DAFTAR PUSTAKA

Abdollahpoorrostam, A., Abroshan, M., & Moosavi-Dezfooli, S.-M. (2024). *Revisiting DeepFool: generalization and improvement*. http://arxiv.org/abs/2303.12481

Agac, S., & Durmaz Incel, O. (2023). On the Use of a Convolutional Block Attention Module in Deep Learning-Based Human Activity Recognition with Motion Sensors. *Diagnostics*, *13*(11). https://doi.org/10.3390/diagnostics13111861

Agarap, A. F. (2019). *Deep Learning using Rectified Linear Units (ReLU)*. http://arxiv.org/abs/1803.08375

Aggarwal, C. C. (2018). Neural Networks and Deep Learning: A Textbook. In *Neural Networks and Deep Learning: A Textbook*. Springer International Publishing. https://doi.org/10.1007/978-3-319-94463-0

Ahmed, I. A., Senan, E. M., Shatnawi, H. S. A., Alkhraisha, Z. M., & Al-Azzam, M. M. A. (2023). Multi-Techniques for Analyzing X-ray Images for Early Detection and Differentiation of Pneumonia and Tuberculosis Based on Hybrid Features. *Diagnostics*, *13*(4). https://doi.org/10.3390/diagnostics13040814

Akhtom, D. M., Singh, M. M., & XinYing, C. (2024). Enhancing trustworthy deep learning for image classification against evasion attacks: a systematic literature review. *Artificial Intelligence Review*, *57*(7). https://doi.org/10.1007/s10462-024-10777-4

ALBAWI, S. (2017). *2017 International Conference on Engineering and Technology (ICET)*. IEEE.

Al Nufaiei, Z. F., & Alshamrani, K. M. (2025). Comparing Ultrasound, Chest X-Ray, and CT Scan for Pneumonia Detection. In *Medical Devices: Evidence and Research* (Vol. 18, pp. 149–159). Dove Medical Press Ltd. https://doi.org/10.2147/MDER.S501714

Alshazly, H., Linse, C., Abdalla, M., Barth, E., & Martinetz, T. (2021). COVID-Nets: deep CNN architectures for detecting COVID-19 using chest CT scans. *PeerJ Computer Science*, *7*, 1–40. https://doi.org/10.7717/peerj-cs.655

Alzubaidi, L., AL–Dulaimi, K., Obeed, H. A. H., Saihood, A., Fadhel, M. A., Jebur, S. A., Chen, Y., Albahri, A. S., Santamaría, J., Gupta, A., & Gu, Y. (2024). MEFF – A model ensemble feature fusion approach for tackling adversarial attacks in medical imaging. *Intelligent Systems with Applications*, *22*. https://doi.org/10.1016/j.iswa.2024.200355

Ambati, A., & Dubey, S. R. (2022). *AC-CovidNet: Attention Guided Contrastive CNN for Recognition of Covid-19 in Chest X-Ray Images*. http://arxiv.org/abs/2105.10239

Artificial Intelligence Technology. (2022). In *Artificial Intelligence Technology*. Springer Nature. https://doi.org/10.1007/978-981-19-2879-6

Ashraf, S. N., Siddiqi, R., & Farooq, H. (2024). Auto encoder-based defense mechanism against popular adversarial attacks in deep learning. *PloS One*, *19*(10), e0307363. https://doi.org/10.1371/journal.pone.0307363

Asif, S., Zhao, M., Tang, F., & Zhu, Y. (2024). LWSE: a lightweight stacked ensemble model for accurate detection of multiple chest infectious diseases including COVID-19. *Multimedia Tools and Applications*, *83*(8), 23967–24003. https://doi.org/10.1007/s11042-023-16432-4

Athalye, A., Carlini, N., & Wagner, D. (2018). *Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples*. http://arxiv.org/abs/1802.00420

Awad, Z., Zakaria, M., & Hassan, R. (2025). An enhanced ensemble defense framework for boosting adversarial robustness of intrusion detection systems. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-94023-z

Bashar, A., Latif, G., Brahim, G. Ben, Mohammad, N., & Alghazo, J. (2021). COVID-19 pneumonia detection using optimized deep learning techniques. *Diagnostics*, *11*(11). https://doi.org/10.3390/diagnostics11111972

Beerens, L., & Higham, D. J. (2023). *Vulnerability Analysis of Transformer-based Optical Character Recognition to Adversarial Attacks*. http://arxiv.org/abs/2311.17128

Bigolin Lanfredi, R., Schroeder, J. D., & Tasdizen, T. (2023). Quantifying the preferential direction of the model gradient in adversarial training with projected gradient descent. *Pattern Recognition*, *139*. https://doi.org/10.1016/j.patcog.2023.109430

Bjorck, J., Gomes, C., Selman, B., & Weinberger, K. Q. (2018). *Understanding Batch Normalization*. http://arxiv.org/abs/1806.02375

Bortsova, G., González-Gonzalo, C., Wetstein, S. C., Dubost, F., Katramados, I., Hogeweg, L., Liefers, B., van Ginneken, B., Pluim, J. P. W., Veta, M., Sánchez, C. I., & de Bruijne, M. (2021). Adversarial attack vulnerability of medical image analysis systems: Unexplored factors. *Medical Image Analysis*, *73*. https://doi.org/10.1016/j.media.2021.102141

Cabot, J. H., & Ross, E. G. (2023). Evaluating prediction model performance. *Surgery (United States)*, *174*(3), 723–726. https://doi.org/10.1016/j.surg.2023.05.023

Ca, P. V., Edu, L. T., Lajoie, I., Ca, Y. B., & Ca, P.-A. M. (2010). Stacked Denoising Autoencoders: Learning Useful Representations in a Deep Network with a Local Denoising Criterion Pascal Vincent Hugo Larochelle Yoshua Bengio Pierre-Antoine Manzagol. In *Journal of Machine Learning Research* (Vol. 11).

Chandrinos, N., Loi, I., Zachos, P., Symeonidis, I., Spiliotis, A., Panou, M., & Moustakas, K. (2024). *Effectiveness of L2 Regularization in Privacy-Preserving Machine Learning*. http://arxiv.org/abs/2412.01541

Chlap, P., Min, H., Vandenberg, N., Dowling, J., Holloway, L., & Haworth, A. (2021). A review of medical image data augmentation techniques for deep learning applications. In *Journal of Medical Imaging and Radiation Oncology* (Vol. 65, Issue 5, pp. 545–563). John Wiley and Sons Inc. https://doi.org/10.1111/1754-9485.13261

Chollet, F. (2017). *Xception: Deep Learning with Depthwise Separable Convolutions*. http://arxiv.org/abs/1610.02357

Clevert, D.-A., Unterthiner, T., & Hochreiter, S. (2016). *Fast and Accurate Deep Network Learning by Exponential Linear Units (ELUs)*. http://arxiv.org/abs/1511.07289

Costa, J. C., Roxo, T., Proença, H., & Inácio, P. R. M. (n.d.). *Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000. How Deep Learning Sees the World: A Survey on Adversarial Attacks & Defenses*. https://doi.org/10.1109/ACCESS.2023.0322000

Cui, X., Xiao, J., & Zheng, W. (2024). Model Adversarial Attack and Defense Based on Network Reorganization. *Proceedings - 2024 China Automation Congress, CAC 2024*, 2025–2029. https://doi.org/10.1109/CAC63892.2024.10865492

Dai, Y., Qian, Y., Lu, F., Wang, B., Gu, Z., Wang, W., Wan, J., & Zhang, Y. (2023). Improving adversarial robustness of medical imaging systems via adding global attention noise. *Computers in Biology and Medicine*, *164*. https://doi.org/10.1016/j.compbiomed.2023.107251

Das, A., Yenala, H., Chinnakotla, M., & Shrivastava, M. (2016). Together we stand: Siamese networks for similar question retrieval. *54th Annual Meeting of the Association for Computational Linguistics, ACL 2016 - Long Papers*, *1*, 378–387. https://doi.org/10.18653/v1/p16-1036

Dubey, S. R., Singh, S. K., & Chaudhuri, B. B. (2022). *Activation Functions in Deep Learning: A Comprehensive Survey and Benchmark*. http://arxiv.org/abs/2109.14545

Dumoulin, V., & Visin, F. (2018). *A guide to convolution arithmetic for deep learning*. http://arxiv.org/abs/1603.07285

Eleftheriadis, C., Symeonidis, A., & Katsaros, P. (2024). Adversarial robustness improvement for deep neural networks. *Machine Vision and Applications*, *35*(3). https://doi.org/10.1007/s00138-024-01519-1

Elharrouss, O., Mahmood, Y., Bechqito, Y., Serhani, M. A., Badidi, E., Riffi, J., & Tairi, H. (2025). *Loss Functions in Deep Learning: A Comprehensive Review*. http://arxiv.org/abs/2504.04242

Fan, S., Li, J., Zhang, Y., Tian, X., Wang, Q., He, X., Zhang, C., & Huang, W. (2020). On line detection of defective apples using computer vision system combined with deep learning methods. *Journal of Food Engineering*, *286*. https://doi.org/10.1016/j.jfoodeng.2020.110102

Fkirin, A., Moursi, A. S., Attiya, G., El-Sayed, A., & Shouman, M. A. (2024). Hybrid two-level protection system for preserving pre-trained DNN models ownership. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-024-10304-0

Fred, T., & Sam, J. (2024). *Adversarial Attacks and Robustness in Deep Learning Models*.

Gal, Y., & Ghahramani, Z. (2016). *Dropout as a Bayesian Approximation: Representing Model Uncertainty in Deep Learning*. http://arxiv.org/abs/1506.02142

Goceri, E. (2023). Medical image data augmentation: techniques, comparisons and interpretations. *Artificial Intelligence Review*, *56*(11), 12561–12605. https://doi.org/10.1007/s10462-023-10453-z

Gondara, L. (2016). *Medical image denoising using convolutional denoising autoencoders*. https://doi.org/10.1109/ICDMW.2016.0041

Gu, J., Wang, Z., Kuen, J., Ma, L., Shahroudy, A., Shuai, B., Liu, T., Wang, X., Wang, G., Cai, J., & Chen, T. (2018). Recent advances in convolutional neural networks. *Pattern Recognition*, *77*, 354–377. https://doi.org/10.1016/j.patcog.2017.10.013

Hancock, J. T., Khoshgoftaar, T. M., & Johnson, J. M. (2023). Evaluating classifier performance with highly imbalanced Big Data. *Journal of Big Data*, *10*(1). https://doi.org/10.1186/s40537-023-00724-5

Han, L., Zhao, Y., Lv, H., Zhang, Y., Liu, H., & Bi, G. (2022). Remote Sensing Image Denoising Based on Deep and Shallow Feature Fusion and Attention Mechanism. *Remote Sensing*, *14*(5). https://doi.org/10.3390/rs14051243

He, W., Wei, J., Chen, X., Carlini, N., & Song, D. (2017). *Adversarial Example Defenses: Ensembles of Weak Defenses are not Strong*. http://arxiv.org/abs/1706.04701

Hicks, S. A., Strümke, I., Thambawita, V., Hammou, M., Riegler, M. A., Halvorsen, P., & Parasa, S. (2022). On evaluation metrics for medical applications of artificial intelligence. *Scientific Reports*, *12*(1). https://doi.org/10.1038/s41598-022-09954-8

Hou, X., Wang, L., Zhu, D., Guo, L., Weng, J., Zhang, M., Zhou, Z., Zou, D., Ji, Q., Guo, X., Wu, Q., Chen, S., Yu, R., Chen, H., Huang, Z., Zhang, X., Wu, J., Wu, J., & Jia, W. (2023). Prevalence of diabetic retinopathy and vision-threatening diabetic retinopathy in adults with diabetes in China. *Nature Communications*, *14*(1). https://doi.org/10.1038/s41467-023-39864-w

Ioffe, S., & Szegedy, C. (2015). *Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift*. http://arxiv.org/abs/1502.03167

Iqbal, S., Khan, T. M., Naveed, K., Naqvi, S. S., & Nawaz, S. J. (2022). Recent trends and advances in fundus image analysis: A review. In *Computers in Biology and Medicine* (Vol. 151). Elsevier Ltd. https://doi.org/10.1016/j.compbiomed.2022.106277

Jinsakul, N., Tsai, C. F., Tsai, C. E., & Wu, P. (2019). Enhancement of deep learning in image classification performance using Xception with the swish activation function for colorectal polyp preliminary screening. *Mathematics*, *7*(12). https://doi.org/10.3390/MATH7121170

Kansal, K., Krishna, P. S., Jain, P. B., R, S., Honnavalli, P., & Eswaran, S. (2022). Defending against adversarial attacks on Covid-19 classifier: A denoiser-based approach. *Heliyon*, *8*(10). https://doi.org/10.1016/j.heliyon.2022.e11209

Karner, M., Peltola, J., Jerne, M., Kulas, L., & Priller, P. (2024). *Studies in Computational Intelligence 1147 Intelligent Secure Trustable Things*.

Kascenas, A., Sanchez, P., Schrempf, P., Wang, C., Clackett, W., Mikhael, S. S., Voisey, J. P., Goatman, K., Weir, A., Pugeault, N., Tsaftaris, S. A., & O'Neil, A. Q. (2023).

The role of noise in denoising models for anomaly detection in medical images. *Medical Image Analysis*, *90*. https://doi.org/10.1016/j.media.2023.102963

Kaur, N., Singh, S., Shivaji Deore, D., Vidhate, D. A., Haridas, D., Varma Kosuri, G., & Ravindra Kolhe, M. (2024). Robustness and Security in Deep Learning: Adversarial Attacks and Countermeasures. In *J. Electrical Systems* (Vol. 20, Issue 3).

Khalifa, A. Ben, & Frigui, H. (2016). *Multiple Instance Fuzzy Inference Neural Networks*. http://arxiv.org/abs/1610.04973

Koo, I., Chae, D. K., & Lee, S. C. (2023). Improving Adversarial Robustness via Distillation-Based Purification. *Applied Sciences (Switzerland)*, *13*(20). https://doi.org/10.3390/app132011313

Krichen, M. (2023). Convolutional Neural Networks: A Survey. *Computers*, *12*(8). https://doi.org/10.3390/computers12080151

Kukker, A., & Sharma, R. (2021). Modified Fuzzy Q Learning Based Classifier for Pneumonia and Tuberculosis. *IRBM*, *42*(5), 369–377. https://doi.org/10.1016/j.irbm.2020.10.005

Labib, S. M. F. R., Mondal, J. J., Manab, M. A., Xiao, X., & Newaz, S. (2025). Tailoring adversarial attacks on deep neural networks for targeted class manipulation using DeepFool algorithm. *Scientific Reports*, *15*(1). https://doi.org/10.1038/s41598-025-87405-w

Lal, S., Rehman, S. U., Shah, J. H., Meraj, T., Rauf, H. T., Damaševičius, R., Mohammed, M. A., & Abdulkareem, K. H. (2021). Adversarial attack and defence through adversarial training and feature fusion for diabetic retinopathy recognition. *Sensors*, *21*(11). https://doi.org/10.3390/s21113922

Lecun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. In *Nature* (Vol. 521, Issue 7553, pp. 436–444). Nature Publishing Group. https://doi.org/10.1038/nature14539

Liao, F., Liang, M., Dong, Y., Pang, T., Hu, X., & Zhu, J. (2018). *Defense against Adversarial Attacks Using High-Level Representation Guided Denoiser*. http://arxiv.org/abs/1712.02976

Lim, G., Bellemo, V., Xie, Y., Lee, X. Q., Yip, M. Y. T., & Ting, D. S. W. (2020). Different fundus imaging modalities and technical factors in AI screening for diabetic retinopathy: a review. In *Eye and Vision* (Vol. 7, Issue 1). BioMed Central Ltd. https://doi.org/10.1186/s40662-020-00182-7

Li, Q., Chen, W., Chen, X., Hu, J., Su, X., Ji, Z., & Wu, Y. (2024). Object Detection in Remote Sensing Images of Pine Wilt Disease Based on Adversarial Attacks and Defenses. *Forests*, *15*(9). https://doi.org/10.3390/f15091623

Liu, L., Wu, F. X., Wang, Y. P., & Wang, J. (2020). Multi-receptive-field CNN for semantic segmentation of medical images. *IEEE Journal of Biomedical and Health Informatics*, *24*(11), 3215–3225. https://doi.org/10.1109/JBHI.2020.3016306

Liu, W., Wang, Z., Liu, X., Zeng, N., Liu, Y., & Alsaadi, F. E. (2017). A survey of deep neural network architectures and their applications. *Neurocomputing*, *234*, 11–26. https://doi.org/10.1016/j.neucom.2016.12.038

Liu, Z., Du, J., Wang, M., & Ge, S. S. (2020). ADCM: attention dropout convolutional module. *Neurocomputing*, *394*, 95–104. https://doi.org/10.1016/j.neucom.2020.02.007

Liu, Z., Xu, Z., Jin, J., Shen, Z., & Darrell, T. (2023). *Dropout Reduces Underfitting*. http://arxiv.org/abs/2303.01500

Li, X., Wang, W., Hu, X., & Yang, J. (2019). Selective kernel networks. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, *2019-June*, 510–519. https://doi.org/10.1109/CVPR.2019.00060

Li, Y., & Liu, S. (2023). The Threat of Adversarial Attack on a COVID-19 CT Image-Based Deep Learning System. *Bioengineering*, *10*(2). https://doi.org/10.3390/bioengineering10020194

Li, Z., Li, X., Zhu, Z., Zeng, S., Wang, Y., Wang, Y., & Li, A. (2019). Signal Analysis of Electrocardiogram and Statistical Evaluation of Myocardial Enzyme in the Diagnosis and Treatment of Patients with Pneumonia. *IEEE Access*, *7*, 113751–113759. https://doi.org/10.1109/ACCESS.2018.2889354

Madry, A., Makelov, A., Schmidt, L., Tsipras, D., & Vladu, A. (2019). *Towards Deep Learning Models Resistant to Adversarial Attacks*. http://arxiv.org/abs/1706.06083

Makhlouf, A., Maayah, M., Abughanam, N., & Catal, C. (2023). The use of generative adversarial networks in medical image augmentation. In *Neural Computing and Applications* (Vol. 35, Issue 34, pp. 24055–24068). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/s00521-023-09100-z

Malang, U. M. (2021). *Klasifikasi COVID-19 menggunakan Filter Gabor dan CNN dengan Hyperparameter Tuning*. *9*(3), 493–504.

Matsumoto, S., & Novak, J. (2010). *Primitive factorizations, Jucys-Murphy elements, and matrix models*. http://arxiv.org/abs/1005.0151

Mienye, I. D., Swart, T. G., Obaido, G., Jordan, M., & Ilono, P. (2025). Deep Convolutional Neural Networks in Medical Image Analysis: A Review. In *Information (Switzerland)* (Vol. 16, Issue 3). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/info16030195

MINARNO, A. E., MANDIRI, M. H. C., & ALFARIZY, M. R. (2021). Klasifikasi COVID-19 menggunakan Filter Gabor dan CNN dengan Hyperparameter Tuning. *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, *9*(3), 493. https://doi.org/10.26760/elkomika.v9i3.493

Minarno, A. E., Rifal Alfarizy, M., Hendryawan, A., Syaifuddin, S., & Munarko, Y. (2021). Pneumonia Classification using Gabor-Convolutional Neural Networks and Image Enhancement. *2021 9th International Conference on Information and Communication Technology, ICoICT 2021*, 180–185. https://doi.org/10.1109/ICoICT52021.2021.9527427

Mirsky, Y., Mahler, T., Shelef, I., & Elovici, Y. (2019). *CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning*. http://arxiv.org/abs/1901.03597

Mosquera, C., Ferrer, L., Milone, D. H., Luna, D., & Ferrante, E. (2024). Class imbalance on medical image classification: towards better evaluation practices for discrimination and calibration performance. *European Radiology*, *34*(12), 7895–7903. https://doi.org/10.1007/s00330-024-10834-0

Nair, V., & Hinton, G. E. (2010). *Rectified Linear Units Improve Restricted Boltzmann Machines*.

Nam, W., & Kil, H. (2023). AESOP: Adjustable Exhaustive Search for One-Pixel Attacks in Deep Neural Networks. *Applied Sciences (Switzerland)*, *13*(8). https://doi.org/10.3390/app13085092

Nam, W., Kim, K., Moon, H., Noh, H., Park, J., & Kil, H. (2024). RISOPA: Rapid Imperceptible Strong One-Pixel Attacks in Deep Neural Networks. *Mathematics*, *12*(7). https://doi.org/10.3390/math12071083

Nguyen, K. N. T., Zhang, W., Lu, K., Wu, Y., Zheng, X., Tan, H. L., & Zhen, L. (2025). *A Survey and Evaluation of Adversarial Attacks for Object Detection*. http://arxiv.org/abs/2408.01934

Oltu, B., Güney, S., Yuksel, S. E., & Dengiz, B. (2025). Automated classification of chest X-rays: a deep learning approach with attention mechanisms. *BMC Medical Imaging*, *25*(1). https://doi.org/10.1186/s12880-025-01604-5

Osman, M., Manosuthi, W., Kaewkungwal, J., Silachamroon, U., Mansanguan, C., Kamolratanakul, S., & Pitisuttithum, P. (2021). Etiology, clinical course, and outcomes of pneumonia in the elderly: A retrospective and prospective cohort study in thailand. *American Journal of Tropical Medicine and Hygiene*, *104*(6), 2009–2016. https://doi.org/10.4269/ajtmh.20-1393

Pang, T., Xu, K., Du, C., Chen, N., & Zhu, J. (2019). *Improving Adversarial Robustness via Promoting Ensemble Diversity*. http://arxiv.org/abs/1901.08846

Paschali, M., Conjeti, S., Navarro, F., & Navab, N. (2018). *Generalizability vs. Robustness: Adversarial Examples for Medical Imaging*. http://arxiv.org/abs/1804.00504

Perez, L., & Wang, J. (2017). *The Effectiveness of Data Augmentation in Image Classification using Deep Learning*. http://arxiv.org/abs/1712.04621

Proschek, P., & Vogl, T. (2016). Chest and mediastinum. In *Diagnostic and Interventional Radiology* (pp. 479–587). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-44037-7_19

Qin, Q., & Chen, Y. (2024). A review of retinal vessel segmentation for fundus image analysis. In *Engineering Applications of Artificial Intelligence* (Vol. 128). Elsevier Ltd. https://doi.org/10.1016/j.engappai.2023.107454

Radočaj, P., Radočaj, D., & Martinović, G. (2025). Optimizing Convolutional Neural Network Architectures with Optimal Activation Functions for Pediatric Pneumonia Diagnosis Using Chest X-Rays. *Big Data and Cognitive Computing*, *9*(2). https://doi.org/10.3390/bdcc9020025

Rahman, A., Hossain, M. S., Alrajeh, N. A., & Alsolami, F. (2021). Adversarial Examples - Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices. *IEEE Internet of Things Journal*, *8*(12), 9603–9610. https://doi.org/10.1109/JIOT.2020.3013710

Ramachandran, P., Zoph, B., & Le, Q. V. (2017). *Searching for Activation Functions*. http://arxiv.org/abs/1710.05941

Reddy Mopuri, K., Shaj, V., & Venkatesh Babu, R. (n.d.). *Adversarial Fooling Beyond "Flipping the Label."*

Rekha, S., Jahan, S., & Quadri, A. H. (2018). Deep Indian Delicacy: Classification of Indian Food Images using Convolutional Neural Networks. *SJ Impact Factor: 6*, *887*. www.ijraset.com2653

Rice, L., Wong, E., & Kolter, J. Z. (2020). *Overfitting in adversarially robust deep learning*. https://github.com/

Rosenblatt, M., Dadashkarimi, J., & Scheinost, D. (2023). *Gradient-based enhancement attacks in biomedical machine learning*. http://arxiv.org/abs/2301.01885

Rudnitskaya, E. A., & Poltavtseva, M. A. (2022). Adversarial Machine Learning Protection Using the Example of Evasion Attacks on Medical Images. *Automatic Control and Computer Sciences*, *56*(8), 934–941. https://doi.org/10.3103/S0146411622080211

Salmi, M., Atif, D., Oliva, D., Abraham, A., & Ventura, S. (2024). Handling imbalanced medical datasets: review of a decade of research. *Artificial Intelligence Review*, *57*(10). https://doi.org/10.1007/s10462-024-10884-2

Santurkar, S., Tsipras, D., Ilyas, A., & Madry, A. (2019). *How Does Batch Normalization Help Optimization?* http://arxiv.org/abs/1805.11604

Scherer, D., Müller, A., & Behnke, S. (n.d.). *Evaluation of Pooling Operations in Convolutional Architectures for Object Recognition*. http://www.ais.uni-bonn.de

Sermanet, P., Eigen, D., Zhang, X., Mathieu, M., Fergus, R., & LeCun, Y. (2014). *OverFeat: Integrated Recognition, Localization and Detection using Convolutional Networks*. http://arxiv.org/abs/1312.6229

Shanthi, T., Sabeenian, R. S., & Anand, R. (2020). Automatic diagnosis of skin diseases using convolution neural network. *Microprocessors and Microsystems*, *76*. https://doi.org/10.1016/j.micpro.2020.103074

Shen, D., Wu, G., & Suk, H.-I. (2025). *Deep Learning in Medical Image Analysis*. *43*, 20. https://doi.org/10.1146/annurev-bioeng-071516

Shi, X., Peng, Y., Chen, Q., Keenan, T., Thavikulwat, A. T., Lee, S., Tang, Y., Chew, E. Y., Summers, R. M., & Lu, Z. (2022). Robust convolutional neural networks against adversarial attacks on medical images. *Pattern Recognition*, *132*. https://doi.org/10.1016/j.patcog.2022.108923

Shorten, C., & Khoshgoftaar, T. M. (2019). A survey on Image Data Augmentation for Deep Learning. *Journal of Big Data*, *6*(1). https://doi.org/10.1186/s40537-019-0197-0

Shvetsova, N., Bakker, B., Fedulova, I., Schulz, H., & Dylov, D. V. (2021). *Anomaly Detection in Medical Imaging with Deep Perceptual Autoencoders*. https://doi.org/10.1109/ACCESS.2021.3107163

Simonyan, K., & Zisserman, A. (2015). *Very Deep Convolutional Networks for Large-Scale Image Recognition*. http://arxiv.org/abs/1409.1556

Sirazitdinov, I., Kholiavchenko, M., Mustafaev, T., Yixuan, Y., Kuleev, R., & Ibragimov, B. (2019). Deep neural network ensemble for pneumonia localization from a large-scale chest x-ray database. *Computers and Electrical Engineering*, *78*, 388–399. https://doi.org/10.1016/j.compeleceng.2019.08.004

Smagulova, K., Bacha, L., Fouda, M. E., Kanj, R., & Eltawil, A. (2024). Robustness and Transferability of Adversarial Attacks on Different Image Classification Neural Networks. *Electronics (Switzerland)*, *13*(3). https://doi.org/10.3390/electronics13030592

Sokolova, M., & Lapalme, G. (2009). A systematic analysis of performance measures for classification tasks. *Information Processing and Management*, *45*(4), 427–437. https://doi.org/10.1016/j.ipm.2009.03.002

Srivastava, N., Hinton, G., Krizhevsky, A., & Salakhutdinov, R. (2014). Dropout: A Simple Way to Prevent Neural Networks from Overfitting. In *Journal of Machine Learning Research* (Vol. 15).

Su, J., Vargas, D. V., & Sakurai, K. (2019). One Pixel Attack for Fooling Deep Neural Networks. *IEEE Transactions on Evolutionary Computation*, *23*(5), 828–841. https://doi.org/10.1109/TEVC.2019.2890858

Tan, C. S. H., Chew, M. C. Y., Lim, L. W. Y., & Sadda, S. R. (2016). Advances in retinal imaging for diabetic retinopathy and diabetic macular edema. *Indian Journal of Ophthalmology*, *64*(1), 76–83. https://doi.org/10.4103/0301-4738.178145

Terven, J., Cordova-Esparza, D. M., Ramirez-Pedraza, A., Chavez-Urbiola, E. A., & Romero-Gonzalez, J. A. (2025). *Loss Functions and Metrics in Deep Learning*. https://doi.org/10.1007/s10462-025-11198-7

Terven, J., Cordova-Esparza, D. M., Romero-González, J. A., Ramírez-Pedraza, A., & Chávez-Urbiola, E. A. (2025). A comprehensive survey of loss functions and metrics in deep learning. *Artificial Intelligence Review*, *58*(7). https://doi.org/10.1007/s10462-025-11198-7

Tian, C., Fei, L., Zheng, W., Xu, Y., Zuo, W., & Lin, C. W. (2020). Deep learning on image denoising: An overview. In *Neural Networks* (Vol. 131, pp. 251–275). Elsevier Ltd. https://doi.org/10.1016/j.neunet.2020.07.025

Ullah, N., Khan, J. A., Khan, M. S., Khan, W., Hassan, I., Obayya, M., Negm, N., & Salama, A. S. (2022). An Effective Approach to Detect and Identify Brain Tumors Using Transfer Learning. *Applied Sciences (Switzerland)*, *12*(11). https://doi.org/10.3390/app12115645

Villegas-Ch, W., Jaramillo-Alcázar, A., & Luján-Mora, S. (2024). Evaluating the Robustness of Deep Learning Models against Adversarial Attacks: An Analysis with FGSM, PGD and CW. *Big Data and Cognitive Computing*, *8*(1). https://doi.org/10.3390/bdcc8010008

Vincent, P., Larochelle, H., Bengio, Y., & Manzagol, P.-A. (2008). *Extracting and Composing Robust Features with Denoising Autoencoders*.

Vyas, D., & Kapadia, V. V. (2024). Designing defensive techniques to handle adversarial attack on deep learning based model. *PeerJ Computer Science*, *10*. https://doi.org/10.7717/peerj-cs.1868

Wang, G., Liu, X., Li, C., Xu, Z., Ruan, J., Zhu, H., Meng, T., Li, K., Huang, N., & Zhang, S. (2020). A Noise-Robust Framework for Automatic Segmentation of COVID-19 Pneumonia Lesions from CT Images. *IEEE Transactions on Medical Imaging*, *39*(8), 2653–2663. https://doi.org/10.1109/TMI.2020.3000314

Wang, Q., Wu, B., Zhu, P., Li, P., Zuo, W., & Hu, Q. (2020). *ECA-Net: Efficient Channel Attention for Deep Convolutional Neural Networks*. http://arxiv.org/abs/1910.03151

Wang, Q., Yang, D., Li, Z., Zhang, X., & Liu, C. (2020). Deep regression via multi-channel multi-modal learning for pneumonia screening. *IEEE Access*, *8*, 78530–78541. https://doi.org/10.1109/ACCESS.2020.2990423

Wang, W., Wildgruber, M., & Wang, Y. (2024). Attacking medical images with minimal noise: exploiting vulnerabilities in medical deep-learning systems. *Quantitative Imaging in Medicine and Surgery*, *14*(12), 9374–9384. https://doi.org/10.21037/qims-24-1764

Woo, S., Park, J., Lee, J.-Y., & Kweon, I. S. (2018). *CBAM: Convolutional Block Attention Module*. http://arxiv.org/abs/1807.06521

Wu, D., Wang, Y., Xia, S.-T., Bailey, J., & Ma, X. (2020). *Skip Connections Matter: On the Transferability of Adversarial Examples Generated with ResNets*. http://arxiv.org/abs/2002.05990

Xie, C., Wu, Y., van der Maaten, L., Yuille, A., & He, K. (2019). *Feature Denoising for Improving Adversarial Robustness*. http://arxiv.org/abs/1812.03411

Xu, B., Wang, N., Chen, T., & Li, M. (2015). *Empirical Evaluation of Rectified Activations in Convolutional Network*. http://arxiv.org/abs/1505.00853

Yamashita, R., Nishio, M., Do, R. K. G., & Togashi, K. (2018). Convolutional neural networks: an overview and application in radiology. In *Insights into Imaging* (Vol. 9, Issue 4, pp. 611–629). Springer Verlag. https://doi.org/10.1007/s13244-018-0639-9

Yang, J., Li, Z., Liu, S., Hong, B., & Wang, W. (2023). Joint contrastive learning and frequency domain defense against adversarial examples. *Neural Computing and Applications*, *35*(25), 18623–18639. https://doi.org/10.1007/s00521-023-08688-6

Yani, M., Irawan, B., & Setiningsih, C. (2019). Application of Transfer Learning Using Convolutional Neural Network Method for Early Detection of Terry's Nail. *Journal of Physics: Conference Series*, *1201*(1). https://doi.org/10.1088/1742-6596/1201/1/012052

Zarie, M., Jahedsaravani, A., & Massinaei, M. (2020). Flotation froth image classification using convolutional neural networks. *Minerals Engineering*, *155*. https://doi.org/10.1016/j.mineng.2020.106443

Zhang, K., Zuo, W., Chen, Y., Meng, D., & Zhang, L. (2017). Beyond a Gaussian denoiser: Residual learning of deep CNN for image denoising. *IEEE Transactions on Image Processing*, *26*(7), 3142–3155. https://doi.org/10.1109/TIP.2017.2662206

Zhang, W., Jin, L., Song, E., & Xu, X. (2019). Removal of impulse noise in color images based on convolutional neural network. *Applied Soft Computing Journal*, *82*. https://doi.org/10.1016/j.asoc.2019.105558

Zhan, Y., Zheng, B., Liu, D., Deng, B., & Yang, X. (2025). Exploring black-box adversarial attacks on Interpretable Deep Learning Systems. *Computer Vision and Image Understanding*, *259*. https://doi.org/10.1016/j.cviu.2025.104423

Zhao, X., Wang, L., Zhang, Y., Han, X., Deveci, M., & Parmar, M. (2024). A review of convolutional neural networks in computer vision. *Artificial Intelligence Review*, *57*(4). https://doi.org/10.1007/s10462-024-10721-6

Zhong, C., Hu, J., Xie, M., & Fang, M. (2024). Efficient transfer attacks via enhancing perturbation robustness. *Metaverse*, *5*(2). https://doi.org/10.54517/m.v5i2.2764

Zhou, B., Khosla, A., Lapedriza, A., Oliva, A., & Torralba, A. (2016). Learning Deep Features for Discriminative Localization. *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, *2016-December*, 2921–2929. https://doi.org/10.1109/CVPR.2016.319

Zhou, T., Agrawal, S., & Manocha, P. (2022). *Optimizing One-pixel Black-box Adversarial Attacks*. http://arxiv.org/abs/2205.02116