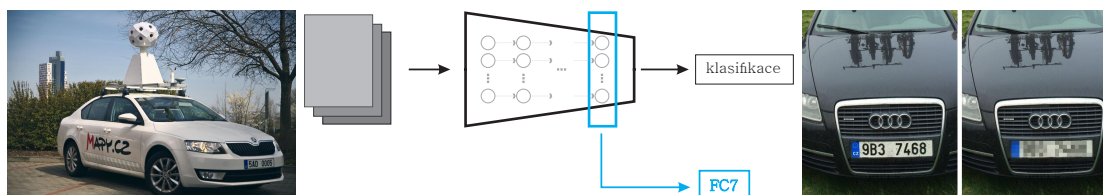


Anonymizace SPZ vozidel

Barbora Skřivánková



Abstrakt

Při procházení online map jsou dnes dostupné i souvislé snímky prohlížených míst. Pokud jsou však snímky pořizovány ve veřejném prostoru, nacházejí se na nich také kolemjdoucí lidé a kolemjdoucí vozidla. V rámci této práce je zpracovávána problematika automatizované anonymizace státních poznávacích značek (SPZ) v obrazových datech zachycených na veřejných prostranstvích.

Problém anonymizace SPZ vozidel je v této práci rozdělen do dvou fází. V první fázi jsou ze snímku pořízeného na veřejném prostranství vybrána místa, na kterých se nachází vozidla s SPZ. Toto je řešeno s využitím hluboké neuronové sítě. Ve druhé fázi je potom ve vybrané části obrázku s vozidlem lokalizována konkrétní oblast, na které se SPZ vozidla nachází a která je tedy určena k anonymizačnímu zpracování. Tato fáze je zpracovávána pomocí dopředné neuronové sítě napojené na předposlední vrstvu sítě z fáze 1.

Tato práce je zadána společností Seznam.cz a.s., která automatizovaný SPZ anonymizér poptává pro využití při tvorbě webové služby Panorama. Komerční řešení, které je v současné době ve společnosti Seznam.cz a.s. využíváno má výrazné nedostatky (zejména častá falešně pozitivní detekce SPZ), které budou v rámci této práce odbourány.

Klíčová slova: Detekce anonymizace státní poznávací značka registrační značka neuronová síť hluboká neuronová síť zpracování osobních údajů.

Příložené materiály: N/A

*xskriv01@stud.fit.vutbr.cz, Faculty of Information Technology, Brno University of Technology

1. Úvod

Automatizovaná anonymizace státních poznávacích značek (SPZ) automobilů zachycených na fotografiích má velký potenciál posunout uživatelské možnosti na internetu. Společnost Seznam.cz a.s. (dále jen Seznam.cz) – provozovatel portálu Mapy.cz – neustále posouvá a vylepšuje možnosti, které uživatelé při procházení online map mají.

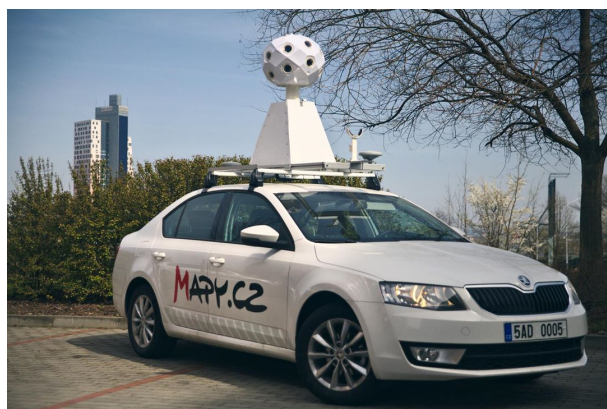
Jedním z výrazných vylepšení je zpřístupnění služby Panorama, která umožňuje uživateli prohlédnout si místo na mapě z pohledu, který by se mu naskytl, pokud by na místě fyzicky byl. Data pro tuto službu jsou snímána speciálně upraveným automobilem při

průjezdu oblastí. Vzhledem k tomu, že veřejné prostranství je vždy snímáno za běžného dne, spolu s terénem, který je zachycen, jsou nasnímány i další objekty, které se v daném prostranství vyskytují (lidé, vozidla a další). Dle zákona 101/2001 Sb. O ochraně osobních údajů veškeré informace, které mohou prozradit jakékoliv 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 jeho umístění na internet by tento zákon porušovalo. Před dalším využitím je tedy nutné data anonymizovat.

14
15
16
17
18
19
20
21
22
23
24
25
26



Obrázek 1. Problémy stávajícího řešení anonymizace SPZ v Panoramě. Chybně anonymizované nápisy nad obchody jsou na obrázku vyznačeny červenou barvou.



Obrázek 2. Automobil s 15 kamerami umístěnými na snímací hlavě na střeše.

V této práci je hledán způsob, jakým lze ohromné množství dat zaznamenané v rámci přípravy materiálů pro službu Panorama automatizovaně oprostít od SPZ jakýchkoliv vozidel tak, aby bylo možné data přímo použít k vystavení na internetu bez dalšího lidského zásahu. Tento úkol je náročný hlavně z toho důvodu, že fotografie jsou snímány ve 360° úhlu ze střechy snímacího automobilu a SPZ jsou tak zachyceny v nespočtu různých úhlů a téměř vždy jsou zdeformovány. To však nebrání jejich čitelnosti lidským okem a tedy jejich umístění na internet by bylo porušením ochrany osobních údajů.

V současné době je ve společnosti Seznam.cz využíváno komerčního řešení, jehož implementační detaily jsou utajeny. Při jeho využívání však dochází k velkému množství falešně pozitivních výsledků detekce (viz obrázek 1), která vedou k tomu, že ve výsledném obraze jsou anonymizovány i další texty, nikoliv jen SPZ vozidel. Toto zásadním způsobem omezuje použitelnost služby Panorama, protože největší přínos má tato služba právě v okamžiku, kdy uživatel hledá nějaké konkrétní místo, např. podobu budovy s určitou adresou, případně vchod do obchodu. Pokud je tedy nápis nad dveřmi obchodu anonymizován, jedná se o fatální selhání, které může vést až k poklesu počtu uživatelů.

V rámci této práce je navržen nový přístup – rozdělení procesu anonymizace do fáze hledání automobilu a fáze hledání SPZ. Algoritmus hledání SPZ tedy probíhá na už vybrané množině automobilů a nápisy na zdech, billboardech a obchodech už lokalizátorem SPZ vůbec neprocházejí. V první fázi, tedy ve fázi detekce automobilů, je využito hlubokých neuronových sítí. Ve druhé fázi – ve fázi lokalizace SPZ na automobilu – je potom využita dopředná neuronová síť, na jejímž vstupu stojí výstup předposlední vrstvy hluboké neuronové sítě pro detekci automobilů.

2. Obrazová data pro službu Panorama

Obrazová data pro tuto práci byla dodána společností Seznam.cz. Většina informací pro tuto část práce

byla získána v rámci několika konzultací s jejími zaměstnanci, Ing. Adamem Kolářem a Ing. Miroslavem Taláškem. Ze společnosti Seznam.cz byla dále poskytnuta neveřejná prezentace o snímání obrazových dat pro službu Panorama [1], ze které bylo při přípravě tohoto textu také vycházeno.

Fotografie jsou snímány speciálně upraveným vozem s 15 kamerami rozmístěnými na střeše. Tyto kamery zabírají 360° okolí snímacího automobilu. Způsob, jakým jsou kamery na střeše automobilu umístěny, je znázorněn na obrázku 2.

Při snímání se auto pohybuje rychlostí 70 km/h. Snímání se provádí na všech 15 kamerách současně každé 3 metry. Aby bylo možné později fotografii co nejvíce přiblížit tomu, jak prostředí vnímá člověk, který se v něm pohybuje, při každém snímku se zaznamená ještě sada metadat.

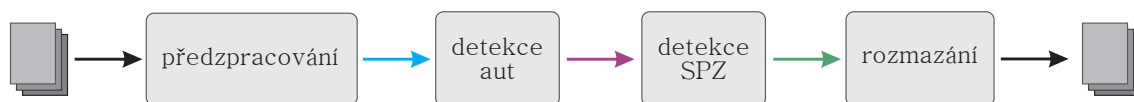
Než se nasnímaná data dostanou ke koncovému uživateli, je třeba nad nimi provést sekvenci náročných operací, mezi něž patří vysokorychlostní ukládání fotografií na disk přímo ve snímacím automobilu, sešívání 15 fotografií do jedinného panoramatického snímku, vyrovnávání horizontu, namapování na kouli pro zobrazení uživateli a anonymizace.

3. Navržená anonymizace SPZ vozidel

V této práci je problém anonymizace rozdělen do čtyř dílčích kroků:

1. předzpracování obrazových dat,
2. detekce automobilů,
3. detekce SPZ,
4. vlastní anonymizace,

z nichž stěžejními jsou kroky 2. a 3. Schéma navrženého přístupu je zobrazeno na obrázku 3.



Obrázek 3. Základní struktura programu.



Obrázek 4. Rozčlenění panoramatické fotografie na sekce.

dosahováno velmi dobrých výsledků. Proto byly zvoleny jako stěžejní mechanismus řešení této problematiky hluboké neuronové sítě [2].

Hluboké neuronové sítě jsou neuronové sítě navržené speciálně pro zpracovávání obrazových dat [2]. Na rozdíl od plně propojených neuronových sítí, hluboké neuronové sítě dokáží pomocí konvolučních vrstev s výhodou využít prostorového uspořádání jednotlivých vstupních hodnot načítaných z obrázku.

Konvoluční vrstva je stěžejním elementem hlubokých neuronových sítí. Skládá z několika map rysů (*feature maps*), které pracují nezávisle na sobě. Mapa rysů popisuje primitiva, která se v analyzovaném obraze nacházejí. Oproti standardnímu vektoru rysů však mapa rysů ukazuje i jejich přesnou polohu ve zdrojovém obrázku. Každá mapa rysů však dokáže obraz prohledávat se zacílením na jediné primitivum, v reálných aplikacích je tedy těchto map použitých vždy více.

Každá mapa rysů pracuje nezávisle na ostatních způsobem, který je zobrazen na obrázku 6. Vezměme v potaz obrázek o rozměrech 10×10 pixelů, který už máme načtený ve vstupní vrstvě. Hodnota každého neuronu v konvoluční vrstvě je vypočtena z hodnot podmnožiny neuronů vstupní vrstvy - z tzv. *lokálního pole*, nikoliv ze všech jako tomu je u plně propojených sítí. V našem případě se jedná o podčást pole neuronů vstupní vrstvy o rozměrech 4×4 neurony (v obrázku 6 označeno modře). Jakmile je vypočtena hodnota, pole se posouvá a je vypočtena hodnota dalšího neuronu z nové podmnožiny neuronů vstupní vrstvy (v obrázku 6 označeno růžově). Složením několika map rysů vzniká konvoluční vrstva.

Implementace neuronové sítě v rámci této práce

3.1 Předzpracování obrazových dat

V rámci předzpracování obrazových dat jsem panoramatický obraz rozdělila na 9 částí (Obrázek 4) a ručním porovnáním obrázků z trénovací množiny zjistila, že vozidla se nacházejí pouze v částech 7-9. Části 1-6 proto nemusejí být pro detekci vozidel uvažovány. V částech 7-9 byla následně ručně lokalizována vozidla a byla odvozena běžná velikost vyfocení vozidla (Obrázek 5).

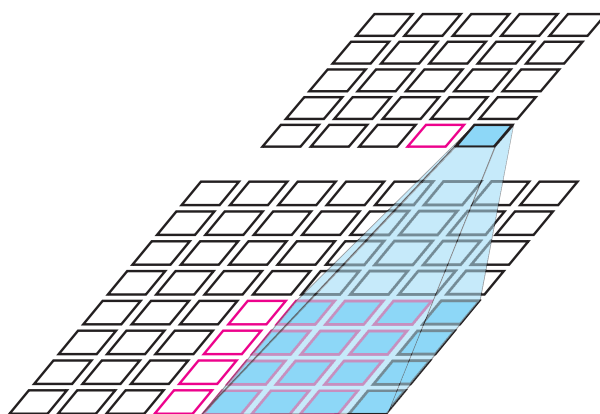
Části 7-9 z jedné panoramatické fotografie byly následně rozřezány na 259 nepřekrývajících se výsečí o velikosti průměrného vozidla (medián). Nad těmito výsečemi je pracováno v dalších fázích zpracování.

3.2 Detekce vozidel

Je-li úloha detekce vozidla ve fotografii nasnímané pro službu Panorama redukována na nejmenší řešený problém, jedná se o problém klasifikační – na zachycené části prostředí se buď to nachází nebo nenachází vozidlo. Zvažíme-li způsoby klasifikace vzorků do n tříd, s neuronovými sítěmi je nad touto problematikou



Obrázek 5. Rozptyl velikostí aut v obrázku.



Obrázek 6. Schéma konvoluční vrstvy sítě.

není stěžejním problémem, proto je s výhodou využito jednoho z dostupných frameworků. Jako nejrobustnější framework pro práci s hlubokými neuronovými sítěmi s podporou učení na grafické kartě byl vybrán framework Caffe (C++) [3]. V poslední době však došlo na tomto poli k pozitivnímu vývoji a pro Caffe vznikl velmi slibný konkurent - framework Torch [4].

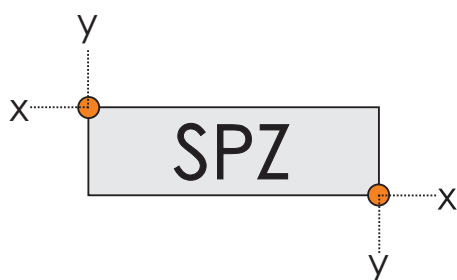
Pro účely této práce byla využita již naučená neuronová síť, která vznikla v rámci contestu ILSVRC 2012 [5]. Ta byla natrénována ke klasifikaci do jedné z 1000 tříd a pro její natrénování bylo použito přes 14 milionů obrázků. Pro potřeby klasifikace do dvou tříd – *autolneauto* – byla síť dotrénována na 6 000 obrázcích přímo ze služby Panorama, přičemž byly měněny váhy pouze mezi předposlední a poslední vrstvou - tzv. *fine-tuning*. Výstupem tohoto kroku je podmnožina výšečí klasifikovaných jako *auto*.

Protože se jedná o časově velmi náročný výpočet, je v této práci s výhodou využito možnosti výpočtu na GPU, což díky paralelizaci vede ke zkrácení výpočetního času. Toto je realizováno pomocí technologie Cuda.

3.3 Detekce SPZ

Výstupem předchozí fáze je klasifikace všech výšečí do jedné ze tříd - *autolneauto*. K dalšímu zpracování v detektoru SPZ pokračují pouze výšeče, které jsou klasifikovány jako *auto*.

K detekci SPZ byla využita dopředná neuronová síť s třemi plně propojenými vrstvami, která byla sestavena a učena pomocí frameworku Keras. Na vstupu této sítě jsou načteny vektory rysů jednotlivých výšečí. Tyto jsou získány z předposlední vrstvy konvoluční neuronové sítě pro detekci *aut* - tzv. vrstvy FC7, která obsahuje 4096 hodnot typu float. Výstupem této fáze je identifikace části fotografie, ve které se nachází SPZ. Tato je popsána pomocí čtyř čísel ukazujících polohu levého horního a pravého dolního rohu SPZ (viz obrázek 7).



Obrázek 7. Souřadnice detekované SPZ.

3.4 Anonymizace detekované SPZ

V poslední fázi jsou ze souřadnic s detekovanou SPZ dopočítány souřadnice v originální fotografii a na tuto oblast je potom aplikován rozostřovací filtr. Toto bylo zajištěno pomocí nástroje ImageMagick a jeho funkce blur. Parametry byly nastaveny následujícím způsobem: $\sigma = 8$, $\text{radius} = 0$. Při nastavení parametru radius na 0 je pro každý rozostřovaný obrázek vypočítána optimální hodnota radius automaticky.

4. Ověření funkčnosti modelu

Učení neuronové sítě probíhá nad trénovací sadou, která byla poskytnuta ze společnosti Seznam.cz. Tato trénovací sada byla vybrána s ohledem na okrajové případy, které mohou při snímání materiálu pro službu Panorama nastat. V rámci předzpracování byly fotografie automaticky rozřezány na 259 výřezů pomocí nástroje ImageMagick. Nad každým ze vzniklých 23 000 výřezů poté byly ručně vyhodnoceny tři parametry:

- na obrázku se nachází auto,
- na obrázku se nachází auto s viditelnou SPZ,
- na obrázku se nachází auto ve vzdálenosti zneumožňující čitelnost SPZ.

Pro zrychlení hodnocení a ukládání těchto tří parametrů byl v rámci práce vytvořen jednoduchý zobrazovač v jazyce JavaScript.

Testovací sada, která bude dodána po dokončení anonymizéru bude také ručně klasifikována a poté budou porovnány výsledky aktuálně využívaného komerčního anonymizéru s nově vyvinutým anonymizérem v rámci této práce.

V současném okamžiku je práce ve stavu, kdy je dokončen mechanismus poloautomatického předzpracování dat. Hluboká neuronová síť sloužící k detekci automobilů je naučena a na testovací množině, která nemá s trénovací množinou žádný průnik dosáhla výsledků uvedených v tabulce 1. Z té plyne, že velký počet chybně klasifikovaných vzorků spadá do kategorie *false positive*. Vzhledem k tomu, že jde pouze o první fázi klasifikace, ve které se selektují vzorky, které pokračují do dalšího zpracování, velká část těchto chybně klasifikovaných vzorků bude odfiltrována v dalším kroku.

V celé trénovací sadě byly ručně mapovány souřadnice SPZ, které slouží k učení sítě a vypočtení průměrné chyby sítě (odchylky jednotlivých souřadnic v pixelech). Stejným způsobem bude anotována testovací sada. Testování spolehlivosti nově vyvinutého anonymizéru bude provedeno pomocí automatizovaného testování, které bude na stejné datové sadě prove-

Tabulka 1. Výsledky klasifikace automobilů.

True positive	1.345 %
True negative	78.205 %
False positive	20.420 %
False negative	0.030 %

připravena předem, čímž se i zpracovávání této práce
zpožďuje.

Poděkování

Na tomto místě bych ráda poděkovala svojí vedoucí
Ing. Michaela Drahošové za důsledné vedení a mo-
tivaci při zpracovávání této práce. Dále bych chtěla
poděkovat Ing. Adamu Kolářovi za věcné a velmi
poučné konzultace nad rámec jeho povinností a týmu
Mapy.cz, který mi pod vedením Ing. Miroslava Taláška
poskytoval perfektní zázemí pro zpracování této práce.

Literatura

- [1] Miroslav Talášek. *Mapy.cz Panorama*. Seznam.cz
[interní materiál], Praha, 2015.
- [2] Michael Nielsen. *Neural net-
works and deep learning*. <http://neuralnetworksanddeeplearning.com>, 2015.
- [3] Berkeley Vision and Learning Center. *Caffe*
— deep learning framework. <http://caffe.berkeleyvision.org>, 2016.
- [4] Koray Ronan, Clément and Soumith. *Torch* —
scientific computing for luajit. <http://torch.ch>, 2016.
- [5] Stanford Vision Lab. *Imagenet large scale
visual recognition challenge*. <http://www.image-net.org/challenges/LSVRC/>,
2015.

deno jak na aktuálně využívaném komerčním anonymi-
zéro, tak na nově vyvinutém anonymizéro popsaném v
této práci. Pro každou z metod budou vypočteny:

- průměrná odchylka lokalizované a ručně anoto-
vané SPZ v pixelech,
- počet a velikost falešně pozitivních detekcí,
- počet falešně negativních detekcí.

Výsledky jednotlivých metod budou porovnány a na
základě toho bude rozhodnuto, zda metoda anonymiza-
ce navržená v této práci přinesla do služby Panorama
zlepšení.

5. Shrnutí

V rámci této práce je zpracovávána problematika au-
tomatizované anonymizace SPZ vozidel ve fotografiích
zachycených na veřejném prostranství. Oproti aktuál-
nímu komerčnímu řešení využívanému ve společnosti
Seznam.cz má ambice snížit množství falešných de-
tekci, které způsobují značné omezení uživatelského
významu celé služby Panorama.

V současném stavu práce jsou připravena trénovací
a validační data ve finální podobě. Mechanismus
pro přípravu testovacích dat je připravený, jakmile
tedy budou k dispozici, bude možné je ihned zpraco-
vat. Hluboká neuronová síť pro detekci automobilů
je naučena a na předem neznámé testovací množině
dosahuje úspěšnosti klasifikace 79,55 %. Tato přesnost
bude dále navyšována, protože pouze vzorky, které
jsou v první fázi klasifikovány jako automobil pokraču-
jí do druhé fáze - detekce SPZ. Tato fáze dále vyloučí
obrázky, které obsahují automobil, nikoliv však SPZ.

Spolupráce se společností Seznam.cz probíhá na
úrovni externí spolupráce. Protože data, nad kterými
je práce zpracovávána podléhají přísným pravidlům,
není možné je vynášet ven ze společnosti. Proto je
nutné veškerou práci na serveru, na kterém jsou data
nahrána provádět v lokální kabelové síti v kancelářích
společnosti na Londýnském náměstí v Brně.

Při řešení této práce mám možnost spolupracovat
přímo s týmem vyvíjejícím službu Panorama a tak
se přímo konfrontovat se způsobem práce ve firmě
pracující na komerčních produktech. Pro studenta je
velkým překvapením, že vývojová prostředí nejsou