SciFetch Report

Generated on: 2025-06-28 22:48 UTC

Request: Applications of federated learning in privacy-preserving medical image analysis

Summary

Federated learning (FL) has emerged as a transformative approach in privacy-preserving medical image analysis, addressing the critical need for data privacy and security in healthcare. This decentralized learning paradigm allows for the training of machine learning models across multiple institutions without the need to share sensitive patient data, thereby complying with data protection regulations. 1. **"Federated Learning Framework for Brain Tumor Detection Using MRI Images in Non-IID Data Distributions"**: This paper highlights the application of FL in brain tumor detection using MRI images. It addresses the challenges posed by non-independent and identically distributed (non-IID) data, which is common in medical datasets. The study demonstrates how FL can facilitate collaborative model training across decentralized devices while maintaining data privacy, thus overcoming the limitations of traditional centralized approaches. 2. **"Assessing the Impact of Federated Learning and Differential Privacy on Multi-centre Polyp Segmentation"**: This research explores the integration of differential privacy with FL to enhance privacy-preserving capabilities in medical image analysis. By focusing on multi-centre polyp segmentation, the paper underscores the importance of protecting patient identity during the central aggregation process, which remains a vulnerability in FL systems. 3. **"Federated Brain Tumor Segmentation: An

Extensive Benchmark"**: This paper provides a comprehensive benchmark for federated learning in brain tumor segmentation, categorizing various federated training schemes into global, personalized, and hybrid methods. It evaluates their applicability on the Federated Brain Tumor Segmentation 2022 dataset, offering insights into the effectiveness of different FL strategies in aggregating multi-center data while preserving privacy. 4. **"Privacy-Preserving Breast Cancer Classification: A Federated Transfer Learning Approach"**: The study presents a federated transfer learning approach for breast cancer classification, addressing the challenges of data privacy and data silos in the medical domain. By leveraging federated learning, the paper demonstrates how early and accurate detection of breast cancer can be achieved without compromising patient privacy. 5. **"A Comparative Study of Federated Learning Methods for COVID-19 Detection"**: This paper examines various federated learning methods for COVID-19 detection, highlighting the efficacy of FL in enabling model training across multiple hospitals while preserving data privacy. It discusses the resource-intensive nature of FL deployment and the need for robust models that can operate effectively under privacy constraints. These papers collectively illustrate the potential of federated learning in revolutionizing medical image analysis by enabling privacy-preserving, decentralized model training across diverse healthcare institutions. They address key challenges such as data heterogeneity, privacy leakage, and the need for robust and scalable solutions in the medical imaging field.

Relevant Articles

1. Whole-Body Conditioned Egocentric Video Prediction

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21552v1

Abstract: We train models to Predict Ego-centric Video from human Actions (PEVA), given the past video and an action represented by the relative 3D body pose. By conditioning on kinematic pose trajectories, structured by the joint hierarchy of the body, our model learns to simulate how physical human actions shape the environment from a first-person point of view. We train an auto-regressive conditional diffusion transformer on Nymeria, a large-scale dataset of real-world egocentric video and body pose ca...

2. mTSBench: Benchmarking Multivariate Time Series Anomaly Detection and Model Selection at Scale

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21550v1

Abstract: Multivariate time series anomaly detection (MTS-AD) is critical in domains like healthcare, cybersecurity, and industrial monitoring, yet remains challenging due to

complex inter-variable dependencies, temporal dynamics, and sparse anomaly labels. We introduce mTSBench, the largest benchmark to date for MTS-AD and unsupervised model selection, spanning 344 labeled time series across 19 datasets and 12 diverse application domains. mTSBench evaluates 24 anomaly detection methods, including large l...

3. Where to find Grokking in LLM Pretraining? Monitor Memorization-to-Generalization without Test

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21551v1

Abstract: Grokking, i.e., test performance keeps improving long after training loss converged, has been recently witnessed in neural network training, making the mechanism of generalization and other emerging capabilities such as reasoning mysterious. While prior studies usually train small models on a few toy or highly-specific tasks for thousands of epochs, we conduct the first study of grokking on checkpoints during one-pass pretraining of a 7B large language model (LLM), i.e., OLMoE. We compute the tr...

4. SiM3D: Single-instance Multiview Multimodal and Multisetup 3D Anomaly Detection Benchmark

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21549v1

Abstract: We propose SiM3D, the first benchmark considering the integration of multiview and multimodal information for comprehensive 3D anomaly detection and segmentation (ADS), where the task is to produce a voxel-based Anomaly Volume. Moreover, SiM3D focuses on a scenario of high interest in manufacturing: single-instance anomaly detection, where only one object, either real or synthetic, is available for training. In this respect, SiM3D stands out as the first ADS benchmark that addresses the challeng...

5. HalluSegBench: Counterfactual Visual Reasoning for Segmentation Hallucination Evaluation

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21546v1

Abstract: Recent progress in vision-language segmentation has significantly advanced grounded visual understanding. However, these models often exhibit hallucinations by

producing segmentation masks for objects not grounded in the image content or by incorrectly labeling irrelevant regions. Existing evaluation protocols for segmentation hallucination primarily focus on label or textual hallucinations without manipulating the visual context, limiting their capacity to diagnose critical failures. In respons...

6. DeOcc-1-to-3: 3D De-Occlusion from a Single Image via Self-Supervised Multi-View Diffusion

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21544v1

Abstract: Reconstructing 3D objects from a single image is a long-standing challenge, especially under real-world occlusions. While recent diffusion-based view synthesis models can generate consistent novel views from a single RGB image, they generally assume fully visible inputs and fail when parts of the object are occluded. This leads to inconsistent views and degraded 3D reconstruction quality. To overcome this limitation, we propose an end-to-end framework for occlusion-aware multi-view generation. O...

7. StruMamba3D: Exploring Structural Mamba for Self-supervised Point Cloud Representation Learning

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21541v1

Abstract: Recently, Mamba-based methods have demonstrated impressive performance in point cloud representation learning by leveraging State Space Model (SSM) with the efficient context modeling ability and linear complexity. However, these methods still face two key issues that limit the potential of SSM: Destroying the adjacency of 3D points during SSM processing and failing to retain long-sequence memory as the input length increases in downstream tasks. To address these issues, we propose StruMamba3D, ...

8. WorldVLA: Towards Autoregressive Action World Model

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21539v1

Abstract: We present WorldVLA, an autoregressive action world model that unifies action and image understanding and generation. Our WorldVLA intergrates Vision-Language-Action (VLA) model and world model in one

single framework. The world model predicts future images by leveraging both action and image understanding, with the purpose of learning the underlying physics of the environment to improve action generation. Meanwhile, the action model generates the subsequent actions based on image observations, ...

9. Maximal Matching Matters: Preventing Representation Collapse for Robust Cross-Modal Retrieval

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21538v1

Abstract: Cross-modal image-text retrieval is challenging because of the diverse possible associations between content from different modalities. Traditional methods learn a single-vector embedding to represent semantics of each sample, but struggle to capture nuanced and diverse relationships that can exist across modalities. Set-based approaches, which represent each sample with multiple embeddings, offer a promising alternative, as they can capture richer and more diverse relationships. In this paper, ...

10. ResQ: A Novel Framework to Implement Residual Neural Networks on Analog Rydberg Atom Quantum Computers

Date: 2025-06-26

Source: arXiv

URL: http://arxiv.org/abs/2506.21537v1

Abstract: Research in quantum machine learning has recently proliferated due to the potential of quantum computing to accelerate machine learning. An area of machine learning that has not yet been explored is neural ordinary differential equation (neural ODE) based residual neural networks (ResNets), which aim to improve the effectiveness of neural networks using the principles of ordinary differential equations. In this work, we present our insights about why analog Rydberg atom quantum computers are esp...

11. Shadow defense against gradient inversion attack in federated learning.

Date: 2025-06-21

Source: PubMed

DOI: 10.1016/j.media.2025.103673

URL: https://pubmed.ncbi.nlm.nih.gov/40570807

Abstract: Federated learning (FL) has emerged as a transformative framework for privacy-preserving distributed training, allowing clients to collaboratively train

a global model without sharing their local data. This is especially crucial in sensitive fields like healthcare, where protecting patient data is paramount. However, privacy leakage remains a critical challenge, as the communication of model updates can be exploited by potential adversaries. Gradient inversion attacks (GIAs), for instance, allow...

12. Federated Learning Framework for Brain Tumor Detection Using MRI Images in Non-IID Data Distributions.

Date: 2025-03-24

Source: PubMed

DOI: 10.1007/s10278-025-01484-9

URL: https://pubmed.ncbi.nlm.nih.gov/40128502

Abstract: Brain tumor detection from medical images, especially magnetic resonance imaging (MRI) scans, is a critical task in early diagnosis and treatment planning. Traditional machine learning approaches often rely on centralized data, raising concerns about data privacy, security, and the difficulty of obtaining large annotated datasets. Federated learning (FL) has emerged as a promising solution for training models across decentralized devices while maintaining data privacy. However, challenges remain...

13. Assessing the Impact of Federated Learning and Differential Privacy on Multi-centre Polyp Segmentation.

Date: 2025-05-01

Source: PubMed

DOI: 10.1109/EMBC53108.2024.10782682

URL: https://pubmed.ncbi.nlm.nih.gov/40039412

Abstract: Federated Learning (FL) is emerging in the medical field to address the need for diverse datasets while complying with data protection regulations. This decentralised learning paradigm allows hospitals (clients) to train machine learning models locally, ensuring that patient data remains within the confines of its originating institution. Nonetheless, FL by itself is not enough to guarantee privacy, as the central aggregation process may still be susceptible to identity-exposing attacks, potenti...

14. DEeR: Deviation Eliminating and Noise Regulating for Privacy-Preserving Federated Low-Rank Adaptation.

Date: 2025-04-03

Source: PubMed

DOI: 10.1109/TMI.2024.3518539

URL: https://pubmed.ncbi.nlm.nih.gov/40030741

Abstract: Integrating low-rank adaptation (LoRA) with federated learning (FL) has received widespread attention recently, aiming to adapt pretrained foundation models (FMs) to downstream medical tasks via privacy-preserving decentralized training. However, owing to the direct combination of LoRA and FL, current methods generally undergo two problems, i.e., aggregation deviation, and differential privacy (DP) noise amplification effect. To address these problems, we propose a novel privacy-preserving feder...

15. Federated brain tumor segmentation: An extensive benchmark.

Date: 2024-07-14

Source: PubMed

DOI: 10.1016/j.media.2024.103270

URL: https://pubmed.ncbi.nlm.nih.gov/39059241

Abstract: Recently, federated learning has raised increasing interest in the medical image analysis field due to its ability to aggregate multi-center data with privacy-preserving properties. A large amount of federated training schemes have been published, which we categorize into global (one final model), personalized (one model per institution) or hybrid (one model per cluster of institutions) methods. However, their applicability on the recently published Federated Brain Tumor Segmentation 2022 datase...

16. Integrated approach of federated learning with transfer learning for classification and diagnosis of brain tumor.

Date: 2024-05-15

Source: PubMed

DOI: 10.1186/s12880-024-01261-0

URL: https://pubmed.ncbi.nlm.nih.gov/38750436

Abstract: Brain tumor classification using MRI images is a crucial yet challenging task in medical imaging. Accurate diagnosis is vital for effective treatment planning but is often hindered by the complex nature of tumor morphology and variations in imaging. Traditional methodologies primarily rely on manual interpretation of MRI images, supplemented by conventional machine learning techniques. These approaches often lack the robustness and scalability needed for precise and automated tumor classificatio...

17. Privacy-Preserving Breast Cancer Classification: A Federated Transfer Learning Approach.

Date: 2024-02-29

Source: PubMed

DOI: 10.1007/s10278-024-01035-8

URL: https://pubmed.ncbi.nlm.nih.gov/38424280

Abstract: Breast cancer is deadly cancer causing a considerable number of fatalities among women in worldwide. To enhance patient outcomes as well as survival rates, early and accurate detection is crucial. Machine learning techniques, particularly deep learning, have demonstrated impressive success in various image recognition tasks, including breast cancer classification. However, the reliance on large labeled datasets poses challenges in the medical domain due to privacy issues and data silos. This stu...

18. A comparative study of federated learning methods for COVID-19 detection.

Date: 2024-02-16

Source: PubMed

DOI: 10.1038/s41598-024-54323-2

URL: https://pubmed.ncbi.nlm.nih.gov/38365940

Abstract: Deep learning has proven to be highly effective in diagnosing COVID-19; however, its efficacy is contingent upon the availability of extensive data for model training. The data sharing among hospitals, which is crucial for training robust models, is often restricted by privacy regulations. Federated learning (FL) emerges as a solution by enabling model training across multiple hospitals while preserving data privacy. However, the deployment of FL can be resource-intensive, necessitating efficien...

19. Federated Learning for Decentralized Artificial Intelligence in Melanoma Diagnostics.

Date: 2024-03-01

Source: PubMed

DOI: 10.1001/jamadermatol.2023.5550

URL: https://pubmed.ncbi.nlm.nih.gov/38324293

Abstract: The development of artificial intelligence (AI)-based melanoma classifiers typically calls for large, centralized datasets, requiring hospitals to give away their patient data, which raises serious privacy concerns. To address this concern, decentralized federated learning has been proposed, where classifier development is distributed across hospitals....

20. Personalized and privacy-preserving federated heterogeneous medical image analysis with PPPML-HMI.

Date: 2023-12-19

Source: PubMed

DOI: 10.1016/j.compbiomed.2023.107861

URL: https://pubmed.ncbi.nlm.nih.gov/38141449

Abstract: Heterogeneous data is endemic due to the use of diverse models and settings of devices by hospitals in the field of medical imaging. However, there are few open-

source frameworks for federated heterogeneous medical image analysis with personalization and privacy protection without the demand to modify the existing model structures or to share any private data. Here, we proposed PPPML-HMI, a novel open-source learning paradigm for personalized and privacy-preserving federated heterogeneous medica...

Developed by: Íñigo Rodríguez, AI & Data Engineer

GitHub: @irdsn

Powered by LangChain, FastAPI, Python & Next.js · Using OpenAI Models.

Integrated with APIs from arXiv, CrossRef, EuropePMC, OpenAlex and PubMed.

For more information, visit the project repository here.