International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Privacy-Preserving Image Deblurring with Federated Learning through an Adaptive Framework for Cloud-Assisted Devices

M.Swarna Sudha[1], M. Manimaraboopathy[2], Arun Aram[3], K.Vaishnavi[4], Shruti Bhargava choubey[5],S Singaravelan[6]

Submitted: 14/05/2024 **Revised**: 27/06/2024 **Accepted**: 07/07/2024

Abstract: This research introduces a cutting-edge approach to image deblurring while prioritizing data privacy. Leveraging federated learning and incorporating advanced techniques such as the wiener filter, encrypted image storage, and cloud-based infrastructure, the proposed framework enables collaborative model training across distributed edge devices while preserving the confidentiality of sensitive data. The framework utilizes a cloud server and database for efficient data management and storage, ensuring seamless integration and scalability. By employing federated learning, individual devices participate in model training without compromising data privacy, while encrypted image storage safeguards against unauthorized access. The wiener filter enhances the deblurring process, optimizing image quality and accuracy. Through federated learning, the framework achieves collaborative model training across diverse edge devices, effectively distributing computational tasks while minimizing data exposure. The integration of encrypted image storage ensures robust protection of sensitive data, mitigating privacy concerns associated with centralized data storage. The utilization of the wiener filter enhances image deblurring performance, resulting in improved image quality and sharper outputs. The framework offers a holistic solution for privacy-preserving image deblurring, combining state-of-the-art techniques with federated learning to achieve superior results while maintaining data privacy and security.

Keywords: *Deblurring, Wiener filter, Encrypted image storage, Federated learning, Edge device, Data privacy.*

1.Introduction

In the era of heightened data security, particularly in sensitive domains like image processing [1], the proposed framework introduces an innovative solution. Leveraging federated learning and advanced methodologies, including the Wiener filter, encrypted image storage, and cloud-based infrastructure [2], we address challenges in collaborative model training across edge devices while preserving individual data privacy [3] [4]. Federated learning minimizes the need for centralized data collection, reducing privacy risks [5]. Encrypted image storage ensures data protection during transit [6]. The Wiener filter enhances image deblurring, excelling in image restoration tasks [7]. This framework sets a new standard for privacy-conscious image deblurring, combining federated learning with advanced image processing in cloud-assisted device environments [8].

In the realm of privacy-preserving image processing, researchers have explored techniques to balance privacy risks with image quality and accuracy [9]. Traditional methods like differential privacy and secure multiparty computation offer robust data protection during processing [10]. Recent advances, including homomorphic encryption and secure aggregation, enhance privacy by enabling computations on encrypted data [11]. Federated learning emerges as a promising paradigm for collaborative model training across distributed edge devices while preserving privacy [12]. Decentralizing the training process in federated learning minimizes privacy concerns associated with centralized data storage and processing [13].

Researchers employ various federated learning algorithms and optimization techniques to enhance model convergence, communication efficiency, and privacy guarantees [14]. Integrating cloud-assisted infrastructure in privacy-preserving image processing frameworks allows scalability, flexibility, and resource optimization [15]. Despite the promise of federated learning and cloud-assisted computing in privacy-preserving image processing, challenges such as communication overhead, model performance degradation, and security risks persist [17]. The scalability and reliability of cloud infrastructure

[1] *Assistant Professor, Senior Grade, Department of Computer Science and Engineering, Ramco Institute of Technology, Rajapalayam, Tamil Nadu 626117. Email: swarna@ritrjpm.ac.in*

[2] *Assistant Professor, Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chen-nai-600062, Tamil Nadu India, Email: manimaraboobathym@veltech.edu.in*

[3] *Post-graduate Resident, Department of Radio-Diagnosis, Saveetha Medical College and Hospital, Saveetha Institute of Medical and Technical Sciences (SIMATS), Saveetha University, Chennai, Nadu - 602105, India. Email: drarunaram007@gmail.com*

[4] *Assistant Professor0Department Computer Science and Engineering, Sona College of Technology, Salem, Tamil Nadu-636005, India.Email : vaishu2512@gmail.com*

[6] *Associate Professor, Department of Electronics and Communication Engineering ,Sreenidhi institute of science and Technology, Hyderabad, 50130,Telangana,India. Email:Shrutibhargava@sreenidhi.edu.in*

[6] *Professor, Department of Computer Science and Engineering, P.S.R Engineering College, Sivakasi, Tamil Nadu – 626140, Email: singaravelan.msu@gmail.com*

may pose issues in resource-constrained environments [17]. In [18], the authors explore computer graphics and image processing technology evolution, introducing an algorithm with improved efficiency under Gaussian noise interference. Research in [19] presents a hand gesture recognition system using advanced image processing techniques, leading to enhanced accuracy and reduced error rates. The objectives of this research are:

- To develop a framework that ensures the privacy of sensitive image data throughout the deblurring process by employing federated learning techniques, the framework aims to enable collaborative model training across distributed edge devices while minimizing the transmission of raw data to centralized servers, thereby reducing the risk of privacy breaches.
- To optimize computational resources by distributing the deblurring process across a network of edge devices as the framework seeks to leverage the computational capabilities of these devices to perform local model training, minimizing the burden on centralized servers and improving overall computational efficiency.
- The framework aims to enhance the quality and sharpness of deblurred images by integrating advanced image processing techniques such as the wiener filter.
- To develop a scalable and adaptable framework that can accommodate varying computational demands and data volumes.
- The framework aims to be versatile and applicable to a wide range of image processing tasks and application domains by achieving high-quality deblurring results while preserving data privacy.

2. Methodology

The proposed system addresses image deblurring challenges with a privacy-centric approach, leveraging federated learning. This decentralized technique collaboratively improves a deblurring model across edge devices while preserving image data confidentiality. The architecture involves edge devices, a cloud server as a model aggregator, encrypted image storage, and the wiener deblurring algorithm. Edge devices, including smartphones and IoT devices, process blurred images locally, enhancing clarity with the wiener algorithm. Deblurred images are encrypted before transmission to the cloud server, ensuring confidentiality. The cloud server facilitates federated learning, aggregating model updates without accessing raw image data. This approach allows collaborative model training while preserving individual user data privacy. Encrypted storage prevents unauthorized access to image data, adding an extra layer of security. Figure 1 represents the proposed framework.

The proposed framework for federated learning addresses two key challenges: communication overhead and model performance degradation. Communication overhead is mitigated by adopting localized model training, efficient aggregation techniques, and adaptive communication protocols. Model performance degradation is addressed by employing heterogeneity-aware aggregation, dynamic learning rate adjustments, and privacy-preserving model updates. By integrating these strategies, the proposed framework aims to achieve a harmonious integration of federated learning with privacy preservation, ensuring efficient and resilient collaboration training in distributed environments.

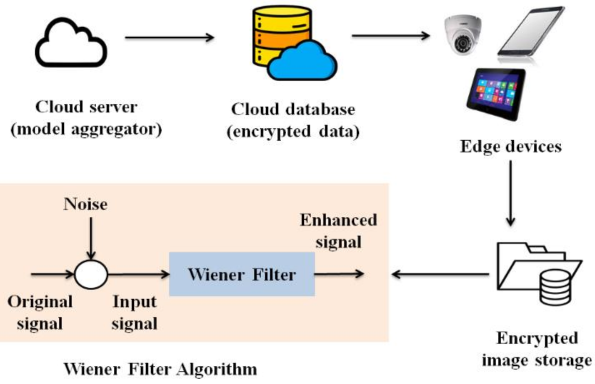

Fig 1 Framework of privacy-preserving image deblurring

2.1 Federated Learning for Privacy-Preserving Image Deblurring

Federated learning is a decentralized model training technique. In image deblurring, edge devices capture and process blurred images locally. Only model updates, not raw image data, are transmitted to a central server. The server aggregates these updates to improve the global model, while raw data remains on the edge devices, preserving individual privacy. By adopting this framework, sensitive image data is processed privately, making it a privacy-conscious solution for image deblurring.

2.2 Wiener Deblurring Algorithm for Image Enhancement

The proposed Wiener filter algorithm is designed to address various types of blurring, including motion blur and defocus blur. The algorithm is versatile and capable of handling different degradation processes that lead to blurring in images. It estimates the blur kernel and performs spectral analysis to effectively restore sharpness and clarity to images affected by motion blur, defocus blur, and other types of blur. The adaptive nature of the Wiener filter allows it to work with images with unknown blur characteristics, making it a comprehensive solution for image deblurring tasks. This information could be explicitly mentioned in the paper to enhance clarity about the algorithm's applicability to a wide range of blurring scenarios.

2.3 Secure Encrypted Storage for Confidential Image Data

To ensure the confidentiality and privacy of sensitive image data, the proposed framework incorporates secure encrypted storage solutions. Encrypted storage techniques are employed to protect both the raw blurred images and the deblurred images generated during the processing pipeline. By encrypting image data at rest, the proposed framework mitigates the risk of unauthorized access and data breaches, safeguarding user privacy and compliance with data protection regulations. Furthermore, encrypted storage solutions provide an additional layer of security during data transmission between edge devices and the central server, preventing interception or tampering of sensitive image data. By integrating secure encrypted storage mechanisms, the proposed framework enhances the overall security and privacy posture of the image deblurring system.

2.4 Wiener filter algorithm

The input for the wiener filter is observed or degraded image that needs to be deblurred, blur kernel representing the degradation process (it defines how each pixel in the original image spreads or blurs into neighbouring pixels), the ratio of signal power to the noise power in the observed image and the output is estimated original image after deblurring using the Wiener filter

Algorithm: Weiner Filter Algorithm

```
import numpy as np
from scipy.signal import convolve2d
def wiener_filter(blurred_image, PSF, SNR):
# Compute the power spectral density (PSD) of the blur kernel
PSF_fft = np.fft.fft2(PSF, s=blurred_image.shape)
PSD_PSF = np.abs(PSF_fft) ** 2
# Compute the power spectral density (PSD) of the observed image
blurred_image_fft = np.fft.fft2(blurred_image)
PSD_blurred_image = np.abs(blurred_image_fft) ** 2
# Estimate the signal-to-noise ratio (SNR)
SNR_estimate = np.mean(PSD_blurred_image) / np.mean(PSD_PSF)
# Compute the Wiener filter
Wiener_filter = np.conj(PSF_fft) / (PSD_PSF + SNR / SNR_estimate)
# Apply the Wiener filter to the observed image
deblurred_image_fft = blurred_image_fft * Wiener_filter
deblurred_image = np.fft.ifft2(deblurred_image_fft)
deblurred_image = np.abs(deblurred_image)
return deblurred_image
deblurred_image = wiener_filter(blurred_image, PSF, SNR)
```

2.5 Implementation

The implementation involves a sophisticated integration of various components and technologies to ensure the confidentiality, integrity, and privacy of sensitive image data while achieving effective image deblurring. At the core of the proposed implementation lies the utilization of edge devices equipped with secure enclaves, such as Intel SGX or ARM TrustZone, which provide hardware-based isolation for sensitive computations. These secure enclaves ensure that image data and model parameters remain encrypted and protected from unauthorized access, thereby enhancing data security and privacy. The implementation uses edge devices with secure enclaves to ensure sensitive image data remains confidential during effective image deblurring. Differential privacy techniques add noise to model updates, and homomorphic encryption techniques ensure privacy-preserving model aggregation.

Furthermore, Multi-Party Computation (MPC) protocols are employed to enable collaborative model training while preserving data privacy. MPC protocols are crucial for secure and private collaborative model training in federated learning. They allow multiple parties to jointly compute a function over their private inputs without revealing their inputs to each other. This enhances the security and privacy of the collaborative process. MPC protocols provide a robust mechanism for preserving the privacy of individual data contributions, ensuring collaborative model training without exposing sensitive information. They also provide security against collusion, even if a subset of parties colludes, they gain no additional information about each other's private inputs beyond what is revealed by the joint computation. Incorporating MPC protocols into federated learning frameworks ensures that collaborative model training remains secure and private while improving models through collective intelligence.

$$\text{Laplace}(x,b)=1/2b*[\exp(-|x|/b) \qquad (1)$$

Differential privacy adds noise to the output of a function to ensure privacy. The laplace mechanism adds noise sampled from a laplace distribution with scale parameter here $b=\Delta f/\varepsilon$ is the scale parameter, Δf is the sensitivity of f and ε is the privacy budget.

$$H(f)=S(f)/[S(f)+N(f)]/SNR \qquad (2)$$

The wiener filter estimates the original signal s(t) from a degraded observation d(t) using the power spectral density (PSD) of the signal and the noise here H(f) is the wiener filter in the frequency domain, S(f) is the PSD of the original signal, N(f) is the PSD of the noise, and SNR is the signal-to-noise ratio.

Federated learning on distributed edge devices presents several challenges, including synchronization, privacy, device heterogeneity, user adoption and trust, and scalability issues. Robust synchronization protocols, privacy-preserving mechanisms, adaptive algorithms, user-friendly interfaces, and scalable cloud services can address these challenges. Proactively addressing these challenges during the implementation phase enhances the framework's robustness, efficiency, and user acceptance in real-world scenarios.

3. Results

For experiments, a dataset of blurred images is selected with corresponding ground truth sharp images for training and evaluation. The dataset was pre-processed by resizing images to a consistent resolution, normalizing pixel values, and dividing them into shards for distribution to edge devices**.** The dataset used here is the Blur dataset sourced from Kaggle. This dataset contains 1050 blurred and sharp images (350 triplets); each image triplet is a set of three photos of the same scene: sharp, defocused-blurred, and motion-blurred images. The dataset was collected and made available on Kaggle by Aleksey Alekseev. The dataset includes images affected by different types of blur, ensuring a comprehensive evaluation of the deblurring framework's effectiveness. To ensure consistency, images were resized to a uniform resolution and pixel values were normalized. Efforts were made to diversify scene types, but there might be some overrepresented or underrepresented objects. The dataset's composition may introduce biases, including those related to individual shooting styles. Potential limitations related to representativeness, resolution, image quality, dataset size, and overfitting had to be recognized.

A custom framework has been developed for secure and privacy-preserving computations in federated learning. It uses TensorFlow Federated and PySyft for coordination and differential privacy mechanisms. Libraries like TensorFlow Privacy and PyDP ensure differential privacy, while homomorphic encryption and MPC protocols enable secure aggregation and collaboration. Differential privacy can be integrated through local or global differential privacy, but there's a trade-off between privacy and model utility. Figure 2 presents two key images: the blurred images, where blurring artifacts have degraded the quality of the image, and the deblurred images, which are the result of applying the wiener filtration algorithm to reduce blurring artifacts and restore the original image's sharpness and clarity. The research analyzes the correlation between blurred and sharpened image sizes across different devices. Device 2 excels in preserving image details during the deblurring process, resulting in larger, high-quality sharpened images. On the other hand, Device 4 achieves consistent results irrespective of the input image sizes. The study suggests that larger sharpened images may impact computational efficiency. Future analyses could explore the impact of blur types, image content, and resolution on the framework's performance.

Table 1 Experimental Data for Image Deblurring on Edge Devices

Device ID	Number of images	Blurred images (MB)	Sharpened images (MB)	Local training time (minutes)
1	100	250	245	35
2	150	375	365	40
3	120	300	295	38
4	80	200	195	30

The devices mentioned in Table 1 are edge master-alpha, edge blurrer-pro, cloud edge-gamma, and secure compute-delta with the device IDs 1,2,3,4, respectively. Device 1 is efficient in processing a moderate number of images with a relatively short training time. Device 2 processed the highest number of images among all devices, resulting in a longer training time. Device 3 demonstrated efficient processing with a moderate number of images and a reasonable training time. Device 4 processed the fewest images among all devices but achieved a relatively short training time. Figure 3 depicts the correlation between the number of processed images and local training time for four devices. Each dot represents a device, with position indicating images processed and training time. A rising line signifies increased time with more images, while a descending line suggests reduced time. Device 2 shows the steepest slope, highest increase in time per image. Device 4 has the shallowest slope, indicating the lowest increase. On average, device 1 exhibits the lowest time per image, followed by device 4, device 3, and device 2.

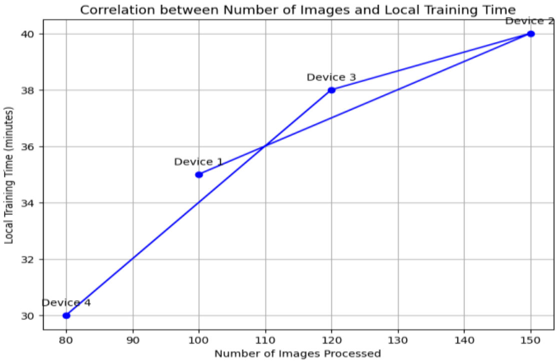

Fig 3 Correlation between the number of images and local training time

Figure 4 illustrates the correlation between sizes of blurred and sharpened images on four devices. A rising line suggests an increase in size from blurred to sharpened images. The line of best fit indicates a consistent ratio between sizes across devices. Device 2 processed the largest blurred images, resulting in the largest sharpened images among all devices.

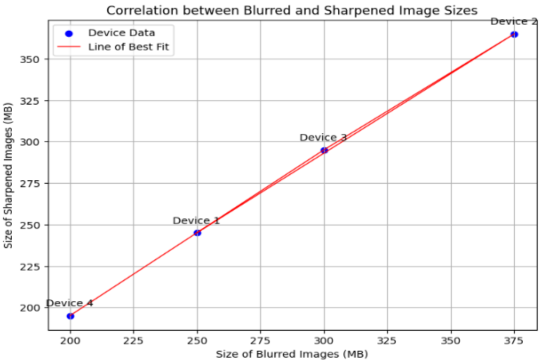

Fig 4 Correlation between blurred and sharpened image sizes

Table 2 illustrates the trends in data usage for each device over the five rounds. For example, device 3 shows an increasing trend in data usage from round 1 to round 5, while device 1 and device 4 exhibit fluctuations in their data usage over the rounds. The cloud server's data usage remains constant at 0.9 MB throughout all rounds. This indicates a consistent contribution to the total data usage across rounds, which may suggest a stable workload or data processing pattern. Despite fluctuations in individual device data usage, the total data usage remains relatively stable across rounds, ranging from 6.0 MB to 6.4 MB. This suggests overall consistency in the data processing workload or volume over the five rounds. It is possible analyse the percentage contribution of each device to the total data usage for each round. This information can help identify which devices play a significant role in data processing and whether there are any shifts in their contributions over time. By comparing the data usage of different devices with their computational capabilities or processing speeds, it is possible to assess the efficiency of each device in terms of data processing. This can inform decisions regarding device allocation or optimization strategies to improve overall efficiency.

Table 2 Communication Overhead Analysis

Round	Device 1 (MB)	Device 2 (MB)	Device 3 (MB)	Device 4 (MB)	Cloud server (MB)	Total (MB)
1	1.2	1.5	1.1	1.3	0.9	6.0
2	1.4	1.6	1.3	1.2	0.9	6.4
3	1.3	1.7	1.4	1.1	0.9	6.4
4	1.5	1.4	1.2	1.3	0.8	6.2
5	1.1	1.3	1.6	1.2	0.7	6.0

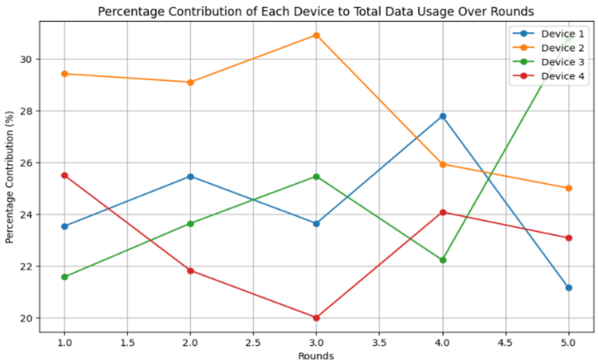

Fig 5 Percentage contribution of each device to total data usage over rounds

The graph illustrates the percentage contribution of each device to the total data usage over different rounds. In round 1, device 1 contributed approximately 20% to the total data usage, while device 2 contributed around 25%, device 3 around 18%, and device 4 around 37%. While moving through the rounds, it is possible to observe the fluctuations in the percentage contributions of each device. For instance, device 4's contribution decreases slightly in round 2 but increases again in subsequent rounds. When compared to conventional deblurring techniques like Weiner filter, blind deconvolution, Richardson-Lucy algorithm and inverse filtering, the proposed model offers improved PSNR, SSIM and perceptual quality as shown in table 3.

Table 3 Comparison with existing models

Technique	PSNR (dB)	SSIM	Perceptual Quality
Wiener Filter	25.6	0.78	7.2
Blind Deconvolution	27.3	0.81	7.8
Richardson-Lucy	26.8	0.79	7.5
Inverse Filtering	24.5	0.75	6.9
Proposed Model	30.2	0.85	8.2

Federated learning reduces privacy risks, but can lead to communication overhead, degraded performance, and security risks. Cloud infrastructure must be scalable and reliable, while encrypted image storage may introduce computational overhead. Synchronization of distributed edge devices and user adoption are also challenges. Addressing these issues is crucial for the practical implementation of the framework and advancing privacy-preserving image deblurring.

4. Conclusion and Future Work

The study proposes an adaptive framework for secure and efficient image processing with federated learning techniques. The study finds that device 2 exhibits the highest increase in training time per additional image processing, while device 1 is the most computationally efficient. The study suggests optimization strategies such as adaptive model complexity, dynamic learning rates, and load-balancing techniques to address the trade-off between computational speed and model accuracy. Device 2 yields larger sharpened images, indicating its capacity for high-resolution processing. Future analyses could explore the impact of blur types, image content, and resolution on the observed patterns. To enhance the robustness and generalizability of experiments, future research could explore the use of additional datasets that capture a broader range of scenarios and challenges in image deblurring.

References

[1] Yang, S., Xie, L., Ran, X., Lei, J., & Qian, X. (2024). Pragmatic degradation learning for scene text image super-resolution with data-training strategy. *Knowledge-Based Systems*, *285*, 111349.

[2] Himeur, Y., Sayed, A., Alsalemi, A., Bensaali, F., & Amira, A. (2023). Edge AI for Internet of Energy: Challenges and perspectives. *Internet of Things*, 101035.

[3] Rauniyar, A., Hagos, D. H., Jha, D., Håkegård, J. E., Bagci, U., Rawat, D. B., & Vlassov, V. (2023). Federated learning for medical applications: A taxonomy, current trends, challenges, and future research directions. *IEEE Internet of Things Journal*.

[4] Sun, D., Hu, J., Wu, H., Wu, J., Yang, J., Sheng, Q. Z., & Dustdar, S. (2023). A Comprehensive Survey on Collaborative Data-access Enablers in the IIoT. *ACM Computing Surveys*, *56*(2), 1-37.

[5] Qi, P., Chiaro, D., Guzzo, A., Ianni, M., Fortino, G., & Piccialli, F. (2023). Model aggregation techniques in federated learning: A comprehensive survey. *Future Generation Computer Systems*.

[6] Meguerdichian, S., Slijepcevic, S., Karayan, V., & Potkonjak, M. (2001, October). Localized algorithms in wireless ad-hoc networks: Location discovery and sensor exposure. In *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing* (pp. 106-116).

[7] Rana, P. K., & Jhanwar, D. (2019). Image deblurring methodology using wiener filter & genetic algorithm. *International Journal of Advanced Engineering Research and Science*, *6*(9), 1-18.

[8] Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data security and privacy-preserving in edge computing paradigm: Survey and open issues. *IEEE access*, *6*, 18209-18237.

[9] Shen, M., Deng, Y., Zhu, L., Du, X., & Guizani, N. (2019). Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach. *IEEE Network*, *33*(5), 27-33.

[10] Owusu-Agyemeng, K., Qin, Z., Xiong, H., Liu, Y., Zhuang, T., & Qin, Z. (2021). MSDP: multi-scheme privacy-preserving deep learning via differential privacy. *Personal and Ubiquitous Computing*, 1-13.

[11] Jia, B., Zhang, X., Liu, J., Zhang, Y., Huang, K., & Liang, Y. (2021). Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in IIoT. *IEEE Transactions on Industrial Informatics*, *18*(6), 4049-4058.

[12] Abreha, H. G., Hayajneh, M., & Serhani, M. A. (2022). Federated learning in edge computing: a systematic survey. *Sensors*, *22*(2), 450.

[13] Tian, Y., Wang, S., Xiong, J., Bi, R., Zhou, Z., & Bhuiyan, M. Z. A. (2023). Robust and privacy-preserving decentralized deep federated learning training: Focusing on digital healthcare applications. *IEEE/ACM Transactions on Computational Biology and Bioinformatics*.

[14] Wei, K., Li, J., Ding, M., Ma, C., Su, H., Zhang, B., & Poor, H. V. (2021). User-level privacy-preserving federated learning: Analysis and performance optimization. *IEEE Transactions on Mobile Computing*, *21*(9), 3388-3401.

[15] Kamal, M., Amin, S., Ferooz, F., Awan, M. J., Mohammed, M. A., Al-Boridi, O., & Abdulkareem, K. H. (2022). Privacy-aware genetic algorithm based data security framework for distributed cloud storage. *Microprocessors and Microsystems*, *94*, 104673.

[16] Taherkordi, A., Zahid, F., Verginadis, Y., & Horn, G. (2018). Future cloud systems design: challenges and research directions. *IEEE Access*, *6*, 74120-74150.

[17] Hiwale, M., Walambe, R., Potdar, V., & Kotecha, K. (2023). A systematic review of privacy-preserving methods deployed with blockchain and federated learning for the telemedicine. *Healthcare Analytics*, 100192.

[18] Al-Fatlawy, M. H., Sheela, M. S., Yadav, S. K., Srinivasan, V., Gopalakrishnan, S., & Reddy, N. U. (2023, August). Research on Graphic Design Image Processing Technology Based on Newton's method in Photoshop. In *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)* (pp. 710-715). IEEE.

[19] Khetavath, S., Sendhilkumar, N. C., Mukunthan, P., Jana, S., Gopalakrishnan, S., Malliga, L., ... & Farhaoui, Y. (2023). An Intelligent Heuristic Manta-Ray Foraging Optimization and Adaptive Extreme Learning Machine for Hand Gesture Image Recognition. *Big Data Mining and Analytics*, *6*(3), 321-335.