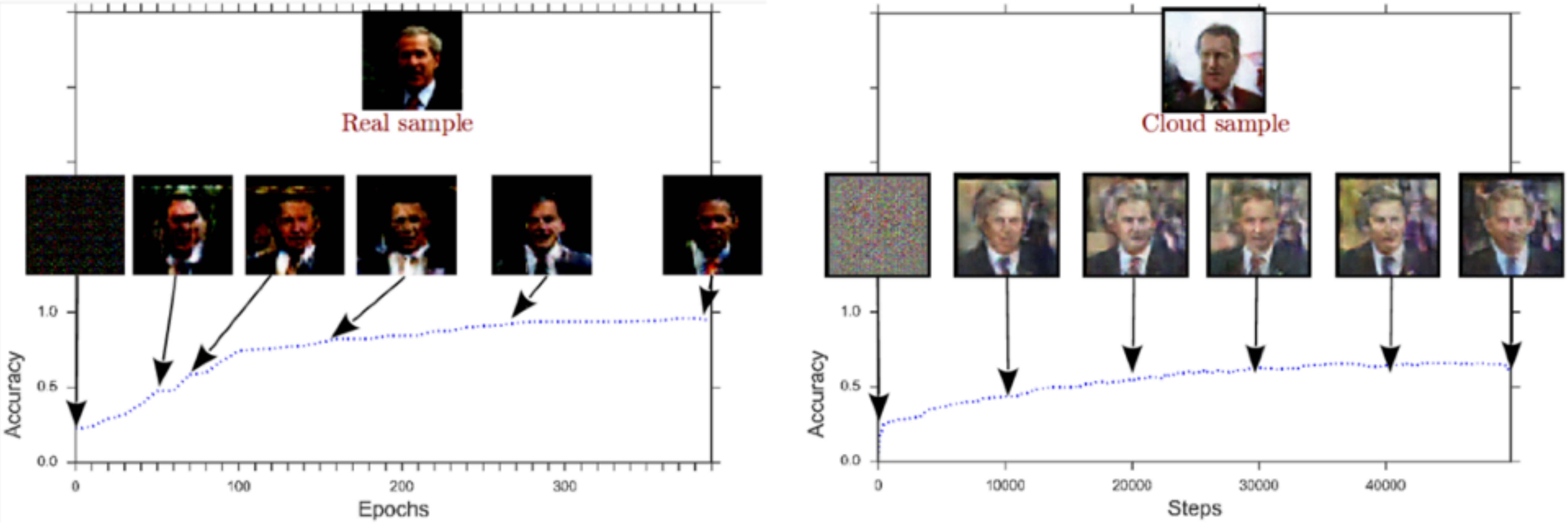
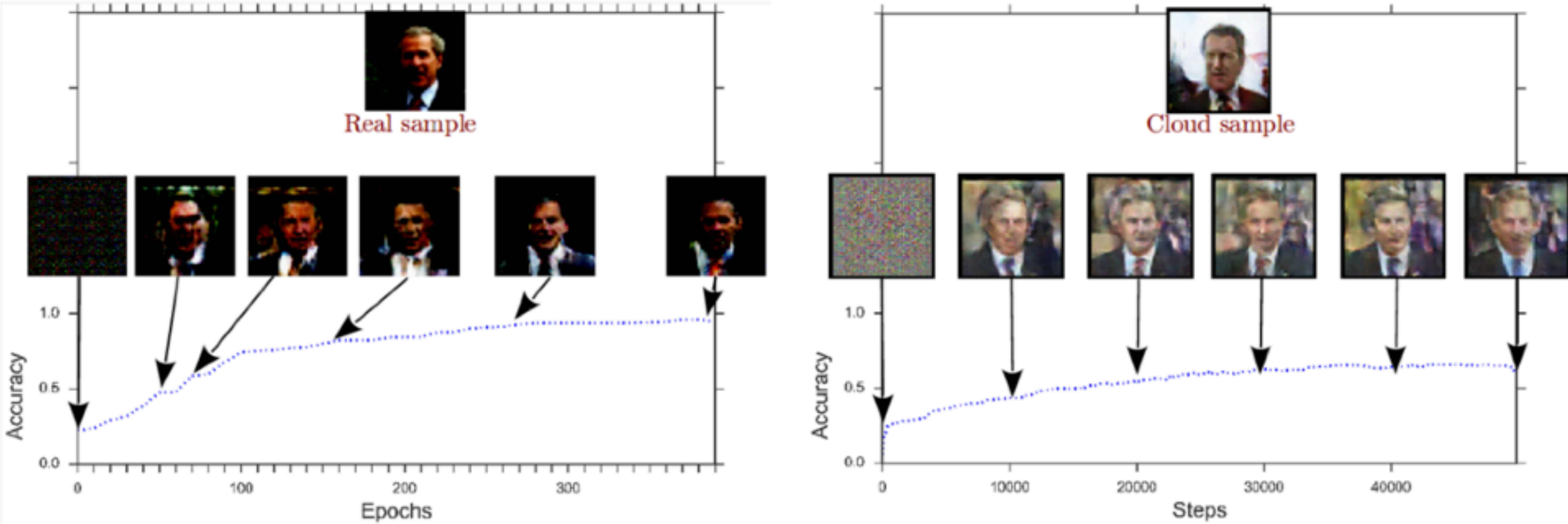
24



(a) White-box attack

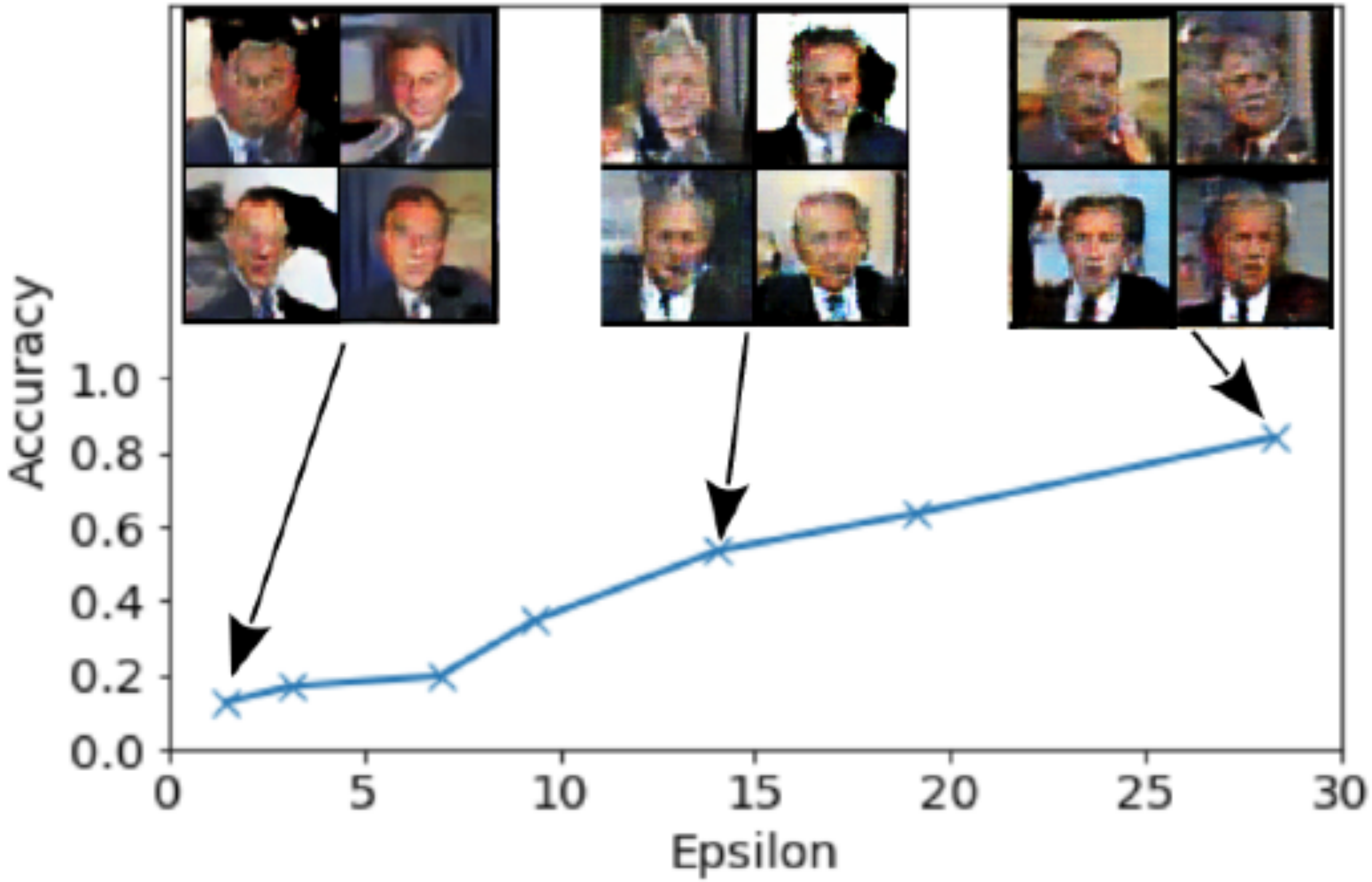
(b) Black-box attack



(a) White-box attack

(b) Black-box attack

Defense? Differentially Private GAN?



White-box, LFW, top ten classes

Triastcyn et al. “Generating differentially private datasets using GANs.”