DAFTAR PUSTAKA

Agrawal, K., & Bhatnagar, C. (2023). M-SAN: a patch-based transferable adversarial attack using the multi-stack adversarial network. *Journal of Electronic Imaging*, *32*(2), 023033. https://doi.org/10.1117/1.JEI.32.2.023033

Aloraini, F., Javed, A., & Rana, O. (2024). Adversarial Attacks on Intrusion Detection Systems in In-Vehicle Networks of Connected and Autonomous Vehicles. *Sensors*, *24*(12), 3848. https://doi.org/10.3390/s24123848

Anthi, E., Williams, L., Rhode, M., Burnap, P., & Wedgbury, A. (2021). Adversarial attacks on machine learning cybersecurity defences in Industrial Control Systems. *Journal of Information Security and Applications*, *58*, 102717. https://doi.org/10.1016/j.jisa.2020.102717

Chen, P.-Y., Zhang, H., Sharma, Y., Yi, J., & Hsieh, C.-J. (2017). ZOO: Zeroth Order Optimization Based Black-box Attacks to Deep Neural Networks without Training Substitute Models. *Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security*. https://doi.org/10.1145/3128572.3140448

Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2022). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *44*(10), 5962–5979. https://doi.org/10.1109/TPAMI.2021.3087709

Dharmawan, D. A., & Nugroho, A. S. (2024). Towards Deep Face Spoofing: Taxonomy, Recent Advances, and Open Challenges. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. https://doi.org/10.1109/TBIOM.2024.3417372

Dong, Y., Su, H., Wu, B., Li, Z., Liu, W., Zhang, T., & Zhu, J. (2019). Efficient Decision-based Black-box Adversarial Attacks on Face Recognition. *arXiv preprint arXiv:1904.04433*. http://arxiv.org/abs/1904.04433

Guerreiro, J., Tomás, P., Garcia, N., & Aidos, H. (2023). Super-resolution of magnetic resonance images using Generative Adversarial Networks. *Computerized Medical Imaging and Graphics*, *108*, 102280. https://doi.org/10.1016/j.compmedimag.2023.102280

Ilyas, A., Engstrom, L., Athalye, A., & Lin, J. (2018). Black-box Adversarial Attacks with Limited Queries and Information. *arXiv preprint arXiv:1804.08598*. http://arxiv.org/abs/1804.08598

Islam, M. T., Ahmed, T., Rashid, A. B. M. R., Islam, T., Rahman, M. S., & Habib, M. T. (2022). Convolutional Neural Network Based Partial Face Detection. *arXiv preprint arXiv:2206.14350*. https://arxiv.org/abs/2206.14350

Khamaiseh, S. Y., Bagagem, D., Al-Alaj, A., Mancino, M., & Alomari, H. W. (2022). Adversarial Deep Learning: A Survey on Adversarial Attacks and Defense Mechanisms on Image Classification. *IEEE Access*, *10*, 102266–102291. https://doi.org/10.1109/ACCESS.2022.3208131

Kingma, D. P., & Ba, J. (2015). Adam: A Method for Stochastic Optimization. *Proceedings of the 3rd International Conference on Learning Representations (ICLR)*.

Kong, Z., Xue, J., Wang, Y., Huang, L., Niu, Z., & Li, F. (2021). A Survey on Adversarial Attack in the Age of Artificial Intelligence. *Wireless Communications and Mobile Computing*, *2021*, 1–22. https://doi.org/10.1155/2021/4907754

Li, C., Wang, H., Zhang, J., Yao, W., & Jiang, T. (2022). An Approximated Gradient Sign Method Using Differential Evolution for Black-Box Adversarial Attack. *IEEE Transactions on Evolutionary Computation*, *26*(5), 976–990. https://doi.org/10.1109/TEVC.2022.3151373

Liu, S., Leiva, V., Zhuang, D., Ma, T., & Figueroa-Zúñiga, J. I. (2022). Matrix differential calculus with applications in the multivariate linear model and its diagnostics. *Journal of Multivariate Analysis*, *188*, 104849. https://doi.org/10.1016/j.jmva.2021.104849

Munir, R. (2015). *Metode Numerik* (Revisi Keempat). Informatika Bandung.

Pal, B., Gupta, D., Rashed-Al-Mahfuz, M., Alyami, S., & Moni, M. A. (2021). Vulnerability in Deep Transfer Learning Models to Adversarial Fast Gradient Sign Attack for COVID-19 Prediction from Chest Radiography Images. *Applied Sciences*, *11*(9), 4233. https://doi.org/10.3390/app11094233

Pal, S., Rahman, S., Beheshti, M., Habib, A., Jadidi, Z., & Karmakar, C. (2024). The Impact of Simultaneous Adversarial Attacks on Robustness of Medical Image Analysis. *IEEE Access*, *12*, 66478–66494. https://doi.org/10.1109/ACCESS.2024.3396566

Redgrave, T., & Crum, C. (2023). *Generating Adversarial Samples in Mini-Batches May Be Detrimental To Adversarial Robustness*. arXiv preprint arXiv:2303.17720. http://arxiv.org/abs/2303.17720

Ren, K., Zheng, T., Qin, Z., & Liu, X. (2020). Adversarial Attacks and Defenses in Deep Learning. *Engineering*, *6*(3), 346-360. https://doi.org/10.1016/j.eng.2019.12.012

Rozsa, A., Günther, M., & Boult, T. E. (2016). LOTS about Attacking Deep Features. *arXiv preprint arXiv:1611.06179*. http://arxiv.org/abs/1611.06179

Sengupta, S., Chen, J.-C., Castillo, C., Patel, V. M., Chellappa, R., & Jacobs, D. W. (2016). Frontal to Profile Face Verification in the Wild. *2016 IEEE Winter Conference on Applications of Computer Vision (WACV)*, 1–9.

Serengil, S., & Özpınar, A. (2024). A Benchmark of Facial Recognition Pipelines and Co-Usability Performances of Modules. *Bilişim Teknolojileri Dergisi*, *17*(2), 95–107. https://doi.org/10.17671/gazibtd.1399077

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. *Proceedings of the ACM Conference on Computer and Communications Security*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Simonyan, K., & Zisserman, A. (2015). Very Deep Convolutional Networks for Large-Scale Image Recognition. *arXiv preprint arXiv:1409.1556*. https://doi.org/10.48550/arXiv.1409.1556

Sorin, V., Soffer, S., Glicksberg, B. S., Barash, Y., Konen, E., & Klang, E. (2023). Adversarial attacks in radiology – A systematic review. *European Journal of Radiology*, *167*, 111085. https://doi.org/10.1016/j.ejrad.2023.111085

Steck, H., Ekanadham, C., & Kallus, N. (2024). Is Cosine-Similarity of Embeddings Really About Similarity? *Proceedings of the 17th ACM International Conference on Web Search and Data Mining*. https://doi.org/10.1145/3589335.3651526

Symolon, W., & Dagli, C. H. (2021). Single-Image Super Resolution using Convolutional Neural Network. *Procedia Computer Science*, *185*, 213–222. https://doi.org/10.1016/j.procs.2021.05.022

Tieleman, T., & Hinton, G. (2012). *Lecture 6.5-rmsprop, COURSERA: Neural Networks for Machine Learning*. University of Toronto, Technical Report.

Wang, X., & He, K. (2021). Enhancing the Transferability of Adversarial Attacks through Variance Tuning. *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 1924–1933. https://doi.org/10.1109/CVPR46437.2021.00196

Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks. *IEEE Signal Processing Letters*, *23*(10), 1499-1503.

Zhong, Y., & Deng, W. (2020). Towards Transferable Adversarial Attack against Deep Face Recognition. *arXiv preprint arXiv:2004.05790*. https://doi.org/10.48550/arXiv.2004.05790