Journal of Computer Technology and Applied Mathematics
Vol. 1, No. 1, 2024

Enhancing Federated Semi-Supervised Learning with Out-of-Distribution Filtering Amidst Class Mismatches

JIN, Jiajun [1*] NI, Fanghao [2] DAI, Shuying [3] LI, Keqin [4] HONG, Bo [2]

[1] University of Maine at Presque Isle, USA
[2] Northern Arizona University, USA
[3] Indian Institute of Technology Guwahati, India
[4] AMA University, Philippines

**** JIN, Jiajun is the corresponding author, E-mail: naifenall@outlook.com***

Abstract: Federated Learning (FL) has gained prominence as a method for training models on edge computing devices, enabling the preservation of data privacy by eliminating the need to share sensitive informa- tion. While the majority of FL approaches have been developed with a focus on supervised learning, a limited number of studies have explored the incorporation of unlabeled data. These studies typically operate under the assumption that labeled and unlabeled data share identical class distributions. However, in practical scenarios, where unlabeled data may include classes absent from the labeled dataset, the performance of existing methodologies can significantly decline. This paper delves into federated semi-supervised learning amidst discrepancies between the classes of labeled and unlabeled data. We introduce an innovative FL framework designed to alleviate the adverse effects of class mismatches. Our framework features a pioneering historic global ensemble consistency loss and a server-based adjustment mechanism for out-of-distribution (OOD) filtering, effectively enhancing model performance in the presence of class mismatches.

Keywords: Federated Learning, Semi-Supervised Learning, Class Mismatch.

DOI: https://doi.org/10.5281/zenodo.11068390

1 Introduction

Machine Learning has been a hot topic over the past years. [35, 70-76] With the advancement of technology [17–19, 32], mobile devices have ascended as paramount computing assets, amassing a wealth of data invaluable for the training of machine learning models. Given the concerns around privacy and security, conventional distributed machine learning methodologies have become obsolete. Federated Learning (FL), which advocates for local training on clients and global aggregation on servers without the exchange of data, has validated its practicality and effectiveness across both Independent and Identically Distributed (IID) and Non-IID settings [1, 3, 4]. Predominantly, current FL frameworks concentrate on supervised scenarios, necessitating fully labeled data. However, due to FL's inherent privacy constraints, the complete labeling of data by clients is unattainable. Thus, the exploration of federated semi-supervised learning frameworks that exploit unlabeled data has emerged as a novel focal point.

As the initiative to incorporate unlabeled data into federated learning gains momentum [7], a handful of federated semi-supervised learning (FSSL) strategies have embarked on this endeavor by melding semi-supervised learning methodologies with the FL framework. Notably, the semi-supervised federated learning approach for activity recognition [6, 45] employs an autoencoder to extract features from unlabeled data, integrating it into the supervised learning workflow [20, 36]. In contrast, FedMatch [2] advances the amalgamation of federated learning with semi-supervised learning by introducing an innovative inter-client consistency loss and the bifurcation of parameters for distinct learning processes on labeled and unlabeled data. [22]

While these approaches augment accuracy beyond mere combinations of FL and semi-supervised learning, their efficacy presumes identical class distributions in labeled and unlabeled data [23,31, 50-52]—an assumption not always aligned with reality. Considering the predominance of personal mobile devices among FL participants, evading class disparities between labeled and unlabeled data presents a formidable challenge, underscoring the necessity for an efficacious FSSL framework tailored to class mismatch scenarios. [43]

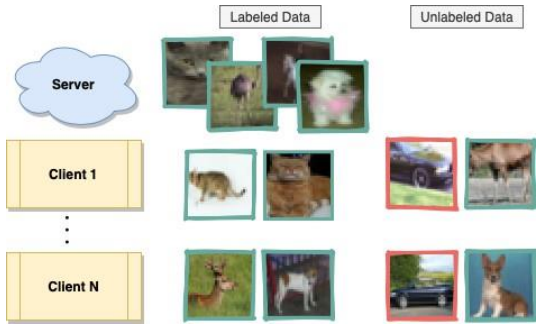

Figure 1: Illustration of a more realistic FSSL setting. Server has some representative labeled data with K classes. Each client has both labeled data and unlabeled data. The classes of client labeled data is a subset of K, while unlabeled data contains classes are not seen in K.s

In the realm of class mismatches within semi-supervised learning, DSSSL [9] and UASD [8] epitomize state-of-the-art methodologies. DSSSL [9] harnesses a shallow neural network for the calibration of unsupervised loss weights and parameter estimation through bi-level optimization, predicated on a cleanly labeled dataset. Conversely, UASD [8] pioneers an accumulative ensemble technique to sift through potentially irrelevant samples and refine soft target predictions. The straightforward adoption of these sophisticated SSL methods on clients to update local weights, followed by the aggregation of these weights on the server using federated algorithms, presents as a naive notion within the FL paradigm. [48, 53] Nevertheless, the intrinsic characteristics of FL, such as the Non-IID distribution of client data and the prohibition against inter-client information exchange, render such direct applications impracticable:

- Non-IID: In realistic federated learning environments, class variances among different clients are commonplace.[26] The simplistic application of UASD [8] to amalgamate all local models for smoother predictions at the client level would lead to the degradation of the globally aggregated model, despite potential benefits in local out-of-distribution detection.
- In the domain of Federated Learning (FL), the privacy of data is a cornerstone principle, enforcing a strict prohibition against direct data exchange between clients, thereby safeguarding user data security and privacy. This prohibition theoretically poses a barrier to the implementation of the DSSSL [9] method within an FL framework, where bi-level optimization is necessitated to calibrate unsupervised loss weights and estimate parameters based on a cleanly labeled dataset. Optimizing local models without direct access to other clients' data becomes challenging because the bi-level optimization process requires cross-client data information to evaluate the loss function and adjust weights. To circumvent this, the development of novel mechanisms that allow the aggregation of multi-client information in some form without violating the data privacy directive is needed. This could involve the use of differential privacy techniques or secure multi-party computation protocols to indirectly infer the information necessary for global optimization without the direct sharing of data. Clients might share encrypted gradients or model updates instead of raw data, and through such means, the global model could benefit from the learning across all clients while maintaining privacy. Additionally, techniques peculiar to FL such as model pruning, knowledge distillation, or meta-learning can be leveraged to enhance the capacity for bi-level optimization within a communication-constrained environment. These approaches offer a potential pathway through which effective aggregation of global models on the server can be realized, without compromising the core privacy-preserving advantages of Federated Learning, by enabling independent model training on each client.

To surmount these hurdles, we introduce a pioneering FSSL framework. This framework capitalizes on a limited set of representative labeled data on the server to refresh the threshold every global round and dispatch this threshold to all participating clients. Subsequently, clients employ this threshold to sift through out-of-distribution samples within their unlabeled datasets.[30] Moreover, in our proposed framework, clients chronicle the global models dispatched from the server at each round.[81-83] This protocol ensures consistency between the average predictions of previous global models and current local predictions, thereby diminishing the potential adverse effects of class mismatches. [37, 38, 49, 54, 60-64, 77] In summary, our contributions are manifold:

- We delve into a realistic FSSL scenario where unlabeled data encompasses classes not present in labeled data. To the best of our knowledge, our endeavor is the inaugural attempt to tackle this predicament.
- We put forth a novel FSSL framework aimed at mitigating the detrimental impacts of class mismatches.

2 Problem Statement

For a realistic scenario, we consider that there are small amount of labeled data at both server and clients. We assume that the labeled data $L_S = (x^s, y^s)$ distribution in server can represent the overall labeled data distribution and the total classes for server labeled image is K. Further, we assume the labeled data in each client $L_{C_j} = (x^{C_j}, y^{C_j})$ has K_j classes where K_j is a subset of K. Then we consider there are abundant unlabeled data $U_{C_j} = (x^{C_j}, y^{C_j})$ only in each client while any unlabeled sample x^{C_j} is not guaranteed to be one of the known classes in K.

In this work, we delineate the class that belongs to the set K as an in-distribution class, indicating that it falls within the range of classes that the server's labeled data can represent. The in-distribution classes are therefore recognized as categories that the model has been exposed

to during training and is expected to understand and classify correctly. These classes are a part of the model's established knowledge base, having been derived from the labeled data that the server possesses, which mirrors the broad labeled data distribution across the federated network.

Conversely, we categorize any class that lies outside the set K as an out-distribution class. These are classes that the model has not been trained on and hence does not 'know' or expect. They represent new, previously unseen categories that are not covered by the labeled data available at the server or clients. Out-distribution classes pose a significant challenge in that they can disrupt the learning process by introducing elements that the model cannot readily identify or classify based on its current state of knowledge.

The distinction between in-distribution and out-distribution classes is pivotal in this context, as it underpins the model's approach to handling new data. Recognizing whether a data point is in-distribution or out-distribution is critical for making informed decisions on how to manage that data within the learning algorithm. It affects the confidence of the model's predictions and informs the subsequent steps in the learning process, such as updating the model, recalibrating thresholds, and adjusting learning strategies to accommodate new information.

2.1 Related Works

Semi-supervised Learning has been highly developed over the past few years. The most important component of recent state-of-the-art SSL algorithms is consistency regularization. [27, 78] Consistency regularization is based on the assumption that the model should output similar predictions when give different augmented versions of the same input. All [10–13] build their unsupervised classification loss [25, 46, 77-80] base on consistency regularization and achieve great performances. [47, 56-59].

Federated Learning [1–7, 16] becomes a popular learning framework which is used to train a global model at server without sharing client local data. The classic federated learning framework contains two main parts:

- Client Update: At communication round t, server randomly select M clients and broadcast them the global model θ_t. For each selected local client$k$, it uses θ_t and their local labeled data to update their local model $\theta^k{}_{t+1}$
- Server Aggregate: After the server collects all $\theta^k{}_{t+1}$ for any k belongs to $(1, 2, ..., M)$, it aggregates and update the global model for communication round $t + 1$

The technique of Out-of-distribution Detection (OOD Detection) is pivotal in assessing the reliability of a model's predictions. This approach typically employs the highest softmax probabilities as a metric of confidence to discern whether a sample aligns with the distribution seen during training or not. Despite its straightforwardness, this method may experience performance degradation due to the model's overconfidence in its predictions, often leading to misjudgment about the novelty of the data. To mitigate this issue, as suggested by sources [14] and [55], one can modulate the softmax probabilities to form a softer, less overconfident probability distribution. This method essentially involves adjusting the 'temperature' parameter in the softmax function to smooth the resulting probabilities. The effect of temperature scaling softens the probability distribution over classes, which can yield a more conservative and discerning confidence score, better equipping the system to recognize when a sample falls outside the distribution of its training data. Furthermore, the adoption of temperature scaling has been empirically validated to diminish the adverse effects of overconfidence, thereby enhancing the model's ability to perform robust OOD detection. This becomes increasingly critical in practical scenarios where models encounter diverse and unforeseen inputs, ensuring that their deployment remains reliable and secure against unexpected data distributions.

3 Proposal Framework

3.1 Server adjust OOD threshold

As our problem assumption, the server is equipped with a limited quantity of representative labeled data, which reflects the broader distribution of classes typically encountered in the federated learning environment. With this dataset as a benchmark, at every communication interval—denoted by round t—the server engages in the pivotal task of updating the Out-of-Distribution (OOD) threshold. This OOD threshold is pivotal in discerning whether new, unlabeled data points should be considered as belonging to known classes or as anomalies.

$$\tau = \backslash frac\{1\}\{L\}\backslash max(S(\theta(x_S), T)) \qquad (1)$$

Where Si is the temperature scaling equation, the implementation of which is integral to the model's ability to make nuanced predictions. By incorporating the temperature parameter T, the equation effectively recalibrates the confidence of the softmax outputs from the global model θt at each communication round t. This recalibration allows for a more discerning threshold τt, critical for differentiating between in-distribution classes and anomalies.

The premise of temperature scaling is rooted in the concept of smoothing the probability distribution over classes. By adjusting T, we can control the sharpness of the softmax probability distribution, which is particularly useful when dealing with uncertain or ambiguous data. In a federated learning scenario, where data is decentralized and varied, maintaining such flexibility is key for robust model performance.

Moreover, temperature scaling serves a dual purpose. Not only does it regulate the probability distribution for a

clearer demarcation between known and unknown data points, but it also standardizes the threshold to be in alignment with the distributed nature of client data. This standardization is essential because it ensures that the threshold for identifying OOD data is not arbitrarily set but is instead reflective of the collective understanding of the network's current state.

The equation Si, therefore, represents more than just a mathematical function; it is a pivotal component that embodies the dynamic adaptability of the system. It enables the server to make informed decisions on whether new data is typical of the model's learned distribution or if it should be flagged for further investigation. The importance of Si, and by extension the temperature scaling it encompasses, cannot be understated, as it ultimately shapes the fidelity and security of the learning process in a federated environment.

- **Average Maximum Softmax probability**: Since server labeled data contains all in-distribution class and is representative, the average value of maximum softmax probability reflects whether an unlabeled input should belongs to in-distribution classes or out-distribution classes.[21] If one's maximum softmax probability is higher than the average maximum softmax probability of the samples which are all belongs to in-distribution classes, it must have a high probability being in-distribution class.[24,33] On the other, if one's maximum softmax probability is lower than the average maximum softmax probability of the samples which are all belongs to in-distribution classes, it is risky to classify this unlabeled input as in-distribution.

Temperature Scaling Softmax: In the federated learning framework, temperature scaling softmax is adopted in lieu of the traditional softmax to modulate the predicted probabilities for unlabeled data across client updates. This technique is delineated in studies [26, 28, 38, 39], which highlight its utility in ensuring that the softmax probabilities are appropriately softened. By integrating the temperature parameter, local models at each client can recalibrate the predicted probabilities, which [34, 40, 41] emphasize is essential to mitigate overconfidence in model predictions.

This recalibration facilitates a uniform threshold that can be applied consistently across the diverse data subsets present within each client in the federated network. As the research in [44, 66-69] underpins, temperature scaling serves as a harmonizer, bringing the disparate models' outputs to a comparable level. This is especially pertinent for the federated learning paradigm where decentralized data can lead to significant variances in local model behavior.

Through temperature scaling, as explicated in [34, 40, 41], the predicted probabilities of unlabeled data are rendered more conservative, which is vital for maintaining the reliability of the federated model's global predictions. This process allows for the creation of a comparative baseline which is crucial when considering the heterogeneity of client data contributions as discussed in [44, 66-69]. By implementing a standardized approach to probability assessment, federated learning models can benefit from increased robustness against variations in local data distributions, ultimately leading to a more resilient and trustworthy global model.

3.2 Unlabeled Data Filter

Inspired by USAD [8] in Semi-supervised learning, we also propose historic average value as predictive confidence score for each unlabeled samples in our FSSL framework. For unlabeled data i in client j at communication round t, the predictive confidence as:

$$c_i = \max\left(S_{i\left(q_{t\left(x_{\{C,j\}}\right),T}\right)}\right) \quad (2)$$

where qt is average soften probability distribution of global models θ1, θ2, ..., θt. Instead of building an ensemble by aggregating all the historic updated networks at each clients, we only aggregate the historic global networks. Then we set an OOD filter for each client to discard the possible out-distribution samples:

$$S_{i(x;T)} = \frac{\left\{\exp\left(\frac{f_{i(x)}}{T}\right)\right\}}{} \quad (3)$$

3.3 Novel consistency loss

As we have the filter to reject the potential out-distribution unlabeled data, we define our novel consistency loss for FSSL framework as below:

$$LU = \text{filter} * CE(qt, Si(\theta t(u), T)) + w(t)\text{filter} * CE(q\hat{}t, \theta t(A(u))) \quad (4)$$

where u is an unlabeled sample, w(t) is an increasing function with low initial value, q^t is the one-hot labels for qt We define this novel consistency loss for the following considerations:

- The first part $filter * CE(q_t, S_i(\theta_t(u), T))$ emphasizes the consistency between historic average softened probability distribution and current model predict softened probability distribution. This part is based on the assumption that if an unlabeled sample is not consistently belongs to a class, it is highly possible in out-distribution classes.
- The second part $w(t)filter * CE(q\hat{}_t, \theta_t(A(u)))$ emphasizes the data-level consistency which is similar to FixMatch [10]. This part is based on the assumption that model should output similar predictions when fed original version and augmented version of a same image. Since at the beginning few rounds, the model's ability on detecting out-distribution data is quite poor, including the misrecognized (i.e. mistakenly classify out-distribution unlabeled data as in-distribution class

[29]) data-level consistency loss will seriously decay the model performance. [84-87] We assign a small weight to second part at beginning rounds and keep increasing this weight as the model have stronger OOD detection ability.

We assign a small weight to the second part at the beginning rounds and keep increasing this weight as the model develops stronger OOD detection capabilities. This gradual increment of the weight w(t) for the data-level consistency loss reflects a strategic progression in the model's learning curve. Initially, the model's understanding of the data distribution is limited, and its ability to distinguish between in-distribution and out-distribution data is relatively undeveloped. Consequently, applying a smaller weight minimizes the potential adverse effects of incorrectly categorized out-distribution data on the model's learning.

As the model matures, benefiting from multiple rounds of federated learning, it garners a more nuanced understanding of the underlying data distribution. Its proficiency in identifying out-distribution samples becomes more pronounced. This enhanced detection ability justifies a corresponding increase in the weight assigned to the data-level consistency loss. Incrementally increasing w(t) allows the model to place greater emphasis on aligning the predictions for the original and augmented versions of a sample, fostering a stronger and more reliable consistency.

This dynamic weighting mechanism serves as a safeguard against early misclassifications while enabling the model to progressively focus more on consistency as its confidence in identifying OOD data solidifies. Such a carefully modulated approach ensures that the model does not become overly penalized for its initial uncertainty, yet evolves to prioritize data consistency as a hallmark of its growing competence.

3.4 Federated Framework

Following the state-of-art SSL method, we finally define our objective for each local update as the combination of supervised cross-entropy loss and unsupervised consistency loss:

$$L = CE(yL, \text{softmax}(\theta t(xL))) + LU \quad (5)$$

where yL is the true label of each labeled image xL and LU is from the Eq (4). Our proposed federated semi-supervised learning framework is summarized in the following:

Algorithm 1 Federated Semi-supervised Learning under Class Mismatch

Require: Server labeled data L_S, Client j labeled data L_C,j, Client j unlabeled data U_C,j, Local learning rate η
Part 1: Server Aggregate:
1. Use labeled data L_S to train initial θ0, τ0
2. for Communication Round, t = 1, 2, . . . do
3. Broadcast θ_t, τ_t to each client
4. for Involved Client, j = 1, 2, . . . , J do
5. θ^(j)_t+1 ← Local Update(θ_t)
6. end for
7. θ_t+1 = 1/J ∑ θ^(j)_t+1
8. τ_t+1 is updated by Eq (1) with θ_t+1
9. end for
Part 2: Local Update:
1. Compute filter by Eq (2) and Eq (3)
2. for each local epoch, e = 1, 2, . . . do
3. for mini batch, b = 1, 2, . . . do
4. Use Eq (5), L_C,j, U_C,j and filter to compute L
5. θ^(j)_t+1 ← Update θ_j using gradient descent on L with learning rate η
6. end for
7. end for

4 Conclusion

In this study, we delved into a Federated Semi-Supervised Learning (FSSL) framework, designed to strategically utilize unlabeled data within federated learning networks. This is particularly relevant in settings where data originates from a myriad of personal mobile devices, leading to a disparity between the distribution of classes in labeled and unlabeled datasets. Our approach stands out for its innovative combination of advanced semi-supervised learning strategies and the decentralized nature of federated learning.

The essence of our framework is its ability to adapt to the innate complexities presented by Non-IID data distributions—a staple in client-based data scenarios. Furthermore, it strictly adheres to the protocols of federated learning that prevent the sharing of client data, thus maintaining the confidentiality of individual datasets. Through this integration, our FSSL framework ensures that the learning models not only maintain their efficacy but also their integrity, without compromising on the privacy of the data involved.

To conclude, our exploration and introduction of this novel FSSL framework represent a significant stride towards resolving the prevalent challenges of class mismatches in unlabeled datasets. By embedding semi-supervised learning principles into the federated learning model, we offer a solution that respects privacy constraints while enhancing data utilization, ultimately paving the way for more sophisticated and privacy-conscious machine learning applications.

Acknowledgments

The authors thank the editor and anonymous reviewers for their helpful comments and valuable suggestions.

Funding

Not applicable.

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Conflict of Interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Author Contributions

Not applicable.

About the Authors

JIN, Jiajun

Independent researcher.

NI, Fanghao

Independent researcher.

DAI, Shuying

Independent researcher.

LI, Keqin

Independent researcher.

HONG, Bo

Independent researcher.

References

[1] McMahan, B., Moore, E., Ramage, D., Hampson, S. Arcas, B.A.y.. (2017). Communication-Efficient Learning of Deep Networks from Decentralized Data. Proceedings of the 20th International Conference on Artificial Intelligence and Statistics, in PMLR 54:1273-1282

[2] Jeong W, Yoon J, Yang E, Hwang SJ. FEDERATED SEMI-SUPERVISED LEARNING WITH INTER-CLIENT CONSISTENCY DISJOINT LEARNING.

[3] Li T, Sahu AK, Zaheer M, Sanjabi M, Talwalkar A, Smith V. Federated optimization in heterogeneous networks. arXiv preprint arXiv:1812.06127. 2018 Dec 14

[4] Zhao Y, Li M, Lai L, Suda N, Civin D, Chandra V. Federated learning with non-iid data. arXiv preprint arXiv:1806.00582. 2018 Jun 2.

[5] Bian, Jieming, Cong Shen, and Jie Xu. "Federated learning via indirect server-client communications." 2023 57th Annual Conference on Information Sciences and Systems (CISS). IEEE, 2023.

[6] Zhao Y, Liu H, Li H, Barnaghi P, Haddadi H. Semi-supervised Federated Learning for Activity Recognition. arXiv preprint arXiv:2011.00851. 2020 Nov 2.

[7] Jin Y, Wei X, Liu Y, Yang Q. Towards utilizing unlabeled data in federated learning: A survey and prospective. arXiv e-prints. 2020 Feb:arXiv-2002.

[8] Chen Y, Zhu X, Li W, Gong S. Semi-supervised learning under class distribution mismatch. InProceedings of the AAAI Conference on Artificial Intelligence 2020 Apr 3 (Vol. 34, No. 04, pp. 3569-3576).

[9] Guo LZ, Zhang ZY, Jiang Y, Li YF, Zhou ZH. Safe deep semi-supervised learning for unseen-class unlabeled data. InInternational Conference on Machine Learning 2020 Nov 21 (pp. 3897-3906). PMLR.

[10] Sohn K, Berthelot D, Li CL, Zhang Z, Carlini N, Cubuk ED, Kurakin A, Zhang H, Raffel C. Fixmatch: Simplifying semi-supervised learning with consistency and confidence. arXiv preprint arXiv:2001.07685. 2020 Jan 21.

[11] Xie Q, Dai Z, Hovy E, Luong MT, Le QV. Unsupervised data augmentation for consistency training. arXiv preprint arXiv:1904.12848. 2019 Apr 29.

[12] Berthelot D, Carlini N, Goodfellow I, Papernot N, Oliver A, Raffel C. Mixmatch: A holistic approach to semi-supervised learning. arXiv preprint arXiv:1905.02249. 2019 May 6.

[13] Berthelot D, Carlini N, Cubuk ED, Kurakin A, Sohn K, Zhang H, Raffel C. Remixmatch: Semi-supervised learning with distribution alignment and augmentation anchoring. arXiv preprint arXiv:1911.09785. 2019 Nov 21.

[14] Liang S, Li Y, Srikant R. Enhancing the reliability of out-of-distribution image detection in neural networks. arXiv preprint arXiv:1706.02690. 2017 Jun 8.

[15] Hendrycks D, Gimpel K. A baseline for detecting misclassified and out-of-distribution examples in neural

networks. arXiv preprint arXiv:1610.02136. 2016 Oct 7.

[16] Bian, J., Fu, Z., Xu, J. (2021). FedSEAL: semi-supervised federated learning with self-ensemble learning and negative learning. arXiv preprint arXiv:2110.07829.

[17] Peng, Yuanzhe. "A survey on modern recommendation system based on big data." arXiv preprint arXiv:2206.02631 (2022).

[18] Sun, Anchen, et al. "Who Said What? An Automated Approach to Analyzing Speech in Preschool Classrooms." arXiv preprint arXiv:2401.07342 (2024).

[19] Sun, Anchen, et al. "Multimodal Data Integration and User Interaction for Avatar Simulation in Augmented Reality." IJMDEM vol.13, no.1 2022: pp.1-19. http://doi.org/10.4018/IJMDEM.304391

[20] Tan, Z., Beigi, A., Wang, S., Guo, R., Bhattacharjee, A., Jiang, B., Karami, M., Li, J., Cheng, L., & Liu, H. (2024). Large Language Models for Data Annotation: A Survey. ArXiv Preprint ArXiv:2402.13446.

[21] Tan, Z., Cheng, L., Wang, S., Bo, Y., Li, J., & Liu, H. (2023). Interpreting pretrained language models via concept bottlenecks. ArXiv Preprint ArXiv:2311.05014.

[22] Zhao, S., Gan, L., Tuan, L. A., Fu, J., Lyu, L., Jia, M., & Wen, J. (2024). Defending Against Weight-Poisoning Backdoor Attacks for Parameter-Efficient Fine-Tuning. ArXiv Preprint ArXiv:2402.12168.

[23] Zhao, S., Jia, M., Tuan, L. A., Pan, F., & Wen, J. (2024). Universal vulnerabilities in large language models: Backdoor attacks for in-context learning. ArXiv Preprint ArXiv:2401.05949.

[24] Xin, Y., Luo, S., Jin, P., Du, Y., & Wang, C. (2023). Self-Training with Label-Feature-Consistency for Domain Adaptation. International Conference on Database Systems for Advanced Applications, 84–99.

[25] Wang, Q., Wang, C., Lai, Z., & Zhou, Y. (2024). InsectMamba: Insect Pest Classification with State Space Model. ArXiv Preprint ArXiv:2404.03611.

[26] Nian, Y., Jin, W., & Lin, L. (2023). In-process global interpretation for graph learning via distribution matching. ArXiv Preprint ArXiv:2306.10447.

[27] Su, J., Nair, S., & Popokh, L. (2023). EdgeGYM: a reinforcement learning environment for constraint-aware NFV resource allocation. 2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC), 1–7.

[28] Ning, Q., Zheng, W., Xu, H., Zhu, A., Li, T., Cheng, Y., Feng, S., Wang, L., Cui, D., & Wang, K. (2022). Rapid segmentation and sensitive analysis of CRP with paper-based microfluidic device using machine learning. Analytical and Bioanalytical Chemistry, 414(13), 3959–3970.

[29] Yang, W., Jiang, Y., Chi, Y., Xu, Z., & Wei, W. (2024). Long-Term Network Structure Evolution Investigation for Sustainability Improvement: An Empirical Analysis on Global Top Full-Service Carriers. Aerospace, 11(2), 128.

[30] Chen, S., Kann, B. H., Foote, M. B., Aerts, H. J., Savova, G. K., Mak, R. H., & Bitterman, D. S. (2023). Use of artificial intelligence chatbots for cancer treatment information. JAMA Oncology, 9(10), 1459–1462.

[31] Derton, A., Guevara, M., Chen, S., Moningi, S., Kozono, D. E., Liu, D., Miller, T. A., Savova, G. K., Mak, R. H., & Bitterman, D. S. (2023). Natural language processing methods to empirically explore social contexts and needs in cancer patient notes. JCO Clinical Cancer Informatics, 7, e2200196.

[32] Guevara, M., Chen, S., Thomas, S., Chaunzwa, T. L., Franco, I., Kann, B. H., Moningi, S., Qian, J. M., Goldstein, M., Harper, S., & others. (2024). Large language models to identify social determinants of health in electronic health records. NPJ Digital Medicine, 7(1), 6.

[33] Wang, C., Chen, F., Zhang, Y., Wang, S., Yu, B., & Cheng, J. (2022). Temporal stability of factors affecting injury severity in rear-end and non-rear-end crashes: A random parameter approach with heterogeneity in means and variances. Analytic Methods in Accident Research, 35, 100219.

[34] Deng, T., Xie, H., Wang, J., & Chen, W. (2023). Long-Term Visual Simultaneous Localization and Mapping: Using a Bayesian Persistence Filter-Based Global Map Prediction. IEEE Robotics & Automation Magazine, 30(1), 36–49.

[35] Ning, Q., Zheng, W., Xu, H., Zhu, A., Li, T., Cheng, Y., ... & Wang, K. (2022). Rapid segmentation and sensitive analysis of CRP with paper-based microfluidic device using machine learning. Analytical and Bioanalytical Chemistry, 414(13), 3959-3970.

[36] Ru, J., Yu, H., Liu, H., Liu, J., Zhang, X., & Xu, H. (2022). A Bounded Near-Bottom Cruise Trajectory Planning Algorithm for Underwater Vehicles. Journal of Marine Science and Engineering, 11(1), 7.

[37] Yao, J., Wu, T., & Zhang, X. (2023). Improving depth gradientcontinuity in transformers: A comparative study on monocular depth estimation with cnn. ArXiv Preprint ArXiv:2308.08333.

[38] Wang, X., Qiao, Y., Xiong, J., Zhao, Z., Zhang, N., Feng, M., & Jiang, C. (2024). Advanced Network Intrusion Detection with TabTransformer. Journal of Theory and Practice of Engineering Science, 4(03), 191-198.

[39] Liu, T., Cai, Q., Xu, C., Hong, B., Ni, F., Qiao, Y., & Yang, T. (2024). Rumor Detection with A Novel Graph Neural Network Approach. Academic Journal of Science

and Technology, 10(1), 305–310.

[40] Wang, R., Chen, X., Khalilian-Gourtani, A., Chen, Z., Yu, L., Flinker, A., & Wang, Y. (2020). Stimulus speech decoding from human cortex with generative adversarial network transfer learning. 2020 IEEE 17th International Symposium on Biomedical Imaging (ISBI), 390–394.

[41] Chen, X., Wang, R., Khalilian-Gourtani, A., Yu, L., Dugan, P., Friedman, D., Doyle, W., Devinsky, O., Wang, Y., & Flinker, A. (2023). A Neural Speech Decoding Framework Leveraging Deep Learning and Speech Synthesis. BioRxiv, 2023–09.

[42] Su, J., Nair, S., & Popokh, L. (2022, November). Optimal resource allocation in sdn/nfv-enabled networks via deep reinforcement learning. In 2022 IEEE Ninth International Conference on Communications and Networking (ComNet) (pp. 1-7). IEEE.

[43] Tang, Z., Wang, Y., & Chang, T.-H. (2024). z-SignFedAvg: A Unified Stochastic Sign-Based Compression for Federated Learning. Proceedings of the AAAI Conference on Artificial Intelligence, 38(14), 15301–15309.

[44] Liu, T., Cai, Q., Xu, C., Hong, B., Xiong, J., Qiao, Y., & Yang, T. (2024). Image Captioning in News Report Scenario. Academic Journal of Science and Technology, 10(1), 284–289.

[45] Liu, H., Shen, Y., Yu, S., Gao, Z., & Wu, T. (2024). Deep Reinforcement Learning for Mobile Robot Path Planning. ArXiv Preprint ArXiv:2404.06974.

[46] Tang, Z., Chang, T.-H., Ye, X., & Zha, H. (2023). Low-rank matrix recovery with unknown correspondence. Uncertainty in Artificial Intelligence, 2111–2122.

[47] Su, J., Jiang, C., Jin, X., Qiao, Y., Xiao, T., Ma, H., Wei, R., Jing, Z., Xu, J., & Lin, J. (2024). Large Language Models for Forecasting and Anomaly Detection: A Systematic Literature Review. ArXiv Preprint ArXiv:2402.10350.

[48] Yi, X., & Qiao, Y. (2024). GPU-Based Parallel Computing Methods for Medical Photoacoustic Image Reconstruction. arXiv preprint arXiv:2404.10928.

[49] Xin, Y., Du, J., Wang, Q., Lin, Z., & Yan, K. (2024, March). VMT-Adapter: Parameter-Efficient Transfer Learning for Multi-Task Dense Scene Understanding. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 38, No. 14, pp. 16085-16093).

[50] Zhu, A., Li, J., & Lu, C. (2021). Pseudo view representation learning for monocular RGB-D human pose and shape estimation. IEEE Signal Processing Letters, 29, 712-716.

[51] Xin, Y., Du, J., Wang, Q., Yan, K., & Ding, S. (2024, March). Mmap: Multi-modal alignment prompt for cross-domain multi-task learning. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 38, No. 14, pp. 16076-16084).

[52] Zhu, Armando, Keqin, Li, Tong, Wu, Peng, Zhao, Wenjing, Zhou, Bo, Hong. "Cross-Task Multi-Branch Vision Transformer for Facial Expression and Mask Wearing Classification". arXiv preprint arXiv:2404.14606. (2024).

[53] Delezenne, Q., Petrunin, I., Xu, Z., Neptune, J., & Bleakley, T. (2024). Autonomous Navigation with Taxiway Crossings Identification using Camera Vision and Airport Map. AIAA SCITECH 2024 Forum, 1300.

[54] Zhao, S., Jia, M., Tuan, L. A., Pan, F., & Wen, J. (2024). Universal vulnerabilities in large language models: Backdoor attacks for in-context learning. ArXiv Preprint ArXiv:2401.05949.

[55] Read, A. J., Zhou, W., Saini, S. D., Zhu, J., & Waljee, A. K. (2023). Prediction of Gastrointestinal Tract Cancers Using Longitudinal Electronic Health Record Data. Cancers, 15(5), 1399.

[56] Chen, J., Chen, X., Wang, R., Le, C., Khalilian-Gourtani, A., Jensen, E., Dugan, P., Doyle, W., Devinsky, O., Friedman, D., & others. (2024). Subject-Agnostic Transformer-Based Neural Speech Decoding from Surface and Depth Electrode Signals. BioRxiv, 2024–03.

[57] Deng, T., Chen, Y., Zhang, L., Yang, J., Yuan, S., Wang, D., & Chen, W. (2024). Compact 3D Gaussian Splatting For Dense Visual SLAM. ArXiv Preprint ArXiv:2403.11247.

[58] Yan, C., Qiu, Y., & Zhu, Y. (2021). Predict Oil Production with LSTM Neural Network. Proceedings of the 9th International Conference on Computer Engineering and Networks, 357–364.

[59] Zhu, A., Li, J., & Lu, C. (2021). Pseudo view representation learning for monocular RGB-D human pose and shape estimation. IEEE Signal Processing Letters, 29, 712–716.

[60] Yao, J., Pan, X., Wu, T., & Zhang, X. (2024). Building lane-level maps from aerial images. ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and SignalProcessing (ICASSP), 3890–3894.

[61] Peng, Q., Zheng, C., & Chen, C. (2023). Source-free domain adaptive human pose estimation. Proceedings of the IEEE/CVF International Conference on Computer Vision, 4826–4836.

[62] Peng, Q., Ding, Z., Lyu, L., Sun, L., & Chen, C. (2023). RAIN: regularization on input and network for black-box domain adaptation. Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence, 4118–4126.

[63] Tian, Y., Han, Y., Chen, X., Wang, W., & Chawla, N. V. (2024). TinyLLM: Learning a Small Student from Multiple Large Language Models. ArXiv Preprint

ArXiv:2402.04616.

[64] Wu, J., Lai, Z., Chen, S., Tao, R., Zhao, P., & Hovakimyan, N. (2024). The new agronomists: Language models are experts in crop management. ArXiv Preprint ArXiv:2403.19839.

[65] Jing, Z., Su, Y., Han, Y., Yuan, B., Liu, C., Xu, H., & Chen, K. (2024). When Large Language Models Meet Vector Databases: A Survey. ArXiv Preprint ArXiv:2402.01763.

[66] Liu, T., Xu, C., Qiao, Y., Jiang, C., & Yu, J. (2024). Particle Filter SLAM for Vehicle Localization. Journal of Industrial Engineering and Applied Science, 2(1), 27-31.

[67] Zhu, A., Li, K., Wu, T., Zhao, P., Zhou, W., & Hong, B. (2024). Cross-Task Multi-Branch Vision Transformer for Facial Expression and Mask Wearing Classification. ArXiv Preprint ArXiv:2404.14606.

[68] Weng, Y., & Wu, J. (2024). Fortifying the global data fortress: a multidimensional examination of cyber security indexes and data protection measures across 193 nations. International Journal of Frontiers in Engineering Technology, 6(2).

[69] Wang, C., Abdel-Aty, M., & Han, L. (2024). Effects of speed difference on injury severity of freeway rear-end crashes: Insights from correlated joint random parameters bivariate probit models and temporal instability. Analytic Methods in Accident Research, 100320.

[70] Li, Z., Huang, Y., Zhu, M., Zhang, J., Chang, J., & Liu, H. (2024). Feature manipulation for ddpm based change detection. ArXiv Preprint ArXiv:2403.15943.

[71] Yao, J., Li, C., Sun, K., Cai, Y., Li, H., Ouyang, W., & Li, H. (2023). Ndc-scene: Boost monocular 3d semantic scene completion in normalized devicecoordinates space. 2023 IEEE/CVF International Conference on Computer Vision (ICCV), 9421–9431.

[72] Wang, C., Easa, S. M., Chen, F., & Cheng, J. (2023). Difference in perception-reaction time of plain and plateau drivers at expressway exit ramps. Transportation Research Part F: Traffic Psychology and Behaviour, 98, 318–336.

[73] Peng, Q., Zheng, C., & Chen, C. (2024). A Dual-Augmentor Framework for Domain Generalization in 3D Human Pose Estimation. ArXiv Preprint ArXiv:2403.11310.

[74] Deng, T., Wang, Y., Xie, H., Wang, H., Wang, J., Wang, D., & Chen, W. (2024). NeSLAM: Neural Implicit Mapping and Self-Supervised Feature Tracking With Depth Completion and Denoising. ArXiv Preprint ArXiv:2403.20034.

[75] Popokh, L., Su, J., Nair, S., & Olinick, E. (2021). IllumiCore: Optimization Modeling and Implementation for Efficient VNF Placement. 2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 1–7.

[76] Xiong, S., Payani, A., Kompella, R., & Fekri, F. (2024). Large language models can learn temporal reasoning. ArXiv Preprint ArXiv:2401.06853.

[77] Guo, F., Wu, J. Z., & Pan, L. (2023, July). An Empirical Study of AI Model's Performance for Electricity Load Forecasting with Extreme Weather Conditions. In International Conference on Science of Cyber Security (pp. 193-204). Cham: Springer Nature Switzerland.

[78] Guo, F. (2023, July). A Study of Smart Grid Program Optimization Based on K-Mean Algorithm. In 2023 3rd International Conference on Electrical Engineering and Mechatronics Technology (ICEEMT) (pp. 711-714). IEEE.