Posudek oponenta bakalářské práce

Student: Hrabal Matěj
Téma: Matení algoritmů počítačového vidění (id 21949)
Oponent: Bartl Vojtěch, Ing., UPGM FIT VUT

1. Náročnost zadání **průměrně obtížné zadání**

Přestože zadání vyžadovalo nastudování množství informací, které se běžně nevyučují v rámci bakalářského studijního programu, tak se obtížnost neodchyluje od ostatních zadaní se zaměřením na zpracování obrazu.

2. Splnění požadavků zadání **zadání téměř splněno s drobnými výhradami**

Za částečně nesplněný lze považovat bod 4 zadání, kde bylo cílem navrhnout přístupy k učení neuronových sítí aby byly odolnější vůči záměrnému matení. Na druhou stranu byly navrženy přístupy k detekci napadení obrázku a zotavení se z takového útoku. Součástí zadání bylo vytvoření plakátu a videa, což ale nebylo splněno.

3. Rozsah technické zprávy **je v obvyklém rozmezí**

Poměrně velkou část práce zabírají obrázky, což je ale vzhledem k tématu práce pochopitelné.

4. Prezentační úroveň předložené práce **80 b. (B)**

Struktura práce je dobře navržena a jednotlivé kapitoly na sebe logicky navazují. Kapitola 4 popisující neobvyklé metody matení algoritmů počítačového vidění mohla být sloučena s některou z předchozích kapitol. V práci chyběla zmínka o tom jaká neuronová síť je použita pro vyhodnocování navržených algoritmů. Celkově se práce dobře čte a je snadno pochopitelná.

5. Formální úprava technické zprávy **70 b. (C)**

Samotný text práce je napsán pečlivě s minimem chyb. Citace nejsou často správně uvozeny (jen číslo citace). Chybné jsou obrázky bez jakýchkoliv referencí, kdy jsou vloženy na místo, kde na ně navazuje text. Lepší by bylo se na obrázky odkazovat na místech, kde je to relevantní. Oceňuji napsání práce v anglickém jazyce.

6. Práce s literaturou **75 b. (C)**

Citovaná literatura je relevantní a vztahuje se k danému problému. Trochu problematické je citování vývojových nástrojů, které nemusely být vyloženě citovány, ale stačila by na ně poznámka pod čarou. Pro citování algoritmu diffrential evolution by mělo být využito původního článku autorů a nikoliv internetové stránky.

7. Realizační výstup **78 b. (C)**

Naimplementované programy pro provedení i odhalování útoků na neuronové sítě jsou použitelné a lze je rozšířit pro vlastní testy konvolučních neuronových sítí. Lze tedy vyzkoušet odolnost neuronových sítí vůči různým typům útoků. Vzhledem k náročnosti výpočtů je samotný běh programu velice pomalý a mohlo být využito paralelních výpočtů.

8. Využitelnost výsledků

Principy útoků na neuronvé sítě vycházejí z již známých algoritmů. Byly ovšem navrženy nové přístupy k detekci útoků a případného zotavení se z nich. Mnohem lépe mohly být provedeny experimenty, které jsou vyhodnoceny jen na jedné neuronové síti. Experimenty s různými typy sítí by mohly přinést nové informace o robustnosti různých architektur konvolučních neuronových sítí.

9. Otázky k obhajobě

- Zkoušel jste jiný algoritmus pro minimalizaci/maximalizaci hledaných pixelů než differential evolution?
- Proč jste nezkusil vyhodnotit odolnost vůči útokům i na jiných architekturách konvolučních neuronových sítí?

10. Souhrnné hodnocení **78 b. dobře (C)**

Práce se věnuje tématu útoků na konvoluční neuronové sítě, což je velice zajímavé a relevantní téma. Byly vyzkoušeny různé varianty útoků na neuronové sítě a byly rovněž navrženy postupy pro detekci takovýchto útoků. Určitě by bylo velice zajímavé porovnání různých architektur konvolučních neuronových sítí a jejich robustnost vůči různým útokům, což ale v práci chybí.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 30. května 2019

.....
podpis