Robust Heterogeneous Federated Learning under Data Corruption

Xiuwen Fang, Mang Ye*, Xiyuan Yang
National Engineering Research Center for Multimedia Software, Institute of Artificial Intelligence,
Hubei Key Laboratory of Multimedia and Network Communication Engineering,
School of Computer Science, Hubei Luojia Laboratory, Wuhan University, Wuhan, China

https://github.com/FangXiuwen/AugHFL

Additional Experiments

In this section, we discuss the extensive applicability of our proposed method. Considering that label noise is also another form of data corruption, we validate the effectiveness of AugHFL in heterogeneous federated learning under label noise scenarios. Our approach to generating label noise follows the Fang *et al.* [1]. Here we compare the performance of AugHFL with the SOTA methods under various label noise scenarios (Tabs. 1 and 2), where the noise rate is 0.1 or 0.2, and the noise type is pairflip or symmetric. The baseline refers to the method in which the clients train local models on individual private datasets without federated learning. The experimental results demonstrate that our proposed method exhibits robustness against label noise in various noise settings. In the label noise scenarios, AugHFL is not as effective as RHFL, which is designed for solving the label noise problem. However, AugHFL outperforms other existing strategies under various noise settings. Overall, AugHFL can handle various forms of data corruption effectively, mitigating the negative effects of image corruption and demonstrating robust performance in label noise scenarios.

*Corresponding Author: Mang Ye (yemang@whu.edu.cn)

References

[1] Xiuwen Fang and Mang Ye. Robust federated learning with noisy and heterogeneous clients. In CVPR, pages 10062–10071, 2022. 1

[2] Wenke Huang, Mang Ye, and Bo Du. Learn from others and be yourself in heterogeneous federated learning. In CVPR, pages 10133–10143, 2022. 1

[3] Daliang Li and Junpu Wang. Fedmd: Heterogenous federated learning via model distillation. In NeurIPS Workshop, 2019. 1

[4] Tao Lin, Lingjing Kong, Sebastian U Stich, and Martin Jaggi. Ensemble distillation for robust model fusion in federated learning. 2020. 1

Table 1. Compare with the state-of-the-art methods when the noise rate $\mu = 0.1$. (θ_k represents the local model of the client c_k. The optimal accuracy is marked in bold and the sub-optimal accuracy is underlined. These notes are the same for others.)

Method	Pairflip					Symflip				
	θ_1	θ_2	θ_3	θ_4	Avg	θ_1	θ_2	θ_3	θ_4	Avg
Baseline	77.98	76.75	66.89	74.33	73.99	76.20	76.05	64.96	74.31	72.88
FedMD [3]	74.98	76.89	67.10	<u>76.64</u>	73.90	73.23	73.66	67.72	75.54	72.54
FedDF [4]	76.26	75.51	68.41	76.04	74.06	72.07	75.18	67.38	74.47	72.28
RHFL [1]	78.86	<u>78.76</u>	<u>69.60</u>	71.83	74.76	<u>78.40</u>	**78.36**	**69.47**	**76.93**	<u>75.79</u>
FCCL [2]	**79.26**	78.45	**71.11**	**78.74**	**76.97**	72.07	75.18	67.38	74.47	72.28
AugHFL	<u>79.16</u>	**79.26**	67.50	74.91	<u>75.21</u>	**80.03**	<u>78.26</u>	<u>68.68</u>	<u>76.28</u>	**75.81**

Table 2. Compare with the state-of-the-art methods when the noise rate $\mu = 0.2$.

Method	Pairflip					Symflip				
	θ_1	θ_2	θ_3	θ_4	Avg	θ_1	θ_2	θ_3	θ_4	Avg
Baseline	72.31	71.84	61.78	69.67	68.90	72.01	70.15	59.62	69.42	67.80
FedMD [3]	68.00	67.81	65.67	<u>74.02</u>	68.88	67.31	68.54	<u>64.48</u>	71.75	68.02
FedDF [4]	68.66	69.68	62.36	72.12	68.21	67.36	68.56	63.60	70.83	67.59
RHFL [1]	**77.81**	**76.09**	**66.61**	72.78	**73.32**	**78.14**	<u>76.77</u>	64.23	**73.90**	<u>73.26</u>
FCCL [2]	74.17	72.73	<u>66.06</u>	**74.94**	71.98	72.07	75.18	67.38	74.47	72.28
AugHFL	<u>74.32</u>	<u>75.85</u>	65.88	73.22	<u>72.32</u>	<u>76.87</u>	**78.81**	**65.92**	<u>71.83</u>	**73.36**