Deep Learning-Based Anonymization of Chest Radiographs: A Utility-Preserving Measure for Patient Privacy

Kai Packhäuser[(✉)], Sebastian Gündel, Florian Thamm, Felix Denzinger, and Andreas Maier

Friedrich-Alexander-Universität Erlangen-Nürnberg, Erlangen, Germany
`kai.packhaeuser@fau.de`

Abstract. Robust and reliable anonymization of chest radiographs constitutes an essential step before publishing large datasets of such for research purposes. The conventional anonymization process is carried out by obscuring personal information in the images with black boxes and removing or replacing meta-information. However, such simple measures retain biometric information in the chest radiographs, allowing patients to be re-identified by a linkage attack. Therefore, there is an urgent need to obfuscate the biometric information appearing in the images. We propose the first deep learning-based approach (PriCheXy-Net) to targetedly anonymize chest radiographs while maintaining data utility for diagnostic and machine learning purposes. Our model architecture is a composition of three independent neural networks that, when collectively used, allow for learning a deformation field that is able to impede patient re-identification. Quantitative results on the ChestX-ray14 dataset show a reduction of patient re-identification from 81.8% to 57.7% (AUC) after re-training with little impact on the abnormality classification performance. This indicates the ability to preserve underlying abnormality patterns while increasing patient privacy. Lastly, we compare our proposed anonymization approach with two other obfuscation-based methods (Privacy-Net, DP-Pix) and demonstrate the superiority of our method towards resolving the privacy-utility trade-off for chest radiographs.

Keywords: Image Anonymization · Patient Privacy · Data Utility

1 Introduction

Deep learning (DL) [19] has positively contributed to the development of diagnostic algorithms for the detection and classification of lung diseases in recent years [11,20]. This progress can largely be attributed to the availability of public chest X-ray datasets [4,5,14,15,27]. However, as chest radiographs inherently

contain biometric information (similar to a fingerprint), the public release of such data bears the risk of automated patient re-identification by DL-based linkage attacks [22]. This would allow patient-related information, e.g., age, gender, or disease findings to be revealed. Therefore, there is an urgent need for stronger privacy mechanisms for chest X-ray data to alleviate the risk of linkage attacks.

Perturbation-based anonymization approaches [16] – such as differential privacy (DP) [7,8] – have become the gold standard to obfuscate biometric identifiers from sensitive data. Such approaches are based on the postulate that the global statistical distribution of a dataset is retained while personal information is reduced. This can be realized by applying randomized modifications, i.e. noise, to either the inputs [2,6,8], the computational results, or to algorithms [1,28]. Although originally proposed for statistical data, DP has been extended to image data with the differentially private pixelization method (DP-Pix) [9,10]. This method involves pixelizing an image by averaging the pixel values of each $b \times b$ grid cell, followed by adding Laplace noise with 0 mean and $\frac{255m}{b^2\epsilon}$ scale. Parameter ϵ is used to determine the privacy budget (smaller values indicate greater privacy), while the m-neighborhood represents a sensitivity factor. However, one major drawback of perturbation-based anonymization is the potential degradation of image quality and an associated reduction in data utility.

In recent years, DL has emerged as a prominent tool for anonymizing medical images. In this context, synthetic image generation with privacy guarantees is currently actively explored, aimed at creating fully anonymous medical image datasets [21,24]. Furthermore, adversarial approaches – such as Privacy-Net [17] – have been proposed, which focus on concealing biometric information while maintaining data utility. Privacy-Net is composed of a U-Net encoder that predicts an anonymized image, an identity discriminator, and a task-specific segmentation network. Through the dual process of deceiving the discriminator and optimizing the segmentation network, the encoder acquires the ability to obfuscate patient-specific patterns, while preserving those necessary for the downstream task. However, while originally designed for utility preservation on MRI segmentation tasks, the direct applicability and transferability of Privacy-Net to other image modalities and downstream tasks (e.g. chest X-ray classification) is limited. As we will experimentally demonstrate in our study, more sophisticated constraints are required for the utility-preserving anonymization of chest radiographs in order to successfully maintain fine-grained abnormality details that are crucial for reliable classification tasks.

In this work, we aim to resolve the privacy-utility trade-off by proposing the – to the best of our knowledge – first adversarial image anonymization approach for chest radiography data. Our proposed model architecture (PriCheXy-Net) is a composition of three independent neural networks that collectively allow for the learning of targeted image deformations to deceive a well-trained patient verification model. We apply our method to the publicly available ChestX-ray14 dataset [27] and evaluate the impact of different deformation degrees on anonymization capability and utility preservation. To evaluate the effectiveness
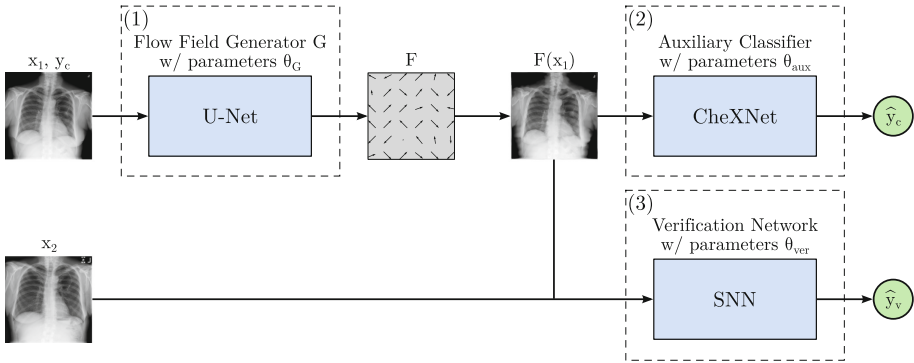
Fig. 1. PriCheXy-Net: Proposed adversarial image anonymization architecture.

of image anonymization, we perform linkage attacks on anonymized data and analyze the respective success rates. Furthermore, to quantify the extent of data utility preservation despite the induced image deformations, we compare the performance of a trained thoracic abnormality classification system on anonymized images versus the performance on real data. Throughout our study, we utilize Privacy-Net [17] and DP-Pix [9,10] as baseline obfuscation methods.

2   Methods

2.1   Data

We use X-ray data from the ChestX-ray14 dataset [27], a large-scale collection of 112,120 frontal-view chest radiographs from 30,805 unique patients. The 8-bit gray-scale images are provided with a resolution of 1024×1024 pixels. We resize the images to a size of 256×256 pixels for further processing. On average, the dataset contains ≈ 3.6 images per patient. The corresponding 14 abnormality labels include Atelectasis, Cardiomegaly, Consolidation, Edema, Effusion, Emphysema, Fibrosis, Hernia, Infiltration, Mass, Nodule, Pleural Thickening, Pneumonia, and Pneumothorax. A patient-wise splitting strategy is applied to roughly divide the data into a training, validation, and test set by ratio 70:10:20, respectively. Based on this split, we utilize available follow-up scans to randomly construct positive image pairs (two unique images from the same patient) and negative image pairs (two unique images from two different patients) – 10,000 for training, 2,000 for validation, and 5,000 for testing. The resulting subsets are balanced with respect to the number of positive and negative samples.

2.2   PriCheXy-Net: Adversarial Image Anonymization

The proposed adversarial image anonymization approach is depicted in Fig. 1. It is composed of three trainable components: (1) A U-Net generator G that

predicts a flow field F used to deform the original image x_1 of abnormality class y_c, (2) an auxiliary classifier that takes the modified image $F(x_1)$ resulting in corresponding class predictions $\hat{y}_c$, and (3) a siamese neural network (SNN) that receives the deformed image $F(x_1)$ as well as another real image x_2 of either the same or a different patient and yields the similarity score $\hat{y}_v$ for patient verification. The U-Net serves as an anonymization tool aiming to obfuscate biometric information through targeted image deformations, while the auxiliary classifier and the patient verification model contribute as guidance to optimize the flow field generator.

U-Net. The U-Net [26] architecture is implemented according to Buda et al. [3]. Its last sigmoid activation function is replaced by a hyperbolic tangent activation function to predict a 2-channel flow field F, bounded by $[-1, 1]$. During training, especially in early stages, the raw output of the U-Net may lead to random deformations that destroy the content of the original images, thus revoking the diagnostic utility. To circumvent this issue, the following constraints are imposed for F. First, to ensure that the learned flow field F does not substantially deviate from the identity F_{id}, it is weighted with factor μ and subsequently subtracted from the identity according to

$$F = F_{id} - \mu F. \tag{1}$$

Factor μ controls the degree of deformation, with larger values allowing for more deformation. Note that the exclusive use of F_{id} would result in the original image, i. e., $x = F(x)$, assuming the deformation factor is being set to $\mu = 0$. The resulting flow field F is Gaussian filtered (kernel size 9, $\sigma = 2$) to ensure smooth deformations in the final image. The corresponding parameters were selected manually in preliminary experiments.

Auxiliary Classifier. To ensure the preservation of underlying abnormality patterns and image utility during deformation, PriCheXy-Net integrates an auxiliary classifier using CheXNet [25], a densely connected convolutional network (DenseNet) [13] consisting of 121 layers. It outputs a 14-dimensional probability vector $\hat{y}_c$ indicating the presence or absence of each abnormality appearing in the ChestX-ray14 dataset. Its parameters θ_{aux} are initialized using a pre-trained model that achieves a mean AUC of 80.5%.

Patient Verification Network. The incorporated patient verification model is represented by the SNN architecture presented by Packhäuser et al. [22], consisting of two ResNet-50 [12] branches that are merged using the absolute difference of their resulting 128-dimensional feature vectors. A fully-connected layer with a sigmoid activation function produces the final verification score $\hat{y}_v$ in the value range of $[0, 1]$, indicating the probability of whether or not the two input images belong to the same patient. For initializing the network parameters θ_{ver}, we employ a pre-trained network that has been created according to [22] yielding an AUC value of 99.4% for a patient verification task.

2.3   Objective Functions

Similar to most adversarial models, our system undergoes training through the use of dual loss functions that guide the model towards opposing directions. To enforce the U-Net not to eliminate important class information while deforming a chest radiograph, we introduce the auxiliary classifier loss $L_{aux}(\theta_G, \theta_{aux})$ realized by the class-wise binary cross entropy (BCE) loss according to Eq. 2

$$L_{aux}(\theta_G, \theta_{aux}) = -\sum_{i=1}^{14}[y_{c,i}\log(\hat{y}_{c,i}) + (1 - y_{c,i})\log(1 - \hat{y}_{c,i})], \qquad (2)$$

where i represents one out of 14 abnormality classes. Conversely, to guide the U-Net with deceiving the incorporated patient verification model, we utilize its output as an additional verification loss term $L_{ver}(\theta_G, \theta_{ver})$ (see Eq. 3):

$$L_{ver}(\theta_G, \theta_{ver}) = -\log(1 - \hat{y}_v) \ , \ \text{with } \hat{y}_v = \text{SNN}\big(F(x_1), x_2\big) \qquad (3)$$

The total loss to be minimized (see Eq. 4) results from the sum of the two partial losses $L_{aux}(\theta_G, \theta_{aux})$ and $L_{ver}(\theta_G, \theta_{ver})$:

$$\underset{\theta_G}{\arg\min}\, L(\theta_G, \theta_{aux}, \theta_{ver}) = L_{aux}(\theta_G, \theta_{aux}) + L_{ver}(\theta_G, \theta_{ver}) \qquad (4)$$

Lastly, both the auxiliary classifier and the verification model are updated by minimizing the loss terms in Eq. 5 and Eq. 6, respectively. Note that the similarity labels for positive and negative pairs are encoded using $y_v = 1$ and $y_v = 0$.

$$\underset{\theta_{aux}}{\arg\min}\, L(\theta_G, \theta_{aux}) \quad (5) \qquad \underset{\theta_{ver}}{\arg\min}\, [-y_v\log\hat{y}_v - (1 - y_v)\log(1 - \hat{y}_v)] \quad (6)$$

3   Experiments and Results

3.1   Experimental Setup

For all experiments, we used PyTorch (1.10.2) [23] and Python (3.9.5). We followed a multi-part experimental setup consisting of the following steps.

Pre-training of the Flow Field Generator. The incorporated U-Net architecture was pre-trained on an autoencoder-like reconstruction task for 200 epochs using the mean squared error (MSE) loss, Adam [18], a batch size of 64 and a learning rate of 10^{-4} to enable faster convergence. The model that performed best on the validation set was then used for weight initialization in step 2.

Training of PriCheXy-Net. After pre-training, PriCheXy-Net was trained in an end-to-end fashion for 250 epochs using the Adam optimizer [18], a batch size of 64 and a learning rate of 10^{-4} using the objective functions presented above. To evaluate the effect of the deformation degree μ on anonymization capability and image utility, we performed multiple training runs with various values $\mu \in \{0.001, 0.005, 0.01\}$. For each configuration, the U-Net that performed best on the validation set was then used for further evaluations in steps 3 and 4.
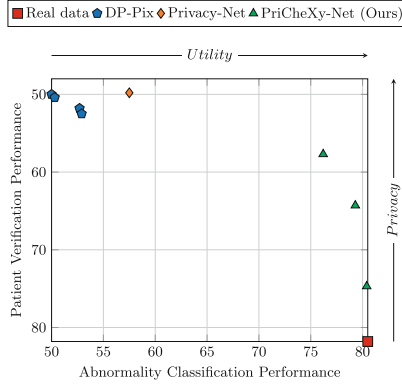
Re-training and Evaluation of the Verification Model. To assess the anonymization capability of PriCheXy-Net and to determine if the anonymized images can reliably deceive the verification model, we re-trained the incorporated SNN for each model configuration by using deformed images only. We then simulated multiple linkage attacks by comparing deformed images with real ones. Training was conducted until early stopping (patience $p = 5$) using the BCE loss, the Adam optimizer [18], a batch size of 32 and a learning rate of 10^{-4}. For each model configuration, we performed 10 independent training and testing runs. We report the means and standard deviations of the resulting AUC values.

Evaluation of the Classification Model on Anonymized Data. To assess the extent to which underlying abnormalities, and thus data utility, were preserved during the anonymization process, each individually trained anonymization network was used to perturb the images of our test set. Then, the pre-trained auxiliary classifier was evaluated using the resulting images. We report the mean of the 14 class-wise AUC values. To quantify the uncertainty, the 95% confidence intervals (CIs) from 1,000 bootstrap runs were computed.

Comparison with Other Obfuscation-Based Methods. To compare our proposed system with other obfuscation-based methods, we additionally analyzed the anonymization capability and utility preservation of Privacy-Net [17] and DP-Pix [9,10]. Since Privacy-Net was originally proposed for segmentation tasks, we replaced its segmentation component with the auxiliary classifier. Then, the network was trained and evaluated in the exact same setting as PriCheXy-Net. For DP-Pix, we investigated the effect of different cell sizes $b \in \{1, 2, 4, 8\}$ at a common privacy budget $\epsilon = 0.1$. The m-neighborhood was set to the smallest possible value ($m = 1$) to prevent the added Laplace noise (mean: 0; scale: $\frac{255m}{b^2\epsilon}$) from destroying the complete content of the images.

Table 1. Quantitative comparison of all examined methods. The baseline performance results from leveraging non-anonymized real data. Verification: AUC (mean ± std) over 10 independent training and testing runs; Classification: mean AUC + 95% CIs. Performance scores of 50% indicate random decisions.

Task	Baseline (real data)	Privacy-Net [17]	PriCheXy-Net (Ours) $\mu = 0.001$	$\mu = 0.005$	$\mu = 0.01$
Ver. ↓	81.8 ± 0.6	49.8 ± 2.2	74.7 ± 2.6	64.3 ± 5.8	57.7 ± 4.0
Class. ↑	$80.5 \ _{80.1}^{80.9}$	$57.5 \ _{56.9}^{58.1}$	$80.4 \ _{79.9}^{80.8}$	$79.3 \ _{78.9}^{79.7}$	$76.2 \ _{75.8}^{76.6}$
		DP-Pix [9,10] $b = 1$	$b = 2$	$b = 4$	$b = 8$
Ver. ↓	81.8 ± 0.6	50.0 ± 0.7	50.4 ± 0.6	51.8 ± 1.3	52.5 ± 3.2
Class. ↑	$80.5 \ _{80.1}^{80.9}$	$50.0 \ _{49.4}^{50.6}$	$50.3 \ _{49.7}^{51.0}$	$52.7 \ _{52.0}^{53.3}$	$52.9 \ _{52.2}^{53.5}$

Fig. 2. Visual illustration of the results and the associated privacy-utility trade-off. The patient verification performance (y-axis) measures the amount of privacy, whereas the abnormality classification performance (x-axis) represents the level of data utility.

(a) real   (b) $\mu = 0.001$ (c) $\mu = 0.005$ (d) $\mu = 0.01$
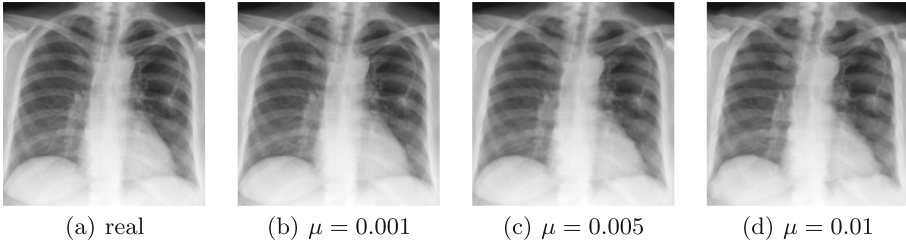
Fig. 3. Chest radiographs resulting from PriCheXy-Net when using different deformation degrees μ. Images were cropped to better highlight the diagnostically relevant area.

3.2   Results

Baseline and Comparison Methods. The results of all conducted experiments are shown in Table 1. Compared to real (non-anonymized) data, which enables a successful re-identification with an AUC of 81.8%, the patient verification performance desirably decreases after applying DP-Pix (50.0%–52.5%) and Privacy-Net (49.8%). However, while the classification performance on real data indicates a high data utility with a mean AUC of 80.5%, we observe a sharp drop for images that have been modified with DP-Pix (50.0%–52.9%) and Privacy-Net (57.5%). This suggests that relevant class information and specific abnormality patterns are destroyed during the obfuscation process. Resulting example images for both comparison methods are provided in Suppl. Fig. 1.

PriCheXy-Net. The results of our proposed PriCheXy-Net (see Table 1) show more promising behavior. As can be seen, increasing deformation degrees μ lead to a successive decline in patient verification performance. Compared to the

baseline, the AUC decreases to 74.7% ($\mu = 0.001$), to 64.3% ($\mu = 0.005$), and to 57.7% ($\mu = 0.01$), indicating a positive effect on patient privacy and the obfuscation of biometric information. In addition, PriCheXy-Net hardly results in a loss of data utility, as characterized by the constantly high classification performance with a mean AUC of 80.4% ($\mu = 0.001$), 79.3% ($\mu = 0.005$), and 76.2% ($\mu = 0.01$). These findings are further visualized in the privacy-utility trade-off plot in Fig. 2. In contrast to the examined comparison methods, the data point corresponding to our best experiment with PriCheXy-Net (green) lies near the top right corner, highlighting the capability to closely satisfy both objectives in the privacy-utility trade-off. Examples of deformed chest radiographs resulting from a trained model of PriCheXy-Net are shown in Fig. 3. More examples are given in Suppl. Fig. 1. Difference maps are provided in Suppl. Fig. 2.

4   Discussion and Conclusion

To the best of our knowledge, we presented the first adversarial approach to anonymize thoracic images while preserving data utility for diagnostic purposes. Our proposed anonymization approach – PriCheXy-Net – is a composition of three independent neural networks consisting of (1) a flow field generator, (2) an auxiliary classifier, and (3) a patient verification network. In this work, we were able to show that collective utilization of these three components enables learning of a flow field that targetedly deforms chest radiographs and thus reliably deceives a patient verification model, even after re-training was performed. For the best hyper-parameter configuration of PriCheXy-Net, the re-identification performance drops from 81.8% to 57.7% in AUC for a simulated linkage attack, whereas the abnormality classification performance only decreases from 80.5% to 76.2%, which indicates the effectiveness of the proposed approach. We strongly hypothesize that the promising performance of PriCheXy-Net can be largely attributed to the constraints imposed on the learned flow field F. The limited deviation of the flow field from the identity (cf. Eq. 1) ensures a realistic appearance of the resulting deformed image to a considerable extent, thereby avoiding its content from being completely destroyed. This idea has a positive impact on preserving relevant abnormality patterns in chest radiographs, while allowing adequate scope to obfuscate biometric information. Such domain-specific constraints are not integrated in examined comparison methods such as Privacy-Net (which directly predicts an anonymized image without ensuring realism) and DP-Pix (which does not contain any mechanism to maintain data utility). This is, as we hypothesize, the primary reason for their limited ability to preserve data utility and the overall superiority of our proposed system. Interestingly, PriCheXy-Net's deformation fields primarily focus on anatomical structures, including lungs and ribs, as demonstrated in Fig. 3, Suppl. 1, and Suppl. Fig. 2. This observation aligns with Packhäuser et al.'s previous findings [22], which revealed that these structures contain the principal biometric information in chest radiographs.

In future work, we aim to further improve the performance of PriCheXy-Net by incorporating additional components into its current architecture. For

instance, we plan to integrate a discriminator loss into the model, which may positively contribute to achieving perceptual realism. Furthermore, we also consider implementing a region of interest segmentation step into the pipeline to ensure not to perturb diagnostically relevant image areas. Lastly, we hypothesize that our method is robust to variations in image size or compression rate, and posit its applicability beyond chest X-rays to other imaging modalities as well. However, confirmation of these hypotheses requires further exploration to be conducted in forthcoming studies.

Data Use Declaration. This research study was conducted retrospectively using human subject data made available in open access by the National Institutes of Health (NIH) Clinical Center [27]. Ethical approval was not required as confirmed by the license attached with the open-access data.

Code Availability. The source code of this study has been made available at https://github.com/kaipackhaeuser/PriCheXy-Net.

References

1. Abadi, M., et al.: Deep learning with differential privacy. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 308–318 (2016)
2. Bu, Z., Dong, J., Long, Q., Su, W.J.: Deep learning with gaussian differential privacy. Harv. Data Sci. Rev. **2020**(23) (2020)
3. Buda, M., Saha, A., Mazurowski, M.A.: Association of genomic subtypes of lower-grade gliomas with shape features automatically extracted by a deep learning algorithm. Comput. Biol. Med. **109** (2019)
4. Bustos, A., Pertusa, A., Salinas, J.M., de la Iglesia-Vayá, M.: PadChest: a large chest x-ray image dataset with multi-label annotated reports. Med. Image Anal. **66**, 101797 (2020)
5. Cohen, J.P., Morrison, P., Dao, L., Roth, K., Duong, T.Q., Ghassemi, M.: COVID-19 image data collection: prospective predictions are the future. arXiv preprint arXiv:2006.11988 (2020)
6. Dong, J., Roth, A., Su, W.J.: Gaussian differential privacy. arXiv preprint arXiv:1905.02383 (2019)
7. Dwork, C.: Differential privacy: a survey of results. In: Agrawal, M., Du, D., Duan, Z., Li, A. (eds.) TAMC 2008. LNCS, vol. 4978, pp. 1–19. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-79228-4_1

8. Dwork, C., McSherry, F., Nissim, K., Smith, A.: Calibrating noise to sensitivity in private data analysis. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 265–284. Springer, Heidelberg (2006). https://doi.org/10.1007/11681878_14

9. Fan, L.: Image pixelization with differential privacy. In: Kerschbaum, F., Paraboschi, S. (eds.) DBSec 2018. LNCS, vol. 10980, pp. 148–162. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-95729-6_10

10. Fan, L.: Differential privacy for image publication. In: Theory and Practice of Differential Privacy (TPDP) Workshop, vol. 1, p. 6 (2019)

11. Gündel, S., Grbic, S., Georgescu, B., Liu, S., Maier, A., Comaniciu, D.: Learning to recognize abnormalities in chest x-rays with location-aware dense networks. In: Vera-Rodriguez, R., Fierrez, J., Morales, A. (eds.) CIARP 2018. LNCS, vol. 11401, pp. 757–765. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-13469-3_88

12. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 770–778 (2016)

13. Huang, G., Liu, Z., Van Der Maaten, L., Weinberger, K.Q.: Densely connected convolutional networks. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 4700–4708 (2017)

14. Irvin, J., et al.: CheXpert: a large chest radiograph dataset with uncertainty labels and expert comparison. In: Proceedings of the AAAI Conference on Artificial Intelligence, vol. 33, pp. 590–597 (2019)

15. Johnson, A.E., et al.: MIMIC-CXR, a de-identified publicly available database of chest radiographs with free-text reports. Sci. Data **6**(1), 1–8 (2019)

16. Kaissis, G.A., Makowski, M.R., Rückert, D., Braren, R.F.: Secure, privacy-preserving and federated machine learning in medical imaging. Nat. Mach. Intell. **2**(6), 305–311 (2020)

17. Kim, B.N., Dolz, J., Jodoin, P.M., Desrosiers, C.: Privacy-net: an adversarial approach for identity-obfuscated segmentation of medical images. IEEE Trans. Med. Imaging **40**(7), 1737–1749 (2021)

18. Kingma, D.P., Ba, J.: Adam: a method for stochastic optimization. arXiv preprint arXiv:1412.6980 (2014)

19. LeCun, Y., Bengio, Y., Hinton, G.: Deep learning. Nature **521**(7553), 436–444 (2015)

20. Maier, A., Syben, C., Lasser, T., Riess, C.: A gentle introduction to deep learning in medical image processing. Z. Med. Phys. **29**(2), 86–101 (2019)

21. Packhäuser, K., Folle, L., Thamm, F., Maier, A.: Generation of anonymous chest radiographs using latent diffusion models for training thoracic abnormality classification systems. arXiv preprint arXiv:2211.01323 (2022)

22. Packhäuser, K., Gündel, S., Münster, N., Syben, C., Christlein, V., Maier, A.: Deep learning-based patient re-identification is able to exploit the biometric nature of medical chest X-ray data. Sci. Rep. **12**(1), 1–13 (2022)

23. Paszke, A., et al.: PyTorch: an imperative style, high-performance deep learning library. In: Advances in Neural Information Processing Systems, vol. 32, pp. 8026–8037 (2019)

24. Pinaya, W.H., et al.: Brain imaging generation with latent diffusion models. In: Mukhopadhyay, A., Oksuz, I., Engelhardt, S., Zhu, D., Yuan, Y. (eds.) DGM4MICCAI 2022. LNCS, vol. 13609, pp. 117–126. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-18576-2_12

25. Rajpurkar, P., et al.: CheXNet: radiologist-level pneumonia detection on chest x-rays with deep learning. arXiv preprint arXiv:1711.05225 (2017)

26. Ronneberger, O., Fischer, P., Brox, T.: U-net: convolutional networks for biomedical image segmentation. In: Navab, N., Hornegger, J., Wells, W.M., Frangi, A.F. (eds.) MICCAI 2015. LNCS, vol. 9351, pp. 234–241. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-24574-4_28
27. Wang, X., Peng, Y., Lu, L., Lu, Z., Bagheri, M., Summers, R.M.: ChestX-ray8: hospital-scale chest x-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 2097–2106 (2017)
28. Ziller, A., Usynin, D., Braren, R., Makowski, M., Rueckert, D., Kaissis, G.: Medical imaging deep learning with differential privacy. Sci. Rep. **11**(1), 1–8 (2021)