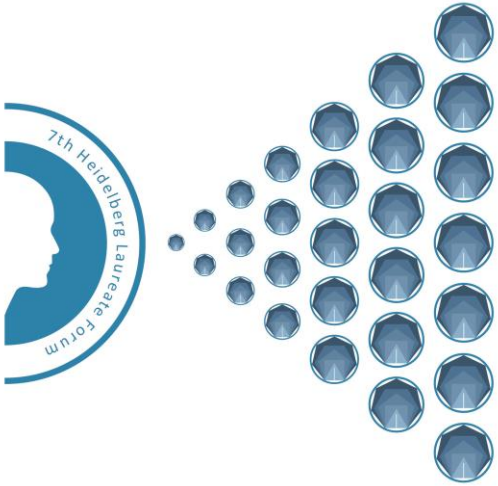


Laureates of mathematics and computer science meet the next generation

HEIDELBERG LAUREATE FORUM

Poster-Flash

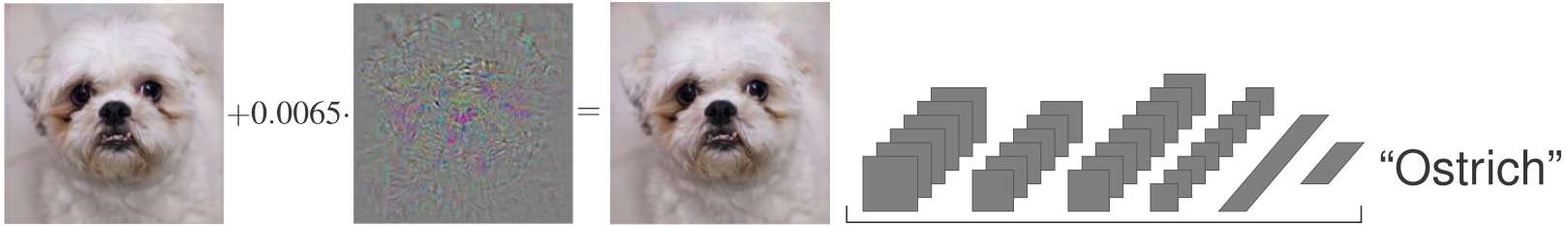
David Stutz

Disentangling Adversarial Robustness and Generalization of Deep Neural Networks

Adversarial Machine Learning

HEIDELBERG LAUREATE FORUM

Adversarial example (i.e., evasion attack):



- Severe security threat;
- and serious lack of understanding.

Adversarial Robustness

HEIDELBERG LAUREATE FORUM

Are accurate *and* robust neural networks possible?