2018.

[6] A. Graese, A. Rozsa, and T. E. Boult, “Assessing threat of adversarial examples on deep neural networks,” in 15th IEEE International Conference on Machine Learning and Applications (ICMLA), 2016.

[7] A. Prakash, N. Moran, S. Garber, A. DiLillo, and J. Storer, “Deflecting adversarial attacks with pixel deflection,” in IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2018.

[8] Z. Yang, B. Li, P.-Y. Chen, and D. Song, “Towards mitigating audio adversarial perturbations,” 2018. [Online]. Available: https: //openreview.net/forum?id=SyZ2nKJDz

[9] D. Lemmond and R. Fitzgibbons, “Adversarial examples in audio,” 2018, CS4860 Final Project Report, University of Colorado, Colorado Springs Spring 2018.

[10] J.-M. Valin, “Speex: A free codec for free speech,” in Proceedings of linux.conf.au, 2006. [Online]. Available: https://arxiv.org/abs/1602. 08668

[11] J.-M. Valin, K. Vos, and T. B. Terriberry, “Definition of the Opus audio codec,” RFC 6716, 2012.

[12] M. R. Schroeder and B. S. Atal, “Code-excited linear prediction (CELP): High-quality speech at very low bit rates,” in IEEE International Conference on Acoustics, Speech and Signal Processing, 1985, pp. 937– 940.

[13] W. Xu, D. Evans, and Y. Qi, “Feature Squeezing: Detecting Adversarial Examples in Deep Neural Networks,” 2018 Network and Distributed System Security Symposium (NDSS’18), Feb. 2018.

[14] P. Warden, “Speech commands: A dataset for limited-vocabulary speech recognition,” arXiv preprint, no. 1804.03209, 2018.

[15] T. N. Sainath and C. Parada, “Convolutional neural networks for small-footprint keyword spotting,” in INTERSPEECH, 2015.

[16] R. L. Warren, S. Ramamoorthy, N. Ciganović, Y. Zhang, T. M. Wilson, T. Petrie, R. K. Wang, S. L. Jacques, T. Reichenbach, A. L. Nuttall, and A. Fridberger, “Minimal basilar membrane motion in low-frequency hearing,” Proceedings of the National Academy of Sciences, vol. 113, no. 30, Jul. 2016.

[17] W. He, J. Wei, X. Chen, N. Carlini, and D. Song, “Adversarial example defense: Ensembles of weak defenses are not strong,” in 11th USENIX Workshop on Offensive Technologies, WOOT 2017, 2017.