

ZADÁNÍ VÝZKUMNÉHO ÚKOLU

Student: Bc. Pavel Jakš
Studijní program: Matematická informatika
Název práce (česky): Moderní metody robustního strojového učení
Název práce (anglicky): Modern methods of robust machine learning

Pokyny pro vypracování:

- 1) Nastudovat literaturu v oblasti metrik vizuální podobnosti.
- 2) Nastudovat literaturu v oblasti tvorby adversariálních vzorků.
- 3) Nastudovat dokumentaci k relevantním knihovnám robustního strojového učení (RobustBench, Foolbox).
- 4) Implementace vybraných metrik vizuální podobnosti.
- 5) Využití naimplementovaných metod vizuální podobnosti pro tvorbu adversariálních vzorku.

Doporučená literatura:

- 1) Naveed Akhtar, Ajmal Mian, Navid Kardan, Mubarak Shah, Advances in adversarial attacks and defenses in computer vision: A survey. IEEE Access 9, 2021, 155161-155196.
- 2) W., Eric, F. Schmidt, Z. Kolter, Wasserstein adversarial examples via projected sinkhorn iterations. International Conference on Machine Learning, PMLR, 2019.
- 3) J. Rauber, R. Zimmermann, M. Bethge, W. Brendel, Foolbox: A Python toolbox to benchmark the robustness of machine learning models. Reliable Machine Learning in the Wild Workshop, 34th International Conference on Machine Learning, 2017.

Jméno a pracoviště vedoucího výzkumného úkolu:

Mgr. Lukáš Adam, Ph.D.

Katedra počítačů, Fakulta elektrotechnická, České vysoké učení technické v Praze, Karlovo náměstí 13, 121 35 Praha 2

Jméno a pracoviště konzultanta:

Mgr. Vojtěch Čermák

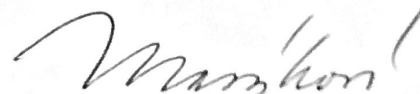
Katedra počítačů, Fakulta elektrotechnická, České vysoké učení technické v Praze, Karlovo náměstí 13, 121 35, Praha 2

Datum zadání výzkumného úkolu: 31.10.2022

Datum odevzdání výzkumného úkolu: 21.5.2023

Doba platnosti zadání je dva roky od data zadání.

V Praze dne 31. října 2022



vedoucí katedry