stable learning and good results when using sequential learning, where one client is trained first and then the other. However, by using federated learning methods, we were able to achieve the same metric values as in the case of balanced data. This is primarily because, during aggregation, the global model aims to acquire knowledge from all clients and average them.

Each of the client models learned to predict the classes present in its own dataset very well. However, when it comes to predicting classes that were rarely encountered before, the client models struggle on the test data. Nonetheless, the central model aggregated information from all the data, which can potentially improve its ability to predict such classes.

Thus, federated learning methods enable us to mitigate the impact of data heterogeneity when training models.

In the figure 10 is shown the graph of accuracy for heterogeneous data

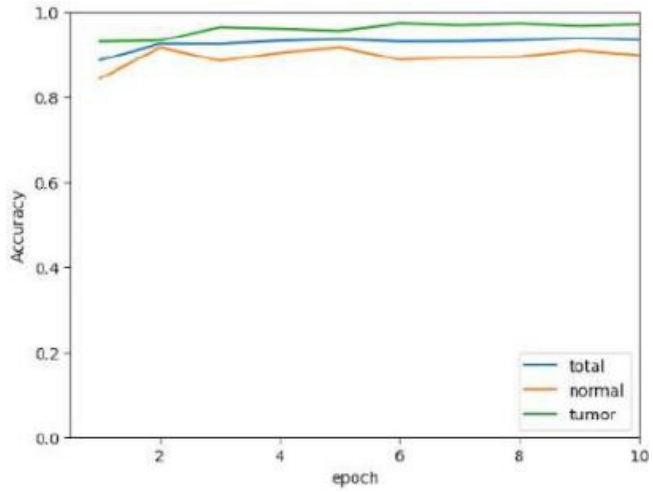

Figure 10: Graph of accuracy for heterogeneous data.

VI. Semantic technologies application

In addition to the above applications, you can use semantic technologies in federated learning. For example as follows.

- Distributed knowledge representation: Semantic technologies enable the representation of knowledge in a structured manner using formal languages. This can be useful in distributed model training, where each device can have its local knowledge representation and then combine these representations on a central server
- Semantic data analysis: Semantic technologies can assist in the analysis and understanding of data collected from distributed devices. For example, they can be used to extract meaning and relationships between data, which can be beneficial for aggregation and merging of models on a central server.
- Unification of semantic understanding: Semantic technologies can help unify the understanding of data across different devices or servers. They can be used to create a shared model of knowledge or a semantic network, which can be utilized for harmonizing and collaboratively training models on different devices.

VII. Conclusion

In this article, the main problems arising in the task of biomedical image analysis were described, and a method to avoid them was proposed. Furthermore, experiments were conducted to demonstrate its practical applicability. Has been shown that federated learning helps preserve data confidentiality and also provides a significant improvement in quality when different clients have data from different classes. Various approaches to solving the problem of heterogeneous learning have been considered. The obtained conclusions and recommendations can be valuable for researchers in the field of biomedical informatics and medicine who aim to utilize advanced machine learning methods for image analysis in privacypreserving conditions.

Acknowledgment

This research was supported by the United Institute of Informatics Problems of the National Academy of Sciences of Belarus (UIIP NASB).

References

[1] H. Brendan McMahan, E. Moore, D. Ramage, S.Hampson, B. Agüera y Arcas, "Communication-efficient learning of deep networks from decentralized data," Artificial Intelligence and Statistics, 1273–1282 (2017).

[2] P. Qi, D. Chiaro, A. Guzzo, M. Ianni, G. Fortino, F. Piccialli "Model aggregation techniques in federated learning: A comprehensive survey". Future Generation Computer System, 150, 272- 293 (2023).

[3] Federated Learning for Mobile Keyboard Prediction, McMahan, Brendan, et al., 2017.

[4] EU. Regulation (eu) 2016/679 of the european parliament and of the council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). https://eur-lex.europa.eu/legal-content/EN/TXT., 2018.

[5] Brendan McMahan, Eider Moore, Daniel Ramage, Seth Hampson, and Blaise Agüera y Arcas. Communicationefficient learning of deep networks from decentralized data. In Aarti Singh and Xiaojin (Jerry) Zhu, editors, Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, AISTATS 2017, 20-22 April 2017, Fort Lauderdale, FL, USA, volume 54 of Proceedings of Machine Learning Research, pp. 1273–1282. PMLR, 2017.

[6] Kairouz Peter, McMahan H Brendan, Avent Brendan, Bellet Aurélien, Bennis Mehdi, Bhagoji Arjun Nitin, Bonawitz Keith, Charles Zachary, Cormode Graham, Cummings Rachel, et al. Advances and open problems in federated learning. arXiv preprint arXiv:1912.04977, 2019.

[7] Hard Andrew, Rao Kanishka, Mathews Rajiv, Ramaswamy Swaroop, Beaufays Françoise, Augenstein Sean, Eichner Hubert, Kiddon Chloé, and Ramage Daniel. Federated learning for mobile keyboard prediction. arXiv preprint arXiv:1811.03604, 2018.

[8] Jin Yilun, Wei Xiguang, Liu Yang, and Yang Qiang. A survey towards federated semi-supervised learning. arXiv preprint arXiv:2002.11545, 2020.

[9] Tian Li, Anit Kumar Sahu, Ameet Talwalkar, and Virginia Smith. Federated learning: Challenges, methods, and future directions. IEEE Signal Process. Mag., 37(3):50–60, 2020.

[10] Zengpeng Li, Vishal Sharma, and Saraju P. Mohanty. Preserving data privacy via federated learning: Challenges and solutions. IEEE Consumer Electronics Magazine, 9(3):8–16, 2020.

ПРОБЛЕМЫ КОНФИДЕНЦИАЛЬНОСТИ И НЕОДНОРОДНОСТИ ПРИЛОЖЕНИЙ ФЕДЕРАТИВНОГО ОБУЧЕНИЯ ПРИ АНАЛИЗЕ МЕДИЦИНСКИХ ИЗОБРАЖЕНИЙ

Гимбицкий А. В., Зеленковский В. П.,
Жидович М. С., Ковалёв В. А.

В последнее время машинное обучение стало одним из самых многообещающих направлений в работе с медицинскими данными. Модели глубоких нейронных сетей являются наиболее эффективными и точными, но требуют больших объемов информации для обучения. Это общая проблема в случае медицинских данных, особенно изображений, так как их создание включает значительные затраты. Одним из решений для повышения качества моделей глубокого обучения без увеличения обучающего набора данных является агрегация моделей. Однако возникает проблема сохранения конфиденциальности медицинских изображений. Например, если одна модель обучается на изображении, содержащем информацию о конкретном пациенте, другие модели, участвующие в агрегации, также могут получить доступ к этой информации. В результате информация о конкретном пациенте может быть раскрыта.

В попытке решить описанную выше проблему, данная работа направлена на исследование и разработку методов агрегации моделей машинного обучения с сохранением конфиденциальности медицинских изображений, в особенности методов федеративного обучения.

Received 13.03.2024

Evaluation Metrics and Multi-level GAN Approach for Medical Images

Galina Kovbasa
Belarusian State University of Informatics and Radioelectronics
Minsk, Belarus
g.kovbasa@gmail.com

***Abstract*—This article examined methods for using GANs in medicine, their prospects, as well as problems with training generative adversarial networks associated with the increasing use of generated images for training other networks. The analysis of single-layer and multi-layer GANs concluded that although multi-layer GANs perform better statistically, they do not exactly match the distribution of the original dataset and, without medical supervision, such synthetic data should not be used when training new networks. Problems associated with the phenomenon of recursive learning, biased assessments of image realism, and non-optimized structures are considered. Approach is described in context of integrating generative adversarial network models into the OSTIS Technology based hybrid computer systems.**

***Keywords*—Multi-level GANs, recursive learning, synthetic data**

I. Introduction

Generative adversarial networks (GANs) are a remarkably popular technique for generating realistic synthetic data. Modern GANs can have different layers, backgrounds , complexity and be trained by semi-supervised and unsupervised learning. They gain their popularity because of the ability to implicitly modeling highdimensional data distributions. [1] GANs are of particular interest in the processing, classification and evaluation of medical images, in the future making it possible to speed up and improve the analysis of the results of magnetic resonance imaging, computed tomography, Xrays and others. This can be solved by integrating a GAN neural networks into the OSTIS Technology. [2]

Integration with third-party technologies based on neural networks allows the development of universal hybrid systems. GANs are capable of not only processing images, but also creating new synthetic data on demand, which makes them valuable for creating datasets, anonymous educational materials, etc. GANs are actively changing during development and all these changes can be formalized in the OSTIS system using SC code. [3]

Thus, network artifacts of the processes of creation, training and further tuning, such as numbers and types of layers, weights, activation functions, can be stored in a general form and saved, supporting further replenishment and expansion of the general knowledge base. [4] The OSTIS intelligent system is also capable of saving several versions of the same model for later use, even restoration from a previous point. [5]

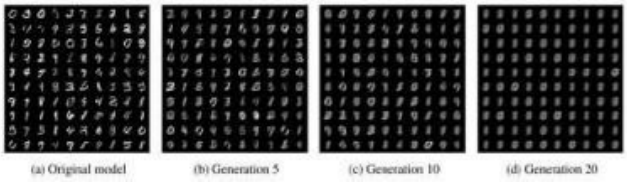

Figure 1. Model collapsing. Over generations, the generated data begins to look unimodal.

But one of the worst challenges facing GANs in medicine is that medical images are susceptible to various noise and artifacts common to different modalities and, what most important is, have a very little variety of datasets to be used. It should also be noted that much medical information is 3D structures, which can make it difficult to train a GAN on only 2D images.

A. The recursive learning problem

No generative adversarial network can reliably recreate the distribution of the original sample data. It may make mistakes or recreate the same data, that is, clone it. We must train the network so that it does not go beyond the distribution, but also does not repeat the picture. This solution allows us to avoid modern problems with GAN.

Generative adversarial networks are able to generate high-quality images on demand using the same distribution that is given, the score is also high. However, this does not mean that GAN can be used as a universal method or classifier, since it is impossible to assume that the distribution will be reliable or true. Likewise, the images produced by networks cannot be considered representative for training other networks.

However, more and more people are using GANs for reconstruction and generation, but this only leads to the fact that it can be used for a training set, since the generated materials are in the public domain. As a result, the networks degenerate, and the results of reconstruction and generation deteriorate. And as a result, the so-called mode collapse occurs (Fig. 1). [6]

This phenomenon (using generated images as training materials) is most dangerous for image generation,