REFERENCES

[1] Yue, Chang, et al, "Invisible Backdoor Attacks Using Data Poisoning in the Frequency Domain," arXiv preprint arXiv:2207.04209 2022

[2] Tianyu Gu, Kang Liu, Brendan Dolan-Gavitt, Siddharth Garg, "Badnets: Evaluating Backdooring Attacks on Deep Neural Networks," IEEE Access, 7:47230– 47244, 2019

[3] Xinyun Chen, Chang Liu, Bo Li, Kimberly Lu, Dawn Xiaodong Song, "Targeted backdoor attacks on deep learning systems using data poisoning," ArXiv, abs/1712.05526, 2017

[4] Wang, Yinggui, et al. 'Privacy-Preserving Face Recognition in the Frequency Domain," 2022

[5] Ji, Jiazhen, et al, "Privacy-Preserving Face Recognition with Learnable Privacy Budgets in Frequency Domain," arXiv preprint arXiv:2207.07316 2022

[6] Keiron O'Shea, Ryan Nash, "An Introduction to Convolutional Neural Networks," arXiv:1511.08458v2, 2015

[7] Siddharth Sharma, Simone Sharma, Anidhya Athaiya, "ACTIVATION FUNCTIONS IN NEURAL NETWORKS", International Journal of Engineering Applied Sciences and Technology, 2020 Vol. 4, Issue 12, ISSN No. 2455-2143, Pages 310-316

[8] Sergey Ioffe, Christian Szegedy, "Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift," arXiv:1502.03167, 2015

[9] Connor Shorten, Taghi M. Khoshgoftaar, "A survey on Image Data Augmentation for Deep Learning," Shorten and Khoshgoftaar J Big Data 2019

[10] Alexey Dosovitskiy, Lucas Beyer, Alexander Kolesnikov, Dirk Weissenborn, Xiaohua Zhai, Thomas Unterthiner, Mostafa Dehghani, Matthias Minderer, Georg Heigold, Sylvain Gelly, Jakob Uszkoreit, Neil Houlsby, "AN IMAGE IS WORTH 16X16 WORDS: TRANSFORMERS FOR IMAGE RECOGNITION AT SCALE," ICLR 2021

[11] Michal Podpora, Grzegorz Pawel Korbas, Aleksandra Kawala-Janik, " Yuv vs rgb-choosing a color space for human-machine interaction," FedCSIS, 2014

[12] Kai Xu, Minghai Qin, Fei Sun, Yuhao Wang, Yen kuang Chen, and Fengbo Ren, "Learning in the frequency domain," Conference on Computer Vision and Pattern Recognition (CVPR), pages 1737–1746, 2020

[13] Hongsheng Hu, Zoran Salcic, Lichao Sun, Gillian Dobbie, Philip S. Yu, Xuyun Zhang, "Membership Inference Attacks on Machine Learning: A Survey," arXiv:2103.07853, 2021

[14] Martín Abadi, Andy Chu, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Kunal Talwar, Li Zhang, "Deep Learning with Differential Privacy," arXiv:1607.00133 , 2016