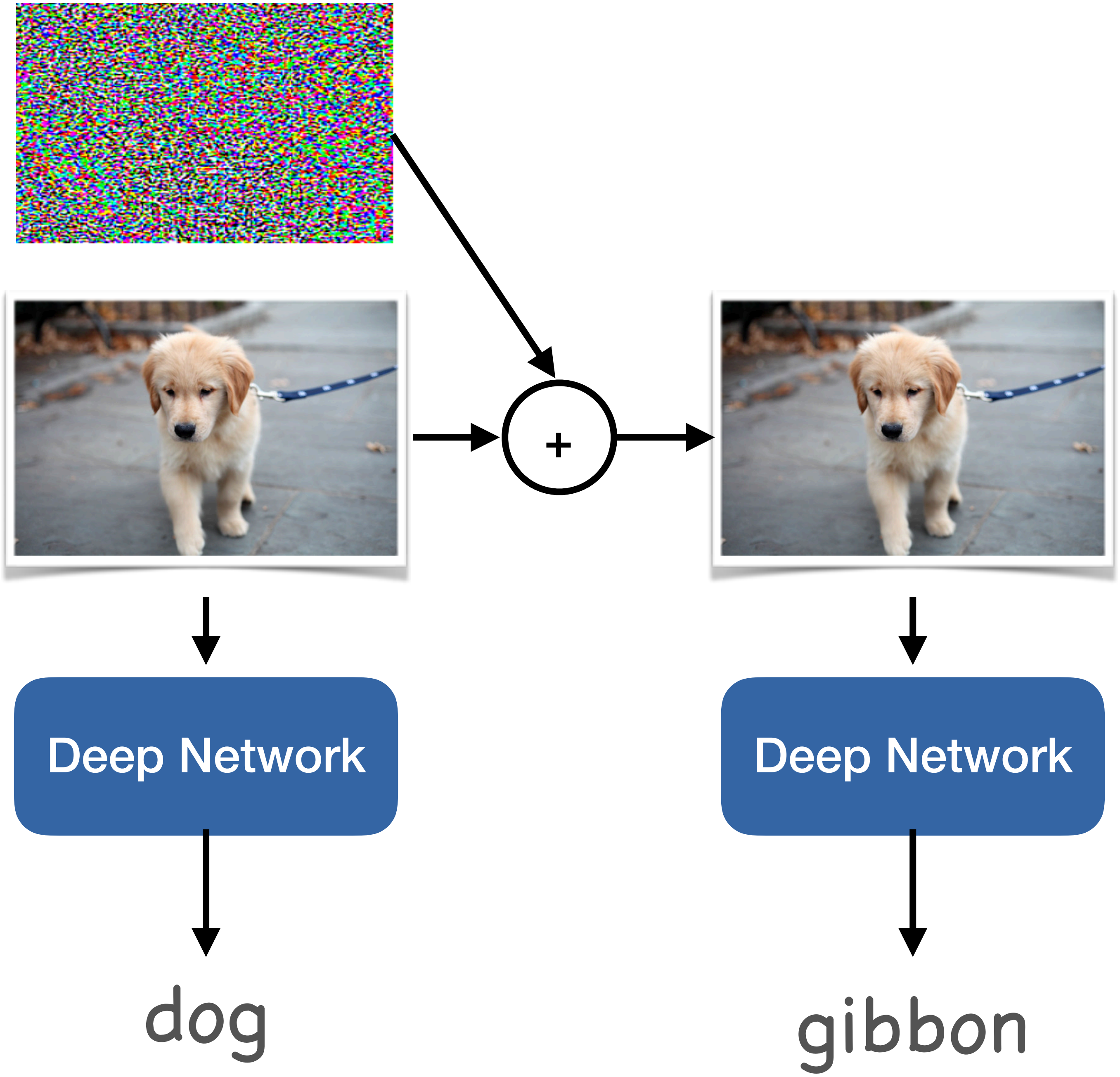
Summary

Easy to attack deep networks

- Small noise easily fools networks
  - Hard to defend against



+

Deep Network

Deep Network

dog

gibbon