# Enhanced Privacy in Optical Image Restoration: A Federated Deep Memory-Integrated Neural Network Approach

Muhammad Jahanzeb Khan [1], Suman Rath [2], and Muhammad Hassan zaib [2]

[1]University of Nevada
[2]Affiliation not available

December 7, 2023



**Abstract**

In the realm of remote sensing images, restoration and privacy preservation stand as dual challenges. While the intricate characteristics of these images render conventional restoration methods inadequate, concerns regarding data privacy pose a significant barrier to their optimal utilization. Addressing this multifaceted challenge, this study synergizes the Deep Memory Connected Network (DMCN) with federated learning, enabling data-driven model improvements without direct access to the raw image data. This federated approach, while bolstering data privacy, introduces inherent noise into the learning process. To counteract this, techniques such as Gaussian image denoising were employed, ensuring restoration quality. Notably, the federated DMCN exhibited commendable performance, showcasing only a marginal accuracy degradation in the face of noise. Downsampling Units, integral to DMCN, further contributed by reducing computational overheads. Comprehensive evaluations on remote sensing datasets underscore the promise of this federated approach, balancing data privacy with restoration fidelity, and charting a viable path for future applications.

# Enhanced Privacy in Optical Image Restoration: A Federated Deep Memory-Integrated Neural Network Approach

M. Jahanzeb Khan[1], Suman Rath[1], and Muhammad Hassan Zaib[2]

[1] Department of Computer Science and Engineering, University of Nevada, Reno, USA

[2] Department of Computer Science, Air University, Islamabad, Pakistan

**Abstract.** In the realm of remote sensing images, restoration and privacy preservation stand as dual challenges. While the intricate characteristics of these images render conventional restoration methods inadequate, concerns regarding data privacy pose a significant barrier to their optimal utilization. Addressing this multifaceted challenge, this study synergizes the Deep Memory Connected Network (DMCN) with federated learning, enabling data-driven model improvements without direct access to the raw image data. This federated approach, while bolstering data privacy, introduces inherent noise into the learning process. To counteract this, techniques such as Gaussian image denoising were employed, ensuring restoration quality. Notably, the federated DMCN exhibited commendable performance, showcasing only a marginal accuracy degradation in the face of noise. Downsampling Units, integral to DMCN, further contributed by reducing computational overheads. Comprehensive evaluations on remote sensing datasets underscore the promise of this federated approach, balancing data privacy with restoration fidelity, and charting a viable path for future applications.

**Keywords:** Federated Learning, Deep Memory Connected Neural Network (DMCN), Optical Remote Sensing, Image Restoration, Privacy Preservation, Distributed Machine Learning, Federated Image Processing, Data Privacy, Remote Sensing Data, Collaborative Machine Learning

## 1 Introduction

The widespread availability of high-resolution images and the progress in sensor technology have greatly enhanced the importance of optical remote sensing in several applications, including object detection and image classification [4, 6]. Nevertheless, despite the significant improvement in data quality, the difficulties related to image deterioration caused by ambient conditions, sensor noise, and other variables have become increasingly noticeable. Particularly in the field of object detection, even little image degradations can result in substantial differences in detection precision. Image noising is a special type of deterioration

that significantly impairs the effectiveness of object detection [5]. Therefore, the importance of picture restoration is clear and indisputable, since it not only improves visual quality but also maintains the precision of subsequent applications.

Conventional methods for image restoration have had challenges in keeping up with the sophisticated intricacies of modern remote sensing images, despite their effectiveness. Recent approaches, such as the Deep Memory Connected Neural Network (DMCN) [7], have attempted to overcome this limitation by utilizing the capabilities of deep learning to enhance the restoration procedure [1]. However, solely concentrating on image restoration fails to comprehensively tackle the overall difficulties. In order to achieve accurate object detection, it is important to use an integrated strategy that successfully addresses image noise while keeping the fundamental properties of the image.

Federated learning is a paradigm that decentralizes machine learning processes, ensuring both data privacy and more widespread network collaboration. The implementation of this technology in the field of remote sensing has the potential to completely transform the way data is utilized, especially for tasks such as object detection and image categorization [3]. By merging federated learning methodologies with sophisticated picture restoration techniques, it is possible to unite the advantages of both domains, guaranteeing superior image quality and resilient object detection.

Given the complicated environment of optical remote sensing images and the growing demand for precise object detection in such images, there is a clear need to efficiently reduce image noise. The success rate of object detection systems is severely impacted by image noise, which also reduces visual clarity. Although conventional restoration approaches offer temporary relief, there is a requirement for a more comprehensive solution that combines the advantages of advanced restoration techniques with the distributed capabilities of federated learning.

We propose a novel method that combines the advantages of modern image restoration techniques, specifically the DMCN, with the federated learning paradigm. This guarantees the restoration of images with superior quality, while simultaneously safeguarding the crucial characteristics necessary for object detection. Our methodology specifically deals with the issue of image noising and its impact on object detection. Our technique showcases substantial enhancements in detection accuracy, especially when dealing with degraded image conditions. In addition, we enhance our framework by incorporating feedback loops, which enable the distributed nodes to acquire knowledge not only from centralized updates but also from the achievements and shortcomings of peer nodes. This improves the resilience of the object detection process. In this paper, we thoroughly examine our technique, the empirical evidence supporting our assertions, and the wider ramifications of our work in the rapidly changing field of optical remote sensing.

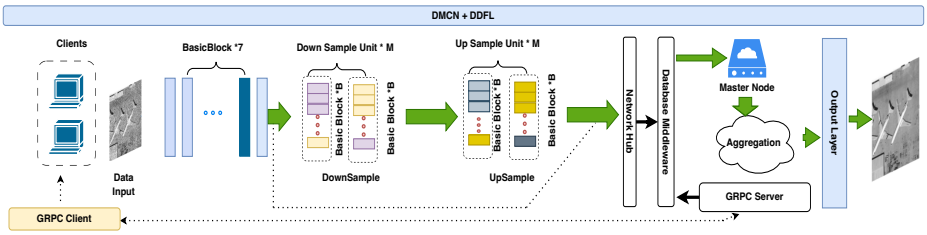


Fig. 1: DMCN + DDFL

## 2 Methodology

### 2.1 Architecture of DMCN

In this paper, we have integrated the potency of the Deep Multiscale Convolutional Neural Network (DMCN) [7] with the privacy-centric approach of Data-Decoupled Federated Learning (DDFL) [3]. This synergy is visually encapsulated in the architecture diagram, detailing a federated learning system where data remains localized on the client side while promoting robust model learning.

### 2.2 System Components and Workflow

**Clients and Data Input** The system commences with multiple clients, each equipped with a unique set of data. The data, visually represented as grayscale images in the architecture, suggests its applicability to image processing and computer vision tasks. Notably, data never leaves the client's premises, aligning with DDFL's principle of decoupling data from learning.

**Deep Multiscale Convolutional Neural Network (DMCN)** The heart of the architecture lies in the DMCN:

**BasicBlock * 7:** The model consists of seven sequential BasicBlocks, which are foundational convolutional blocks. Each block is adept at extracting features from the input data, with successive blocks refining these features for more complex patterns.

**Down Sample Unit * M:** Post initial feature extraction, the data is passed through 'M' down-sampling units. Down-sampling reduces the spatial dimensions of the data, compressing features and enabling the model to recognize larger patterns.

**Up Sample Unit * M:** After down-sampling, up-sampling units restore the data's spatial dimensions. These units help in refining and sharpening the features, making them more discernible. This duality of down-sampling followed by up-sampling creates a U-shaped network, often found effective in image segmentation tasks.

### 2.3 Middleware and Network Management

**Database Middleware** Positioned after DMCN's processing, the database middleware serves as the liaison between the neural network and various databases. By streamlining data requests and ensuring efficient data retrieval, it mitigates potential lags that might emanate from disparate databases.

**Network Hub** This centralized hub manages network requests, ensuring smooth data traffic flow. It plays a pivotal role in facilitating communication between the myriad clients and the master node.

**Master Node and Aggregation** The master node represents the fulcrum of the federated learning setup. All the model updates from clients converge here:

**Aggregation:** In this phase, the master node collates and aggregates model updates from diverse clients. Using FedAvg aggregation algorithm ensures that the global model benefits from the knowledge of all participating nodes.

**GRPC Communication** The architecture leverages GRPC [2], an efficient, open-source framework, for seamless remote procedure calls (RPCs):

**GRPC Client/Server:** This bi-directional setup ensures that clients can swiftly send their model updates to the master node and similarly receive refined model parameters for local updates. The usage of GRPC underscores the system's commitment to speed and efficiency.

**Output Generation** Post-aggregation and model refinement at the master node, the final model is adept at making predictions or inferences. The grayscale image at the architecture's terminus symbolizes this output, a culmination of collective learning without compromising data privacy. This architecture excels in its seamless integration. Data from the client undergoes transformation through DMCN, interacts with databases, and culminates in collective learning at the master node, all while DDFL principles ensure privacy and transfer of knowledge over raw data. In essence, it melds deep learning with federated learning's privacy focus, offering strong performance without centralized data risks, and heralding a new era of distributed machine learning systems.

## 3 Experiment

### 3.1 Datasets

To evaluate our approach, we utilize three datasets of different spatial resolutions: *UCMERCED:* [8] Features 21 land-use scene classes in high-resolution RGB. We use 80% for edge device training and the remaining for server testing.

### 3.2 Hardware Configuration

Our setup consists of three nodes: two as client nodes, each with a local model, and a master node overseeing the global model. The hardware for all nodes includes; *Processor:* Intel Xeon CPU E5-2690 v4 @ 2.60GHz, *RAM:* 377GB, *Network Interface:* 2x Ethernet Controller X710 for 10GbE SFP+, *GPU: Tesla P100-PCIE-12GB*. A shared high-speed network ensures efficient communication and model update transfers among nodes.

### 3.3 Network Depth and DDFL Consideration

The architecture's depth is regulated by two parameters: (1) M: Number of DownsampleUnit and UpsampleUnit incorporated in the DDFL framework, and (2) B: Number of Basic Blocks within each Unit.

To assess how varying depths affect performance in a DDFL setting, we experimented with diverse M and B combinations. As illustrated in Figure 7, depth fluctuates from 15 (with M = 1, B = 1) to 113 (M = 3, B = 8).

**Observations**:

1. For M = 1: A surge in PSNR was noted with growing B, attributed to the expanding receptive field.
2. For M = 2: PSNR ascends until B=3. Beyond B=4, the depth causes convergence difficulties within the 30-epoch limit.
3. For M = 3: The excessive depth, combined with the DDFL's data distribution mechanism, led to convergence challenges and possible loss of detail due to DownsampleUnits.

Incorporating performance and computational efficiency, our final model comprises M = 2 and B = 3, resulting in a depth of 38.

### 3.4 Federated Network Width and DDFL Configuration

Experiments were conducted to determine the most suitable network width for federated DDFL deployment. Various network widths of 32, 64, 128, and 256 were examined for processing 256x256 images. The optimal balance of efficiency and performance was achieved with a width of 64. Although wider networks are theoretically capable, the federated setting imposes computational constraints, leading to increased processing times. The integration of DDFL at this width is most conducive to the federated resources available.

### 3.5 Evaluation of Downsample and Upsample Units in DDFL

To deduce the ramifications of Downsample and Upsample Units within the DDFL framework, ablation experiments were conducted on the UCMERCED dataset. Table 2 encapsulates the results, highlighting that Downsample Units, when incorporated in a DDFL setup, markedly enhance speed and curtail memory utilization without compromising performance.

| **Width** | 32 | 64 | 128 | 256 |
|---|---|---|---|---|
| **Time (s)*** | 0.7054 | 1.4053 | 2.8604 | 5.1259 |
| **PSNR (dB)** | 29.99 | 30.06 | 29.99 | 29.94 |

Table 1: Federated DMCN performance with different network widths, showing average processing time and PSNR quality metrics.

| **Model** | **Memory (MB)** | **Time (Sec)** | **PSNR (dB)** |
|---|---|---|---|
| Dis_D_U | 8265 | 0.037 | 34.17 |
| DMCN | 3849 | 0.012 | 34.19 |
| DMCN + DDFL | 4821 | 0.193 | 33.68 |

Table 2: Comparison of the effects of integrating the DDFL approach with the DMCN model. The table provides an evaluation in terms of memory usage, processing time, and PSNR values. Dis_D_U serves as a baseline, representing a network without the Downsample and Upsample Units. The experiments are based on super-resolution tasks on the UCMERCED dataset with an upscale factor of 2.

### 3.6 Effect of Memory Connection in DDFL

The role of memory links in the DDFL structure was examined. Tests revealed that complete memory link integration achieved swift convergence and optimal results. In Figure 2, the red line denotes DMCN's PSNR, contrasted with the Bicubic interpolation method, depicted by the black dashed line. The green and blue lines display PSNR values with global and local memory links omitted, respectively.

Significantly, when all memory links are removed (yellow line), the network doesn't converge. The purple dashed line showcases the enhanced DMCN with DDFL, indicating its improved performance. These tests were conducted on super-resolution tasks using the UCMERCED dataset at an upscale factor of 2.

### 3.7 Batch Normalization (BN) and PReLU in DDFL

Incorporating DDFL, the influence of BN and PReLU was inspected. As indicated in Figures 3 and 4, the integration of PReLU enabled brisker convergence, and the synergy of BN and PReLU within the DDFL framework fostered optimal PSNR results.

### 3.8 Gaussian Denoising in Federated Learning: A Study on UCMERCED Dataset

In the realm of federated learning, image denoising remains pivotal, especially when handling datasets like UCMERCED. When it comes to denoising, one often

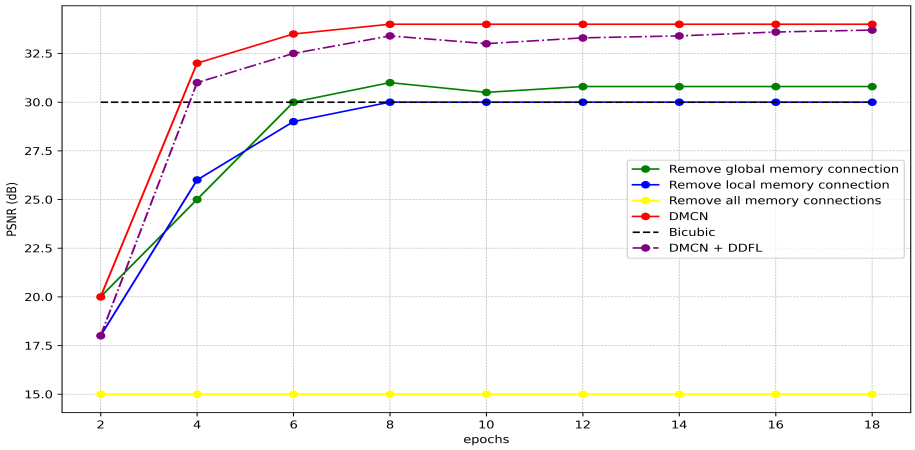


Fig. 2: Extended ablation study illustrating the importance of memory connections and the integration of DDFL within the DMCN framework.

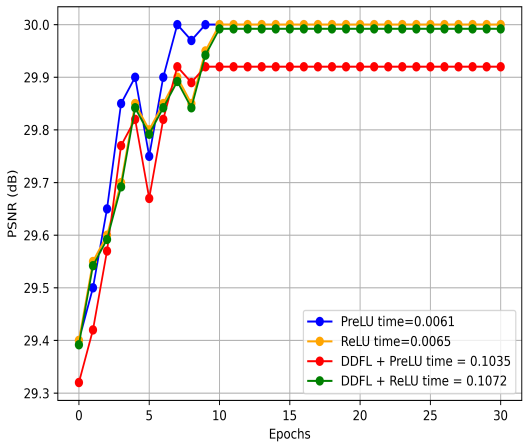


Fig. 3: PSNR (dB) results of networks with PReLU or without PReLU as baseline alongside with DDFL PReLU or without DDFL PReLU Time means the average time when processing an image measuring 256 $\times$ 256.

hypothesizes the underlying clean image, x, being disrupted by additive white Gaussian noise, N. Therefore, the resultant observed image can be described as y = x + N.

For our study, we adopted noise levels $\sigma = 15, 25, 35, 45$, and 55. We initiated training the DMCN-S specifically for Gaussian denoising at each noise level. Later, the DMCN-B model was extended to cater to blind noise levels by training it across the spectrum of noise levels. With this configuration, even if a test image

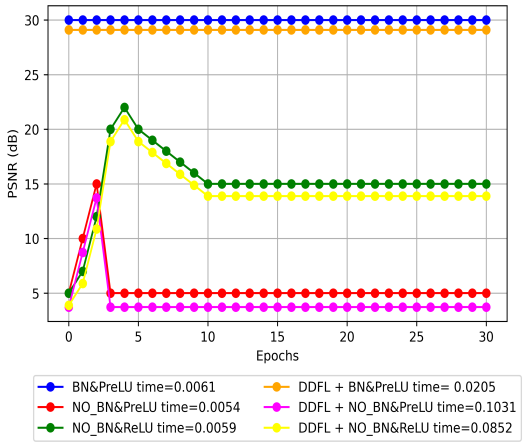


Fig. 4: PSNR (dB) results of networks with BN or without BN (as baseline) alongside with DDFL BN or without BN. Time means the average time of processing an image measuring 256 $\times$ 256.

| **Noise Level ($\sigma$)** | **Noisy** | **DMCN-B** | **DMCN-S** | **DDFL (B)** | **DDFL (S)** |
|---|---|---|---|---|---|
| 15 | 24.68/0.7928 | 32.30/0.9450 | 32.38/0.9672 | 31.80/0.9400 | 31.90/0.9622 |
| 25 | 20.32/0.7530 | 29.94/0.9132 | 30.07/0.9155 | 29.44/0.9100 | 29.57/0.9125 |
| 35 | 17.52/0.7094 | 28.45/0.8863 | 28.64/0.9031 | 27.95/0.8820 | 28.14/0.8990 |
| 45 | 15.50/0.6825 | 27.36/0.8627 | 27.59/0.8649 | 26.86/0.8580 | 27.09/0.8605 |
| 55 | 13.96/0.6177 | 26.49/0.8399 | 26.73/0.8597 | 25.99/0.8350 | 26.23/0.8550 |

Table 3: Evaluation on UC dataset

possesses an unknown noise level, the DMCN-B model can adequately denoise it.

**Training Specifics for Federated Learning** While focusing on the UCMERCED dataset within a federated learning context, the DMCN-S model dedicated to a particular noise level was trained. Training patches of 50 x 50 were extracted. Echoing past research methodologies, our denoising approach was confined to grayscale images. The learning rate was fixed at 1e-3, subjected to decay every ten epochs. ADAM optimizer was utilized, and the loss function outlined in Equation (3.8) was optimized. For comparative analysis, we benchmarked our approach against notable denoising methodologies like BM3D, WNNM, and DnCNN.

Given a distorted input image $Y$, our objective is to fine-tune the parameters $\Theta = \{W_i, b_i\}$ by minimizing the disparity between the ground truth high-resolution (HR) image $X$ and the reconstructed image $X_b = F(Y; \Theta)$. The loss

function for DMCN can be formulated as:

$$L(\Theta) = \frac{1}{n}\sum_{i=1}^{n} |cX_i - X_i|$$

**Quantitative Outcomes for UCMERCED Dataset** The UCMERCED dataset's performance metrics, namely PSNR and SSIM, for diverse denoising methods are presented in Table 3. The evaluation demonstrates the pronounced superiority of both DMCN-S and DMCN-B models in terms of PSNR compared to other models. Remarkably, even the DMCN-B model, which is crafted for blind noise levels, outperforms the DnCNN-S model, a specialized model for explicit noise levels.

Remote sensing images in the UCMERCED dataset pose significant challenges for most denoising networks due to their complexity. In this context, the superior performance of the DMCN model, even over the renowned DnCNN model, highlights its robustness in federated learning settings.

The DDFL models, though slightly less effective than the DMCN models, represent the trade-off between privacy preservation and performance. Methods like DDFL, while prioritizing data privacy, might introduce or inadequately remove noise. Still, their performance is commendable and emphasizes that data privacy in federated networks can be achieved without drastically compromising reliability.

In summary, the UCMERCED dataset analysis showcases the DMCN model's prowess in Gaussian denoising tasks and the balance between privacy and performance.

## 4 Conclusion

This paper introduces a federated learning system focused on data security and decentralized processes to bolster data privacy. Using datasets like UCMERCED, we demonstrated the robustness of our method. Our results reveal that merging the DDFL framework with Downsample and Upsample Units results in faster computation and reduced memory use without compromising performance.

Ablation studies underscore the pivotal role of memory links in DDFL, emphasizing faster convergence and improved outcomes when fully utilized. Incorporating PReLU accelerated convergence, while the combined effect of BN and PReLU yielded the best PSNR results in the DDFL setup.

Our analysis on Gaussian denoising, especially with the UCMERCED dataset, confirmed DMCN's superiority in handling both targeted and unknown noise scenarios. Notably, while DMCN outperformed the DnCNN model in processing intricate remote sensing images, the slight performance gap between DDFL and DMCN underlines the trade-offs between data privacy and peak performance.

In conclusion, our work pioneers a balance between data privacy and performance in federated learning, suggesting it can achieve robust confidentiality and competitive outcomes. Future studies could refine these methodologies, bridging the trade-off gap, and broadening their applicability.

## References


1. Chang, H., Yeung, D.-Y., and Xiong, Y. Super-resolution through neighbor embedding. In *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004. CVPR 2004.* (2004), vol. 1, pp. I–I.
2. Contributors, G. Grpc. `https://grpc.io`, 2021. Accessed: September 2021.
3. Khan, M. J., Tawose, O. T., Hu, R., and Zhao, D. Exploring the efficacy of data-decoupled federated learning for image classification and medical imaging analysis. In *International Workshop on Federated Learning for Distributed Data Mining* (2023).
4. Khan, M. J., Zafar, A., Tumanian, V., Yue, D., and Li, G. Object detection boosting using object attributes in detect and describe framework. In *2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI)* (2019), pp. 886–893.
5. Lampert, C. H., Nickisch, H., and Harmeling, S. Attribute-based classification for zero-shot visual object categorization. *IEEE Transactions on Pattern Analysis and Machine Intelligence 36*, 3 (2014), 453–465.
6. Sun, Z., Bebis, G., and Miller, R. Boosting object detection using feature selection. pp. 290– 296.
7. Xu, W., Xu, G., Wang, Y., Sun, X., Lin, D., and Wu, Y. Deep memory connected neural network for optical remote sensing image restoration. *Remote Sensing 10*, 12 (2018).
8. Yang, Y., and Newsam, S. Bag-of-visual-words and spatial extensions for land-use classification. In *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems* (New York, NY, USA, 2010), GIS '10, Association for Computing Machinery, p. 270–279.