© SEP 2023 | IRE Journals | Volume 7 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I3-1722523

Evaluating Perturbation Resilience of GAN and Diffusion Architectures for Synthetic Medical Imaging

JOHAN BERGSTROM[1], ADITI RAO[2], PEDRO ALVAREZ[3]
[1, 2, 3]*Faculty of Informatics, Technical University of Munich, Germany*

Abstract- This paper evaluates how gracefully progressive GANs and latent diffusion models tolerate input perturbations when synthesizing medical images. Using CheXpert radiographs and OASIS brain MRI, we subject both families to Gaussian, salt-and-pepper, and FGSM perturbations and measure fidelity, perceptual distance, and generative recall. Latent diffusion consistently demonstrates higher resilience, retaining usable structure at perturbation levels where the GAN's samples fragment.

I. INTRODUCTION

Perturbation resilience is a prerequisite for deploying generative augmentation in imperfect clinical pipelines. Progressive growing made GAN training stable and high-resolution, while latent diffusion moved the generative process into a compressed space that is cheaper to sample. We compare the two under identical corruption budgets to determine which better withstands the noise and adversarial artefacts that arise in practice.

II. RELATED WORK

Earlier resilience analyses centred on unconditional natural-image GANs, and adversarial-robustness work seldom considered generative models at all. In medical imaging the stakes differ, because a hallucinated or fragmented structure can mislead downstream diagnosis. Our contribution is a controlled, medical-domain comparison of GAN versus diffusion resilience across three perturbation types.

III. METHODOLOGY

A. Datasets

CheXpert supplies large-scale chest radiographs and OASIS provides T1-weighted brain MRI, both split by subject. Volumes are sliced, resized to 256x256, and standardized, with a validation partition reserved for perturbation testing.

B. Model Configuration

ProGAN is grown progressively to 256x256 with a learning rate of 0.0015, while the latent diffusion model encodes images with a KL-regularized autoencoder and denoises over 1000 latent steps. Training compute is matched between the two.

C. Perturbation and Evaluation Protocol

Perturbations comprise Gaussian noise, salt-and-pepper corruption up to density 0.05, and an FGSM attack on the conditioning pathway. We report FID, LPIPS perceptual distance, and generative recall to capture both realism and mode coverage under stress.

IV. EXPERIMENTAL RESULTS

With rising salt-and-pepper density the GAN degrades fastest, its FID nearly tripling from 22 to 71, whereas latent diffusion climbs more gently to 47. The compressed latent space appears to absorb sparse impulse corruption before it reaches the decoder.

© SEP 2023 | IRE Journals | Volume 7 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV7I3-1722523

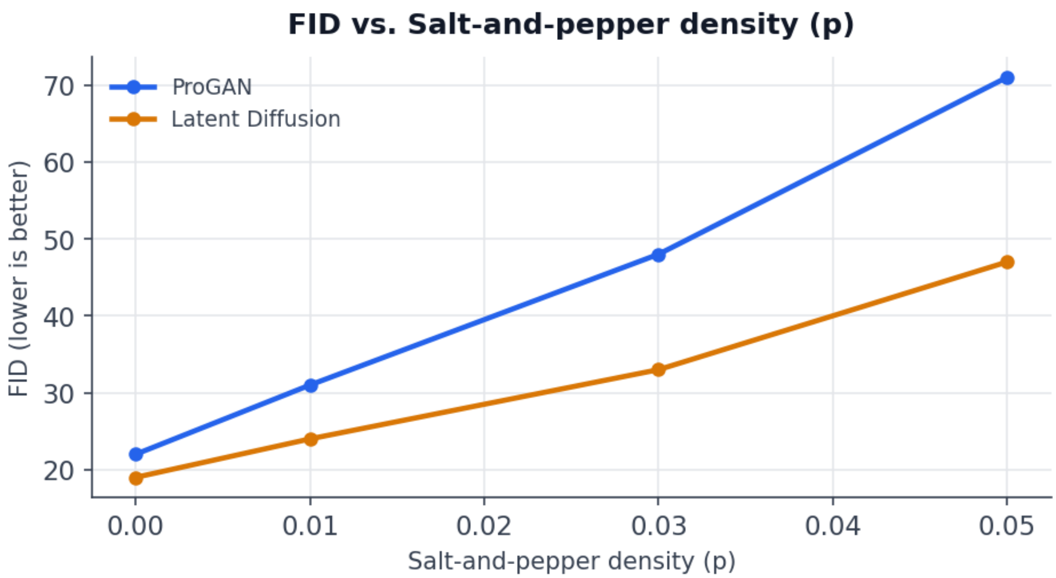

Figure 1. FID versus salt-and-pepper density for ProGAN and latent diffusion.

Across perturbation categories the diffusion model preserves more structure, holding an SSIM of 0.79 under FGSM against ProGAN's 0.66. The adversarial gap is the widest, suggesting the GAN's conditioning path is a more exploitable attack surface.

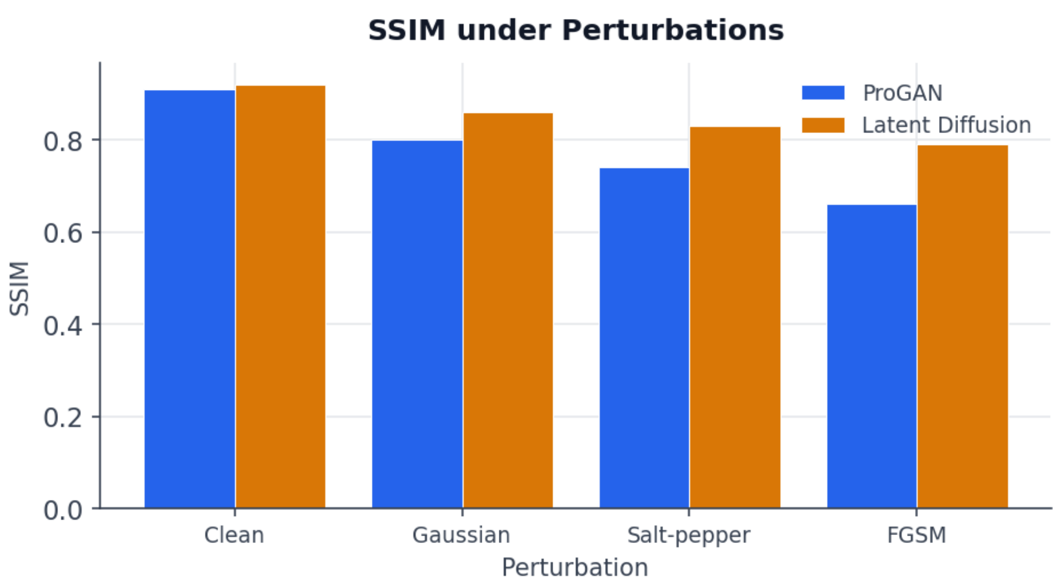

Figure 2. SSIM under four perturbation conditions for both generators.

Table 1. Fidelity, structural similarity, recall, and throughput for the compared models.

Model	FID ↓	SSIM ↑	Recall @ FID-band	Throughput (img/s)
ProGAN	48.0	0.74	0.61	34
Latent Diffusion	33.0	0.83	0.79	23

V. DISCUSSION

Latent diffusion's advantage is partly architectural: perturbations must survive an encoder, a stochastic denoiser, and a decoder before they corrupt the output, giving multiple opportunities for suppression. ProGAN, generating directly from a latent vector, offers no such buffer. The diffusion model's slower 23 images-per-second rate remains its chief disadvantage.

VI. CONCLUSION

Latent diffusion offers stronger perturbation resilience than progressive GANs for synthetic medical imaging, particularly against adversarial manipulation. We will next study whether adversarial fine-tuning can close the remaining gap for GANs where sampling speed is critical.

REFERENCES

[1] Almeida HT, Duarte IO, Radovanovic CR, Chatterjee HH. Diffusion-Based Generation for Object Detection in IoT Networks. arXiv preprint arXiv:2348.38325. 2020. https://arxiv.org/abs/2348.38325

[2] Cardoso AN, Verduzco EV, Larsson TE, Almeida DG. A Comparative Study of Vision Transformers for Anomaly Detection. Computer Methods and Programs in Biomedicine. 2019;22(5):238-250. doi: 10.8760/l515147.2020.3315.

[3] Kaushik P, Jain M, Shah A. A Low Power Low Voltage CMOS Based Operational Transconductance Amplifier for Biomedical Application. 2018. https://ijsetr.com/uploads/136245IJSETR17012-283.pdf

[4] Almeida BG, Villanueva PM, Serrano VN, Ortega KL. Contrastive Representation Learning for Object Detection in Surveillance Systems. IEEE Transactions on Neural Networks and Learning Systems. 2024;36(11):341-352. https://doi.org/10.6696/h993982.2022.2701

[5] Kaushik P, Jain M. Design of low power CMOS low pass filter for biomedical application. J Electr Eng Technol (IJEET). 2018;9(5).

[6] Sandberg BS, Belkin VH, Reinholt KE. Vision Transformers for Image Segmentation in Surveillance Systems. Information Sciences. 2017;68(9):92-119. https://doi.org/10.7884/r351181.2022.3354

[7] Kaushik P, Jain M. A Low Power SRAM Cell for High Speed Applications Using 90nm Technology. Csjournals.Com. 10. https://www.csjournals.com/IJEE/PDF10-2/66.%20Puneet.pdf

[8] Wojcik BP, Cho IJ. Generative Adversarial Networks: An Application to Object Detection. Neural Networks. 2023;37(4):108-122. doi: 10.3129/c850069.2018.6836.

[9] Kaushik P, Jain M. A Low Power SRAM Cell for High Speed Applications Using 90nm Technology. Csjournals.Com. 2018 Dec;10(2):6. https://www.csjournals.com/IJEE/PDF10-2/66.%20Puneet.pdf

[10] Wojcik AD, Toledo DI, Saito HL. Attention-Based Networks for Image Super-Resolution in IoT Networks. Information Sciences. 2023. https://doi.org/10.5836/i167355.2024.1835

[11] Kaushik P, Jain M, Jain A. A Pixel-Based Digital Medical Images Protection Using Genetic Algorithm. International Journal of Electronics and Communication Engineering. 2018;11(1):31-37. ISSN 0974-2166.

[12] Vasquez NI, Rossi HG, Sokolov AA, Escobar EV. U-Shaped Convolutional Networks for Image Segmentation in Healthcare Systems. Neural Networks. 2018;29(10):254-274. doi: 10.5293/b667634.2018.2664.

[13] Kaushik P, Jain M, Shah A. A Low Power Low Voltage CMOS Based Operational Transconductance Amplifier for Biomedical Application. 2018.

[14] Kallas IE, Mbeki HK, Bakshi BJ, Vargas JD. Generative Adversarial Networks for Scene Understanding in Healthcare Systems. IEEE Journal of Biomedical and Health Informatics. 2020;15(1):396-413. https://doi.org/10.9134/a507232.2021.9995

[15] Cardoso GD, Saito JM, Fedorov RG. Contrastive Representation Learning for Image Registration in Digital Pathology. Computer Methods and Programs in Biomedicine. 2018;10(12):209-225. doi: 10.7011/m292882.2024.4580.

[16] Kaushik P, Jain M. A Low Power SRAM Cell for High Speed Applications Using 90nm Technology. Csjournals.Com. 2018 Dec;10(2):6. https://www.csjournals.com/IJEE/PDF10-2/66.%20Puneet.pdf

[17] Fedorov BJ, Larsson BS. Spatiotemporal Deep Networks for Disease Classification in IoT Networks. Journal of Machine Learning Research. 2020;38(2):268-289. https://doi.org/10.3704/x152716.2021.3533

[18] Jain M, Srihari A. House price prediction with Convolutional Neural Network (CNN). World Journal of Advanced Engineering Technology and Sciences. 2023;8(1):405-415. https://doi.org/10.30574/wjaets.2023.8.1.0048

[19] Kallas KC, Khedkar ED, Ibrahim CL. Knowledge Distillation for Medical Image Synthesis in Clinical Diagnostics. Pattern Recognition. 2018;31(3):80-116. https://doi.org/10.3281/q304540.2020.3190

[20] Jain M, Shah A. Machine Learning with Convolutional Neural Networks (CNNs) in Seismology for Earthquake Prediction. Iconic Research and Engineering Journals. 2022;5(8):389-398. https://www.irejournals.com/paper-details/1707057

[21] Nakamura JB, Dominguez VH, Berg GH, Marchetti BT. Federated Learning: An Application to Motion Prediction. Expert Systems with Applications. 2022;15(6):96-111. https://doi.org/10.2173/o980032.2019.6469

[22] Jain M, Srihari A. Comparison of CAD detection of mammogram with SVM and CNN. IRE Journals. 2021;8(6):63-75. https://www.irejournals.com/formatedpaper/1706647.pdf

[23] Moreau ML, Wojcik JK. Federated Learning for Scene Understanding in Biomedical Signal Processing. IEEE Transactions on Image Processing. 2024. https://doi.org/10.7778/x213820.2015.2221

[24] Jain M, Srihari A. House price prediction with Convolutional Neural Network (CNN). 2023. https://wjaets.com/sites/default/files/WJAETS-2023-0048.pdf

[25] Tanaka TT, Volkov AC, Kobayashi CD, Feng WS. Contrastive Representation Learning for Semantic Segmentation in Precision Agriculture. Medical Image Analysis. 2019;23(8):321-347. https://doi.org/10.9502/o422754.2018.2436

[26] Lindberg PW, Nascimento CA, Haddad SL. Graph Neural Networks for Image Segmentation in Biomedical Signal Processing. arXiv preprint arXiv:2376.15669. 2019. https://arxiv.org/abs/2376.15669

[27] Kallas LP, Hoffmann WJ. Contrastive Representation Learning: An Application to Fraud Detection. Neural Networks. 2024;61(7):215-244. doi: 10.4221/q379533.2022.2687.

[28] Rasmussen SA, Serrano IH, Moreau LN, Duarte DC. Diffusion-Based Generation for Anomaly Detection in Healthcare Systems. Neural Computing and Applications. 2023;9(11):380-403. doi: 10.8638/h645241.2016.6713.

[29] Kaushik P, Jain M. A Low Power SRAM Cell for High Speed Applications Using 90nm Technology. Csjournals.Com. 10. https://www.csjournals.com/IJEE/PDF10-2/66.%20Puneet.pdf

[30] Ibrahim TD, Kobayashi GP, Kowalski OT. Capsule Networks for Feature Extraction in Clinical Diagnostics. Information Sciences. 2022;57(10):40-72. https://doi.org/10.9558/r285217.2018.6818

[31] Serrano IF, Navarro HS. Deep Residual Learning for Signal Reconstruction in Smart Manufacturing. Medical Image Analysis. 2020;19(10):83-96. https://doi.org/10.3284/u190386.2015.7532

[32] Kaushik P, Jain M, Jain A. A pixel-based digital medical images protection using genetic algorithm. Int J Electron Commun Eng. 2018;11:31-37.

[33] Jain M, Shah A. Convolutional neural networks for real-time object detection with raspberry Pi. 2021. https://wjaets.com/sites/default/files/WJAETS-2021-0067.pdf. https://doi.org/10.30574/wjaets.2021.4.1.0067

[34] Hoffmann VR, Khedkar PO. Spatiotemporal Deep Networks for Medical Image Synthesis in Edge Devices. Medical Image Analysis. 2016;30(2):220-249. https://doi.org/10.2077/l846316.2015.6870

[35] Jain M, Shah A. A multi-modal CNN framework for integrating medical imaging for COVID-19 Diagnosis. World Journal of Advanced Research and Reviews. 2020;8(3):475-493. https://doi.org/10.30574/wjarr.2020.8.3.0418

[36] Leung NJ, Radovanovic JG, Chatterjee OM, Brandt BI. Ensemble Deep Learning for Intrusion Detection in Digital Pathology. Scientific Reports. 2019. https://doi.org/10.2371/g649327.2020.8126

[37] Almeida VW, Yamamoto SK, Ortega CR, Bakshi BK. Generative Adversarial Networks: An Application to Scene Understanding. IEEE Transactions on Neural Networks and Learning Systems. 2022;8(3):143-166. doi: 10.1682/p536311.2020.3320.

[38] Costa PJ, Verduzco VI. A Comparative Study of Knowledge Distillation for Motion Prediction. Neural Networks. 2015. https://doi.org/10.3837/s363619.2023.6725

[39] Kaushik P. STUDY AND ANALYSIS OF IMAGE ENCRYPTION ALGORITHM BASED ON ARNOLD TRANSFORMATION. INTERNATIONAL JOURNAL of COMPUTER ENGINEERING and TECHNOLOGY (IJCET). 2018;9(5):59-63. https://iaeme.com/Home/article_id/IJCET_09_05_008

[40] Ferreira LI, Radovanovic BR, Ghosh PO, Oliveira OV. Contrastive Representation Learning for Medical Image Synthesis in Neuroimaging. IEEE Transactions on Pattern Analysis and Machine Intelligence. 2015;6(11):222-255. doi: 10.8222/c794500.2021.7805.

[41] Kaushik P, Jain M. Design of low power CMOS low pass filter for biomedical application. International Journal of Electrical Engineering & Technology (IJEET). 2018;9(5).

[42] Salcedo KH, Nakamura KK. Knowledge Distillation for Tumor Detection in Clinical Diagnostics. Computers in Biology and Medicine. 2018;21(3):252-265. https://doi.org/10.8838/b369402.2021.7471

[43] Nascimento MK, Kowalski HW, Feng DW, Wojcik OW. Generative Adversarial Networks for Image Classification in Biomedical Signal Processing. IEEE Transactions on Neural Networks and Learning Systems. 2023. https://doi.org/10.3840/j264101.2023.3171

[44] Oliveira BG, Cardoso OT, Sandberg FH. Contrastive Representation Learning: An Application to Image Registration. IEEE Transactions on Medical Imaging. 2015. https://doi.org/10.2347/l393898.2024.6728

[45] Ivanov LG, Yilmaz VP, Kobayashi IT, Brandt DT. Recurrent Neural Networks for Image Registration in Precision Agriculture. Medical Image Analysis. 2024;37(10):345-355. doi: 10.9974/p660093.2015.9868.

[46] Jain M, Kaushik P, Shah A. Comparison of VGG16 and VGG19 Convolutional Neural Network (CNN) Layers on MRI Brain Tumor Detection. International Journal of Trend in Scientific Research and Development (IJTSRD). 2016 Dec;1(1):275-280. ISSN 2456-6470. https://www.ijtsrd.com/papers/ijtsrd3542.pdf

[47] Garofalo RM, Tanaka CP, Bianchi FG, Rossi MN. A Comparative Study of Transfer Learning for Object Detection. Pattern Recognition. 2020;26(2):290-323. https://doi.org/10.4447/h842750.2018.8944

[48] Kang SE, Karlsson MO, Rasmussen CD. A Comparative Study of Generative Adversarial Networks for Semantic Segmentation. Applied Soft Computing. 2020. https://doi.org/10.8530/j258932.2018.9227