

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

**FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ**

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

ANONYMIZACE SPZ VOZIDEL ZACHYCENÝCH NA FOTOGRAFIÍCH

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

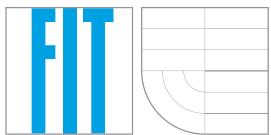
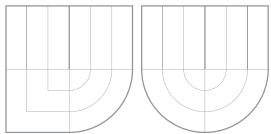
AUTOR PRÁCE
AUTHOR

Bc. BARBORA SKŘIVÁNKOVÁ

BRNO 2016



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF COMPUTER SYSTEMS

ANONYMIZACE SPZ VOZIDEL ZACHYCENÝCH NA FOTOGRAFIÍCH

CAR LICENCE PLATE ANONYMIZATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. BARBORA SKŘIVÁNKOVÁ

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. MICHAELA ŠIKULOVÁ

BRNO 2016

Abstrakt

Abstract

Klíčová slova

Keywords

Citace

Barbora Skřivánková: Anonymizace SPZ vozidel zachycených na fotografiích, diplomová práce, Brno, FIT VUT v Brně, 2016

Anonymizace SPZ vozidel zachycených na fotografiích

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně pod vedením Ing. Michaly Šikulové a uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala. Další informace mi poskytl Ing. Adam Kolář ze společnosti Seznam.cz.

.....
Barbora Skřivánková
25. října 2015

Poděkování

© Barbora Skřivánková, 2016.

Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Obsah

1	Úvod	2
2	Anonymizace obrazových dat	3
2.1	Osobní údaje a jejich ochrana	3
2.2	Anonymizace	4
2.3	Metody využívané v současnosti	4
2.3.1	Manuální anonymizace	6
2.3.2	Automatizovaná anonymizace	6
3	Neuronové sítě	7
3.1	Biologický základ neuronových sítí	7
3.2	Umělý neuron	8
3.2.1	Bázová funkce	9
3.2.2	Perceptron	9
3.2.3	Aktivační funkce	9
3.3	Topologie sítí	9
3.4	Učení	9
3.5	Hluboké neuronové sítě	9
4	Návrh	12
4.1	Použitá neuronová síť	12
4.1.1	Na čem je natrénovaná	12
4.2	Finetunning	12
4.2.1	Zvolená metoda	12
4.3	Detekce SPZ v obrázku s autem	12

Kapitola 1

Úvod

Kapitola 2

Anonymizace obrazových dat

Anonymizace dat je v dnešní době velmi aktuálním tématem. Velmi intenzivně se na ní pracuje jak na úrovni datové, tak na úrovni anonymizace obrazových dat, která je také předmětem této práce. Pokud je společnost schopna zajistit kvalitní anonymizaci dat, která spravuje, nejen, že tím plní svoje zákonné povinnosti, může si tím také vylepšit svoje jméno v očích zákazníků a společností, se kterými spolupracuje.

Tato kapitola se blíže zabývá legislativním podtextem ochrany osobních údajů v sekci , dále potom v sekci / popisem pojmu anonymizace dat a v sekci / jsou popsány metody, které se k anonymizaci dat používají v součastnosti.

2.1 Osobní údaje a jejich ochrana

Ochrana osobních údajů v České republice představuje soubor práv a povinností, které se vztahují k uchovávání a zacházení s daty přímo se týkajícími dané fyzické osoby. Osobní údaje nemusí být vždy přímo identifikující danou osobu (jako je například rodné číslo, jméno a příjmení, adresa trvalého bydliště apod.). Za osobní údaje jsou považovány jakékoliv údaje přímo související se životem konkrétní nebo určitelné osoby. Může jít například o provozování koníčků, členství v politických stranách, účast na specifických událostech, návštěvy různých míst, velikost oblečení a podobně. Ochrana osobních údajů (ochrana osobních dat) je v České republice regulována zákonem č. 101/2001 Sb., o ochraně osobních údajů a o změně některých zákonů a dalšími právními předpisy.

Zákon rozlišuje osoby, které zpracovávají osobní údaje (správce osobních údajů) a osoby, jejichž data správci zpracovávají (subjekt osobních údajů). Správcům jsou zákonem ukládány především povinnosti, zatímco subjektům údajů jsou dána práva. Dodržování práv a povinností obou stran je v České republice kontrolováno prostřednictvím Úřadu na ochranu osobních údajů.

Základní ideou ochrany osobních údajů je ta, že osobní údaje jsou shromažďovány a zpracovávány za nějakým účelem. Každý účel vyžaduje jiný typ osobních údajů a také jiné množství takto zpracovávaných osobních údajů. Ve výše uvedeném zákoně byly pro bližší specifikaci těchto účelů zavedeny pojmy účel zpracování, prostředky zpracování, způsob zpracování, kategorie osobních údajů, kategorie subjektů údajů a kategorie příjemců. V těchto termínech je třeba zpracovávání osobních údajů popsat. [citace ze zakona, pod carou: vyklaď z <http://www.oou.cz/>]

V této práci se budu věnovat zpracovávání obrazového materiálu nasbíraného na veřejném prostranství. Vzhledem k tomu, že veřejné prostranství je vždy snímáno za běžného

dne, spolu s terénem, který je snímán, jsou nasnímáni i lidé a další objekty, které se v daném prostranství pohybují. Jak bylo řečeno dříve v této kapitole, veškeré informace, které mohou prozradit jakékoli údaje přímo související s životem dané osoby jsou považovány za osobní údaje. Z toho vyplývá, že i obrazový materiál nasnímaný na veřejném místě obsahující cizí osoby nebo automobily obsahuje osobní údaje a je třeba se věnovat způsobu jejich zpracování.

V dnešní digitální době máme k dispozici velké množství obrazových dat. V této práci se budu věnovat datům zachytávaným pro účely vizualizace prostoru z mapy nasbírané v rámci služby Panorama společnosti Seznam.cz. Tato data jsou sbírána prostřednictvím speciálně upravené panoramatické kamery, která je umístěna na střeše vozidla. Toto vozidlo při průjezdu zpracovávanou lokalitou snímá svoje okolí a pořízený obrazový materiál se poté zpřístupňuje široké veřejnosti. Publikování obrazového materiálu, na kterém se vyskytují osobní údaje jako jsou SPZ vozidel, obličeje kolemjdoucích a podobně je velmi citlivou záležitostí. Aby bylo minimalizováno riziko zneužití těchto údajů, byla zvolena možnost anonymizace.

2.2 Anonymizace

Anonymizovaná data jsou taková data, která nemohou vést přímo k identifikaci konkrétního člověka. Pokud jsou data obsahující osobní údaje anonymizována, přestávají podléhat přísným regulacím Zákona o ochraně osobních údajů a lze s nimi nakládat volněji.

Hranici, kdy jsou data už anonymizována nelze zcela jednoznačně definovat a anonymizaci je třeba pro každou specifickou skupinu dat posuzovat individuálně. Pouhé začernění jména v dokumentech malé firmy například nemusí vést k tomu, že konkrétní osoba nebude dle dalších vodítek v dokumentech identifikovatelná. Příklad toho, že stejná úroveň anonymizace nemusí mít vždy stejné výsledky může sledovat porovnáním obrázků 2.1 a 2.2. Oba obrázky jsou zpracovány stejným rozostřovacím filtrem. U SPZ na obrázku 2.1 by bylo dekódování původní poznávací značky automobilu

2.3 Metody využívané v současnosti

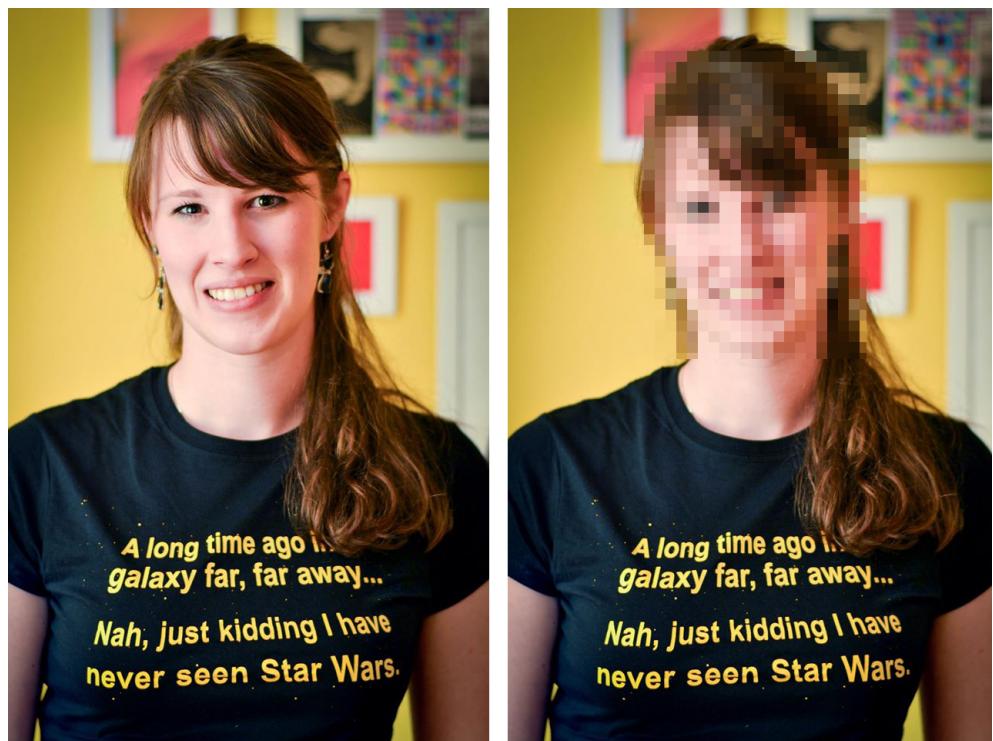
Datová anonymizace dosáhla v současné době uspokojivé úrovně. Úspěšně anonymizována jsou jak data v pdf dokumentech, tak v databázích. Datovou anonymizaci lze v dnešní době provádět plně automaticky prostřednictvím mnoha nástrojů jak komerčních, tak volně dostupných.

Anonymizace v obrazových datech zatím nedosáhla tak vysoké úrovně a to hned z několika důvodů: 1. Anonymizace v obrazových datech je velmi aplikáčně specifická - nemí proto tak velký tlak na její vývoj 2. Anonymizace obrazových dat je výpočetně náročnější než anonymizace na úrovni datové 3.

Anonymizace obrazových dat sestává ze dvou částí: detekce části obrázku určené k anonymizaci a vlastní proces anonymizace. Je zřejmé, že vlastní proces anonymizace už není výpočetně nijak náročný proces. Jedná se zpravidla o aplikaci rozostření, případně o přidání vrstvy, která plně překrývá anonymizované části obrázku. Problematická však je detekce části obrázku určené k anonymizaci.



Obrázek 2.1: Anonymizovaná SPZ vozidla.



Obrázek 2.2: Anonymizovaný obličej.

2.3.1 Manuální anonymizace

Po dlouhou dobu byla anonymizace obrazových dat potřeba většinou na malém objemu dat (například ve zpravodajství a podobně). V takovém případě je naprosto dostačující provádět výběr části obrázku, která je určena k anonymizaci manuálně.

Kvalita takto anonymizovaného obrázku je velmi dobrá, protože člověk přímo vidí výsledek a dokáže korigovat rozsah provedené úpravy tak, aby výsledný obrázek byl skutečně anonymní. Na svoje limity tato metoda však naráží při nárůstu množství anonymizovaných dat.

Pro představu při zpracovávání dat pro službu Panorama vzniknou každý snímací den 4TB obrazového materiálu z každého snímajícího vozidla. Takové množství dat už není v rozumném čase možné zpracovávat manuálně a tak je třeba vytvořit automatizovanou variantu.

2.3.2 Automatizovaná anonymizace

Automatizovaná anonymizace obrazových dat je zatím na počátku svého vývoje.

Eyedea anonymization - to se používá v Seznamu. TODO: zjistit jak to funguje a jaké jsou alternativy.

Zásadním problémem automatizované anonymizace, hlavně při anonymizaci SPZ vozidel, jsou chyby vzniklé při detekci SPZ. Ty jsou totiž často detekovány i na místech, na kterých se sice na fotografii vyskytuje text, nikoliv však SPZ. Při použití anonymizovaných dat pro službu Panorama je tento druh chyb nepřijatelný. Jde totiž o omezení jednoho z důležitých účelů služby Panorama. Uživatelům slouží hlavně pro lepší orientaci v terénu, který neznají. Pokud chce uživatel službu využít k rychlejšímu nalezení nějaké prodejny, je naprosto nežádoucí, aby v rámci automatické anonymizace SPZ vozidel byly anonymizovány i např. nápisy nad vstupy do obchodů a provozoven. V aktuálním stavu automatizované anonymizace je právě tato závada velmi častá. V této práci bude ukázáno, jakým způsobem se těmto chybám vyvarovat.

Kapitola 3

Neuronové sítě

Neuronové sítě jsou jednou ze tří hlavních podskupin vědního oboru soft computing. Dalšími problematikami, které tato vědní disciplína zkoumá jsou fuzzy systémy a evoluční algoritmy. Tato práce se věnuje hlubokým neuronovým sítím pracujícím nad obrázkovými daty. Neuronové sítě jsou uvedeny do širšího kontextu v této kapitole.

3.1 Biologický základ neuronových sítí

Při studiích v oborech biologie a biofyziky bylo během posledních několika dekád odhaleno mnoho principů, díky kterým se můžeme přiblížit pochopení funkce naší nervové soustavy a mozku. Základní stavební jednotkou lidského těla je buňka, základní stavební jednotkou nervové soustavy potom je *neuron*. Hlavní součásti neuronu jsou *dendrity*, *axony* a *tělo buňky (soma)*, jak je znázorněno na obrázku 3.1. Těchto neuronů se v lidské nervové soustavě nachází cca 10^{11} .

Dendrit – Vstupní bod neuronu. Přes dendrity se do těla neuronu dostávají elektricko-chemické vzruchy, jejichž přenos je hlavní činností neuronu.

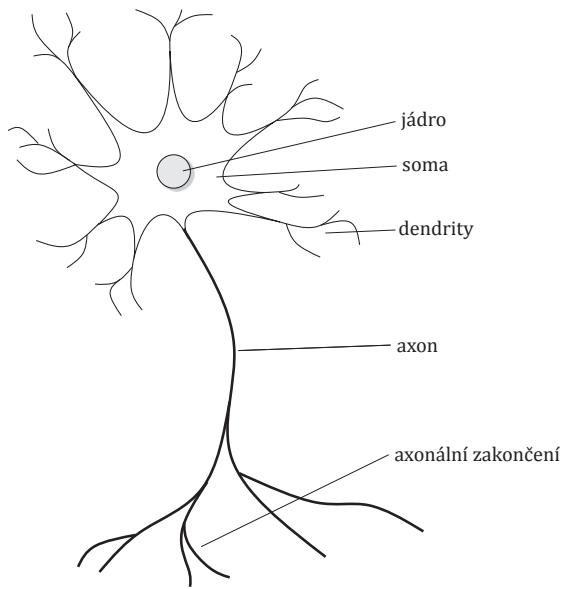
Axon – Část neuronu, která zajišťuje přenos vzruchů. Je ukončena *axonálním zakončením*, které je výstupním bodem neuronu a nachází se velmi blízko dendritu jiného neuronu.

Synapse – Spojení mezi dvěma neurony - přesněji mezi dendritem a axonálním zakončením. V dnešní době není aktivita mozku měřena v počtu neuronů, nýbrž právě v počtu synapsí.

Neurotransmíter – chemická látka, která zajišťuje přenos informací v mozku. V této práci budu mluvit o přenosu elektricko-chemického vzruchu v synapsi, ale neurotransmitery mají v nervové soustavě mnohem širší funkci.

Soma – tělo buňky. Sleduje, zda-li suma potenciálů přicházejících z jednotlivých dendritů nepřesáhla dný prah a pokud se tak stane, vygeneruje nový vzruch.

V okamžiku, kdy se v těle neuronu nashromáždí dostatečně velký potenciál, začne se šířit nervovým vláknem (axonem) až k axonálnímu zakončení. Tady přejde do dalšího neuronu. Velikost signálu přenášená z dendritu do těla neuronu závisí na síle impulzu sousedního neuronu, kterého se dendrit dotýká a také na *synaptické váze*. V těle neuronu se sečtou hodnoty signálů od všech aktivních dendritů. Pokud součet hodnot překročí jistý prah, soma



Obrázek 3.1: Schéma biologického neuronu. Na obrázku je zobrazeno *jádro*, které uchovává genetickou informaci buňky, *soma* je tělo buňky, *dendrity* jsou vstupní body neuronu, *axon* jsou výstupní výběžky tvořená axonovými vlákny a *axonální zakončení* jsou výstupní místa neuronu.

vygeneruje nový impulz a tím se vznich šíří do dalších neuronů. Bezprostředně po vytvoření pulzu se neuron stane na chvíli necitlivým. To má za následek generování nespojitého signálu, jehož frekvence se může pohybovat v rozmezí 0,1-100Hz.

3.2 Umělý neuron

Princip biologického neuronu je napodobován umělým neuronem. Nejzákladnější model umělého neuronu je zobrazen na obrázku 3.2, kde

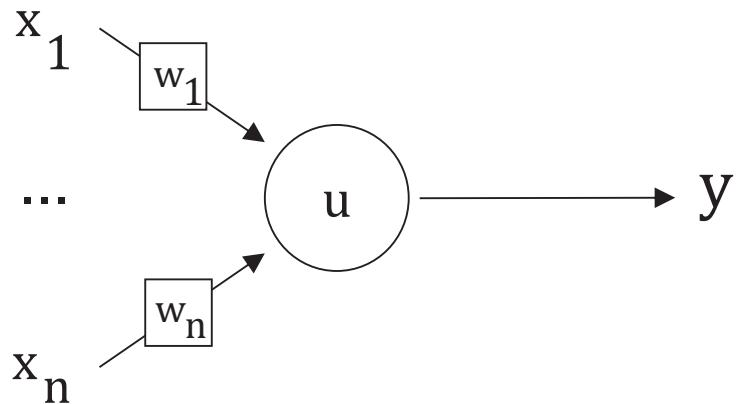
x_i je vstupní hodnota, která může být napojena na primární vstup nebo na výstup jiného neuronu.

w_i je váha propojení. Určuje jak moc bude konkrétní vstup i ovlivňovat výstup neuronu. Váhy se v průběhu výpočtu mění, případně přes neměnnou váhu může být připojen tzv. *bias*.

u je hodnota vnitřního potenciálu, která je závislá na zvolené bázové funkci. Nejčastěji využívané jsou dvě:

- **Lineární**, pro kterou platí

$$u = \sum_{i=1}^n x_i * w_i \quad (3.1)$$



Obrázek 3.2: Obecné schéma umělého neuronu, kde $\vec{x} = (x_1, x_2, \dots, x_n)$ je vstupní vektor, u je vnitřní potenciál a y je výstupní hodnota.

- **Radiální**, pro kterou platí

$$u = \sqrt{\sum_{i=1}^n (x_i - w_i)^2} \quad (3.2)$$

Každý vstup i má svoji váhu w_i , kterou je hodnota x_i vynásobena. Vnitřní potenciál neuronu u je potom vypočten podle následujícího vztahu:

$$u = f(\vec{x}) \sum_{i=1}^n x_i * w_i \quad (3.3)$$

Výstupní funkce je potom vypočtena podle následujícího vztahu:

$$y = g(u) = g(f(\vec{x})) \quad (3.4)$$

Kde $f()$ se nazývá *bázovou funkci* a $g()$ se nazývá *aktivaci funkci* neuronu.

3.2.1 Bázová funkce

Bázovou funkci se označuje vnitřní funkce neuronu, podle které je vypočítávána hodnota vnitřního potenciálu neuronu u .

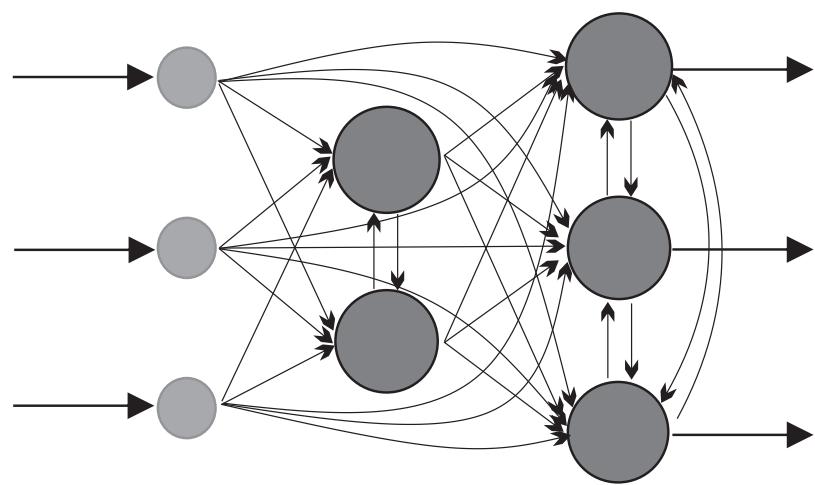
3.2.2 Perceptron

3.2.3 Aktivační funkce

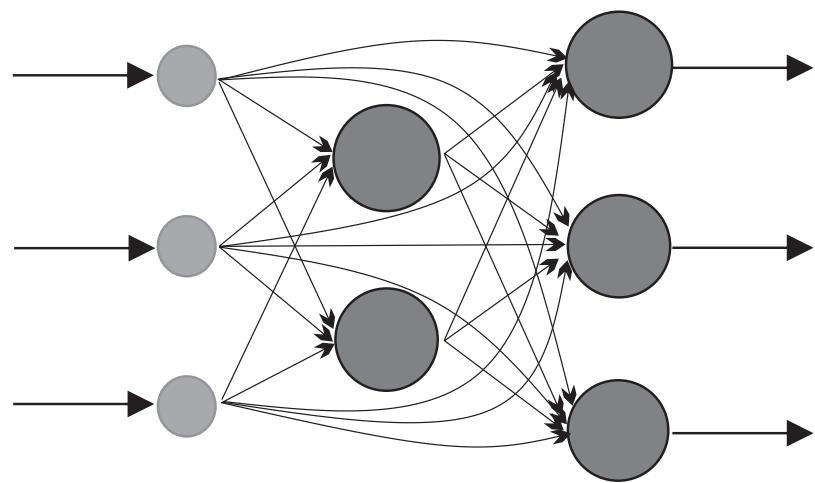
3.3 Topologie sítí

3.4 Učení

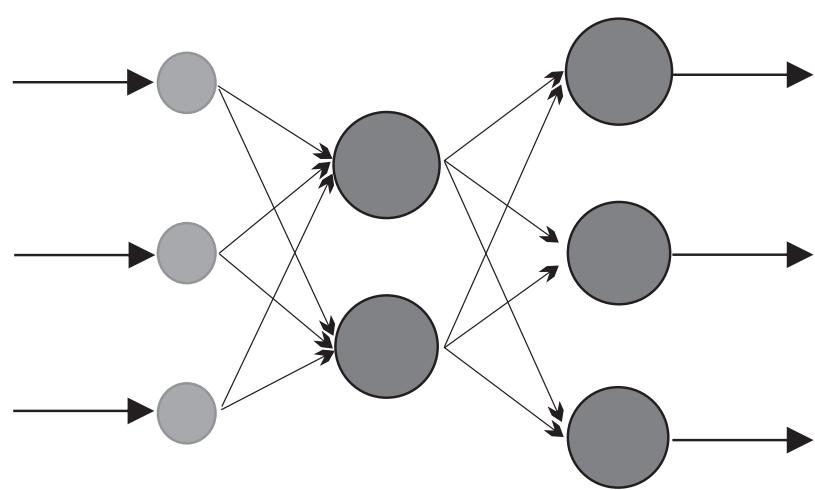
3.5 Hluboké neuronové sítě



Obrázek 3.3: Vrstvová síť. Výstup každého neuronu lze použít v aktuální nebo v každé další vrstvě. Neobsahuje zpětné vazby.



Obrázek 3.4: Acyklická síť. Výstup každého neuronu lze použít v některé z následujících vrstev.



Obrázek 3.5: Dopředná síť. Výstup neuronu lze použít vždy jen v následující vrstvě.

Kapitola 4

Návrh

V této kapitole je popsán návrh implementovaného programu. Struktura programu byla rozčleněna do tří fází, u kterých byla zpracovávána rozdílná data a byly využity různé technologie zpracování. První fáze, výběr už natrénované neuronové sítě je popsán v části 4.1, dále je potom v části 4.2 popsána následující práce s naučenou neuronovou sítí - finetuning a přístup k předposlední vrstvě. Pomocí této nově upravené neuronové sítě bude pro každý obrázek rozhodnuto, zda se na něm nachází automobil či nikoliv. V části 4.3 je potom popsána metoda, která byla zvolena k detekci SPZ v obrázku, o kterém už víme, že se na něm nachází automobil.

4.1 Použitá neuronová síť

ILSVRC network, jak vypadá, jak funguje, co dělá

4.1.1 Na čem je natrénovaná

ImageNet data - popis celé ImageNet množiny obrázků (více než 10M obrázků roztríděných do 1000 tříd) ILSVRC12 - popis ilsvrc soutěže, statistika modelu, umístění v jednotlivých kategoriích

4.2 Finetunning

Jak byl proveden finetunning

4.2.1 Zvolená metoda

To se ještě uvidí jaká

4.3 Detekce SPZ v obrázku s autem

Ještě se uvidí, jak to dělat, zatím to vypadá na jedno z

- Detektor hran
- Neuronka
- Něco vyššího

◦