DAFTAR PUSTAKA

Amirkhani, A. and Karimi, M.P., 2022. Adversarial defenses for object detectors based on Gabor convolutional layers. *The Visual Computer*, 38(6), pp.1929-1944.

Bradski, G., 2000. The OpenCV library. *Dr. DobbâĂŹs Journal of Software Tools*.

Braunegg, A., Chakraborty, A., Krumdick, M., Lape, N., Leary, S., Manville, K., Merkhofer, E., Strickhart, L. and Walmer, M., 2020. Apricot: A dataset of physical adversarial attacks on object detection. In *Computer VisionâĂŞECCV 2020: 16th European Conference, Glasgow, UK, August 23âĂŞ28, 2020, Proceedings, Part XXI 16* (pp. 35-50). Springer International Publishing.

Brendel, W., Rauber, J. and Bethge, M., 2017. Decision-based adversarial attacks: Reliable attacks against black-box machine learning models. *arXiv preprint arXiv:1712,04248*.

Brown, T.B., ManÃľ, D., Roy, A., Abadi, M. and Gilmer, J., 2017. Adversarial patch. *arXiv preprint arXiv:1712,09665*.

Bunzel, N., Frick, R.A., Klause, G., Schwarte, A. and Honermann, J., 2024, July. Signals are all you need: Detecting and mitigating digital and real-world adversarial patches using signal-based features. In *Proceedings of the 2nd ACM Workshop on Secure and Trustworthy Deep Learning Systems* (pp. 24-34).

Carion, N., Massa, F., Synnaeve, G., Usunier, N., Kirillov, A. and Zagoruyko, S., 2020, August. End-to-end object detection with transformers. In *European conference on computer vision* (pp. 213-229). Cham: Springer International Publishing.

Carlini, N. and Wagner, D., 2017, May. Towards evaluating the robustness of neural networks. In *2017 IEEE Symposium on Security and Privacy (pp. 39-57)*. IEEE.

Chen, T. and Guestrin, C., 2016, August. XGBoost: A scalable tree boosting system. In *Proceedings of the 22nd acm sigkdd international conference on knowledge discovery and data mining* (pp. 785-794).

Chen, Z., Dash, P. and Pattabiraman, K., 2023, July. Jujutsu: A two-stage defense against adversarial patch attacks on deep neural networks. In *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security* (pp. 689-703).

Chen, Z., Li, B., Xu, J., Wu, S., Ding, S. and Zhang, W., 2022. Towards practical certifiable patch defense with vision transformer. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 15148-15158).

Chen, T., He, T., Benesty, M., Khotilovich, V., Tang, Y., Cho, H., Chen, K., Mitchell, R., Cano, I., Zhou, T., Li, M., Xie, J., Lin, M., Geng, Y., Li, Y., Yuan, J. and Cortes, D., 2025. xgboost: Extreme Gradient Boosting. R package version 3,2.0,0. Available at: https://github.com/dmlc/xgboost

Chow, K.H., Liu, L., Gursoy, M.E., Truex, S., Wei, W. and Wu, Y., 2020. TOG: targeted adversarial objectness gradient attacks on real-time object detection systems. *arXiv preprint arXiv:2004,04320*.

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A. and Bengio, Y., 2020. Generative adversarial networks. *Communications of the ACM*, *63(11), pp.139-144*.

Goodfellow, I.J., Shlens, J. and Szegedy, C., 2014. Explaining and harnessing adversarial examples. *arXiv preprint arXiv:1412,6572*.

GÃijrel, N.M., Qi, X., Rimanic, L., Zhang, C. and Li, B., 2021, July. Knowledge enhanced machine learning pipeline against diverse adversarial attacks. In *International Conference on Machine Learning* (pp. 3976-3987). PMLR.

Haralick, R.M., Shanmugam, K. and Dinstein, I.H., 1973. Textural features for image classification. *IEEE Transactions on systems, man, and cybernetics, (6)*, pp.610-621.

He, K., Zhang, X., Ren, S. and Sun, J., 2016. Identity mappings in deep residual networks. In *Computer VisionâĂŞECCV 2016: 14th European Conference, Amsterdam, The Netherlands*, October 11âĂŞ14, 2016, Proceedings, Part IV 14 (pp. 630-645). Springer International Publishing.

Heusel, M., Ramsauer, H., Unterthiner, T., Nessler, B. and Hochreiter, S., 2017. GANs trained by a two time-scale update rule converge to a local nash equilibrium. *Advances in neural information processing systems*, 30.

Hu, Y.C.T., Kung, B.H., Tan, D.S., Chen, J.C., Hua, K.L. and Cheng, W.H., 2021. Naturalistic physical adversarial patch for object detectors. In *Proceedings of the IEEE/CVF International Conference on Computer Vision* (pp. 7848-7857).

Huang, H., Chen, Z., Chen, H., Wang, Y. and Zhang, K., 2023. T-SEA: Transfer-based self-ensemble attack on object detection. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition* (pp. 20514-20523).

Jing, L., Wang, R., Ren, W., Dong, X. and Zou, C., 2024. PAD: Patch-Agnostic Defense against Adversarial Patch Attacks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 24472-24481).

Jocher, G., 2020. Ultralytics YOLOv5 (Version 7,0) [software]. Available at: https://github.com/ultralytics/yolov5

Kang, C., Dong, Y., Wang, Z., Ruan, S., Chen, Y., Su, H. and Wei, X., 2024, September. Diffender: Diffusion-based adversarial defense against patch attacks. In *European Conference on Computer Vision (pp. 130-147)*. Cham: Springer Nature Switzerland.

Kirillov, A., Mintun, E., Ravi, N., Mao, H., Rolland, C., Gustafson, L., Xiao, T., Whitehead, S., Berg, A.C., Lo, W.Y. and DollÃąr, P., 2023. Segment anything. In *Proceedings of the IEEE/CVF International Conference on Computer Vision* (pp. 4015-4026).

Krizhevsky, A. and Hinton, G., 2009. Learning multiple layers of features from tiny images.

Li, F., Liu, X., Zhang, X., Li, Q., Sun, K. and Li, K., 2021, May. Detecting localized adversarial examples: A generic approach using critical region analysis. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications (pp. 1-10)*. IEEE.

Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C.Y. and Berg, A.C., 2016, September. SSD: Single Shot Multibox Detector. In *European conference on computer vision* (pp. 21-37). Cham: Springer International Publishing.

Liu, J., Levine, A., Lau, C.P., Chellappa, R. and Feizi, S., 2022. Segment and complete: Defending object detectors against adversarial patch attacks with robust patch detection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 14973-14982).

Lu, M., Li, Q., Chen, L. and Li, H., 2021. Scale-Adaptive Adversarial Patch Attack for Remote Sensing Image Aircraft Detection. *Remote Sensing*, 13(20), p.4078.

Miyato, T., Kataoka, T., Koyama, M. and Yoshida, Y., 2018. Spectral normalization for generative adversarial networks. *arXiv preprint arXiv:1802,05957*.

Mogelmose, A., Trivedi, M.M. and Moeslund, T.B., 2012. Vision-based traffic sign detection and analysis for intelligent driver assistance systems: Perspectives and survey. IEEE transactions on intelligent transportation systems, 13(4), pp.1484-1497.

Natan, O. and Miura, J., 2022, End-to-end autonomous driving with semantic depth cloud mapping and multi-agent. *IEEE Transactions on Intelligent Vehicles*, 8(1), pp.557-571.

Otsu, N., 1975. A threshold selection method from gray-level histograms. *Automatica, 11(285-296)*, pp.23-27.

Pang, Y., Cao, J., Li, Y., Xie, J., Sun, H. and Gong, J., 2020. TJU-DHD: A diverse high-resolution dataset for object detection. *IEEE Transactions on Image Processing*, 30, pp.207-219.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V. et al., 2011. Scikit-learn: Machine learning in Python. *Journal of Machine Learning Research*, 12, pp.2825âĂŞ2830.

Pennebaker, W.B. and Mitchell, J.L., 1992. JPEG: Still image data compression standard. Springer Science Business Media.

Rao, S., Stutz, D. and Schiele, B., 2020, August. Adversarial training against location-optimized adversarial patches. In *European conference on computer vision* (pp. 429-448). Cham: Springer International Publishing.

Redmon, J., Divvala, S., Girshick, R. and Farhadi, A., 2016. You only look once: Unified, real-time object detection. In *Proceedings of the IEEE conference on computer vision and pattern recognition*.

Ronneberger, O., Fischer, P. and Brox, T., 2015, October. U-Net: Convolutional Networks for Biomedical Image Segmentation. In *International Conference on Medical image computing and computer-assisted intervention* (pp. 234-241). Cham: Springer international publishing.

Shannon, C.E., 1948. A mathematical theory of communication. The Bell system technical journal, 27(3), pp.379-423.

Simonyan, K. and Zisserman, A., 2014. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409,1556*.

Stallkamp, J., Schlipsing, M., Salmen, J. and Igel, C., 2011, July. The German traffic sign recognition benchmark: a multi-class classification competition. In The 2011 international joint conference on neural networks (pp. 1453-1460). IEEE.

Szegedy, C., 2013. Intriguing properties of neural networks. *arXiv preprint arXiv:1312,6199*.

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V. and Rabinovich, A., 2015. Going deeper with convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1-9).

Tarchoun, B., Ben Khalifa, A., Mahjoub, M.A., Abu-Ghazaleh, N. and Alouani, I., 2023. Jedi: Entropy-based localization and removal of adversarial patches. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 4087-4095).

Thys, S., Van Ranst, W. and GoedemÃl', T., 2019. Fooling automated surveillance cameras: adversarial patches to attack person detection. In *Proceedings of the IEEE-/CVF conference on computer vision and pattern recognition workshops* (pp. 0-0).

Van der Walt, S., SchÃűnberger, J.L., Nunez-Iglesias, J., Boulogne, F., Warner, J.D., Yager, N., Gouillart, E. and Yu, T., 2014. scikit-image: image processing in Python. *PeerJ*, 2, p.e453.

van Oers, A.M. and Rammers, T., 2025, October. Adversarial Patch Size and Positioning. In *Target and Background Signatures XI: Traditional Methods and Artificial Intelligence* (Vol. 13673, pp. 20-29). SPIE.

Wang, Z., Bovik, A.C., Sheikh, H.R. and Simoncelli, E.P., 2004. Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, 13(4), pp.600-612.

Wang, L., Lin, Z.Q. and Wong, A., 2020. COVID-Net: a Tailored Deep Convolutional Neural Network Design for Detection of COVID-19 Cases from Chest X-ray Images. *Scientific reports*, 10(1), p.19549.

Wang, J., Su, W., Luo, C., Chen, J., Song, H. and Li, J., 2022. CSG: Classifier-aware defense strategy based on compressive sensing and generative networks for visual recognition in autonomous vehicle systems. *IEEE Transactions on Intelligent Transportation Systems*, 23(7), pp.9543-9553.

Wei, X., Pu, B., Lu, J. and Wu, B., 2022. Visually adversarial attacks and defenses in the physical world: A survey. *arXiv preprint arXiv:2211,01671*.

Yamada, Y., Iwamura, M., Akiba, T. and Kise, K., 2019. Shakedrop regularization for deep residual learning. *IEEE Access*, 7, pp.186126-186136.

Zeng, Y., Fu, J., Chao, H. and Guo, B., 2022. Aggregated contextual transformations for high-resolution image inpainting. *IEEE Transactions on Visualization and Computer Graphics*, 29(7), pp.3266-3280.

Zhang, C., Li, H., Wang, X. and Yang, X., 2015. Cross-Scene Crowd Counting via Deep Convolutional Neural Networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 833-841).

Zhou, B., Lapedriza, A., Khosla, A., Oliva, A. and Torralba, A., 2017. Places: A 10 million image database for scene recognition. *IEEE transactions on pattern analysis and machine intelligence*, 40(6), pp.1452-1464.