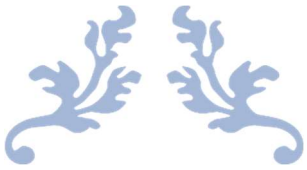
به نام خدا



ثبت اطلاعات منابع در نرم افزار

تمرین سری هفتم

محمد جواد زندیه ۹۸۳۱۰۳۲

۱۱ خرداد ۱۴۰۱

دانشکده مهندسی کامپیوتر، دانشگاه صنعتی امیرکبیر

Chicago 17th Footnote منابع با فرمت

[1] Akhtar, Naveed, and Ajmal Mian. "Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey." *Ieee Access* 6 (2018): 14410-30.

[2] Carlini, Nicholas, Anish Athalye, Nicolas Papernot, Wieland Brendel, Jonas Rauber, Dimitris Tsipras, Ian Goodfellow, Aleksander Madry, and Alexey Kurakin. "On Evaluating Adversarial Robustness." *arXiv pre-print server* (2019-02-20 2019). https://doi.org/None

arxiv:1902.06705.

[3] Dong, Yinpeng, Fangzhou Liao, Tianyu Pang, Hang Su, Jun Zhu, Xiaolin Hu, and Jianguo Li. "Boosting Adversarial Attacks with Momentum." Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition, 2018.

[4] Liao, Fangzhou, Ming Liang, Yinpeng Dong, Tianyu Pang, Xiaolin Hu, and Jun Zhu. "Defense against Adversarial Attacks Using High-Level Representation Guided Denoiser." Paper presented at the Proceedings of the IEEE conference on computer vision and pattern recognition, 2018.

[5] Madry, Aleksander, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. "Towards Deep Learning Models Resistant to Adversarial Attacks." *arXiv preprint arXiv:1706.06083* (2017).

[6] Narodytska, Nina, and Shiva Prasad Kasiviswanathan. "Simple Black-Box Adversarial Attacks on Deep Neural Networks." Paper presented at the CVPR Workshops, 2017.

[7] Papernot, Nicolas, Patrick McDaniel, Xi Wu, Somesh Jha, and Ananthram Swami. "Distillation as a Defense to Adversarial Perturbations against Deep Neural Networks." Paper presented at the 2016 IEEE symposium on security and privacy (SP), 2016.

[8] Ren, Kui, Tianhang Zheng, Zhan Qin, and Xue Liu. "Adversarial Attacks and Defenses in Deep Learning." *Engineering* 6, no. 3 (2020): 346-60.

[9] Xu, Han, Yao Ma, Hao-Chen Liu, Debayan Deb, Hui Liu, Ji-Liang Tang, and Anil K Jain. "Adversarial Attacks and Defenses in Images, Graphs and Text: A Review." *International Journal of Automation and Computing* 17, no. 2 (2020): 151-78.

[10] Zhang, Yuheng, Ruoxi Jia, Hengzhi Pei, Wenxiao Wang, Bo Li, and Dawn Song. "The Secret Revealer: Generative Model-Inversion Attacks against Deep Neural Networks." Paper presented at the Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020.

منابع با فرمت APA 7th

[1] Akhtar, N., & Mian, A. (2018). Threat of adversarial attacks on deep learning in computer vision: A survey. *Ieee Access*, *6*, 14410-14430.

[2] Carlini, N., Athalye, A., Papernot, N., Brendel, W., Rauber, J., Tsipras, D., Goodfellow, I., Madry, A., & Kurakin, A. (2019). On Evaluating Adversarial Robustness. *arXiv pre-print server*. https://doi.org/None

arxiv:1902.06705

[3] Dong, Y., Liao, F., Pang, T., Su, H., Zhu, J., Hu, X., & Li, J. (2018). Boosting adversarial attacks with momentum. Proceedings of the IEEE conference on computer vision and pattern recognition,

[4] Liao, F., Liang, M., Dong, Y., Pang, T., Hu, X., & Zhu, J. (2018). Defense against adversarial attacks using high-level representation guided denoiser. Proceedings of the IEEE conference on computer vision and pattern recognition,

[5] Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. (2017). Towards deep learning models resistant to adversarial attacks. *arXiv preprint arXiv:1706.06083*.

[6] Narodytska, N., & Kasiviswanathan, S. P. (2017). Simple Black-Box Adversarial Attacks on Deep Neural Networks. CVPR Workshops,

[7] Papernot, N., McDaniel, P., Wu, X., Jha, S., & Swami, A. (2016). Distillation as a defense to adversarial perturbations against deep neural networks. 2016 IEEE symposium on security and privacy (SP),

[8] Ren, K., Zheng, T., Qin, Z., & Liu, X. (2020). Adversarial attacks and defenses in deep learning. *Engineering*, *6*(3), 346-360.

[9] Xu, H., Ma, Y., Liu, H.-C., Deb, D., Liu, H., Tang, J.-L., & Jain, A. K. (2020). Adversarial attacks and defenses in images, graphs and text: A review. *International Journal of Automation and Computing*, *17*(2), 151-178.

[10] Zhang, Y., Jia, R., Pei, H., Wang, W., Li, B., & Song, D. (2020). The secret revealer: Generative model-inversion attacks against deep neural networks. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition,

منابع با فرمت Vancouver

1. Akhtar N, Mian A. Threat of adversarial attacks on deep learning in computer vision: A survey. Ieee Access. 2018;6:14410-30.

2. Papernot N, McDaniel P, Wu X, Jha S, Swami A, editors. Distillation as a defense to adversarial perturbations against deep neural networks. 2016 IEEE symposium on security and privacy (SP); 2016: IEEE.

3. Ren K, Zheng T, Qin Z, Liu X. Adversarial attacks and defenses in deep learning. Engineering. 2020;6(3):346-60.

4. Xu H, Ma Y, Liu H-C, Deb D, Liu H, Tang J-L, et al. Adversarial attacks and defenses in images, graphs and text: A review. International Journal of Automation and Computing. 2020;17(2):151-78.

5. Narodytska N, Kasiviswanathan SP, editors. Simple Black-Box Adversarial Attacks on Deep Neural Networks. CVPR Workshops; 2017.

6. Liao F, Liang M, Dong Y, Pang T, Hu X, Zhu J, editors. Defense against adversarial attacks using high-level representation guided denoiser. Proceedings of the IEEE conference on computer vision and pattern recognition; 2018.

7. Madry A, Makelov A, Schmidt L, Tsipras D, Vladu A. Towards deep learning models resistant to adversarial attacks. arXiv preprint arXiv:170606083. 2017.

8. Dong Y, Liao F, Pang T, Su H, Zhu J, Hu X, et al., editors. Boosting adversarial attacks with momentum. Proceedings of the IEEE conference on computer vision and pattern recognition; 2018.

9. Zhang Y, Jia R, Pei H, Wang W, Li B, Song D, editors. The secret revealer: Generative model-inversion attacks against deep neural networks. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition; 2020.

10. Carlini N, Athalye A, Papernot N, Brendel W, Rauber J, Tsipras D, et al. On Evaluating Adversarial Robustness. arXiv pre-print server. 2019.

منابع با فرمت Numbered

1. Akhtar, N. and A. Mian, *Threat of adversarial attacks on deep learning in computer vision: A survey.* Ieee Access, 2018. **6**: p. 14410-14430.

2. Papernot, N., et al. *Distillation as a defense to adversarial perturbations against deep neural networks*. in *2016 IEEE symposium on security and privacy (SP)*. 2016. IEEE.

3. Ren, K., et al., *Adversarial attacks and defenses in deep learning.* Engineering, 2020. **6**(3): p. 346-360.

4. Xu, H., et al., *Adversarial attacks and defenses in images, graphs and text: A review.* International Journal of Automation and Computing, 2020. **17**(2): p. 151-178.

5. Narodytska, N. and S.P. Kasiviswanathan. *Simple Black-Box Adversarial Attacks on Deep Neural Networks*. in *CVPR Workshops*. 2017.

6. Liao, F., et al. *Defense against adversarial attacks using high-level representation guided denoiser*. in *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2018.

7. Madry, A., et al., *Towards deep learning models resistant to adversarial attacks.* arXiv preprint arXiv:1706.06083, 2017.

8. Dong, Y., et al. *Boosting adversarial attacks with momentum*. in *Proceedings of the IEEE conference on computer vision and pattern recognition*. 2018.

9. Zhang, Y., et al. *The secret revealer: Generative model-inversion attacks against deep neural networks*. in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2020.

10. Carlini, N., et al., *On Evaluating Adversarial Robustness.* arXiv pre-print server, 2019.