfaces.html

[17] HOLČÍK, Jiří a Martin KOVENDA. *Matematická biologie: e-learningová učebni ce: Koncept umělé neuronové sítě* [online]. Brno: Masarykova univerzita, 2015 [cit.

2016-05-11]. ISBN 978-80-210-8095-9. Dostupné z: http://portal.matematickabiologie.cz/

[18] YANG, Guangzheng a Thomas S HUANG. Human face detection in a complex background. *Pattern Recognition* [online]. 1994, **27**(1), 53-63 [cit. 2016-04-08]. DOI: 10.1016/0031-3203(94)90017-5. ISSN 00313203. Dostupné z: http://linkinghub.elsevier.com/retrieve/pii/0031320394900175

[19] RUSHTON, Simon K., BEARDSLEY, Scott A. a Lucia M. VAINA (eds.). *Optic flow and beyond*. 1. Dordrecht: Springer, 2011. ISBN 978-904-8165-896.

[20] ZABRODSKY, H., S. PELEG a D. ANVIR. *Symmetry as a Continuous Feature* [online]. Jeruzalém, Izrael, 1995 [cit. 2016-04-09]. Dostupné z: http://www.vision.huji.ac.il/papers/continuous-symmetry.pdf. The Hebrew Uni versity of Jerusalem.

[21] REISFELD, Daniel, Haim WOLFSON a Yehezkel YESHURUN. Context-free at tentional operators: The generalized symmetry transform. *International Journal of Computer Vision* [online]. 1995, **14**(2), 119-130 [cit. 2016-04-10]. DOI: 10.1007/BF01418978. ISSN 0920-5691. Dostupné z: http://link.springer.com/10.1007/BF01418978

[22] *Listina základních práv a svobod*. In: . Praha: Předsednictvo Národní rady České republiky, 1993, ročník 1993, číslo 2. Dostupné také z: http://www.psp.cz/docs/laws/listina.html

[23] *Občanský zákoník*. In: . Praha: Parlament České republiky, 2012, ročník 2012, číslo 89. Dostupné také z: http://www.zakonyprolidi.cz/cs/2012-89

[24] *Zákon o ochraně osobních údajů a změně některých zákonů*. In: . Praha: Parlament České republiky, 2000, ročník 2000, číslo 101. Dostupné také z: https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-ledna-2015/ds-3109/archiv=0&p1=1261

[25] Privacy goggles fool hidden facial-recognition cameras. *The Japanese Times* [onli ne]. Tokyo: The Japanese Times, Ltd., 2013 [cit. 2016-05-15]. Dostupné z: http://www.japantimes.co.jp/news/2013/01/29/national/science-health/privacy-goggles-fool-hidden-facial-recognition-cameras/

[26] Foil face-recognition cameras with Privacy Visor. *Product reviews, how-tos, deals and the latest tech news - CNET* [online]. San Francisco: CBS Interactive, Inc., 2013 [cit. 2016-05-15]. Dostupné z: http://www.cnet.com/news/foil-face- recogniti on-cameras-with-privacy-visor/

[27] Japanese professors design infrared glasses to thwart facial recognition. *Biometric News | Biometric Articles | Biometric Companies* [online]. Toronto: Biometrics Research Group, Inc., 2013 [cit. 2016-05-15]. Dostupné z: http://www.biometricupdate.com/201301/japanese-professors-design-infrared-glasses-to-thwart-facial-recognition

[28] Glasses That Confuse Facial Recognition Systems Are Coming to Japan. *Mother Board* [online]. New York: Vice Media LLC, 2015 [cit. 2016-05-15]. Dostupné z: http://motherboard.vice.com/read/glasses-that-confuse-facial-recognition-systems-are-coming-to-japan

[29] Privacy Visor thwarts facial-recognition tech. *The Japanese Times* [online]. Tokyo: The Japanese Times, Ltd., 2016 [cit. 2016-05-15]. Dostupné z: http://www.japantimes.co.jp/news/2016/05/13/national/privacy-glasses-thwart-face-recognition-tech/

[30] The latest accessory to flummox facial recognition cameras – the Privacy Visor!. *Naked Security by Sophos* [online]. Abingdon (UK): Sophos Ltd., c1997-2016 [cit. 2016-05-24]. Dostupné z: https://nakedsecurity.sophos.com/2015/08/13/the-latest-accessory-to-flummox-facial-recognition-cameras-the-privacy-visor/

Seznam použitých symbolů a zkratek

DNA	Nosič genetické informace
LED	Světlo vyzařující dioda
PC	Osobní počítač
Sb.	Sbírka zákonů České republiky
USA	Spojené Státy Americké

SEZNAM OBRÁZKŮ

SEZNAM TABULEK