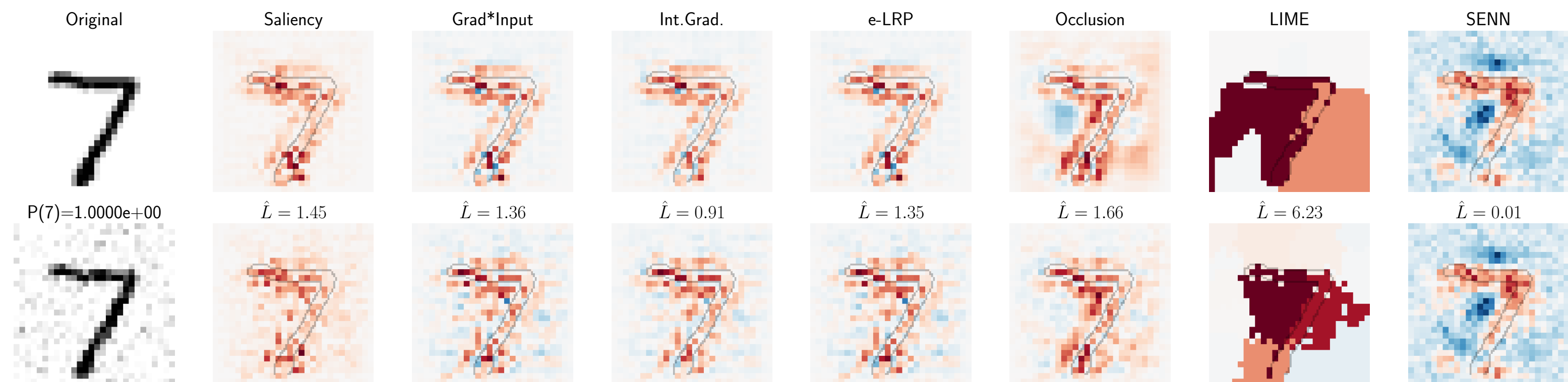


SENN Robustness



SENN Robustness

Adversarial robustness estimation:

$$\hat{L}(x) = \arg \max_{\hat{x} \in B_\epsilon(x)} \|f_{expl}(\hat{x}) - f_{expl}(x)\|_2 / \|h(\hat{x}) - h(x)\|$$

Results aggregated over full dataset:

