Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1473–1486
DOI : 10.47974/JDMSC-2146

A discrete mathematical model and cryptography for secure medical image analysis : Encrypted chest X-ray classification

Ajit Noonia [#]
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Deepti Thakral [†]
Department of Computer Science and Technology
Manav Rachna University
Faridabad 121004
Haryana
India

Priya Mathur [§]
Department of Mathematics
Poornima Institute of Engineering & Technology
Jaipur 302022
Rajasthan
India

Farhan Sheth [‡]
Hammad Shaikh [@]
Amit Kumar Gupta *
Department of Computer Science & Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

[#] *E-mail:* **ajit009noonia@gmail.com**
[†] *E-mail:* **deeptithakral@mru.edu.in**
[§] *E-mail:* **drpriyamathur21@gmail.com**
[‡] *E-mail:* **farhansheth.jb@gmail.com**
[@] *E-mail:* **hammad.shaikh1105@gmail.com**
* *E-mail:* **dramitkumargupta1983@gmail.com;(Corresponding Author)**
amit.gupta@jaipur.manipal.edu

Abstract

This research presents a privacy-preserving approach to chest X-ray image classification utilizing deep learning techniques integrated with Advanced Encryption Standard (AES) encryption and Fully Homomorphic Encryption (FHE) to maintain data confidentiality. The methodology employs various Convolutional Neural Network (CNN) models to classify chest X-rays into three categories: normal, COVID-19 infected, and pneumonia infected, without decrypting the data. The process involves preprocessing the images, determining optimal hyperparameters, and fine-tuning the CNN models through transfer learning. The models evaluated include ResNet50, ResNet101, MobileNetV3 Small, MobileNetV3 Large, DenseNet121, and DenseNet161, with performance metrics such as accuracy, F1-score, precision, recall (sensitivity), and specificity used for comprehensive assessment. Among the tested models, DenseNet161 achieved the highest accuracy of 92.28%, followed by DenseNet121 and ResNet50 with accuracies of 91.41% and 91.26%, respectively. This study demonstrates the feasibility and effectiveness of combining encryption with deep learning for secure and accurate medical image analysis, thereby addressing the critical need for privacy in medical diagnostics.

Subject Classification: *68T07, 68P25.*

Keywords: *Advanced encryption standard, Fully homomorphic encryption, Medical image classification, Privacy-preserving techniques, Chest x-ray analysis, Transfer learning.*

1. Introduction

In the era of digital health, ensuring the privacy of sensitive medical data while achieving accurate diagnostics is a critical challenge. This paper introduces an innovative methodology that integrates Advanced Encryption Standard (AES) cryptography, Fully Homomorphic Encryption (FHE), and Convolutional Neural Networks (CNNs) within a discrete mathematical model framework to securely classify chest X-ray images. AES is a well-established cryptographic technique known for its robustness in securing digital information, while FHE enables computations on encrypted data without decryption, ensuring the confidentiality of patient information. By applying these cryptographic methods in conjunction with advanced CNN architectures, this research aims to maintain data privacy while accurately categorizing chest X-rays into normal, COVID-19 infected, and pneumonia infected classes. The methodology involves preprocessing chest X-ray images, optimizing hyperparameters, and fine-tuning various CNN models through transfer learning. Models evaluated include ResNet50, ResNet101, MobileNetV3 Small, MobileNetV3 Large, DenseNet121, and DenseNet161, with performance assessed based on accuracy, F1-score, precision, recall (sensitivity), and specificity. This approach not only demonstrates the feasibility of analysing encrypted medical images but also highlights the potential of discrete mathematical models in enhancing the security and effectiveness of medical image analysis.

2. Related Study

Aa Recent advancements in cryptography and machine learning have led to significant developments in both fields. [1] introduced the AES, a symmetric key encryption algorithm that has become fundamental in secure communications and data storage. [2] review recent innovations in CNNs, noting their superior performance in image classification and other vision tasks. [3] further advanced cryptography with his fully homomorphic encryption scheme, enabling computations on encrypted data without decryption. This breakthrough has profound implications for data privacy, particularly in cloud computing. The availability of medical imaging datasets, such as the "COVID19, Pneumonia and Normal Chest X-ray PA Dataset" compiled by [4], has facilitated the development of automated diagnostic tools. Preprocessing techniques, as discussed by [5], along with data augmentation methods reviewed by [7], are critical for enhancing the performance of CNNs. [6] demonstrate the feasibility of classifying encrypted images using deep learning models like ResNet50. [7-8] emphasize the impact of data normalization on classification accuracy, while These combined efforts underscore the interdisciplinary nature of advancements in cryptography and machine learning, driving progress in secure data processing and intelligent image analysis. Moreover, research by [9] highlights the implementation of AES in microprocessor-based IoT devices, addressing the balance between security and performance in resource-constrained environments. In addition to AES, [10] provide a comparative analysis of various encryption algorithms, aiding in the selection of appropriate methods for different applications. The specific challenge of encrypting low-detail images has been tackled by [11], who proposed a method using Rijndael and RC6 block ciphers in the electronic codebook mode. This paper presents a novel approach integrating AES cryptography, Fully Homomorphic Encryption (FHE), and CNNs within a discrete mathematical model framework to securely classify chest X-ray images while preserving data privacy.

3. Methods and Material

The methodology adopted for this research employs a privacy-preserving approach to chest X-ray image classification using deep learning techniques. The methodology integrates two crucial components, AES [1] encryption for data privacy with multiple models of CNN [2] for image classification. This novel approach aims to accurately categorize chest X-rays into three distinct classes—normal, COVID-19, and pneumonia infected—while maintaining the confidentiality of patient's data, without decrypting it. By combining encryption with deep learning, we address the critical need for privacy in medical image analysis using a privacy preserving technique—FHE [3] while leveraging the power of machine learning for diagnostic support. Figure 1 illustrates the overview of the methodology.

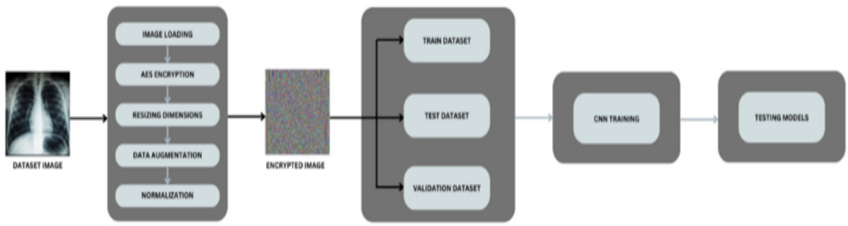

Figure 1

Preprocessing and training demonstration

3.1 *Dataset Characteristics*

The study utilizes a publicly available dataset 'COVID19, Pneumonia and Normal Chest X-ray PA Dataset' uploaded on Mendeley [4], it's a comprehensive collection comprising 4,575 chest X-ray images. These images are equally distributed across three classes: normal chest, COVID-19 infected, and pneumonia infected, with each class containing 1,525 samples. This balanced distribution ensures robust model training and evaluation across all categories. The dataset undergoes several preprocessing steps, including AES [1] encryption for privacy preservation, image resizing for standardization, and various transformations to enhance model learning. These preprocessing [5] techniques are carefully designed to maintain image integrity while adapting the data for optimal neural network performance. Figure 2 showcases a sample image from each class of the dataset.

Figure 2

Sample Images from The Dataset

3.2 Preprocessing

Preprocessing is a crucial in Machine Learning. In the study, it plays a pivotal role in classification of the encrypted images [6] using CNN models as it augments dataset, improve its quality and optimizes model efficacy.

3.2.1 Preprocessing

The preprocessing pipeline employed in this study standardizes all chest X-ray images to 256x256 pixels, balancing detail preservation with computational efficiency. To enhance model robustness, we implement data augmentation techniques [7] on the training set, including random horizontal flips and rotations (±10 degrees). These augmentations simulate variations in patient positioning and X-ray capture angles, effectively expanding the dataset and improving model generalization. The images then undergo tensor conversion and normalization [8], preparing them for efficient processing by the deep learning model.

3.2.2 AES Encryption (Privacy Preserving)

A key innovation in this methodology is the implementation of AES encryption [1] to protect patient privacy. Utilizing the PyCryptodome library's AES module [9], we employ a sophisticated encryption process [10]. A random 16-byte key is generated for each encryption session, ensuring unique protection for each training. The encryption process involves converting each image to an array, flattening it, applying padding to meet AES block size requirements, and then encrypting using AES in Electronic Codebook (ECB) mode [11]. Post-encryption, the data is reshaped back into the original image dimensions. This process ensures the privacy and confidentiality of sensitive medical information while still allowing for effective machine learning analysis, addressing a critical concern in medical data handling. Figure 3 describes the working on AES encryption in our study.

3.2.3 Dataset Splitting

To ensure a robust evaluation of our model, we implemented a systematic approach to partition our chest X-ray dataset. The dataset is split into three distinct subsets: training, testing, and validation. This split ratio of 70:15:15 for training, testing, and validation respectively allows for effective model training while providing sufficient data for unbiased performance [12] evaluation and validation.

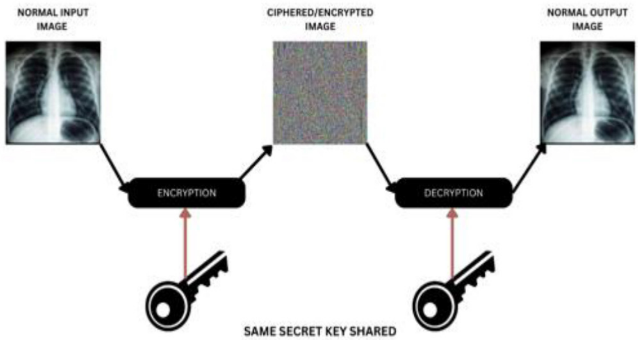

Figure 3

Working Of AES Encryptions

3.3 *Convolutional Neural Network*

CNNs [2] have revolutionized the field of computer vision [13], offering unprecedented accuracy in image analysis tasks. Subsequent pooling layers [14] down sample these feature maps, reducing computational complexity while retaining essential information. The architecture typically culminates in fully connected layers that interpret the extracted features for classification or other tasks. Recent advancements in CNN architectures, such as residual connections [15] and inception modules, have further enhanced their performance and trainability.

$$f(x) = \sigma(W * x + b) \tag{1}$$

Where f(x) is the output feature map σ is the activation function (e.g., ReLU) W is the weight matrix (convolutional kernel) x is the input b is the bias term.

Multiple State-of-the-art CNNs are employed in the study, among which is ResNet50, it's a 50-layer deep convolutional neural network [16] that introduced residual learning. It uses skip connections to address the vanishing gradient problem in deep networks. The core idea is:

$$H(x) = F(\mathrm{x}) + x \tag{2}$$

Where F(x) is the residual function, x is the identity function, and H(x) is the desired underlying mapping. The use of batch normalization, ReLU activation, and skip connections allows for efficient training of this deep architecture. ResNet101 [20] is an extension of ResNet50 with 101 layers, offering deeper feature extraction. It uses the same residual learning principle as ResNet50. MobileNetV3 Small [17] is a lightweight CNN optimized for mobile devices developed by Google. It uses depth-wise separable convolutions and the squeeze-and-excitation block. The network is defined by:

$$Y = \sigma * (W.PWConv * (DWConv * (X)) \tag{3}$$

Where DWConv is depth-wise convolution, PWConv is point-wise convolution, W is the weight matrix, and σ is the activation function. MobileNetV3 Large [18] follows the same design principles as MobileNetV3 Small but with a larger architecture. It offers a balance between model size and accuracy, suitable for scenarios where more computational resources are available, but efficiency is still a priority. Like its smaller counterpart, MobileNetV3 Large uses depth-wise separable convolutions, squeeze-and-excitation blocks, and a mix of activation functions.

DenseNet121 [19] has 121 layers and uses dense connections. Each layer receives inputs from all preceding layers and passes its output to all subsequent layers. The output of the l-th layer is:

$$\mathrm{x}_I = H_I([x_0, x_1, \ldots, x_{I-1}]) \tag{4}$$

Where $[x_0, x_1, \ldots, x_{l-1}]$ represents the concatenation of feature maps from layers 0 to l-1. DenseNet161 model [21] is a deeper version of DenseNet with 161 layers, following the same dense connectivity pattern as DenseNet121 but with increased capacity.

3.4 *Transfer Learning*

In this study, transfer learning was applied to adapt pre-trained convolutional neural networks for the classification of encrypted chest X-rays into COVID-19, normal, and pneumonia categories. The models utilized include ResNet50, ResNet101, MobileNetV3 Small, MobileNetV3 Large, DenseNet121, and DenseNet161, all initially trained on the ImageNet dataset. The transfer learning process began by loading these pre-trained architectures with their ImageNet weights. To adapt the models for the specific three-class problem, only the final fully connected layer was modified to output predictions for the target categories. To address privacy concerns and enhance data protection, the study incorporated an encryption step using the AES algorithm. Before being fed into the models, each chest X-ray image is encrypted using AES in Electronic Codebook (ECB) mode. This encryption process transformed the original image data into an encrypted format, ensuring that the raw medical images were not directly exposed during the training and classification processes. The encryption was implemented as part of a custom dataset class, which applied the AES encryption to each image as it was loaded. This approach allowed the models to learn from and classify the encrypted representations of the X-rays, rather than the original images, thus preserving patient privacy while still enabling effective classification.

4. Results and Discussion

4.1 *Optimal Hyperparameter*

For the selection of optimal hyperparameters, a comprehensive series of experiments was conducted with the MobileNetV3 Small model. These experiments evaluated the model's performance under various conditions, including the use of data augmentation, different weight decay values (1e-04, 1e-05, 1e-06), and scheduler patience settings (2, 3). Each combination was tested with a fixed maximum epoch of 15, batch size of 16 and a learning rate of 0.0001, Table 1 showcase the configuration for choosing hyperparameters. Through these trials, the configuration that consistently delivered the best performance and accuracy was identified as the use of data augmentation, a weight decay of 1e-05, and a scheduler patience of 2, the detailed result over all different configuration sets is shown in Table 2 and the final parameter configuration utilized in this study are shown in Table 3. This configuration was then adopted as the standard setup for further training on various models.

Table 1

Configuration for Choosing Hyperparameter

Configuration	Value	Configuration	Value
Learning rate	0.0001	Max epoch	15
Weight decay	1e-04, 1e-05, 1e-06	Batch size	16
Scheduler patience	2, 3	Optimizer	ADAM

Table 2

Accuracy received on different sets of hyperparameters

Weight Decay	Schedular Patience	Accuracy	Weight Decay	Schedular Patience	Accuracy
1e-04	2	87.48%	1e-05	3	87.62%
1e-04	3	87.77%	1e-06	2	86.17%
1e-05	2	88.64%	1e-06	3	87.04%

Table 3

Parameter Configuration

Sr. no	Parameter	Value	Sr. no	Parameter	Value
1	Optimizer	ADAM	4	Learning Rate	0.0001
2	Batch size	16	5	Weight Decay	1e-05
3	Max Epochs	15			

4.2 *Model Evaluation*

The evaluation of various deep learning models for encrypted lungs X-ray classification was conducted using a balanced dataset, making accuracy a reliable metric for comparison. The models analyzed included ResNet50, ResNet101, MobileNetV3 Small, MobileNetV3 Large, DenseNet121, and DenseNet161. Performance metrics considered were accuracy, F1-score, precision, recall (sensitivity), and specificity, providing a comprehensive assessment of each model's strengths and weaknesses. Table 4 describes the deep learning models performance on different metrics.

Table 4

Encrypted Lungs x-ray Classification Performance

Model	Accuracy (%)	F1 Score (%)	Precision (%)	Recall (%)	Specificity (%)
ResNet50	91.26	91.10	91.60	91.26	95.63
ResNet101	90.97	90.96	91.04	90.97	95.48
MobileNet V3 Small	89.66	89.58	89.94	89.66	94.83
MobileNet V3 Large	91.26	91.16	91.51	91.26	95.63
DenseNet121	91.41	91.26	92.10	91.41	95.70
DenseNet161	92.28	92.19	92.79	92.28	96.14

Upon analyzing the results, ResNet50 demonstrated robust performance, achieving an accuracy of 91.26% with a balanced F1-score of 91.10%. Its high precision (91.60%) and recall (91.26%) indicate a strong ability to correctly identify both positive and negative cases. The model's specificity of 95.63% further underscores its effectiveness in accurately identifying true negatives. On the other hand, ResNet101 exhibited slightly lower performance across all metrics compared to ResNet50, with an accuracy of 90.97% and an F1-score of 90.96%. Despite the slight reduction, ResNet101 maintained a balanced approach, offering reliable results. MobileNet V3 Small, with an accuracy of 89.66%, showed the lowest performance among the models evaluated. Its F1-score was 89.58%, with precision and recall closely aligned at 89.94% and 89.66%, respectively. This indicates a competent yet comparatively less effective model, with a specificity of 94.83%, suggesting a reduced ability to identify true negatives compared to other models. In contrast, MobileNetV3 Large performed similarly to ResNet50, achieving an accuracy of 91.26% and an F1-score of 91.16%. The precision and recall were 91.51% and 91.26%, respectively, with a specificity of 95.63%, highlighting its effectiveness and reliability. DenseNet121 showed slightly better performance than both ResNet50 and MobileNetV3 Large, with an accuracy of 91.41% and an F1-score of 91.26%. The model's precision was notably high at 92.10%, with a recall of 91.41%, and a specificity of 95.70%, indicating a strong ability to accurately identify both positive and negative cases. DenseNet161 emerged as the top-performing model, achieving the highest scores across all metrics. It reached an accuracy of 92.28%, an F1-score of 92.19%, and maintained the highest precision (92.79%), recall (92.28%), and specificity (96.14%). This exceptional performance highlights DenseNet161's robustness in accurately classifying encrypted lungs X-ray images. In summary, DenseNet161 stands out as the most effective model for this classification task, followed closely by DenseNet121 and ResNet50. These models demonstrated high accuracy, balanced precision and recall, along with excellent specificity, making them reliable choices for encrypted lungs X-ray classification. Figure 4 shows the bar plot of the accuracy of the models. Figure 5 showcases the training accuracy and loss plots of the models.

Figure 4

Comparison of models' performance on the test dataset

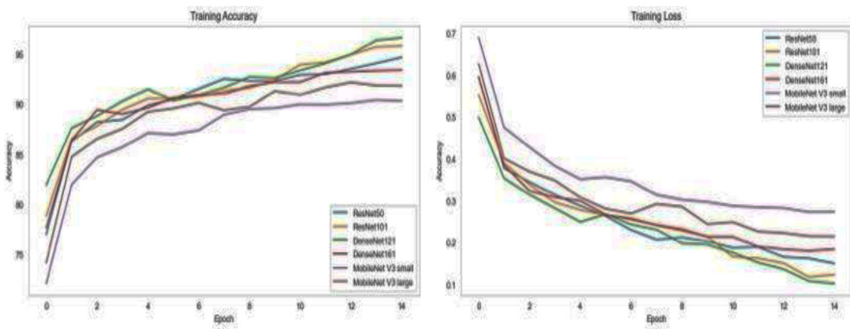

Figure 5

Training accuracy and loss plot of the models

5. Conclusion

This study successfully demonstrates a novel privacy-preserving approach for chest X-ray image classification by integrating AES encryption and FHE with CNNs. The methodology ensures patient data confidentiality while accurately categorizing X-ray images into normal, COVID-19 infected, and pneumonia infected classes without decrypting the data. Various CNN models, including ResNet50, ResNet101, MobileNetV3 Small, MobileNetV3 Large, DenseNet121, and DenseNet161, were evaluated for their performance on encrypted data. The results indicate that DenseNet161 outperformed other models, achieving the highest accuracy of 92.28%, alongside commendable F1-score, precision, recall, and specificity. DenseNet121 and ResNet50 also showed strong performance, with accuracies of 91.41% and 91.26%, respectively. This indicates that deep learning models can effectively handle encrypted medical images, ensuring both high diagnostic accuracy and robust data privacy. In conclusion, this research highlights the potential of combining encryption techniques with advanced machine learning models to address the critical need for privacy in medical image analysis.

References

[1] V. Rijmen and J. Daemen, "Advanced encryption standard," in Proceedings of Federal Information Processing Standards Publications, *National Institute of Standards and Technology*, vol. 19, pp. 22 (2001).

[2] J. Gu, Z. Wang, J. Kuen, L. Ma, A. Shahroudy, B. Shuai, T. Liu, X. Wang, and G. Wang, "Recent advances in convolutional neural networks," *Pattern Recognition*, vol. 77, pp. 354–377 (2018).

[3] C. Gentry, A Fully Homomorphic Encryption Scheme, Stanford University (2009).

[4] Z. I. A. Asraf and Z. Islam, "COVID19, Pneumonia and Normal Chest X-ray PA Dataset," (2021).

[5] K. K. Pal and K. S. Sudeep, "Preprocessing for image classification by convolutional neural networks," in Proceedings of the 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT) (2016).

[6] J. Y. I. Alzamily, S. B. Ariffin, and S. S. Abu-Naser, "Classification of encrypted images using deep learning–ResNet50," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 21, pp. 6610–6620 (2022).

[7] K. Maharana, S. Mondal, and B. Nemade, "A review: Data pre-processing and data augmentation techniques," *Global Transitions Proceedings*, vol. 3, no. 1, pp. 91–99 (2022).

[8] D. Singh and B. Singh, "Investigating the impact of data normalization on classification performance," *Applied Soft Computing*, vol. 97, pp. 105524 (2020).

[9] S. Roy, A. Bhattacharya, A. Roy, A. Chatterjee, and A. Dutta, "Characterization of AES implementations on microprocessor-based IoT devices," in Proceedings of the 2022 IEEE Wireless Communications and Networking Conference (WCNC) (2022).

[10] R. Bhanot and R. Hans, "A review and comparative analysis of various encryption algorithms," *International Journal of Security and Its Applications*, vol. 9, no. 4, pp. 289–306 (2015).

[11] I. F. Elashry, M. M. Tantawy, A. A. Ali, and R. M. El-Aassar, "A new method for encrypting images with few details using Rijndael and RC6 block ciphers in the electronic code book mode," *Information Security Journal: A Global Perspective*, vol. 21, no. 4, pp. 193–205 (2012).

[12] P. R. Halmos, "The theory of unbiased estimation," *The Annals of Mathematical Statistics*, vol. 17, no. 1, pp. 34–43 (1946).

[13] A. Voulodimos, N. Doulamis, A. Doulamis, and E. Protopapadakis, "Deep learning for computer vision: A brief review," *Computational Intelligence and Neuroscience*, vol. 2018, Article ID 7068349 (2018).

[14] D. Yu, J. Li, Q. Liu, and H. Wang, "Mixed pooling for convolutional neural networks," in Proceedings of the 9th International Conference on Rough Sets and Knowledge Technology (RSKT), Shanghai, China, Springer (2014).

[15] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2016).

[16] D. Theckedath and R. R. Sedamkar, "Detecting affect states using VGG16, ResNet50 and SE-ResNet50 networks," *SN Computer Science*, vol. 1, no. 2, pp. 79 (2020).

[17] A. Howard, M. Sandler, G. Chu, L. C. Chen, B. Chen, M. Tan, W. Wang, Y. Zhu, R. Pang, V. Vasudevan, and Q. V. Le, "Searching for MobileNetV3," in Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), pp. 1314–1324 (2019).

[18] A. Howard, M. Sandler, G. Chu, L. C. Chen, B. Chen, M. Tan, W. Wang, Y. Zhu, R. Pang, V. Vasudevan, and Q. V. Le, “Searching for MobileNetV3,” in Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV), pp. 1314–1324 (2019).

[19] M. Chhabra and R. Kumar, “A smart healthcare system based on classifier DenseNet 121 model to detect multiple diseases,” in Mobile Radio Communications and 5G Networks: Proceedings of Second MRCN 2021, Singapore: Springer Nature, pp. 297–312 (2022).

[20] Q. Zhang, “A novel ResNet101 model based on dense dilated convolution for image classification,” *SN Applied Sciences*, vol. 4, pp. 1–13 (2022).

[21] M. Talo, “Automated classification of histopathology images using transfer learning,” *Artificial Intelligence in Medicine*, vol. 101, pp. 101743 (2019).

Received November, 2024