Gradient perturbation

$\|x - x'\|$

How to measure the deep gradient leakage risk?

$\|x - G_r(g + \delta)\|$

Empirical evaluation is expensive and inaccurate

$\|x - x'\| \geq \|J\delta\|/\lambda_{\max}(JJ^\top)$

I^2F: Tractable bound of worst-case risks