

Federated Learning Paper Sharing

Lisen Dai

November 26, 2020

FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning

Sparse Compression Algorithm

Federated
Learning
Paper Sharing

Lisen Dai

FedOpt (Appl.
Sci. 2020,
10(8), 2864)

Goal: reduce the number of communication bits during the models training.

$$\Delta\theta = \mathcal{SGD}_n(\theta, D_{mini-batches}) - \theta$$

θ : Deep Neural Network parameters.

\mathcal{SGD}_n : refers to the set of gradient updates after n epochs of SGD on DNN (deep neural network) parameters θ during the sampling of mini-batches from local data

Once we have the updates $\delta v...$

FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning

Federated
Learning
Paper Sharing

Lisen Dai

FedOpt (Appl.
Sci. 2020,
10(8), 2864)

Input: temporal vector $\Delta\theta$, Sparsity Fraction q

Output: sparse temporal $\Delta\theta^*$

Initialization;

$num^+ \leftarrow top_q(\Delta\theta); num^- \leftarrow top_q(-\Delta\theta)$

$\Psi^+ \leftarrow mean(num^+); \Psi^- \leftarrow mean(num^-)$

if $\Psi^+ \geq \Psi^-$ **then**

return ($\Delta\theta^* \leftarrow \Psi^+(\theta \geq \min(num^+))$);

end

else

return ($-\Delta\theta^* \leftarrow \Psi^-(\theta \geq \min(-num^-))$);

end

Algorithm 1: SCA: Communication Efficiency in FedOpt

FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning

Federated
Learning
Paper Sharing

Lisen Dai

FedOpt (Appl.
Sci. 2020,
10(8), 2864)

“We utilise the additively homomorphic encryption in FedOpt in order to achieve efficiency throughout the learning process.”

Algorithm 2: Pseudocode of Privacy Preserving

Input : Users for local datasets D_i , the cloud server to initialise global parameters ω_0

Output: New global parameters ω

1 **Initialisation:**

2 **while** Cloud server initialise global parameters ω_0 **do**

3 Aggregate global parameters ω_0 to users

4 **while** Users obtain local gradients G_{II} by training local models D_i **do**

5 Add noise ϵ -DP $\leftarrow G_{II}$

6 Encrypt $G_{II} \leftarrow E_\delta(G_{II} + \text{Lap}(\frac{\Delta f_{II}}{\epsilon}))$

7 Generate encrypted local gradients E_{II}

8 Aggregate $E_\delta(\sum_{II=1}^n G_{II})$

9 **end**

10 **while** Cloud server aggregates encrypted local gradients to users II **do**

11 $E_{add} \leftarrow E_\delta(\sum_{II=1}^n G_{II})$

12 Generate cipher-text from E_{II}

13 Generate encrypted global gradients E_{add}

14 **end**

15 **while** Users decrypts E_{add} to get global gradients B_{II} **do**

16 $D_\delta(E_{add}) \leftarrow \sum_{II=1}^n G_{II}$

17 Update existing parameters ω

18 Aggregate new parameters ω to the cloud server

19 **end**

20 **end**

FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning

Federated
Learning
Paper Sharing

Lisen Dai

FedOpt (Appl.
Sci. 2020,
10(8), 2864)

Algorithm 3: FedOpt: Communication-Efficiency and Privacy-Preserving

```
Input : Initial parameters  $\omega_0$ 
Output: Global model with improved parameters  $\omega_0$ 
1 Initialisation: all users  $\Pi_i, i = 1, \dots, [\text{Total number of users}]$  are initialised with the same
   parameters  $v_i \leftarrow v$ . Those users who carry different private datasets  $D_i$  with  $|\{c : (x, y) \in D_i\}| = [\text{total classes per user}]$ . The remaining  $\Pi$  are initialised to zero  $\Delta v, \mathcal{R}_i, \mathcal{R} \leftarrow 0$ .
2 for epoch  $e = 1, \dots, E \mid E = \text{Total number of Epochs}$  do
3   for  $\Pi_i \in \Pi \subseteq \{1, \dots, [\text{Number of users}]\}$  do
4     User  $\Pi_i$  execute:
5     Plain-text =  $\xi \leftarrow \text{downloads}_{CS \rightarrow \Pi_i}(\xi)$ 
6      $\Delta v \leftarrow \text{decrypt}(\xi)$ 
7      $v_i \leftarrow v_i + \Delta v$ 
8      $\Delta v_i \leftarrow \mathcal{R}_i + \text{SGD}(v_i, D_i) - v_i$ 
9      $\Delta \bar{v}_i \leftarrow \text{SCA}_{\text{upload}}(\Delta v_i)$ 
10     $\mathcal{R}_i \leftarrow \Delta v_i - \Delta \bar{v}_i$ 
11     $\xi_i \leftarrow \text{encrypt } \Delta \bar{v}_i$ 
12     $\text{upload}_{\Pi_i \rightarrow CS}(\xi_i)$ 
13  end
14  Cloud Server CS execute:
15   $\text{collect}_{\Pi_i \rightarrow CS}(\Delta \bar{v}_i), e \in \Pi$ 
16   $\Delta v \leftarrow \mathcal{R} + \frac{1}{|\Pi|} \sum_{e \in \Pi} \Delta \bar{v}_i$ 
17   $\Delta \bar{v} \leftarrow \text{SCA}_{\text{download}}(\Delta v)$ 
18   $\mathcal{R} \leftarrow \Delta v - \Delta \bar{v}$ 
19   $v \leftarrow v + \Delta \bar{v}_i$ 
20   $\xi \leftarrow \text{encrypt } \Delta \bar{v}_i$ 
21   $\text{Aggregate}_{CS \rightarrow \Pi_i}(\xi), i = 1, \dots, \text{Global Model}$ 
22 end
23 return  $\omega_0$ 
```

FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning

Federated
Learning
Paper Sharing

Lisen Dai

FedOpt (Appl.
Sci. 2020,
10(8), 2864)

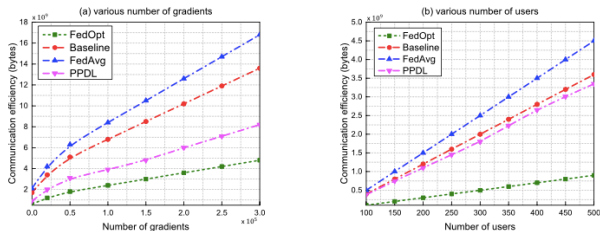


Figure 5. FedOpt communication efficiency on MNIST dataset.

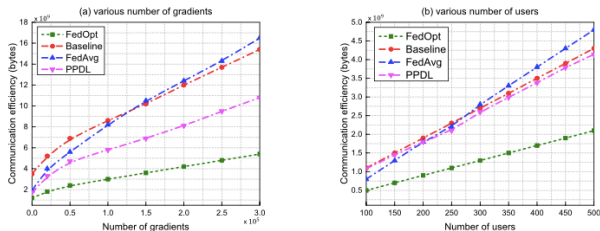


Figure 6. FedOpt communication efficiency on CIFAR-10 dataset.

FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning

Federated
Learning
Paper Sharing

Lisen Dai

FedOpt (Appl.
Sci. 2020,
10(8), 2864)

Table 2. Communication bits required for upload and download to achieve the targeted accuracy.

	MNIST (Accuracy = 91.3)	CIFAR-10 (Accuracy = 87.6)
Baseline	2218/2218 MB	35653 MB/35653 MB
FedAvg <i>epochs</i> = 50	119.65 MB/119.65 MB	2589.5 MB/2589.5 MB
FedAvg <i>epochs</i> = 100	84.73 MB/84.73 MB	1665.7 MB/1665.7 MB
PPDL <i>epochs</i> = 50	98.63 MB/311.6 MB	1472.2 MB/4739.2 MB
PPDL <i>epochs</i> = 100	63.74 MB/432.2 MB	958.3 MB/6342.4 MB
FedOpt <i>epochs</i> = 50	10.2 MB/102 MB	109.23 MB/1090.3 MB
FedOpt <i>epochs</i> = 100	14.6 MB/146 MB	172.3 MB/1723 MB

FedOpt: Towards Communication Efficiency and Privacy Preservation in Federated Learning

Federated
Learning
Paper Sharing

Lisen Dai

FedOpt (Appl.
Sci. 2020,
10(8), 2864)



Muhammad Asad, Ahmed Moustafa, and Takayuki Ito.
Fedopt: Towards communication efficiency and privacy
preservation in federated learning.
Applied Sciences, 10:1–17, 04 2020.