

Katarzyna Filus

Lista publikacji

1. Filus, K., Domańska, J. (2024). Similarity-driven adversarial testing of neural networks. Knowledge-Based Systems, 112621.
2. Filus, K., Domańska, J. (2024). Extracting coarse-grained classifiers from large Convolutional Neural Networks. Engineering Applications of Artificial Intelligence, 138 109377.
3. Filus, K., Domańska, J. (2023). NetSat: Network Saturation Adversarial Attack. IEEE International Conference on Big Data (BigData).
4. Filus, K., Domańska, J. (2023). Recycling of Generic ImageNet-trained Models for Smart-city Applications, IEEE International Conference on Data Science and Advanced Analytics (DSAA).
5. Filus, K., Domańska, J. (2022). Software Vulnerabilities in TensorFlow-Based Deep Learning Applications. Computers & Security, 102948.