MLDS 490 Lab 8

Shuyang Wang Fall 2023

Agenda

- Assignment 3 Part 1 due on Nov. 16th by 10pm:
- Part 2 due on Nov 27th by 10 pm.

    Submit report on Canvas; submit code and instructions on Github.

- Differential Privacy

Differential Privacy

(Informally)

An algorithm is **differentially private** if it is very unlikely to distinguish from the output of an algorithm whether an individual member is included the dataset or not.

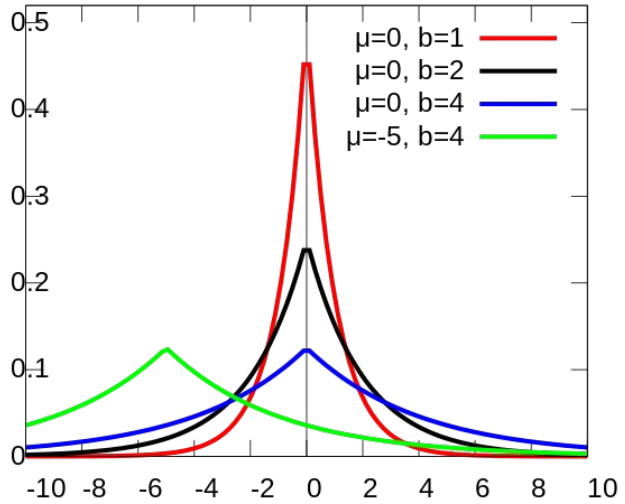
Given two datasets X and Y that differ in only one data sample. The **sensitivity** of a function F captures the maximal possible change in the outputs of F(X) and F(Y).

The Laplace mechanism preserves differential privacy by injecting noises. The larger the sensitivity of the function F, the larger the noise scale needed to preserve differential privacy for F.

Laplace Mechanism

- Laplace distribution has pdf
  - Mean: mu=0
  - Variance = 2b^2
- The larger the b is, the larger the noise scale.

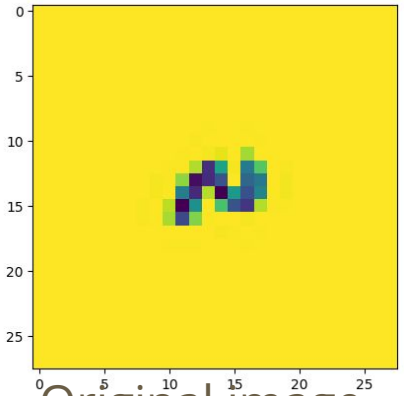
$$\mathrm{Lap}(x|b) = \frac{1}{2b}\exp\left(-\frac{|x|}{b}\right)$$



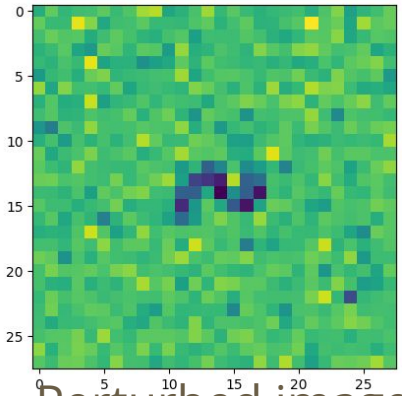
Laplace Mechanism

Perturb the input data by adding Laplace noises: Perturb each pixel of the images by noises of scale b, sample one noise according to the Laplace distribution for each pixel.

Use the perturbed images for training and testing.



Original image



Perturbed image