Communication-Efficient Federated Skin Lesion Classification with Generalizable Dataset Distillation

Yuchen Tian$^{1,*}$, Jiacheng Wang$^{1,*}$, Yueming Jin$^{2}$, Liansheng Wang$^{1(\text{so})}$

$^1$ Department of Computer Science at School of Informatics, Xiamen University, Xiamen, China, 361005
{tianyuchen,Jiachengw}@stu.xmu.edu.cn, lswang@xmu.edu.cn

$^2$ Department of Biomedical Engineering and Department of Electrical and Computer Engineering, National University of Singapore, Singapore, 119276
ymjin@nus.edu.sg

Abstract. Federated learning (FL) has recently been applied to skin lesion analysis, but the challenges of huge communication requirements and non-independent and identical distributions have not been fully addressed. The former problem arises from model parameter transfer between the server and clients, and the latter problem is due to differences in imaging protocols and operational customs. To reduce communication costs, dataset distillation methods have been adopted to distill thousands of real images into a few synthetic images (1 image per class) in each local client, which are then used to train a global model in the server. However, these methods often overlook the possible inter-client distribution drifts, limiting the performance of the global model. In this paper, we propose a generalizable dataset distillation-based federated learning (GDD-FL) framework to achieve communication-efficient federated skin lesion classification. Our framework includes the generalization dataset distillation (GDD) method, which explicitly models image features of the dataset into an uncertain Gaussian distribution and learns to produce synthetic images with features close to this distribution. The uncertainty in the mean and variance of the distribution enables the synthetic images to obtain diverse semantics and mitigate distribution drifts. Based on the GDD method, we further develop a communication-efficient FL framework that only needs to transmit a few synthesized images once for training a global model. We evaluate our approach on a large skin lesion classification dataset and compare it with existing dataset distillation methods and several powerful baselines. Our results show that our model consistently outperforms them, particularly in comparison to the classical FL method. All resources can be found at https://github.com/jcwang123/GDD-FL.

Keywords: Skin lesion classification · Dataset Distillation · Domain Generalization · Federated learning

* Contributed Equally.
1 Introduction

Federated learning is an innovative approach to training deep learning models that allows for collaboration and sharing of knowledge without the need to centralize data. It involves transferring model parameters between different clients to improve model performance. Federated learning is particularly useful in clinical settings where privacy is of utmost importance, as it allows multiple healthcare providers to train models using their own data while keeping patient information secure. Recent studies have shown the potential of federated learning in predicting clinical outcomes [19, 2, 1, 8, 10].

However, federated learning methods require transmitting model parameters between the server and clients at each learning round [15], and the entire learning process typically involves hundreds of epochs. The resultant increase in communication costs has become one of the most significant challenges in federated learning. Moreover, some hospitals with strict privacy regulations do not permit internet access, rendering the communication-reliant federated learning methods infeasible. To address these challenges, previous studies have attempted to limit the number of communications to accelerate convergence and improve communication efficiency [4, 6, 14, 17, 21, 29]. However, such methods still require tens of communications, and parameter transmission remains time-consuming and laborious in the era of large models. Synthesis-based methods are proposed to transfer the local images into synthetic images using GANs [18] and centralize them into the server for task learning, but GANs are hard to train and the generated synthetic images cost a lot of transmission loads. Recently, data distillation has been introduced in the federated learning domain [24]. This technique distills local datasets into a few synthetic images, typically fewer than ten, and sends these synthetic data to a global server for global training. As the transmission requires only one round of communication, and the synthetic data contains no original information, this method inherits the advantages of low communication costs and excellent privacy protection.

Nevertheless, the previous studies mainly discuss the usefulness of small datasets, i.e., handwritten digits. Whether the distilled image retains the abundant semantics for lesion classification is unknown and needed to be investigated. More importantly, this method adopts the oldest distillation algorithm and has not taken into account the distribution drifts among different clients. The drifts will lead to differing distributions of each synthetic dataset, and consequently, the global model trained on such distributed data may exhibit limited performance, which can impact the accuracy and robustness of the model in real-world settings. Solving distribution drifts is a significant challenge in the federated learning community and has been widely studied [3, 12, 13, 26, 25, 16]. However, these strategies are primarily designed for parameter-communication methods, where the clients send their local model updates to the central server for aggregation. In contrast, data distillation aims to minimize the amount of communication by sending synthetic data instead of parameter updates. Therefore, these strategies may not be directly applicable to the data distillation approach.
In this paper, we propose a novel and generalizable data distillation-based federated learning (GDD-FL) framework to address the challenges of communication costs and distribution drifts in skin lesion classification. We first propose a generalizable data distillation (GDD) method that distills each client’s local dataset into a small number of synthetic images and makes synthetic data from different sites located in similar distributions. It is achieved by approximating the possible Gaussian distribution of mean and variance values in one client’s synthetic data and randomly sampling a new distribution to produce synthetic images. Unlike current data distillation methods that align synthetic images to a fixed distribution, our GDD method produces synthetic images with uncertain distribution so they obtain better diversity. Based on the GDD method, we further build a communication-efficient federated learning framework for skin lesion classification. In this process, each client applies the GDD method to distill its local dataset into a small synthetic dataset and sends it to the global server. The global server then trains a brand-new model using the gathered data. By minimizing the communication between clients and the server, our method reduces communication costs and improves privacy protection. We evaluate the performance of our method on the ISIC-2020 dataset in IID and Non-IID federated settings and compare it with the classical federated learning method and other data distillation methods. The experimental results demonstrate that our GDD-FL framework consistently outperforms other methods in terms of classification accuracy while reducing communication costs and protecting privacy. Our proposed framework has great potential for applications in real-world scenarios where large datasets are distributed across different clients with limited communication resources.

2 Method

In summary, we introduce the approximation of the uncertain distribution of a real dataset in Sec. 2.1, how to optimize learnable synthetic images in Sec. 2.2, and the communication-efficient federated learning framework in Sec. 2.3.

2.1 Generalizable Dataset Distillation

The goal of dataset distillation is to condense the large-scale training set $\mathcal{T} = \{(x_1, y_1), \ldots, (x_{|\mathcal{T}|}, y_{|\mathcal{T}|})\}$ with $|\mathcal{T}|$ image and label pairs into a small synthetic set $\mathcal{S} = \{(s_1, y_1), \ldots, (s_{|\mathcal{S}|}, y_{|\mathcal{S}|})\}$ with $|\mathcal{S}|$ synthetic image and label pairs so that models trained on each $\mathcal{T}$ and $\mathcal{S}$ obtain comparable performance on unseen testing data: $\mathbb{E}_{x \sim P_\mathcal{D}} \mathcal{L}(f_{\thetaT}(x), y) \simeq \mathbb{E}_{x \sim P_\mathcal{D}} \mathcal{L}(f_{\thetaS}(x), y)$, where $P_\mathcal{D}$ is the real data distribution, $\mathcal{L}$ is the loss function (i.e. cross-entropy loss), $\Phi$ is a task-specific deep neural network, i.e. ResNet-18, parameterized by $\theta$, and $f_{\thetaT}$ and $f_{\thetaS}$ are the networks that are trained on $\mathcal{T}$ and $\mathcal{S}$ respectively. Similar to techniques [28, 23], our goal is to synthesize data that approximates the distribution of the real training data, instead of selecting a representative subset of training samples as in [27, 32]. The process has been visualized in Fig. 1.

To obtain a small dataset with similar semantics to the real dataset, we approximate the possible Gaussian distribution of real data and align the learnable
Fig. 1. Overall framework of the generalizable data distillation-based federated learning (GDD-FL). Unlike existing data distillation methods, GDD considers the possible distribution drifts inter-clients and proposes to change the target distribution with random deviations (\(\Sigma\)) so that the synthetic images’ distribution can align the distributions of other clients.

We use synthetic data to represent the uncertainty of data distribution, and obtain the uncertainty of mean and variance values to determine the distribution. Instead, to simulate the possible client drift, we estimate the uncertainty of data distribution, and randomly sample new distributions. Specifically, the uncertainty of mean and variance values is estimated as:

$$
\Sigma_\mu^2(x) = \frac{1}{|x|} \sum_{i=1}^{|x|} (\mu(x_i) - \mathbb{E}[\mu(x)])^2, \quad \Sigma_\sigma^2(x) = \frac{1}{|x|} \sum_{i=1}^{|x|} (\sigma(x_i) - \mathbb{E}[\sigma(x)])^2
$$

where \(\Sigma_\mu(x)\) and \(\Sigma_\sigma(x)\) represent the uncertainty estimation of the feature mean \(\mu\) and feature standard deviation \(\sigma\), respectively.

After the estimation of possible client shifts, we randomly sample new feature statistics from the estimated distribution as \(\hat{\mu}(x) \sim \mathcal{N}(\mu, \Sigma_\mu^2)\) and standard deviation \(\hat{\sigma}(x) \sim \mathcal{N}(\sigma, \Sigma_\sigma^2)\) for the corresponding distribution:

$$
\hat{\mu}(x) = \mu(x) + \epsilon_\mu \Sigma_\mu(x) \quad \text{and} \quad \hat{\sigma}(x) = \sigma(x) + \epsilon_\sigma \Sigma_\sigma(x)
$$

where \(\epsilon_\mu, \epsilon_\sigma \sim \mathcal{N}(0, I)\). In the end, the feature after the simulated client shift is formed as: \(\hat{x} = \hat{\mu}(x) + \frac{\hat{\sigma}(x)}{\hat{\sigma}(x)}\). After the distribution change, we optimize the learnable synthetic images to obtain the same distribution with \(\hat{x}\), where the details are introduced next.

2.2 Distillation Process

The training details are presented in Algorithm 1. During each learning epoch, we randomly sample initial parameters \(\theta\) for a typical ConvNet [5], denoted
as $\psi_\theta$, feeding the synthetic images and distribution-changed real data into the network to align the distribution. Before alignment, the read data is modified through the uncertain distribution change and Siamese augmentations. Specifically, the equations in Sec. 2.1 are used to approximate the uncertain distributions. We use $U_p$ to denote the distribution change, where $p = 0.5$ is a controlling variable that represents the probability of performing the change to avoid introducing excessive noise. The differentiable Siamese augmentation [9] is denoted as $A(\cdot)$, processing the real data and synthetic data respectively for better semantic alignment [30]. Finally, the optimization problem with uncertainty estimation is solved as:

$$\min_{\theta, \omega} \mathbb{E}_{\psi_\theta \sim \mathbb{P}_{\theta}, \omega \sim \mathbb{V}} \left( \frac{1}{|T|} \sum_{i=1}^{|T|} \psi_\theta(A(U_p(x_i))) - \frac{1}{|S|} \sum_{j=1}^{|S|} \psi_\omega(A(s_j)) \right)^2.$$ 

### 2.3 Communication-Efficient Federated Learning

Consider a federated learning task with $m$ clients, the client $k$-th owns local dataset $T_k$. We can obtain a set of synthetic datasets through our proposed GDD: $\mathcal{S} = \{\mathcal{S}_k | k = 1, 2, ..., m\}$. The server then collects all synthetic datasets from the local sites and uses the merged data $\mathcal{S}$ to train a brand-new model from scratch. We consider a non-convex neural network objective in the server and train a machine learning model on $\mathcal{S}$. For each iteration, we sample a mini-batch from the synthetic dataset, denoted as $(x, y) \in \mathcal{S}$, and calculate the objective function $L(x, y; w)$, where $L$ represents the typical entropy loss. Note that the sampled mini-batch may contain synthetic images from multiple clients, which enhances feature diversity in each mini-batch. After optimizing for a total of $E$ epochs, the parameter $\bar{w}$ is well-trained.

### 3 Experiment

#### 3.1 Datasets and Evaluation Metrics

**Datasets:** For our experiments, we used the public skin lesion classification ISIC2020 [20] dataset provided by the International Skin Imaging Collaboration archive. The dataset contains a total of 33,126 samples in the public training set. Since the public test set is not available, we divided the training set into the train, validation, and test sets with 26,500, 3,312, and 3,314 samples.

**Client Split:** To simulate the federation, we used two types of splits, IID and Non-IID, as the prior work [11]. For IID federation, we randomly divided the train and validation sets into ten parts ($m = 10$) with equal numbers of positive and negative samples. For Non-IID federation, we used Dirichlet with $\alpha = 1$ to distribute local data. We evaluated the global model using the test set.

**Evaluation Metrics:** We used four widely adopted metrics, namely, Precision ($P$), Recall ($R$), F1 score, and AUC, to comprehensively evaluate the classification performance. Higher values indicate better classification performance.

#### 3.2 Implementation Details

We use ResNet-18 [7] as the base classification model and a classical ConvNet [5] as the image feature extractor for data distillation training. To improve memory
Algorithm 1 Process of Generalizable Data Distillation

**Input:** Training set \( T \)

**Output:** Synthetic samples \( S \) for \( C \) classes

\[
\text{function } \text{ClientDatasetDistillation}(T) \quad \text{ end function}
\]

1: Initialize \( S \) by sampling from random noise

for each iteration do

4: Sample \( \vartheta \sim P_\vartheta \) and augmentation \( A_c \) for every class \( c \)

6: Compute \( O^T_c = \frac{1}{|B^T|} \sum_{(x,y) \in B^T} \psi_\theta(A_c(x)) \) for every class \( c \)

Compute \( O^S_c = \frac{1}{|B^S|} \sum_{(s,y) \in B^S} \psi_\theta(A_c(s)) \) for every class \( c \)

8: Compute \( O^U_c = \frac{1}{|B^U|} \sum_{(x,y) \in B^U} \psi_\theta(A_c(U_p(x))) \) for every class \( c \)

Compute \( L_{S,T} = \sum_{c=0}^{C-1} \|O^T_c - O^S_c\|^2 \)

10: Compute \( L_U = \sum_{c=0}^{C-1} \|O^U_c - O^S_c\|^2 \)

Update \( S \leftarrow S - \eta \nabla_S (L_U + L_{S,T}) \)

end for

return \( S \) for \( C \) classes

usage and computational efficiency, all images are resized to \((224 \times 224)\). During the distillation training, we use the SGD optimizer [22] with an initial learning rate of 1 for 300 epochs and set the batch size to 64. For training the classification model, we use the SGD optimizer with an initial learning rate of 0.01. The model is trained for 50 epochs using a batch size of 64.

### 3.3 Comparison of State-of-the-Arts

We mainly compare our method with the latest data distillation methods, namely DC [32], DSA [30], and DM [31]. Since these techniques have not been used in federated learning, we re-implement them in our settings. In addition, we compare the performance of the classical federated learning framework, FedAVG [15]. Furthermore, we demonstrate several centralized training results, where the "Upper Bound" refers to centralizing all data to train a classification model, and "R.S.@10" and "R.S.@100" denote randomly selecting 10/100 images per lesion class. Since the distillation method used in the prior work [24] is too old without novel designs, we focus on the latest distillation methods.

The quantitative results are shown in Tab. 1. It is seen that GDD outperforms other distillation techniques consistently across all settings. Notably, the improvement is more significant when distilling the dataset into 10 images per class, as the diversity of synthetic images is progressively enhanced. Compared with FedAVG, the results in the IID setting show that data distillation-based methods still have room for improvement. However, data distillation-based methods have a significant advantage over FedAVG in terms of low communication costs. Moreover, GDD-FL shows a substantial improvement in the Non-IID setting for AUC scores, i.e., 5.88% and 6.37% for distilling 1/10 images per class.
Table 1. Comparison with latest data distillation methods on the ISIC-2020 dataset. ** denotes the implementation on our federated setting.

<table>
<thead>
<tr>
<th>Method</th>
<th>AUC</th>
<th>P</th>
<th>R</th>
<th>F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upper Bound</td>
<td>80.97 ± 2.12</td>
<td>97.23 ± 0.03</td>
<td>91.11 ± 2.36</td>
<td>94.07 ± 1.54</td>
</tr>
<tr>
<td>R.S.@10</td>
<td>56.86 ± 1.16</td>
<td>87.29 ± 0.19</td>
<td>59.63 ± 5.08</td>
<td>70.86 ± 3.99</td>
</tr>
<tr>
<td>R.S.@100</td>
<td>60.22 ± 2.70</td>
<td>87.67 ± 0.08</td>
<td>65.56 ± 3.53</td>
<td>75.02 ± 2.54</td>
</tr>
</tbody>
</table>

*Transmit parameters: 12640 MB*

<table>
<thead>
<tr>
<th>Method</th>
<th>AUC</th>
<th>P</th>
<th>R</th>
<th>F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>FedAVG (HD) [15]</td>
<td>75.33 ± 3.21</td>
<td>96.55 ± 0.34</td>
<td>80.12 ± 4.97</td>
<td>87.57 ± 3.13</td>
</tr>
<tr>
<td>FedAVG (Non-HD)</td>
<td>65.97 ± 4.17</td>
<td>83.22 ± 1.34</td>
<td>70.68 ± 6.26</td>
<td>76.44 ± 4.23</td>
</tr>
</tbody>
</table>

*Transmit 1 image per class: 2.88 MB*

<table>
<thead>
<tr>
<th>Method</th>
<th>AUC</th>
<th>P</th>
<th>R</th>
<th>F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC* [32]</td>
<td>66.72 ± 2.98</td>
<td>96.71 ± 0.09</td>
<td>75.26 ± 5.23</td>
<td>84.56 ± 3.25</td>
</tr>
<tr>
<td>DSA* [30]</td>
<td>64.43 ± 2.67</td>
<td>96.76 ± 0.09</td>
<td>74.35 ± 5.78</td>
<td>83.99 ± 3.56</td>
</tr>
<tr>
<td>DM* [31]</td>
<td>68.82 ± 0.22</td>
<td>96.76 ± 0.09</td>
<td>74.35 ± 5.77</td>
<td>83.99 ± 3.56</td>
</tr>
<tr>
<td>GDD-FL (Ours)</td>
<td><strong>71.76 ± 0.04</strong></td>
<td><strong>96.93 ± 0.11</strong></td>
<td><strong>78.55 ± 2.74</strong></td>
<td><strong>86.78 ± 0.04</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Method</th>
<th>AUC</th>
<th>P</th>
<th>R</th>
<th>F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC* [32]</td>
<td>65.18 ± 8.09</td>
<td>96.73 ± 0.04</td>
<td>72.50 ± 12.22</td>
<td>82.42 ± 8.58</td>
</tr>
<tr>
<td>DSA* [30]</td>
<td>68.79 ± 0.88</td>
<td>96.70 ± 0.04</td>
<td>78.66 ± 2.93</td>
<td>86.73 ± 1.77</td>
</tr>
<tr>
<td>DM* [31]</td>
<td>68.41 ± 0.17</td>
<td>96.60 ± 0.12</td>
<td>72.88 ± 0.56</td>
<td>83.08 ± 0.32</td>
</tr>
<tr>
<td>GDD-FL (Ours)</td>
<td><strong>71.85 ± 1.75</strong></td>
<td><strong>97.17 ± 0.55</strong></td>
<td><strong>81.14 ± 3.28</strong></td>
<td><strong>88.41 ± 2.01</strong></td>
</tr>
</tbody>
</table>

*Transmit 10 images per class: 28.81 MB*

<table>
<thead>
<tr>
<th>Method</th>
<th>AUC</th>
<th>P</th>
<th>R</th>
<th>F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC* [32]</td>
<td>66.79 ± 1.41</td>
<td>96.47 ± 0.03</td>
<td>78.21 ± 4.37</td>
<td>86.39 ± 2.35</td>
</tr>
<tr>
<td>DSA* [30]</td>
<td>65.15 ± 3.03</td>
<td>96.69 ± 0.06</td>
<td>76.38 ± 4.67</td>
<td>85.34 ± 2.13</td>
</tr>
<tr>
<td>DM* [31]</td>
<td>69.29 ± 2.35</td>
<td>96.58 ± 0.79</td>
<td>78.21 ± 5.73</td>
<td>86.43 ± 2.24</td>
</tr>
<tr>
<td>GDD-FL (Ours)</td>
<td><strong>73.38 ± 1.50</strong></td>
<td><strong>96.79 ± 0.28</strong></td>
<td><strong>79.80 ± 10.68</strong></td>
<td><strong>87.48 ± 7.09</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Method</th>
<th>AUC</th>
<th>P</th>
<th>R</th>
<th>F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>DC* [32]</td>
<td>65.70 ± 2.47</td>
<td>96.83 ± 0.03</td>
<td>76.42 ± 4.13</td>
<td>85.42 ± 2.48</td>
</tr>
<tr>
<td>DSA* [30]</td>
<td>69.99 ± 0.32</td>
<td>96.80 ± 0.02</td>
<td>79.40 ± 1.89</td>
<td>87.24 ± 3.75</td>
</tr>
<tr>
<td>DM* [31]</td>
<td>69.07 ± 7.25</td>
<td>96.85 ± 0.73</td>
<td>76.75 ± 4.51</td>
<td>85.64 ± 3.28</td>
</tr>
<tr>
<td>GDD-FL (Ours)</td>
<td><strong>73.34 ± 1.28</strong></td>
<td><strong>96.86 ± 0.34</strong></td>
<td><strong>81.37 ± 7.34</strong></td>
<td><strong>87.72 ± 10.73</strong></td>
</tr>
</tbody>
</table>

We also present the visualizations of our synthetic data in Fig. 2, where the first row shows negative samples and the second row shows positive samples. Each column represents the synthetic images distilled by a different client. We observed that the synthetic images underwent style changes based on the original dermoscopy images and contain more texture and style information useful for training a classification model. However, these semantics make the appearance abnormal from the human view, and therefore, it is hard to tell what these images exactly represent.

3.4 Detailed Analysis

Ablation Analysis: We also conduct an ablation study to evaluate the impact of our proposed distribution change. Results are shown in Tab. 1, where we compare the performance of GDD-FL to that of the baseline data distillation
method, DM, and to the results of training a model with a randomly sampled subset of 10 or 100 images per class ("R.S.@10" and "R.S.@100"). The DM method is trained without distribution change. As seen from the table, when trained with the same number of samples, GDD-FL achieves significantly better AUC scores, with an improvement of nearly 6% over random sampling. Moreover, the comparison between DM and GDD-FL further confirms the effectiveness of our proposed distribution change. While the performance of DM drops slightly in the Non-IID setting, GDD-FL demonstrates stable performance across both IID and Non-IID settings. Notably, the significant improvement brought by GDD-FL suggests that the distribution change not only enhances generalization but also leads to more diverse semantics, thereby improving classification learning.

**Computation Analysis:** We further count the computational costs to make a comparison between GDD-FL and the traditional FedAVG. FedAVG trains the model in parallel for 1 hour, requiring 16848 MB GPU. Our method involves distillation training at local sites (1.2 hours, 9561 MB GPU) and classification training at the server (0.1 hours, 16848 MB GPU). It indicates that our method minimizes communication resources while using similar computational resources.

**Privacy Protection:** GDD-FL condenses numerous real images into a smaller set of synthetic images. By treating the synthetic images as learnable variables and inputting them along with real images into a fixed network, we minimize the discrepancy between their feature outputs. This training aligns the synthetic images with the overall distribution of the real dataset, rather than specific individual images. We also apply random perturbations to the real distribution, reducing privacy risks. Consequently, the synthetic data doesn’t contain precise personal information and is not part of the original dataset.

### 4 Conclusion

In this paper, we introduce a communication-efficient federated skin lesions classification framework using generalizable data distillation, named GDD-FL. Unlike current data distillation methods that align synthetic images to a fixed distribution, our GDD simulates the possible inter-client distribution drifts and produces synthetic images with better diversity and distribution alignment. The experimental results on the ISIC-2020 dataset demonstrate that our GDD-FL framework consistently outperforms other methods in terms of classification accuracy while reducing communication costs and protecting privacy.
References