Review

Deep Learning for Medical Image Cryptography: A Comprehensive Review

Kusum Lata [1] and Linga Reddy Cenkeramaddi [2,*]

1   Department of Electronics and Communication Engineering, The LNM Institute of Information Technology, Jaipur 302031, India; kusum@lnmiit.ac.in
2   Department of Information and Communication Technology, University of Agder, 4879 Grimstad, Norway
*   Correspondence: linga.cenkeramaddi@uia.no

Abstract: Electronic health records (EHRs) security is a critical challenge in the implementation and administration of Internet of Medical Things (IoMT) systems within the healthcare sector's heterogeneous environment. As digital transformation continues to advance, ensuring privacy, integrity, and availability of EHRs become increasingly complex. Various imaging modalities, including PET, MRI, ultrasonography, CT, and X-ray imaging, play vital roles in medical diagnosis, allowing healthcare professionals to visualize and assess the internal structures, functions, and abnormalities within the human body. These diagnostic images are typically stored, shared, and processed for various purposes, including segmentation, feature selection, and image denoising. Cryptography techniques offer a promising solution for protecting sensitive medical image data during storage and transmission. Deep learning has the potential to revolutionize cryptography techniques for securing medical images. This paper explores the application of deep learning techniques in medical image cryptography, aiming to enhance the privacy and security of healthcare data. It investigates the use of deep learning models for image encryption, image resolution enhancement, detection and classification, encrypted compression, key generation, and end-to-end encryption. Finally, we provide insights into the current research challenges and promising directions for future research in the field of deep learning applications in medical image cryptography.

Keywords: medical image security; cryptography; deep learning; electronic health records (EHR); privacy; security; image authentication; image encryption; image decryption; IoMT

1. Introduction

Medical image security in the Internet of Medical Things (IoMT) presents several challenges that need to be addressed to ensure the confidentiality, integrity, and availability of medical images. The healthcare industry has always been at the forefront of incorporating new technology to improve patient care, increase efficiency, and enhance overall healthcare delivery. Information technology (IT) has revolutionized the healthcare industry, improving patient care, enhancing communication and collaboration, and optimizing healthcare processes [1–4]. Its continued advancements hold significant potential for further transforming healthcare delivery and promoting positive health outcomes. In such a highly IT-oriented era, it is essential for healthcare organizations and technology providers to prioritize the implementation of robust security measures to protect the confidentiality and integrity of medical image transmission over the internet [5–8]. By adopting security measures, the risks associated with eavesdropping and malicious activities can be significantly reduced, enhancing the overall security of medical image delivery. Three effective techniques—image encryption, image steganography, and image authentication—can reconcile the qualities of medical images with the need for security [8–10]. Deep learning's ability to automatically learn and extract complex features from medical images has significantly advanced the field of medical image processing [11–14]. Its potential for improving diagnosis, treatment

planning, and overall patient care is being explored across various medical imaging modalities, including radiology, pathology, and ophthalmology [15–20]. As research in deep learning continues to evolve, it holds great promise for further revolutionizing medical image analysis and contributing to advancements in healthcare. Since these advancements have the potential to improve patient privacy, protect against malicious attacks, and ensure the integrity and authenticity of medical image analysis [7,8,10,21–24] by leveraging the capabilities of deep learning, researchers are actively exploring innovative approaches to enhance the security of medical image data.

Motivation and Contribution

Artificial intelligence (AI) algorithms are being used in radiology and chronic diseases like cancer to develop precise and effective inventions that will aid in treating people with these conditions and, ideally, finding a cure. AI algorithms have several benefits over conventional analytics and clinical decision-making techniques. As training data are understood by deep learning algorithms, the systems become more accurate. This allows humans to obtain previously unattainable insights into treatment variability, care processes, diagnostics, and patient outcomes. Clinical trials are a crucial component of medical product development because they help to evaluate new treatments' efficacy and uncover any safety concerns. They are also an essential regulatory prerequisite for introducing novel therapies into markets. One of the most difficult and expensive processes in the healthcare sector is conducting clinical studies. Going forward, incorporation of technology would influence clinical development and change the trial procedure. As per the reports of Acumen Research [25], shown in Figure 1, the market for virtual clinical trials was worth USD 10.8 billion in 2021, and it is anticipated to grow to USD 18.6 billion by 2030, at a compound annual growth rate (CAGR) of 6.2% from 2022 to 2030.
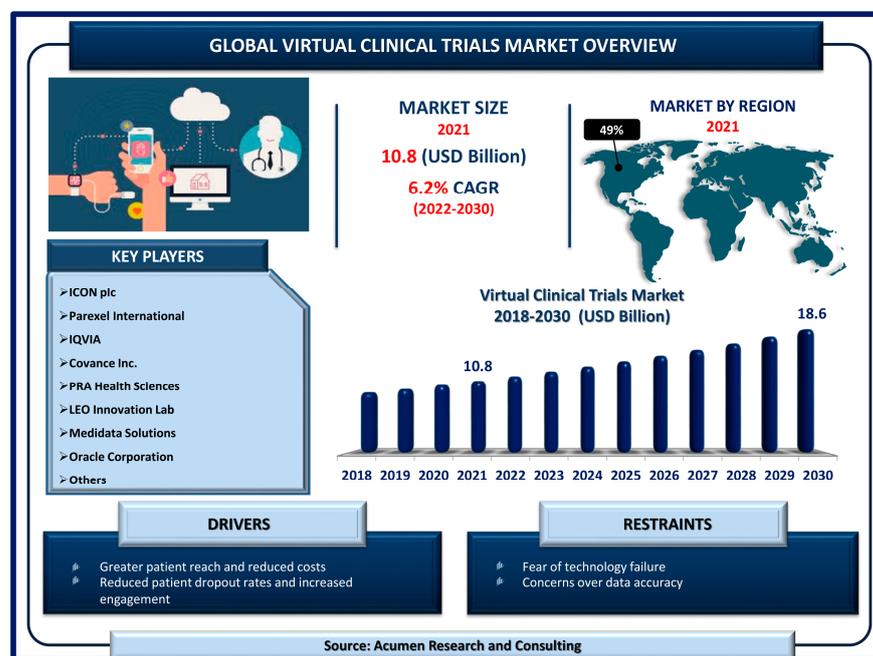

Figure 1. Global virtual clinical trial market overview [25].

According to a research study by Accenture, 26% of U.S. consumers have experienced a healthcare data breach and 50% of them became victims of medical identity theft. The average out-of-pocket cost for victims of medical identity theft is estimated at $2500 per incident. The affected patients either changed their healthcare providers or insurance plans or sought legal counsel. Data breaches most frequently occurred in hospitals, urgent care clinics, pharmacies, physicians' offices and health insurance companies [26]. The cost of

a breach in the healthcare industry went up to 42% since 2020. The average total cost of a data breach in the healthcare industry is USD 10.10 million [27]. Recently, this trend is supported by research from Check Point Software Technologies [28], shown in Figure 2, which found that in Q1 2023, the healthcare industry averaged 1684 attacks per week, up by 22% than past year. In 2023, healthcare will be the third most-targeted sector after banking, insurance, and communications. These statistics and facts demonstrate how vulnerable the data assets of people and businesses are. Alarmingly, attackers are specifically targeting the healthcare sector, making it the most open to assault.
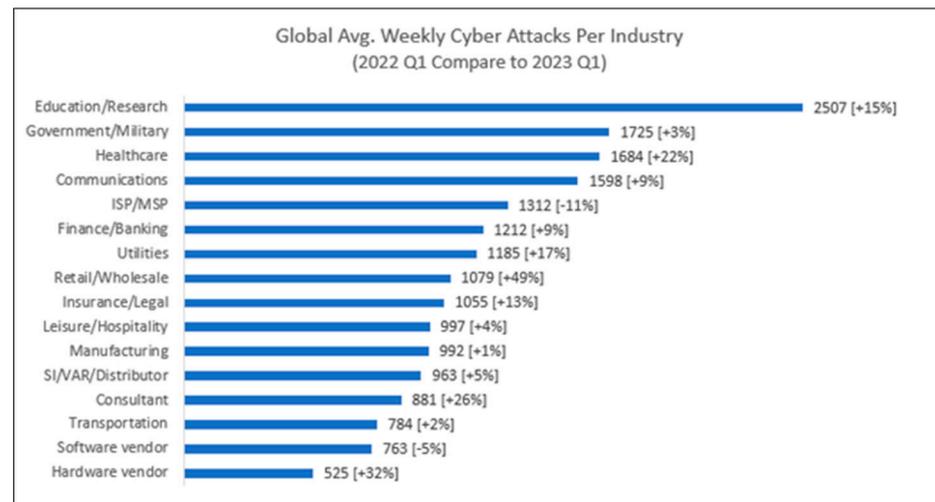

Figure 2. A year-on-year increase of 22% in attacks per week in Q1 2023 [28].

Medical imaging records are also at danger because of healthcare data breaches, along with patient health details such as insurance member ID and Social Security numbers. A crucial component of patient treatment is medical imaging. The exchange of medical images for the purpose of facilitating care delivery is now possible, thanks to the digitization of imaging data and the frequent storage of these records on picture archiving communication systems (PACS).

The broad field of deep learning in medical imaging involves participation from patients, hospitals, research centers, algorithm developers, diagnostic instrument vendors, industry, and legislators. Due to the situation's high level of complexity, the resulting lack of transparency regarding stakeholder motivations and data usage patterns, the ease with which electronic imaging data storage enables data sharing and other factors, the value of individual privacy is threatened, and there is a risk that the restrictions on personal data will be loosened in the name of, at best, scientific advancement and, at worst, financial interests.

The field of secure and privacy-preserving deep learning algorithms provides methods to assist in bridging the gap between the protection of personal data and its use for ordinary clinical and research purposes. To have an extensive overview of the new techniques in this developing field, a survey of the relevant publications already in existence is requisite. To accomplish this, we provide a thorough description of how cryptographic methods have been applied to deep learning-based medical picture processing. We believe our study can act as a blueprint for future field investigations. Our most significant contributions are as follows:

- With an emphasis on their applications in deep learning-based medical image analysis, we present an overview of the current and emerging privacy preservation strategies. To cover the most current progress, we specifically provide a thorough assessment of more than 150 pertinent papers;
- By classifying the publications depending on how they use cryptography in deep learning-based medical image analysis, as shown in Figure 3, we provide a thor-

ough coverage of the subject. We highlight task-specific problems for each of these applications and offer recommendations for resolving them based on the literature research;

- Finally, we provide a critical analysis of the condition of the field, emphasizing major issues, noting unresolved issues, and suggesting possible future approaches.
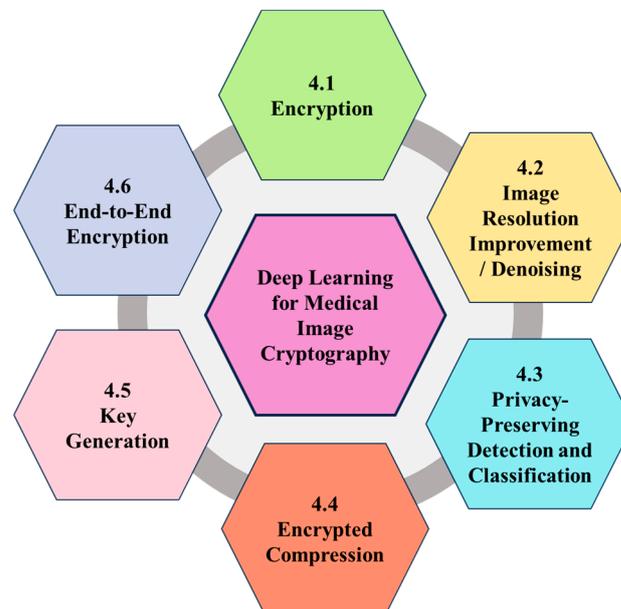

Figure 3. A wide range of cryptography application areas in deep learning-based medical image analysis covered in this survey.

Paper Organization. The rest of this paper is divided into the following sections. With an emphasis on a fundamental notion that underlies deep learning-based medical imaging applications, we present the field's history in Section 2 of our paper. The most well-known adversarial medical image analysis is shown in Section 3, which also examines the weaknesses of deep learning-based medical imaging applications. We thoroughly explore the applications of cryptography in a number of medical imaging tasks, as illustrated in Figure 2. Section 4 presents the various applications of cryptography in deep learning-based medical image analysis. We create a taxonomy and identify task-specific problems for each of these tasks in particular. The discussion and future directions for the entire field are presented in Section 5. Section 6 serves as the paper's conclusion, where we propose suggestions for contending with the field's rapid development.

2. Deep Learning-Based Medical Image Analysis

Medical image analysis plays a crucial role in various aspects of healthcare, including diagnosis, treatment, and health monitoring. It involves the processing and interpretation of images obtained from different modalities to gain insights into the human body and aid in medical decision-making. The integration of deep neural networks and computer vision techniques in medical image analysis has revolutionized the field, enabling earlier and more accurate diagnoses, improved treatment outcomes, and ultimately contributing to the advancement of healthcare and reduction in mortality rates. The development of medical imaging has been shown to extend human life expectancy, according to an intriguing study in [29]. Ultrasonography (US), CT scans, X-rays, PET, and MRI are the medical imaging techniques that are most frequently employed. These image modalities are significant for the detection, segmentation, and classification or diagnosis of anomalies because they offer vital functional and anatomical details about various body organs. Figure 4 displays a typology of significant medical imaging modalities.
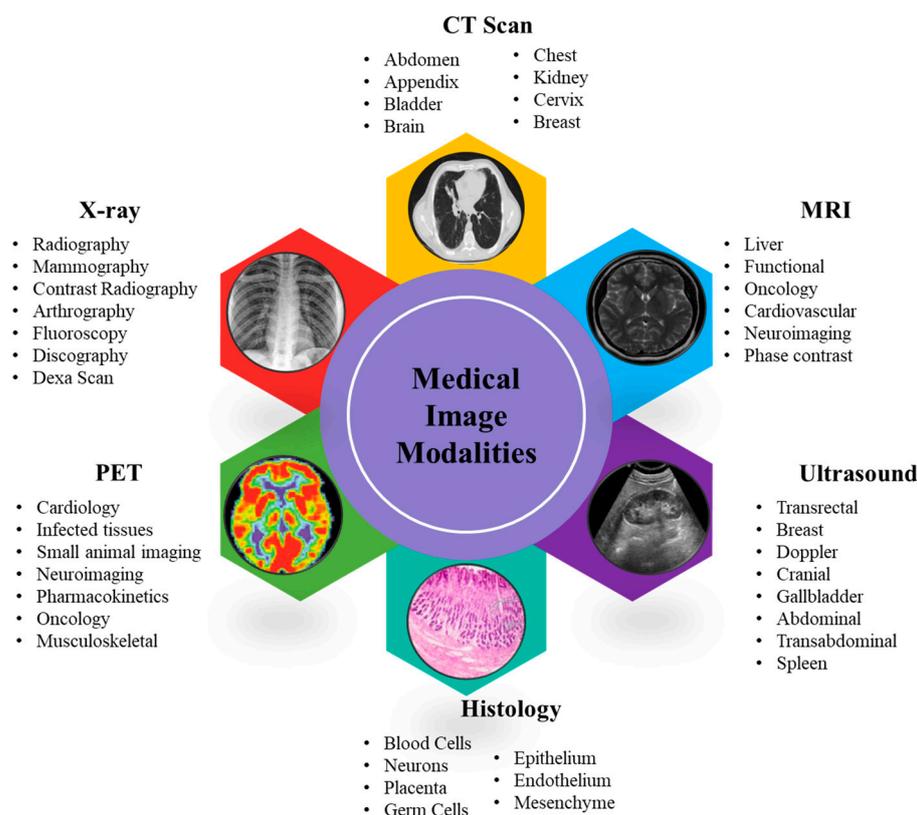
Figure 4. A typology of significant medical imaging modalities (adapted from [30]).

Medical image analysis is primarily used to support radiologists and clinicians in making accurate diagnoses and disease prognoses. Deep learning is used to perform a variety of tasks in medical image analysis, the most essential of which are classification or diagnosis, detection, and segmentation. PET models powered by AI have already demonstrated their ability to execute segmentation, detection, and classification tasks more effectively and objectively than skilled physicians [31–33]. Additionally, it is anticipated that the next generation of healthcare systems will include completely automated intelligent medical picture diagnosis systems. Few survey publications [12,30,34–36] have been written about deep learning-based medical image analysis.

2.1. Classification or Diagnosis

Deep learning applications in medical image analysis fall primarily under the category of classification or computer-aided diagnosis (CAD). In CAD, deep learning models are utilized to classify medical images into different classes or categories based on specific diagnostic tasks. Deep learning models are trained on large datasets of medical images. These datasets consist of images with corresponding classification of the presence or absence of specific diseases. Numerous researchers have reported their findings related to deep learning-based classification while analyzing the medial image datasets. L. et al. [12] have reviewed the application of deep learning in the field of big data analysis and early diagnosis of diseases while analyzing medical images, especially their segmentation and classification. To classify 14 diseases based on an X-ray of the chest, Rajpurkar et al. [37] updated the DenseNet 121 model, known as the CheXNet model. It is also found that the CheXNet exceeds average radiologist's performance on the F1 metric and also the model is able to detect all 14 diseases in ChestX-ray14. Korolev et al. [38] evaluated two approaches based on ResNet [39] and VGGNet [40] architectures for Alzheimer diagnosis. Single-lesion segmentation and recognition have been successfully accomplished using deep learning-based methods. Because there is less fluctuation between lesions, or a greater variety of lesions is present, multiple-lesion recognition is more challenging than

single-lesion recognition. Recent studies have looked into using deep learning-based methods to overcome the difficulty of recognizing multiple lesions. Ref. [41] provides a comprehensive overview and analysis of recent advances in deep learning-based multiple-lesion recognition techniques, including the identification of many diseases throughout the entire body as well as multiple lesions in various body regions.

In most of the research papers, the base algorithm used for different tasks related to medical image analysis is CNN. As a result of its higher accuracy and lower error rate, the CNN model is frequently utilized for image classification. However, in order to generalize the hidden correlations discovered in the learning data, large datasets are required. To enhance/optimize the performance of these CNN-based techniques there are two commonly used approaches reported in the literature, i.e., transfer learning [42–45] and general adversarial network (GAN) [46–48].

2.2. Detection

In addition to classification, medical image analysis techniques aim to detect specific objects, regions, or abnormalities within medical images. It enhances the accuracy, efficiency, and consistency of image interpretation and aids in early diagnosis, treatment planning, and disease monitoring. Accurate and rapid object localization of anatomical or diseased objects, such as organs and landmarks, is crucial for image registration and segmentation tasks [49–51]. Zhang et al. [52] used two stage task-oriented CNN-based regression model for anatomical landmarks extracted from MRIs and CT images. As a result, 1200 brain landmarks from MRIs while 7 prostate landmarks from CT images were detected. The goal of LUNA16 [53] challenge is to improve the ability to detect lung nodules on CT scans, which is essential for pulmonary cancer diagnosis [54]. On the same LUNA 16 dataset, deep ensemble 2D CNN approach [55] comprising three different CNNs with different layers, pooling techniques and kernels is applied and it predicted the outcome with more accuracy. Park et al. [56] used an AI model designed in a cascade structure using deep learning for detecting abdominal hemorrhage lesions in real time. The developed method could achieve reasonably good results in terms of sensitivity and specificity. Xue et al. [57] explores various deep learning techniques such as ResNet152, ResNet50, DenseNet121 and VGG16 for detecting COVID-19 and pneumonia on CT and radiography images. The suggested model outperforms other reported approaches in the literature in diagnosing COVID-19 and pneumonia. Abdelrahman et al. [58] presents the survey on distinct mammography task, i.e., breast density classification, calcification detection, mass detection and classification along with breast density classification, using CNN-based approaches. A comparison is provided with advantages and disadvantages of each CNN-based approach applied to these performed tasks.

2.3. Segmentation

One of the most difficult problems in medical image analysis is medical image segmentation, which involves separating the pixels of organs or lesions from background medical pictures like CT or MRI scans to provide crucial information on the shapes and sizes of these organs. Many researchers have proposed segmentation approaches for medical images using deep learning techniques. There are a few review articles [11,59–63] on deep learning-based medical image segmentation, which shows that deep learning-based segmentation is now firmly established as a robust tool in medical imaging applications. Deep learning techniques are not only used for segmentation in 2D medical imaging but also these techniques are being explored for target volume automatic segmentation in three types of imaging modalities, i.e., CT, PET and MRI. A comprehensive review of deep learning-based retinal blood vessel segmentation methods for five years have been conducted [64]. And it presents trend analyses on the recently published literature and provides possible solutions for the identified gaps. The state-of-the-art work towards volumetric segmentation in three different imaging modalities is presented [65]. In the presented paper, various deep learning architectures related to volumetric segmentation are summarized and compared to

the performance of different models using standard geometric evaluation metrics. Authors in [59] present their 3D deep supervision mechanism, using which they are able to perform volumetric segmentation tasks successfully conducted on liver segmentation from 3D CT scans and vessels segmentation from 3D MRI.

There are few survey papers recently published related to deep learning-based medical image segmentations for various diseases. Krishnapriya et al. [66] have conducted a survey for MRI brain tumor segmentation methods. In this review, the authors have highlighted the publicly available dataset related to brain tumor along with deep learning architectures used and tumor segmentation techniques. Liu et al. [67] have surveyed more than 150 papers for extensively covering the technical aspects related to brain tumor segmentation under imbalanced conditions, different type of network architecture design and also multi-modality processes. The authors have also provided the future research possibilities in this direction. Bonaldi et al. [68] have presented a survey based on bottlenecks and strategies related to deep learning-based segmentation in medical images for musculoskeletal anatomical structures. They have analyzed 140 articles related to anatomical structures, network architectures, bioimaging techniques and various performance indicators.

3. Vulnerability of Deep Learning-Based Medical Image Analysis

Although the deep learning-based medical image analysis has had a breakthrough in healthcare sector, it is still vulnerable to various security threats, including model inversion attack [69], poison attack [70] and several security vulnerabilities [71,72]. Among the reported attacks on medical imaging, adversarial attacks have attracted the most attention from the community of deep learning-based medical image imaging handling security concerns, as it raises a series of potential safety and security issues. Apart from disrupting the inference stage of deep learning algorithms, adversarial attacks can very easily bypass the manual check carried out by experts because of the visual similarity to its clean counterpart. Adversaries can manipulate the input medical images to deceive the deep learning models. By making subtle modifications to the images, they can cause the models to produce incorrect or misleading results, potentially leading to misdiagnosis or compromised patient care [71,73].

3.1. Adversarial Attacks against Medical Images

In this section, we list some of the most popular adversarial strategies that have been suggested for use against medical images. Deep learning model architectures are used to execute various tasks on medical pictures while analyzing a variety of adversarial threats. Systems for medical imaging that rely on deep learning are seriously at risk from these types of attacks. A "White Box Attack" is one in which the attacker has knowledge of the architecture and parameters of the underlying model. On the other hand, the attack is referred to as a "Black Box Attack" if the attacker does not have access to the deployed model architecture. Additionally, "Untargeted Adversarial Attacks" are those that just want the implemented model to be confused and forecast the incorrect class. "Targeted Adversarial Attacks", on the other hand, are those that force the model to forecast a (false) desired output. In this review, the following adversarial attacks from recently released research publications are analyzed:

3.1.1. FGSM (Fast Gradient Sign Method)

The first proposed adversarial attack was the FGSM (fast gradient sign method) [74]. FGSM is a white-box attack that provides computer vision systems with hostile examples. In order to improve the loss function, this approach extracts the adversarial gradient and changes the values of the pixels. For a one-step update along the gradient descending direction, it perturbs a clean sample. The attack is designed as follows:

$$x' = x + \epsilon \times \text{sign}\left(\nabla_x J\left(\theta, x, y\right)\right) \tag{1}$$

where x is the input image, y is the label and θ represents the weights of the model. Moreover, ϵ is the magnitude of perturbation, J (θ, x, y) is the gradient loss, sign $(\cdot)$ is the sign function and $\nabla_x (\cdot)$ is the gradient w.r.t. x.

3.1.2. BIM (Basic Iterative Method) or I-FGSM

An iterative and developing approach of FGSM is the BIM (basic iterative method) or I-FGSM [75]. When the picture is misclassified, it conducts an FGSM with a value and updates its value for T iterations with a minor perturbation. This approach is described as follows:

$$x_{t+1}' = x_t' + \alpha \times \text{sign}\,(\nabla_x \, \text{J}\,(\theta, x_t', y)) \tag{2}$$

where $\alpha \text{T} = \epsilon$ and the α is the magnitude of the perturbation for each iteration.

3.1.3. PGD (Projected Gradient Descent)

The generalization of BIM, known as PGD (projected gradient descent) [76], does not include the condition $\alpha \text{T} = \epsilon$. Perturbations are limited by projecting adversarial samples from each iteration into $\epsilon - L_\infty$ or $\epsilon - L_2$ neighbor of the clean image.

3.1.4. C&W (Carlini & Wanger)

Another state-of-the-art attack is C&W (Carlini & Wagner) [77], which comprises of three techniques: $C \& W\infty$, $C \& W2$ and $C \& W0$, which minimize $L\infty$, $L2$ and $L0$ norms, respectively, to compute the perturbation's value.

3.1.5. JSMA (Jacobian-Based Saliency Map Attack)

A few pixels are affected by the iterative JSMA (Jacobian-based saliency map attack) [78], which only modifies the value of one pixel every iteration while leaving the others unchanged. The saliency map is created in this manner. The region that has had the greatest significant perturbation is then chosen, and it is perturbed in a clean image.

3.1.6. UAP (Universal Adversarial Perturbation)

The UAP (universal adversarial perturbation) attack [79] tries to find the best perturbation that misclassifies the majority of the data points by perturbing all the photos in the dataset.

3.1.7. Deep Fool (DF)

A competing attack called deep fool (DF) aims to use the nearest boundary as an example. According to the authors, this technique resulted in a subtle disturbance as opposed to crude extrapolations of an optimal distributive vector created via FGSM. One loss gradient in l(f(k) and y) is used in the DF attack, as shown below [80].

3.2. Adversarial Medical Image Analysis

The objective of a medical adversarial attack is to produce adversarial cases to thwart medical diagnosis models while they are still in the inference stage. The no-box adversarial approach against systems that analyze medical images was researched by Bortsova et al. in detail [81]. Numerous studies have shown that pre-training can significantly improve the transferability of the surrogate model to the target black-box model. Their findings indicate a relationship between the value of disruption and the effectiveness and perceptibility of the attacks. Finally, attack performance might be affected when the attacker and target have different data and models, which is improved by pre-training models, which also increases adversarial transferability.

Paschali et al. [82] investigated how adversarial attacks affected the classification of skin lesions and brain segmentation. Inception-v3 [83], Inception-v4 [84], and MobileNet [85] models have been used for the classification task, while the segmentation work was carried out using SegNet [86], U-Net [87], and DenseNet [88]. The most effective models for classification and segmentation tasks, according to experiments, were

InceptionV3 and DenseNet. The authors demonstrated that a model's robustness for classification is connected with its depth, whereas a model's efficiency for segmentation is increased by packed blocks and skip connections. The hostile samples were barely evident because the SSIM was 0.97–0.99.

Fundoscopy, dermoscopy, and chest X-ray images were subjected to PGD white and black box attacks by Finlayson et al. [89] using a pre-trained ResNet50 model [39]. In both instances, the model's accuracy was significantly reduced.

In order to perform segmentation tasks, Bortsova et al. [90] experimented with targeted PGD attack in X-rays. The model fragmented the heart symbol rather than the actual heart since they added barely discernible noise to the photographs. Additionally, they used white-box, black-box, and untargeted PGD attacks, which considerably reduced the model's average IoU.

The COVID-19 classification accuracy from X-rays and CT scans was investigated by Pal et al. [91]. They developed adversarial samples using the FGSM attack and evaluated them using the VGG-16 and InceptionV3 models. These models are susceptible, as evidenced by the accuracy declines of up to 90% in VGG-16 and up to 63% in InceptionV3.

Hirano et al. [92] evaluated the vulnerability of CNN-based COVID-Net [93] model which is one of the first deep learning model to detect COVID-19 using chest X-ray (CXR) images and is an open source and also available for general public. Targeted and non-targeted, two types of attacks are explored by applying perturbation generated via the fast gradient sign method (FGSM). The COVID-Net CXR small and CXR big models have both been assessed by the authors. Their findings demonstrated that, after adding 2% universal adversarial perturbations, both models achieved success rates for non-targeted and targeted attacks of >85% and >90%, respectively. Additionally, scientists have demonstrated that these models result in normal and pneumonia test pictures as COVID-19 images with larger perturbations. Furthermore, they examined COVID-Net's susceptibility in comparison to certain other DL models including ResNet and VGG. They employed adversarial retraining as a defense strategy and used the COVIDx dataset.

For the categorization of skin cancer, diabetic retinopathy, pneumonia, and other diseases, Hirano et al. [94] looked into universal adversarial attacks on DNNs. They tested both targeted and non-targeted attacks using a variety of models, including VGG16, VGG19, InceptionV2, DenseNet169, DenseNet121, and ResNet50. They found that, in the majority of situations, adversarial training was ineffective, particularly in attacks that were not specifically targeted. While this was happening, non-targeted attacks had a low transferability rate. Finally, according to the authors, VGG16 and VGG19 appear to be more resilient than the other models.

MRI images for brain tumor segmentation include four different modalities (T1, T2, T1ce, and FLAIR) with various intensities to make it simple to identify and label the brain tumor. Cheng et al. [95] looked at the outcomes of adversarial instances when they are used concurrently across all modalities and on each modality separately. The MICCAI BRATS 2019 [96] dataset and an ensemble U-Net model were used in the experiments. They employed universal random perturbation, which is comparable to [79], for the development of adversarial cases. The findings demonstrated that simultaneous disruption greatly reduces model accuracy, but perturbation of only one modality only marginally lowers accuracy.

On three datasets—ChestX-ray8 [97], ISIC [98], and fundoscopy [99]—Ma et al. [100] analyzed the robustness of the ResNet50 model. They used four cutting-edge white-box attacks—FGSM, PGD, C&W, and BIM—and concentrated on untargeted situations. Additionally, the perturbation value was calculated, and it was discovered that the strongest attacks, C&W, BIM, and PGD, had nearly 100% attack accuracy everywhere. Dermoscopy photos had no significant variation but were slightly more reliable than the other datasets. They also used four detectors, KD [101], LID [102], deep features and quantized deep features-based detectors, which had very high detection accuracy for detecting adversarial samples.

The impact of adversarial instances on retinal images was investigated by Shah et al. [103]. In order to identify diabetic retinopathy, they looked at image-based (CNN-0 [104], CNN-1 [105], and hybrid lesion-based [106] algorithms for medical image analysis. In order to create adversarial images, CNN-0 and I-FGSM were utilized, and CNN-1 and hybrid lesion-based models were tested on them. As evidenced by their respective accuracy reductions of 45% and 0.6%, the results demonstrate that CNN models are relatively susceptible and hybrid lesion-based models are more resilient.

The current attacks on medical imaging are outlined in Table 1. These kinds of attacks were investigated only on tasks involving classification and segmentation. The PGD method appears to be the most successful, and FGSM and PGD were the most widely used strategies. A majority of the investigations also made use of MRI, fundoscopy, dermoscopy, and X-ray images.

Table 1. Summary of attacks on tasks involving classification and segmentation using deep learning models.

Ref.	Year	Task	Image Modality	Model	Attack Scenario	Attack	Performance Degradation
[81]	2021	Classification	X-ray, Fundoscopy, Microscopy	Inception-v3 and Densenet-121	No-box	FGSM, PGD	35%
[82]	2018	Classification, Segmentation	MRI, Dermoscopy	InceptionV3, InceptionV4, MobileNet, SegNet, U Net and DenseNet	White-box, No-box	FGSM, DeepFool, SMA	6–24%/ 19–40%
[89]	2018	Classification	Fundoscopy, Dermoscopy, X-ray	ResNet50	White-box, Black-box	PGD	50–100%
[90]	2021	Segmentation	X-ray	Similar to U-Net	White-box, No-box	PGD	Up to 100%
[91]	2021	Classification	CT, X-ray	VGG-16, Inceptionv3	White-box	FGSM	Up to 90%
[92]	2020	Detection	Chest X-ray	COVID-Net	White-box	FGSM	Up to 45%
[94]	2021	Classification	OCT, X-ray, Dermoscopy	VGG16, VGG19, Inception, DenseNet169, DenseNet121 ResNet50	White-box	UAP	Up to 72%
[95]	2020	Segmentation	MRI scans	U-Net	White-box	UAP	Up to 65%
[100]	2021	Classification	X-ray, Fundoscopy, Dermoscopy	DNN	White-box	FGSM, BIM, PGD, CW	Up to 100%
[103]	2018	Classification	Fundoscopy	CNN, Hybrid lesion-based model	No-box	I-FGSM	45%/0.6%

4. Deep Learning for Medical Image Cryptography

The use of medical images to guide diagnosis and treatment strategies, among other things, is gaining popularity as medical imaging technology becomes more widespread. For instance, images from chest CT scans and brain MRIs can be utilized to help diagnose lung disease and find brain tumors, respectively. However, because these medical images contain private and sensitive information about the patients, their disclosure could have an impact on the patients' right to privacy as well as legal repercussions for the institutions. Therefore, attempts have been made to build security solutions (such as cryptographic primitives) to secure these medical images and safeguard the privacy of the patients.

The schematic of generic secure cloud-based IoMT system within the healthcare sector's heterogeneous environment is shown in Figure 5. In this type of the IoMT systems, it is expected that the medical images are transmitted to the cloud through cryptosystems in the form of encrypted data. Then, there are central cloud computing servers with deep learning models for various medical image analysis applications. These clouds return encrypted results/predictions to different healthcare centers. Readers must note that encrypted results are shown in the image form whereas it may not be necessarily true each time. These results are decrypted by authorized doctors or clinicians for various analysis purposes.
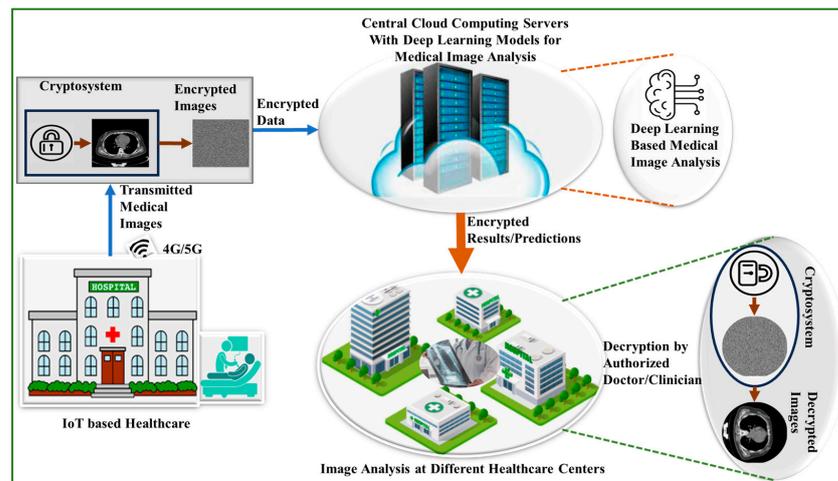
Figure 5. Schematic illustration of a generic secure cloud-based IoMT system within the healthcare sector's heterogeneous environment.

Cryptographic approaches are being used in various ways and reported in the literature. The following subsections cover the reported papers related to each categorized approach. Figure 6 shows the different applications of cryptographic approaches used in deep learning-based medical image processing securely. Figure 6a shows the example of encryption approach used while processing the medical images [107], whereas (b) illustrates the encrypted denoising approaches in the IoT-based healthcare systems. Figure 6c focuses on the tumor classification based on encrypted MRI images using deep learning-based medical image analysis and (d) shows Chest X-ray images encrypted first and then compressed before processing through deep learning-based models, and then these images are decompressed and decrypted by the authorized doctors or clinicians. Figure 6e illustrates the end-to-end encryption scheme in cloud-based services, in which homomorphic encryption is used and deep learning model works on these homomorphic encrypted images only, which is reported as a more secure encrypted approach while performing deep learning-based medical image analysis., and (f) shows the deep learning-based key generation approach for encrypting the medical images while performing various analytical tasks on these images.
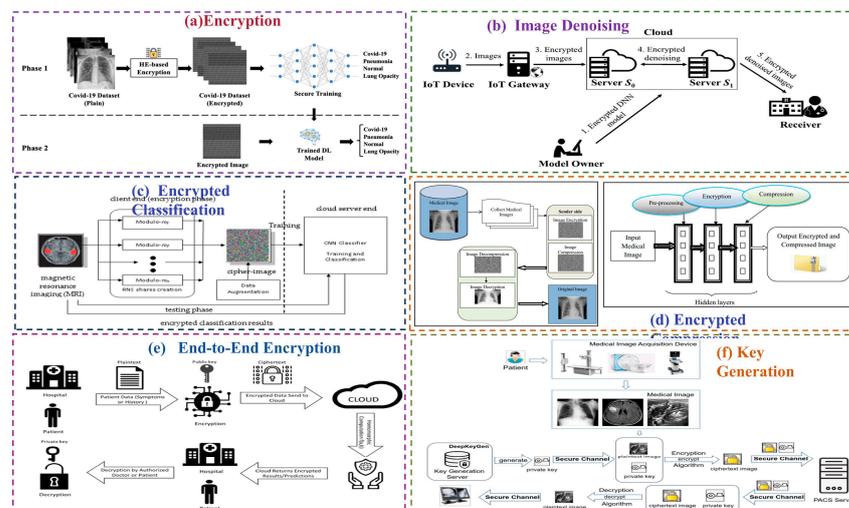

Figure 6. Applications of cryptography in various medical imaging problems along with the deep learning-based approaches. Figure sources: (**a**) [107], (**b**) [108], (**c**) [109], (**d**) [110], (**e**) [111], and (**f**) [22].

4.1. Encryption Algorithms for Deep Learning-Based Medical Image Analysis

Medical imaging is regarded as one of the most sensitive and significant types of data in information systems. A robust encryption scheme that can withstand adversarial or cryptographic attacks is necessary when sending medical images over the network. Confidentiality is the most crucial component that requires careful consideration among the three security objectives for the security of information systems, namely confidentiality, integrity, and availability. When it comes to the encryption of medical images while they are processed by deep learning algorithms, there are two types of techniques, namely cryptography and homomorphic encryption, that are commonly documented in the literature. Here, some of the most recent work in this direction has been discussed.

Radiologists could utilize the technique that Naik et al. [112] demonstrated to identify lung diseases. The DenseNet-121 model is used by the suggested system to process the chest X-ray pictures. Additionally, they used the AES-128 technique to secure the private data that are included in medical photographs before uploading them to the cloud. An online cloud program has been created by Kumar et al. [113] to assess if tumors are visible in MRI images. The photos were sent to the cloud server using the AES-256 cryptographic technique. For tumor inference from the images, they utilized the CNN model which had an accuracy rate of 97.87%.

The smart healthcare system presented by Mohanty et al. [114] incorporates the capability of tumor detection from brain MRI images using CNN-LSTM and additionally the proposed system is secured by using the SHA-256 encryption technique. In the suggested smart healthcare system, the modified SHA-256 algorithm is recommended for safe medical data processing. With the suggested secure medical data processing system, they may attain the accuracy of 98.51%.

Paul et al. [115] presented a strategy based on an LSTM model that is trained on the MIMIC-III dataset and uses homomorphic encryption to protect sensitive data. Because the CKKS encryption system can be used to time series data, such as hourly clinical statistics, homomorphic encryption is used instead. For the goal of predicting in-hospital mortality, they have deployed this encrypted LSTM model with enhanced accuracy.

PINPOINT, a temporal convolutional neural network, was developed by Falcetta et al. [116] to predict time series while maintaining anonymity. It is suggested to use a cloud-based forecasting system with integrated homomorphic encryption and temporal CNN. The suggested system is validated using four different kinds of datasets. Forecasting of new cases for COVID-19 is also included, and it is successfully carried out with positive results.

Munjal et al. [111] presented the systematic review on homomorphic encryption and its applications in the healthcare sector. They have discussed homomorphic encryption evolution and their types along with the applications. In this paper, authors have discussed and compared various approaches using homomorphic encryption for detecting cancer, analyzing heart rate, cardiovascular problems and also secure query generating systems in healthcare.

The privacy-preserving deep learning strategy for categorizing COVID-19 from the chest X-ray pictures was presented by Boulila et al. [107]. In order to classify COVID-19 X-ray images, the COVID-19 dataset is encrypted using partly homomorphic encryption, and the encrypted images are then fed into the MobileNetV2 model. When they use a deep learning model on encrypted photos, they can obtain an accuracy of 93.3%.

Table 2 lists the current encryption techniques for deep learning-based medical image processing. When conducting activities relating to disease detection, classification, segmentation, and COVID-19 forecasting, these encryption algorithms are also used. While researchers have just lately begun to report on homomorphic encryption, AES and SHA are the two most often used cryptographic algorithms.

Table 2. A summary of medical image encryption techniques for deep learning-based medical image analysis.

Ref.	Year	Organ	Task	Image Modality	Datasets	Model	Metrics	Type of Encryption Algorithm	Algorithm Name
[112]	2020	Chest	Lung diseases detection	X-ray	NIH Chest X-rays [117]	DenseNet-121	AUROC scores, Accuracy, Confusion matrix	Symmetric algorithm	AES-128
[115]	2021	Multi-organ	In-hospital mortality prediction task	Multi-modalities	MIMIC-III (CCU Dataset) [118]	RNN-LSTM	Precision, Recall	Homomorphic encryption	CKKS
[113]	2022	Brain	Brain tumor segmentation	MRI	Real-Time Dataset	CNN	Accuracy rate	Symmetric algorithm	AES-256
[114]	2022	Brain	Tumor detection	MRI, EEG	Brain Tumor Dataset [119]	CNN-LSTM, DNN	Accuracy rate	Hash functions	SHA-256
[116]	2022	Chest	COVID-19 New cases forecasting	COVID-19 New cases dataset	NA	PINPOINT (Temporal CNN)	NA	Homomorphic encryption	Brakerski/ Fan–Vercauteren (BFV)
[107]	2022	Chest	COVID-19 Classification	X-ray	COVID-19 Radiography Database [120]	MobileNetV2	Precision, Recall, F1 score, Support	Homomorphic encryption	Paillier Method

4.2. Medical Image Resolution Improvement or Denoising for Deep Learning-Based Medical Image Analysis

Along with the rapid advancement in the digital image processing technology, improving the resolution of the medical images or medical image denoising remains a fundamental challenge to meet the better diagnosis in such a heterogeneous IoMT environment today. Here are some recently published works related to enhancing the resolution of medical images.

More S. et al. [121] presented a CNN-based sparse aware noise reduction strategy for enhancing the quality of reconstructed MR images in order to produce high quality pictures. Additionally, authors have included encryption and decryption in the suggested IoT architecture using the ABE algorithm.

Gayatri S. et al.'s [24] research focus on developing a lightweight cloud infrastructure for processing medical data while maintaining the privacy of the data's contents. The pseudo-predictive deep denoising network (PPDD) was developed using deep learning techniques. The dynamic data are unpacked and a denoise procedure is used at the edge devices to reduce the complexity of the storage system. A comparison of the proposed architecture's validity with earlier related work published in the literature is also included.

Zheng Y. et al. [108] proposed the privacy-preserving DNN-based image denoising on the cloud for IoT multimedia healthcare applications. According to the suggested system design, the model owner initially stores an encrypted trained DNN model in the cloud. The encrypted DNN model that was previously stored is used to perform image denoising in the encrypted domain after the encrypted images have been transmitted to the cloud. Thanks to the suggested security strategy, the DNN model and private picture content are all kept private throughout the entire cloud-based service flow.

Alslman Y. et al. [122] proposed a hybrid encryption approach that encrypts the medical pictures, first using AES first and then a deep learning model (autoencoder). By using autoencoders as a feature extraction method, this hybrid model enables to have control over the size and structure of the medical images being encrypted and then communicated. During decryption, the hybrid encryption approach that has been proposed can also denoise the medical images.

Shafai et al. [123] suggested the implementation of the CADTra model for automatic detection of disorders associated with pneumonia. The constructed model uses autoencoder techniques with a modified loss function to denoise the images and deep learning algorithms to classify data. They have applied transfer learning techniques and a four-layer convolutional neural network to the categorization of pneumonia. With regard to chest X-ray pictures, this model supports the multi-class classification while supporting the binary classification for CT images. Additionally, 98% and 99%, respectively, of the proposed model's correctness have been attained.

The multi-scale denoising convolutional neural network (MSDCNN) model was proposed by Chui et al. [124] for the detection of prostate cancer, and this model is also capable of suppressing noise in MRI data. The process between the noisy picture dataset and the residual image dataset is what constitutes residual learning. The cleaned picture dataset is then created from the residual learning output and subsequently processed using a multi-scale convolutional neural network. For further classification processing, this cleaned picture dataset is modified with smoothing, down sampling, and fine graining.

Table 3 presents the list of recently published works related to enhancing the resolution of medical images while performing the various tasks using deep learning algorithms. In some works, autoencoders are used as image denoising algorithms, whereas few authors have reported modified deep learning algorithms used for denoising of the medical images before performing the classification, detection, or reconstruction-related tasks.

Table 3. List of medical images denoising techniques for deep learning-based medical image analysis.

Ref.	Year	Organ	Task	Image Modality	Datasets	Model	Metrics	Image Denoising Algorithm
[108]	2021	Chest	Classification	X-ray	ChestX-Ray8 [97]	DNN	PSNR, SSIM	DNN-based
[121]	2021	Heart	Reconstruction of high-quality images	MRI scans	Stroke prediction [125]	CNN	PSNR, SSIM, MSE	SARN technique
[123]	2022	Chest	Classification	CT scan, X-ray	COVID-CT [126], Chest X-ray images [127], Chest X-ray and CT images [128]	Deep CNN (CADTra)	Accuracy, Precision, Recall, F1-score, Log loss, PSNR, SSIM	Autoencoder
[124]	2022	Prostate gland	Detection	MRI scans	NaF Prostate [129], TCGA-PRAD [130], Prostate-3T [131], PROSTATE-DIAGNOSIS [132]	Multi-scale denoising convolutional neural network (MSDCNN)	Sensitivity, Specificity, Accuracy	Residual learning
[122]	2022	Eye	Classification	Eye fundus images	Messidor2 [133]	Autoencoder	Loss, Encryption Time	Autoencoder and AES
[24]	2023	Multi-organ	Classification	Real-time CT scans	Real time CT scans	Pseudo-predictive deep denoising network	SNR, SI, CNR, ER	Deep denoising network

4.3. Privacy-Preserving Object Detection and Classification in Medical Image Encryption Algorithms

Deep learning-based analysis of medical images can extract sensitive information through object detection. These medical images include embedded personal information that must be secured. Consideration should be given to the security of the data itself as well as the security of the deep learning-based processing and the information that was collected. Given that it has been utilized and will be employed in several object-detection healthcare applications in the near future, the security issues with the deep learning-based approach becomes crucial. For medical image privacy, some research papers have reported on privacy-preserving object detection along with the image encryption algorithms.

Liu et al. [134] have proposed the lightweight privacy-preserving faster R-CNN framework (SecRCNN) for object detection from medical images. While designing this framework, a secret sharing sub-protocol is added to complete the secure computation in it. To demonstrate the efficiency and secure computation through SecRCNN, comprehensive theoretical analysis is performed along with the extensive experiments. To improve the efficiency of SecRCNN, sub-protocols involved in this R-CNN are modified and authors are able to achieve better computation time and efficiency.

Chao et al. [109] present fully homomorphic encryption tightly integrated with the CNN functions (CaRENets). They present a novel resource-efficient method for homomorphic inference on encrypted images. It has practical implications for secure deep learning inference in medical imaging systems. The authors have considered two ophthalmology applications involving the classification of retinopathy of prematurity (ROP) and diabetic

retinopathy (DR). They have provided the set of experiments to demonstrate that CaRENets can significantly improve both inference and memory efficiency.

Usman et al. [135] proposed an approach for a secure dyslexia biomarkers classification using a deep CNN model and residual number system (RNS) is used to encrypt the dataset. The proposed cascaded deep CNN shows classification outcomes with a performance accuracy of 73.2% on the encrypted data.

Usman et al. [136] proposed a privacy-preserving classification model named as homomorphic residue number system-CNN (HoRNS-CNN). This model is the combination of pre-trained CNN model and RNS-FHE encryption scheme. They are able to obtain encouraging results for classifying the dyslexia neural biomarkers. The collection of recently released articles on privacy-preserving or security mechanisms used for object recognition or classification during the processing of medical images using deep learning models is shown in Table 4.

Table 4. List of Privacy-Preserving Object Detection and Classification in Medical Image Encryption Algorithms.

Ref.	Year	Organ	Task	Image Modality	Datasets	Model	Metrics	Privacy Preserving/Security Mechanism
[109]	2019	Eye	Classification	Fundoscopy	ROP Dataset [137], IDRiD [138]	CNN	Accuracy, Memory Efficiency, Latency	Fully homomorphic encryption
[135]	2020	Brain	Classification	MRI	Kaggle brain MRI dataset	Deep CNN	Accuracy	RNS encryption
[136]	2022	Brain	Classification	Brain MRI	NA	CNN	Accuracy	RNS-FHE
[134]	2022	Multi-organ	Detection	Image CLEF medical image dataset (contains multi-modality images)	CLEF medical image dataset [139]	SecRCNN	Computation overhead	Additive secret sharing-based sub-protocols

4.4. Image Encryption and Compression in Deep Learning-Based Medical Image Processing

The security of medical images for transmission and storage is a crucial concern, given the exponential proliferation of images. An effective strategy frequently used to protect medical image data is encryption. These medical images take up a lot of storage space, so compression is required before transmission. In this section, recently reported work in this direction is presented.

Selvi et al. [110] developed an adaptive sigma filterized synorr certificateless signcryptive Levenshtein entropy coding-based deep neural learning (ASFSCSLEC-DNL) technique to perform encryption and compression on medical images. The objective of the ASSCSLEC-DNL technique is to enhance the security of the medical images during transmission. The proposed approach is applied on chest X-ray medical images and the results are found to be encouraging and comparable with the existing state-of-the-artwork.

A block-based perceptual encryption (PE) algorithm approach that may be used with both grayscale and color medical images was proposed by Ahmad et al. [140]. The JPEG compression technology is used to reduce the size of these images. Chest X-ray images are used for the implementation of a deep learning-based system for TB screening. On three CXR image datasets, the suggested technique is examined in terms of encryption, compression, and DL-based categorization. The lossy manner of compression was used, and it was discovered that the performance of restored images is unaffected by distortion.

Kumar et al. [141] proposed a secure framework, i.e., MediSecFed, for federated learning in a hostile environment. This model relies on the ideas from knowledge distillation and model inversion to ensure additional security and privacy features. This method is evaluated on two chest X-ray datasets. The proposed method was also compared with FedAvg and it outperformed by 15% on both the datasets in a hostile environment.

A novel medical image crypto-compression algorithm is proposed, which is based on artificial neural network (ANN) and the chaotic system, by Hajjaji et al. [142]. The main objective of the proposed approach is to preserve the sensitive information of medical

images. The proposed approach was validated on both the steps, i.e., encryption and compression. Results showed that the security and quality of the compressed images are comparable to the results of uncompressed images. Table 5 summarizes the list of encryption or security algorithms applied along with the compression mechanism while performing deep learning-based images analysis for various tasks.

Table 5. List of encryption or security algorithms with compression mechanism for deep learning-based medical image analysis.

Ref.	Year	Organ	Image Modality	Datasets	Model	Metrics	Encryption/Security Algorithm	Compression Algorithm
[110]	2021	Chest	X-ray	Chest X-ray images (pneumonia) [127]	Deep feed-forward artificial neural network	PSNR, Encryption Time, Compression Ratio	Synorr certificateless signcryption	Levenshtein entropy encoding technique
[140]	2022	Chest	X-ray	Shenzhen dataset [143]	EfficientNetV2	PSNR, SSIM, and MS-SSIM, Accuracy	Perceptual encryption algorithm	JPEG compression algorithm
[141]	2022	Chest	X-ray	COVIDX-8B, COVIDX-8A [93]	ResNet18 and ResNet34	Accuracy	Federated learning	KD
[142]	2019	Brain	MRI	NA	ANN	PSNR, UIQ, SNR and correlation factor	ANN	Piecewice linear chaotic map (PWLCM)

4.5. Key Generation in Encryption Algorithms for Medical Image Analysis

Key generation is a critical component of encryption algorithms used in medical image analysis. Encryption is employed to protect sensitive medical data and ensure its confidentiality, integrity, and authenticity. When it comes to medical image analysis, such as the processing and transmission of medical images, the use of encryption algorithms is particularly important.

Ding et al. [22] proposed a novel deep learning-based key generation network (Deep-KeyGen) to generate the private key, which can be used for encrypting and decrypting of medical images. DeepKeyGen was evaluated on chest X-ray dataset, the BraTS18 dataset and the ultrasonic brachial plexus dataset. The experimental results also show that DeepKeyGen achieves higher levels of security when compared to other key generation algorithms.

Using a neural network with key generation, Krishna et al. [144] introduced a novel dynamic medical image encryption technique. The key generation neural network receives the seed value from the ROI of the image. Following the creation of the key, the input image is encrypted using our inventive encryption algorithm, which is represented here by an encryptor. To further strengthen security, the key is itself encrypted before being transmitted. Although the encryption strength and key strength of the suggested approach are superior, the lengthier encryption time needs to be reduced. To test the proposed dynamic image encryption technique, X-ray images are used in the experiments. Table 6 presents the summary of published work related to key generation algorithms while performing the encryption or security on deep learning-based medical image analysis.

Table 6. Summary of encryption/security algorithms along with key generation mechanism.

Ref.	Year	Organ	Image Modality	Datasets	Metrics	Encryption/Security Algorithm	Key Generation Algorithm
[22]	2020	Chest, Neck, Brain	X-ray, MRI, US	Montgomery County's chest X-ray dataset [143], Ultrasonic brachial plexus dataset [145], BraTS18 dataset [96]	Entropy, NPCR, UACI, Learning Rate, P-value	DeepKeyGen	Generative adversarial network (GAN)
[144]	2022	Hand	X-ray	Dataset from [146]	Entropy, NPCR, Encryption speed	AES-256 and Hill cipher	GAN-based PRNG

4.6. End-to-End Image Encryption for Deep Learning-Based Medical Image Analysis

Deep learning-based image encryption methods have recently drawn a lot of attention. When utilizing end-to end image encryption methods, the content is hidden until it is decrypted using the correct and permitted key. Using an encryption key, the original image is converted into a cipher image, which is then decrypted to reveal the original image using a decryption key.

An image encryption method based on the Cycle-GAN network was proposed by Panwar et al. [147]. The encryption and decryption network can effectively encrypt and decrypt an input image after training. The encrypted images are the same size as the original images in terms of size. The secret keys in this method serve as the trainable parameters. To achieve end-to-end encryption, the authors made sure that the hospital database stored the encrypted images and that only a person with access to the keys could retrieve the original images by utilizing the proposed approach EncipherGAN.

Gaudio et al. [148] proposed the explainable privacy preserving image compression method named as DeepFixCX, which compresses images without learning by removing or obscuring spatial and edge information. DeepFiXCX improves predictive classification performance of a DNN on glaucoma and cervix-type detection and can improve multi-label chest X-ray classification performance.

For end-to-end image diffusion, Zhu et al. [149] developed the flexible image encryption and decryption ResNet (FEDResNet) architecture. The security of the encryption network is improved in the proposed design by serial and parallel distribution of the images. The two crucial planes are built using a user-defined chaotic map to regulate access rights to images. After rigorous testing, they were able to attain high levels of security with acceptable efficiency.

Pati et al. [150] proposed present the community-driven generally nuanced deep learning framework (GaNDLF) as an end-to-end solution for scalable clinical workflows. The proposed GaNDLF is able to process the images of various domain including radiology scans and digitized histology WSIs along with the various workload, e.g., segmentation, regression and classification.

Ding et al. [151] proposed an end-to-end two-stage generative adversarial neural network (ToStaGAN) to improve the brain tumor segmentation from MRI images. In the proposed approach, UNET network is used in the first stage and U-shaped contextual autoencoder (ConEnDer) is used in the second stage. The performance of the proposed two-stage generation network is evaluated on BRATS2015 and it is found that the proposed network achieve better performance than the one-stage network. Table 7 summarizes the list of encryption or security algorithms applied along with the while performing deep learning-based images analysis for various tasks. It can be seen from the table that in this direction most of the work is reported very recently.

Table 7. List of end-to-end encryption or security algorithm with deep learning model.

Ref.	Year	Organ	Image Modality	Datasets	Task	Metrics	Encryption/Security Algorithm	End-to-End Deep Learning Model
[151]	2021	Brain	MRI	BRATS2015 [152]	Segmentation	Dice, Positive predictive value (PPV) and Sensitivity.	Two-stage generative adversarial neural network (ToStaGAN)	UNET and U-shaped contextual autoencoder
[149]	2022	Chest	X-ray	ImageNet	Classification	Accuracy	Image diffusion with dilated ResNet	FEDResNet
[147]	2023	Skin	Dermoscopy	Skin cancer dataset [153]	Classification	PSNR, SSIM, Correlation Coefficient, Entropy	Cycle-GAN network	Encipher GAN
[148]	2023	Chest, Cervix, Eye	X-ray, Fundoscopy, CT scan	Chexpert [154], Intel-MobileODT dataset [155], KimEye dataset [156]	Classification, Detection	Speed and Accuracy	Explainable machine learning	DeepFixCX
[150]	2023		MRI, CT		Classification, Segmentation	Dice similarity coefficient, Hausdorff distance, MSE, Accuracy	UNet, ResUNet	GaNDLF

5. Discussion

This section discusses numerous factors to take into account when implementing deep learning techniques for secure and confidential medical image analysis. In light of deep learning's recent success with these tasks, a roadmap for the future of artificial intelligence in secure medical image analysis is developed as well.

5.1. Various Deep Learning Architectures with Security Features for Medical Image Analysis

In order to protect the confidentiality and integrity of medical image analysis, deep learning architectures with security features are essential. The efficacy of deep learning-based medical image analysis is demonstrated by a variety of recently published literature [12,37–41,49,49–62,64,64,65,157–159]. In the literature, several deep learning architectures have been described to handle various imaging modalities and tasks related to medical image processing with different components of encryption or cryptography [107,110,112–116,123,124,135,136,140,141,144,147–151,160,161]. Multi-layer networks, cascaded networks, training models with partial and complete supervision, transfer learning, and conventional deep learning architectures are some of these designs. Majority of the time, there are few expert reviews and scant data. Medical image processing has typically favored shallow networks over highly deep designs utilized in computer vision applications [40,162]. This survey's analysis reveals that many DCNN network topologies have been implemented or suggested for use in medical image processing. These architectures invest a lot of effort on decreasing the parameter space, speeding up computing, and handling 3D data. It is frequently observed that DCNN-based architectures perform better when processing medical images when compared to other deep learning frameworks.

5.2. Limitations of Deep Learning for Medical Image Cryptography and Future Prospects

The constraints of deep learning for medical image cryptography should be considered by researchers and practitioners. For overcoming the obstacles and identifying opportunities in the future, it is essential to comprehend these constraints. Several drawbacks of deep learning for medical image cryptography are listed below, along with anticipated future developments.

5.2.1. Limited Generalization

Deep learning algorithms that have been trained on a particular dataset may have trouble adapting adequately to new or varied medical image data. In cryptography activities, this may result in decreased performance and compromised security. The development of models that more accurately generalize across various medical imaging modalities, illness types, and patient groups may be the main emphasis of future study.

5.2.2. Adversarial Attack Vulnerability

Deep learning models are vulnerable to adversarial attacks, in which dishonest individuals tamper with the input data to falsify the model's predictions. The security and integrity of the encrypted data can be jeopardized by adversarial attacks in medical imaging cryptography. To develop deep learning models more resistant to such attacks, future research might investigate reliable training techniques and protection mechanisms.

5.2.3. Computationally Expensive

Deep learning models used for medical image cryptography sometimes need expensive hardware and protracted training periods. This may make them less useful, particularly in real-time contexts or contexts with limited resources. Future work should focus on creating hardware accelerators, optimization methods, and more efficient algorithms to lessen the computational load and accelerate cryptographic operations.

5.2.4. Data Availability and Quality

Large-scale high-quality datasets are required for the training of deep learning models. Access to large labeled datasets, however, may be constrained in medical image cryptography because of data scarcity and privacy issues. Future developments could include the creation of privacy-preserving methods that permit the training of models on encrypted or decentralized data sources while retaining the integrity and security of the data.

In a nutshell, despite deep learning's potential for medical image cryptography, it has drawbacks related to generalization, adversarial attacks, processing demands, and the availability of high-quality data. Future possibilities include overcoming these constraints through research and development initiatives targeted at enhancing generality, robustness, efficiency, and accessibility of high-quality data.

6. Conclusions

A comprehensive review of deep learning-based medical image analysis is offered, along with security considerations. In conclusion, classification, detection, and segmentation in all subfields of medical image analysis have found conventional neural network-based deep learning methods to be more acceptable. As a result, researchers are looking into many angles for potential security solutions. The security of deep learning-based medical image analysis and its cryptographic aspects are the only topics covered in this study. This paper investigated six distinct areas of cryptography with an eye toward security, privacy preservation, various encryption approaches, end-to-end encryption, and certain security mechanisms based on deep learning algorithms. New security strategies need to be investigated and studied considering the diversity in how medical images are presented and the use of deep learning algorithms. The availability of more processing power and better DL architectures with security features enable higher performance for larger datasets. This achievement would ultimately lead to better computer-assisted detection and diagnosis methods. To deploy these techniques, additional study as well as security verification that these DL-based systems do not leak patients' private information are needed. Also, for those imaging modalities where these procedures are not already used, more research is needed before adopting these methods. Given the recent developments, combining advanced security practices and procedures with deep learning approaches would greatly increase medical image analysis for smart healthcare applications.

References

1. Lee, D.; Yoon, S.N. Application of Artificial Intelligence-Based Technologies in the Healthcare Industry: Opportunities and Challenges. *Int. J. Environ. Res. Public Health* **2021**, *18*, 271. [CrossRef] [PubMed]
2. Tortorella, G.L.; Saurin, T.A.; Fogliatto, F.S.; Rosa, V.M.; Tonetto, L.M.; Magrabi, F. Impacts of Healthcare 4.0 Digital Technologies on the Resilience of Hospitals. *Technol. Forecast. Soc. Change* **2021**, *166*, 120666. [CrossRef]
3. Aceto, G.; Persico, V.; Pescapé, A. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0. *J. Ind. Inf. Integr.* **2020**, *18*, 100129. [CrossRef]
4. Dhanvijay, M.M.; Patil, S.C. Internet of Things: A Survey of Enabling Technologies in Healthcare and Its Applications. *Comput. Netw.* **2019**, *153*, 113–131. [CrossRef]
5. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of Medical Things Security Assessment Framework. *Internet Things* **2019**, *8*, 100123. [CrossRef]

6. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of Security and Privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 457–464.
7. Somasundaram, R.; Thirugnanam, M. Review of Security Challenges in Healthcare Internet of Things. *Wirel. Netw.* **2021**, *27*, 5503–5509. [CrossRef]
8. Koutras, D.; Stergiopoulos, G.; Dasaklis, T.; Kotzanikolaou, P.; Glynos, D.; Douligeris, C. Security in IoMT Communications: A Survey. *Sensors* **2020**, *20*, 4828. [CrossRef]
9. Priyadharshini, A.; Umamaheswari, R.; Jayapandian, N.; Priyananci, S. Securing Medical Images Using Encryption and LSB Steganography. In Proceedings of the 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 19–20 February 2021; pp. 1–5.
10. Magdy, M.; Hosny, K.M.; Ghali, N.I.; Ghoniemy, S. Security of Medical Images for Telemedicine: A Systematic Review. *Multimed Tools Appl.* **2022**, *81*, 25101–25145. [CrossRef]
11. Liu, X.; Song, L.; Liu, S.; Zhang, Y. A Review of Deep-Learning-Based Medical Image Segmentation Methods. *Sustainability* **2021**, *13*, 1224. [CrossRef]
12. Cai, L.; Gao, J.; Zhao, D. A Review of the Application of Deep Learning in Medical Image Classification and Segmentation. *Ann. Transl. Med.* **2020**, *8*, 713. [CrossRef]
13. Budd, S.; Robinson, E.C.; Kainz, B. A Survey on Active Learning and Human-in-the-Loop Deep Learning for Medical Image Analysis. *Med. Image Anal.* **2021**, *71*, 102062. [CrossRef]
14. Fourcade, A.; Khonsari, R.H. Deep Learning in Medical Image Analysis: A Third Eye for Doctors. *J. Stomatol. Oral Maxillofac. Surg.* **2019**, *120*, 279–288. [CrossRef] [PubMed]
15. Retrouvey, J.-M.; Conley, R.S. Decoding Deep Learning Applications for Diagnosis and Treatment Planning. *Dent. Press J. Orthod.* **2023**, *27*, e22spe5. [CrossRef] [PubMed]
16. Song, E.M.; Park, B.; Ha, C.-A.; Hwang, S.W.; Park, S.H.; Yang, D.-H.; Ye, B.D.; Myung, S.-J.; Yang, S.-K.; Kim, N.; et al. Endoscopic Diagnosis and Treatment Planning for Colorectal Polyps Using a Deep-Learning Model. *Sci. Rep.* **2020**, *10*, 30. [CrossRef] [PubMed]
17. Kalecińska, K.; Fiutowski, T.; Jurgielewicz, P.; Kabat, D.; Rachwał, B.; Kapłon, Ł.; Kopeć, M.; Koperny, S.; Kulig, D.; Moroń, J.; et al. Medical Imaging Data Analysis Using 3D Deep Learning Models towards Improving the Individual Treatment Plans. *Nucl. Instrum. Methods Phys. Res. Sect. A Accel. Spectrometers Detect. Assoc. Equip.* **2023**, *1048*, 167951. [CrossRef]
18. Liu, F.; Yadav, P.; Baschnagel, A.M.; McMillan, A.B. MR-Based Treatment Planning in Radiation Therapy Using a Deep Learning Approach. *J. Appl. Clin. Med. Phys.* **2019**, *20*, 105–114. [CrossRef]
19. Khanagar, S.B.; Al-Ehaideb, A.; Vishwanathaiah, S.; Maganur, P.C.; Patil, S.; Naik, S.; Baeshen, H.A.; Sarode, S.S. Scope and Performance of Artificial Intelligence Technology in Orthodontic Diagnosis, Treatment Planning, and Clinical Decision-Making—A Systematic Review. *J. Dent. Sci.* **2021**, *16*, 482–492. [CrossRef]
20. Asiri, A.F.; Altuwalah, A.S. The Role of Neural Artificial Intelligence for Diagnosis and Treatment Planning in Endodontics: A Qualitative Review. *Saudi Dent. J.* **2022**, *34*, 270–281. [CrossRef]
21. Khalid, N.; Qayyum, A.; Bilal, M.; Al-Fuqaha, A.; Qadir, J. Privacy-Preserving Artificial Intelligence in Healthcare: Techniques and Applications. *Comput. Biol. Med.* **2023**, *158*, 106848. [CrossRef]
22. Ding, Y.; Tan, F.; Qin, Z.; Cao, M.; Choo, K.-K.R.; Qin, Z. DeepKeyGen: A Deep Learning-Based Stream Cipher Generator for Medical Image Encryption and Decryption. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *33*, 4915–4929. [CrossRef]
23. Kaissis, G.A.; Makowski, M.R.; Rückert, D.; Braren, R.F. Secure, Privacy-Preserving and Federated Machine Learning in Medical Imaging. *Nat. Mach. Intell.* **2020**, *2*, 305–311. [CrossRef]
24. Gayathri, S.; Gowri, S. Securing Medical Image Privacy in Cloud Using Deep Learning Network. *J. Cloud Comput.* **2023**, *12*, 40. [CrossRef]
25. Virtual Clinical Trials Market Size, Share and Analysis | Forecast-2030. Available online: https://www.acumenresearchandconsulting.com/virtual-clinical-trials-market (accessed on 28 June 2023).
26. One in Four US Consumers Have Had Their Healthcare Data Breached, Accenture Survey Reveals. Available online: https://newsroom.accenture.com/news/one-in-four-us-consumers-have-had-their-healthcare-data-breached-accenture-survey-reveals.htm (accessed on 5 June 2023).
27. Cost of a Data Breach. 2022. Available online: https://www.ibm.com/reports/data-breach (accessed on 5 June 2023).
28. Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most. Available online: https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/ (accessed on 10 June 2023).
29. Lichtenberg, F.R. The Quality of Medical Care, Behavioral Risk Factors, and Longevity Growth. *Int. J. Health Care Financ. Econ.* **2011**, *11*, 1–34. [CrossRef]
30. Anwar, S.M.; Majid, M.; Qayyum, A.; Awais, M.; Alnowami, M.; Khan, M.K. Medical Image Analysis Using Convolutional Neural Networks: A Review. *J. Med. Syst.* **2018**, *42*, 226. [CrossRef] [PubMed]
31. Weisman, A.J.; Kim, J.; Lee, I.; McCarten, K.M.; Kessel, S.; Schwartz, C.L.; Kelly, K.M.; Jeraj, R.; Cho, S.Y.; Bradshaw, T.J. Automated Quantification of Baseline Imaging PET Metrics on FDG PET/CT Images of Pediatric Hodgkin Lymphoma Patients. *EJNMMI Phys.* **2020**, *7*, 76. [CrossRef]

32. Yang, R.; Yu, Y. Artificial Convolutional Neural Network in Object Detection and Semantic Segmentation for Medical Imaging Analysis. *Front. Oncol.* **2021**, *11*, 638182. [CrossRef]
33. Ma, K.; Harmon, S.A.; Klyuzhin, I.S.; Rahmim, A.; Turkbey, B. Clinical Application of Artificial Intelligence in Positron Emission Tomography: Imaging of Prostate Cancer. *PET Clin.* **2022**, *17*, 137–143. [CrossRef]
34. Islam, M.d.M.; Karray, F.; Alhajj, R.; Zeng, J. A Review on Deep Learning Techniques for the Diagnosis of Novel Coronavirus (COVID-19). *IEEE Access* **2021**, *9*, 30551–30572. [CrossRef]
35. Bhattacharya, S.; Reddy Maddikunta, P.K.; Pham, Q.-V.; Gadekallu, T.R.; Krishnan, S.S.R.; Chowdhary, C.L.; Alazab, M.; Jalil Piran, M. Deep Learning and Medical Image Processing for Coronavirus (COVID-19) Pandemic: A Survey. *Sustain. Cities Soc.* **2021**, *65*, 102589. [CrossRef]
36. Chen, X.; Wang, X.; Zhang, K.; Fung, K.-M.; Thai, T.C.; Moore, K.; Mannel, R.S.; Liu, H.; Zheng, B.; Qiu, Y. Recent Advances and Clinical Applications of Deep Learning in Medical Image Analysis. *Med. Image Anal.* **2022**, *79*, 102444. [CrossRef]
37. Rajpurkar, P.; Irvin, J.; Zhu, K.; Yang, B.; Mehta, H.; Duan, T.; Ding, D.; Bagul, A.; Langlotz, C.; Shpanskaya, K.; et al. CheXNet: Radiologist-Level Pneumonia Detection on Chest X-Rays with Deep Learning. *arXiv* **2017**, arXiv:1711.05225.
38. Korolev, S.; Safiullin, A.; Belyaev, M.; Dodonova, Y. Residual and Plain Convolutional Neural Networks for 3D Brain MRI Classification. In Proceedings of the 2017 IEEE 14th International Symposium on Biomedical Imaging, Melbourne, VIC, Australia, 18–21 April 2017.
39. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep Residual Learning for Image Recognition. *arXiv* **2016**, arXiv:1512.03385, 770–778.
40. Simonyan, K.; Zisserman, A. Very Deep Convolutional Networks for Large-Scale Image Recognition. *arXiv* **2015**, arXiv:1409.1556.
41. Jiang, H.; Diao, Z.; Shi, T.; Zhou, Y.; Wang, F.; Hu, W.; Zhu, X.; Luo, S.; Tong, G.; Yao, Y.-D. A Review of Deep Learning-Based Multiple-Lesion Recognition from Medical Images: Classification, Detection and Segmentation. *Comput. Biol. Med.* **2023**, *157*, 106726. [CrossRef] [PubMed]
42. Çinar, A.; Yildirim, M. Detection of Tumors on Brain MRI Images Using the Hybrid Convolutional Neural Network Architecture. *Med. Hypotheses* **2020**, *139*, 109684. [CrossRef]
43. Waghmare, V.K.; Kolekar, M.H. Brain Tumor Classification Using Deep Learning. In *Internet of Things for Healthcare Technologies*; Chakraborty, C., Banerjee, A., Kolekar, M.H., Garg, L., Chakraborty, B., Eds.; Studies in Big Data; Springer: Singapore, 2021; pp. 155–175. ISBN 9789811541124.
44. Saber, A.; Sakr, M.; Abo-Seida, O.M.; Keshk, A.; Chen, H. A Novel Deep-Learning Model for Automatic Detection and Classification of Breast Cancer Using the Transfer-Learning Technique. *IEEE Access* **2021**, *9*, 71194–71209. [CrossRef]
45. Salama, W.M.; Aly, M.H. Deep Learning in Mammography Images Segmentation and Classification: Automated CNN Approach. *Alex. Eng. J.* **2021**, *60*, 4701–4709. [CrossRef]
46. Ahmad, B.; Sun, J.; You, Q.; Palade, V.; Mao, Z. Brain Tumor Classification Using a Combination of Variational Autoencoders and Generative Adversarial Networks. *Biomedicines* **2022**, *10*, 223. [CrossRef]
47. Chen, L.-C.; Papandreou, G.; Kokkinos, I.; Murphy, K.; Yuille, A.L. DeepLab: Semantic Image Segmentation with Deep Convolutional Nets, Atrous Convolution, and Fully Connected CRFs. *IEEE Trans. Pattern Anal. Mach. Intell.* **2018**, *40*, 834–848. [CrossRef]
48. Decourt, C.; Duong, L. Semi-Supervised Generative Adversarial Networks for the Segmentation of the Left Ventricle in Pediatric MRI. *Comput. Biol. Med.* **2020**, *123*, 103884. [CrossRef]
49. Litjens, G.; Kooi, T.; Bejnordi, B.E.; Setio, A.A.A.; Ciompi, F.; Ghafoorian, M.; van der Laak, J.A.W.M.; van Ginneken, B.; Sánchez, C.I. A Survey on Deep Learning in Medical Image Analysis. *Med. Image Anal.* **2017**, *42*, 60–88. [CrossRef] [PubMed]
50. López-Linares Román, K.; García Ocaña, M.I.; Lete Urzelai, N.; González Ballester, M.Á.; Macía Oliver, I. Medical Image Segmentation Using Deep Learning. In *Deep Learning in Healthcare*; Intelligent Systems Reference Library; Chen, Y.W., Jain, L., Eds.; Springer: Cham, Switzerland, 2020; Volume 171, pp. 17–31. [CrossRef]
51. García Ocaña, M.I.; López-Linares Román, K.; Lete Urzelai, N.; González Ballester, M.Á.; Macía Oliver, I. Medical Image Detection Using Deep Learning. In *Deep Learning in Healthcare: Paradigms and Applications*; Chen, Y.-W., Jain, L.C., Eds.; Intelligent Systems Reference Library; Springer International Publishing: Cham, Switzerland, 2020; Volume 171, pp. 3–16, ISBN 978-3-030-32606-7.
52. Zhang, J.; Liu, M.; Shen, D. Detecting Anatomical Landmarks from Limited Medical Imaging Data Using Two-Stage Task-Oriented Deep Neural Networks. *IEEE Trans. Image Process.* **2017**, *26*, 4753–4764. [CrossRef] [PubMed]
53. Setio, A.A.A.; Traverso, A.; de Bel, T.; Berens, M.S.N.; van den Bogaard, C.; Cerello, P.; Chen, H.; Dou, Q.; Fantacci, M.E.; Geurts, B.; et al. Validation, Comparison, and Combination of Algorithms for Automatic Detection of Pulmonary Nodules in Computed Tomography Images: The LUNA16 Challenge. *Med. Image Anal.* **2017**, *42*, 1–13. [CrossRef] [PubMed]
54. Pandey, S.K.; Bhandari, A.K. A Systematic Review of Modern Approaches in Healthcare Systems for Lung Cancer Detection and Classification. *Arch Comput. Methods Eng.* **2023**. [CrossRef]
55. Shah, A.A.; Malik, H.A.M.; Muhammad, A.; Alourani, A.; Butt, Z.A. Deep Learning Ensemble 2D CNN Approach towards the Detection of Lung Cancer. *Sci. Rep.* **2023**, *13*, 2987. [CrossRef]
56. Park, Y.-J.; Cho, H.-S.; Kim, M.-N. AI Model for Detection of Abdominal Hemorrhage Lesions in Abdominal CT Images. *Bioengineering* **2023**, *10*, 502. [CrossRef]
57. Xue, X.; Chinnaperumal, S.; Abdulsahib, G.M.; Manyam, R.R.; Marappan, R.; Raju, S.K.; Khalaf, O.I. Design and Analysis of a Deep Learning Ensemble Framework Model for the Detection of COVID-19 and Pneumonia Using Large-Scale CT Scan and X-ray Image Datasets. *Bioengineering* **2023**, *10*, 363. [CrossRef]

58. Abdelrahman, L.; Al Ghamdi, M.; Collado-Mesa, F.; Abdel-Mottaleb, M. Convolutional Neural Networks for Breast Cancer Detection in Mammography: A Survey. *Comput. Biol. Med.* **2021**, *131*, 104248. [CrossRef]

59. Hesamian, M.H.; Jia, W.; He, X.; Kennedy, P. Deep Learning Techniques for Medical Image Segmentation: Achievements and Challenges. *J. Digit. Imaging* **2019**, *32*, 582–596. [CrossRef]

60. Malhotra, P.; Gupta, S.; Koundal, D.; Zaguia, A.; Enbeyle, W. Deep Neural Networks for Medical Image Segmentation. *J. Healthc. Eng.* **2022**, *2022*, 9580991. [CrossRef]

61. Rizwan, I.; Haque, I.; Neubert, J. Deep Learning Approaches to Biomedical Image Segmentation. *Inform. Med. Unlocked* **2020**, *18*, 100297. [CrossRef]

62. Wang, R.; Lei, T.; Cui, R.; Zhang, B.; Meng, H.; Nandi, A.K. Medical Image Segmentation Using Deep Learning: A Survey. *IET Image Process.* **2022**, *16*, 1243–1267. [CrossRef]

63. Gou, F.; Wu, J. An Attention-Based AI-Assisted Segmentation System for Osteosarcoma MRI Images. In Proceedings of the 2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Las Vegas, NV, USA, 6–8 December 2022; pp. 1539–1543.

64. Sule, O.O. A Survey of Deep Learning for Retinal Blood Vessel Segmentation Methods: Taxonomy, Trends, Challenges and Future Directions. *IEEE Access* **2022**, *10*, 38202–38236. [CrossRef]

65. Lin, H.; Xiao, H.; Dong, L.; Teo, K.B.-K.; Zou, W.; Cai, J.; Li, T. Deep Learning for Automatic Target Volume Segmentation in Radiation Therapy: A Review. *Quant. Imaging Med. Surg.* **2021**, *11*, 4847–4858. [CrossRef]

66. Krishnapriya, S.; Karuna, Y. A Survey of Deep Learning for MRI Brain Tumor Segmentation Methods: Trends, Challenges, and Future Directions. *Health Technol.* **2023**, *13*, 181–201. [CrossRef]

67. Liu, Z.; Tong, L.; Chen, L.; Jiang, Z.; Zhou, F.; Zhang, Q.; Zhang, X.; Jin, Y.; Zhou, H. Deep Learning Based Brain Tumor Segmentation: A Survey. *Complex Intell. Syst.* **2023**, *9*, 1001–1026. [CrossRef]

68. Bonaldi, L.; Pretto, A.; Pirri, C.; Uccheddu, F.; Fontanella, C.G.; Stecco, C. Deep Learning-Based Medical Images Segmentation of Musculoskeletal Anatomical Structures: A Survey of Bottlenecks and Strategies. *Bioengineering* **2023**, *10*, 137. [CrossRef]

69. Fredrikson, M.; Jha, S.; Ristenpart, T. Model Inversion Attacks That Exploit Confidence Information and Basic Countermeasures. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Association for Computing Machinery. New York, NY, USA, 12 October 2015; pp. 1322–1333.

70. A Comprehensive Survey on Poisoning Attacks and Countermeasures in Machine Learning | ACM Computing Surveys. Available online: https://dl.acm.org/doi/10.1145/3551636 (accessed on 6 June 2023).

71. Tayyab, M.; Marjani, M.; Jhanjhi, N.Z.; Hashem, I.A.T.; Usmani, R.S.A.; Qamar, F. A Comprehensive Review on Deep Learning Algorithms: Security and Privacy Issues. *Comput. Secur.* **2023**, *131*, 103297. [CrossRef]

72. Razzak, M.I.; Naz, S.; Zaib, A. Deep Learning for Medical Image Processing: Overview, Challenges and the Future. In *Classification in BioApps: Automation of Decision Making*; Dey, N., Ashour, A.S., Borra, S., Eds.; Lecture Notes in Computational Vision and Biomechanics; Springer International Publishing: Cham, Switzerland, 2018; pp. 323–350. ISBN 978-3-319-65981-7.

73. Finlayson, S.G.; Bowers, J.D.; Ito, J.; Zittrain, J.L.; Beam, A.L.; Kohane, I.S. Adversarial Attacks on Medical Machine Learning. *Science* **2019**, *363*, 1287–1289. [CrossRef]

74. Goodfellow, I.J.; Shlens, J.; Szegedy, C. Explaining and Harnessing Adversarial Examples. *arXiv* **2015**, arXiv:1412.6572.

75. Papernot, N.; McDaniel, P.; Goodfellow, I. Transferability in Machine Learning: From Phenomena to Black-Box Attacks Using Adversarial Samples. *arXiv* **2016**, arXiv:1605.07277.

76. Madry, A.; Makelov, A.; Schmidt, L.; Tsipras, D.; Vladu, A. Towards Deep Learning Models Resistant to Adversarial Attacks. *arXiv* **2019**, arXiv:1706.06083.

77. Carlini, N.; Wagner, D. Towards Evaluating the Robustness of Neural Networks. *arXiv* **2017**, arXiv:1608.04644.

78. Papernot, N.; McDaniel, P.; Jha, S.; Fredrikson, M.; Celik, Z.B.; Swami, A. The Limitations of Deep Learning in Adversarial Settings. *arXiv* **2015**, arXiv:1511.07528.

79. Moosavi-Dezfooli, S.-M.; Fawzi, A.; Fawzi, O.; Frossard, P. Universal Adversarial Perturbations. In Proceedings of the 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 26 July 2017; pp. 86–94.

80. DeepFool: A Simple and Accurate Method to Fool Deep Neural Networks | IEEE Conference Publication | IEEE Xplore. Available online: https://ieeexplore.ieee.org/document/7780651 (accessed on 30 June 2023).

81. Bortsova, G.; González-Gonzalo, C.; Wetstein, S.C.; Dubost, F.; Katramados, I.; Hogeweg, L.; Liefers, B.; van Ginneken, B.; Pluim, J.P.W.; Veta, M.; et al. Adversarial Attack Vulnerability of Medical Image Analysis Systems: Unexplored Factors. *Med. Image Anal.* **2021**, *73*, 102141. [CrossRef] [PubMed]

82. Paschali, M.; Conjeti, S.; Navarro, F.; Navab, N. Generalizability vs. Robustness: Investigating Medical Imaging Networks Using Adversarial Examples. In Proceedings of the Medical Image Computing and Computer Assisted Intervention—MICCAI 2018, Granada, Spain, 16–20 September 2018; Frangi, A.F., Schnabel, J.A., Davatzikos, C., Alberola-López, C., Fichtinger, G., Eds.; Springer International Publishing: Cham, Switzerland, 2018; pp. 493–501.

83. Szegedy, C.; Vanhoucke, V.; Ioffe, S.; Shlens, J.; Wojna, Z. Rethinking the Inception Architecture for Computer Vision. In Proceedings of the 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, USA, 27–30 June 2016; pp. 2818–2826.

84. Szegedy, C.; Ioffe, S.; Vanhoucke, V.; Alemi, A. Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning. *arXiv* **2016**, arXiv:1602.07261. [CrossRef]

85. Howard, A.G.; Zhu, M.; Chen, B.; Kalenichenko, D.; Wang, W.; Weyand, T.; Andreetto, M.; Adam, H. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. *arXiv* **2017**, arXiv:1704.04861.

86. Badrinarayanan, V.; Kendall, A.; Cipolla, R. SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation. *IEEE Trans. Pattern Anal. Mach. Intell.* **2017**, *39*, 2481–2495. [CrossRef]

87. Ronneberger, O.; Fischer, P.; Brox, T. U-Net: Convolutional Networks for Biomedical Image Segmentation. In Proceedings of the Medical Image Computing and Computer-Assisted Intervention—MICCAI 2015, Munich, Germany, 5–9 October 2015; Navab, N., Hornegger, J., Wells, W.M., Frangi, A.F., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 234–241.

88. Jegou, S.; Drozdzal, M.; Vazquez, D.; Romero, A.; Bengio, Y. The One Hundred Layers Tiramisu: Fully Convolutional DenseNets for Semantic Segmentation. *arXiv* **2017**, arXiv:1611.09326, 11–19.

89. Finlayson, S.G.; Chung, H.W.; Kohane, I.S.; Beam, A.L. Adversarial Attacks Against Medical Deep Learning Systems. *arXiv* **2019**, arXiv:1804.05296.

90. Bortsova, G.; Dubost, F.; Hogeweg, L.; Katramados, I.; de Bruijne, M. Adversarial Heart Attack: Neural Networks Fooled to Segment Heart Symbols in Chest X-ray Images. *arXiv* **2021**, arXiv:2104.00139.

91. Pal, B.; Gupta, D.; Rashed-Al-Mahfuz, M.; Alyami, S.A.; Moni, M.A. Vulnerability in Deep Transfer Learning Models to Adversarial Fast Gradient Sign Attack for COVID-19 Prediction from Chest Radiography Images. *Appl. Sci.* **2021**, *11*, 4233. [CrossRef]

92. Hirano, H.; Koga, K.; Takemoto, K. Vulnerability of Deep Neural Networks for Detecting COVID-19 Cases from Chest X-ray Images to Universal Adversarial Attacks. *PLoS ONE* **2020**, *15*, e0243963. [CrossRef] [PubMed]

93. Wang, L.; Lin, Z.Q.; Wong, A. COVID-Net: A Tailored Deep Convolutional Neural Network Design for Detection of COVID-19 Cases from Chest X-ray Images. *Sci. Rep.* **2020**, *10*, 19549. [CrossRef]

94. Hirano, H.; Minagi, A.; Takemoto, K. Universal Adversarial Attacks on Deep Neural Networks for Medical Image Classification. *BMC Med. Imaging* **2021**, *21*, 9. [CrossRef] [PubMed]

95. Cheng, G.; Ji, H. Adversarial Perturbation on MRI Modalities in Brain Tumor Segmentation. *IEEE Access* **2020**, *8*, 206009–206015. [CrossRef]

96. Menze, B.H.; Jakab, A.; Bauer, S.; Kalpathy-Cramer, J.; Farahani, K.; Kirby, J.; Burren, Y.; Porz, N.; Slotboom, J.; Wiest, R.; et al. The Multimodal Brain Tumor Image Segmentation Benchmark (BRATS). *IEEE Trans. Med. Imaging* **2015**, *34*, 1993–2024. [CrossRef]

97. 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 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, USA, 26 July 2017; pp. 3462–3471.

98. ISIC | International Skin Imaging Collaboration. Available online: https://www.isic-archive.com (accessed on 7 June 2023).

99. Diabetic Retinopathy Detection | Kaggle. Available online: https://www.kaggle.com/c/diabetic-retinopathy-detection (accessed on 7 June 2023).

100. Ma, X.; Niu, Y.; Gu, L.; Wang, Y.; Zhao, Y.; Bailey, J.; Lu, F. Understanding Adversarial Attacks on Deep Learning Based Medical Image Analysis Systems. *Pattern Recognit.* **2021**, *110*, 107332. [CrossRef]

101. Feinman, R.; Curtin, R.R.; Shintre, S.; Gardner, A.B. Detecting Adversarial Samples from Artifacts. *arXiv* **2017**, arXiv:1703.00410.

102. Ma, X.; Li, B.; Wang, Y.; Erfani, S.M.; Wijewickrema, S.; Schoenebeck, G.; Song, D.; Houle, M.E.; Bailey, J. Characterizing Adversarial Subspaces Using Local Intrinsic Dimensionality. *arXiv* **2018**, arXiv:1801.02613.

103. Shah, A.; Lynch, S.; Niemeijer, M.; Amelon, R.; Clarida, W.; Folk, J.; Russell, S.; Wu, X.; Abràmoff, M.D. Susceptibility to Misdiagnosis of Adversarial Images by Deep Learning Based Retinal Image Analysis Algorithms. In Proceedings of the 2018 IEEE 15th International Symposium on Biomedical Imaging (ISBI 2018), Washington, DC, USA, 4–7 April 2018; pp. 1454–1457.

104. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. ImageNet Classification with Deep Convolutional Neural Networks. *Commun. ACM* **2017**, *60*, 84–90. [CrossRef]

105. Paszke, A.; Chaurasia, A.; Kim, S.; Culurciello, E. ENet: A Deep Neural Network Architecture for Real-Time Semantic Segmentation. *arXiv* **2016**, arXiv:1606.02147.

106. Abràmoff, M.D.; Lou, Y.; Erginay, A.; Clarida, W.; Amelon, R.; Folk, J.C.; Niemeijer, M. Improved Automated Detection of Diabetic Retinopathy on a Publicly Available Dataset Through Integration of Deep Learning. *Investig. Ophthalmol. Vis. Sci.* **2016**, *57*, 5200–5206. [CrossRef] [PubMed]

107. Boulila, W.; Ammar, A.; Benjdira, B.; Koubaa, A. Securing the Classification of COVID-19 in Chest X-ray Images: A Privacy-Preserving Deep Learning Approach. *arXiv* **2022**, arXiv:2203.07728.

108. Zheng, Y.; Duan, H.; Tang, X.; Wang, C.; Zhou, J. Denoising in the Dark: Privacy-Preserving Deep Neural Network-Based Image Denoising. *IEEE Trans. Dependable Secur. Comput.* **2021**, *18*, 1261–1275. [CrossRef]

109. Chao, J.; Badawi, A.A.; Unnikrishnan, B.; Lin, J.; Mun, C.F.; Brown, J.M.; Campbell, J.P.; Chiang, M.; Kalpathy-Cramer, J.; Chandrasekhar, V.R.; et al. CaRENets: Compact and Resource-Efficient CNN for Homomorphic Inference on Encrypted Medical Images. *arXiv* **2019**, arXiv:1901.10074.

110. Selvi, C.T.; Amudha, J.; Sudhakar, R. Medical Image Encryption and Compression by Adaptive Sigma Filterized Synorr Certificateless Signcryptive Levenshtein Entropy-Coding-Based Deep Neural Learning. *Multimed. Syst.* **2021**, *27*, 1059–1074. [CrossRef]

111. Munjal, K.; Bhatia, R. A Systematic Review of Homomorphic Encryption and Its Contributions in Healthcare Industry. *Complex Intell. Syst.* **2022**. [CrossRef]

112. Naik, R.; Wani, T.; Bajaj, S.; Ahir, S.; Joshi, A. Detection of Lung Diseases Using Deep Learning. In Proceedings of the 3rd International Conference on Advances in Science & Technology (ICAST), Bahir Dar, Ethiopia, 2–4 October 2020.

113. Kumar, J.N.V.R.S.; Jyothi, G.S.; Indira, D.; Nagamani, T. Secured Cloud Application for Detection of Brain Tumor Using Deep Learning Algorithms. In Proceedings of the 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 21–23 September 2022; pp. 656–663.

114. Mohanty, M.D.; Das, A.; Mohanty, M.N.; Altameem, A.; Nayak, S.R.; Saudagar, A.K.J.; Poonia, R.C. Design of Smart and Secured Healthcare Service Using Deep Learning with Modified SHA-256 Algorithm. *Healthcare* **2022**, *10*, 1275. [CrossRef]

115. Privacy-Preserving Collective Learning with Homomorphic Encryption | IEEE Journals & Magazine | IEEE Xplore. Available online: https://ieeexplore.ieee.org/document/9543673 (accessed on 8 June 2023).

116. Falcetta, A.; Roveri, M. Privacy-Preserving Time Series Prediction with Temporal Convolutional Neural Networks. In Proceedings of the 2022 International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 18–23 July 2022; pp. 1–8.

117. NIH Chest X-rays | Kaggle. Available online: https://www.kaggle.com/datasets/nih-chest-xrays/data (accessed on 3 July 2023).

118. MIMIC-III, a Freely Accessible Critical Care Database | Scientific Data. Available online: https://www.nature.com/articles/sdata201635 (accessed on 3 July 2023).

119. Brain MRI Images for Brain Tumor Detection. Available online: https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection (accessed on 3 July 2023).

120. COVID-19 Radiography Database | Kaggle. Available online: https://www.kaggle.com/datasets/tawsifurrahman/covid19-radiography-database (accessed on 3 July 2023).

121. More, S.; Singla, J.; Song, O.-Y.; Tariq, U.; Malebary, S. Denoising Medical Images Using Deep Learning in IoT Environment. *CMC* **2021**, *69*, 3127–3143. [CrossRef]

122. Alslman, Y.; Alnagi, E.; Ahmad, A.; AbuHour, Y.; Younisse, R.; Abu Al-haija, Q. Hybrid Encryption Scheme for Medical Imaging Using AutoEncoder and Advanced Encryption Standard. *Electronics* **2022**, *11*, 3967. [CrossRef]

123. El-Shafai, W.; Abd El-Nabi, S.; El-Rabaie, M.E.-S.; Ali, M.A.; Soliman, F.N.; Algarni, D.A.; Abd El-Samie, E.F. Efficient Deep-Learning-Based Autoencoder Denoising Approach for Medical Image Diagnosis. *Comput. Mater. Contin.* **2022**, *70*, 6107–6125. [CrossRef]

124. Chui, K.T.; Gupta, B.B.; Chi, H.R.; Arya, V.; Alhalabi, W.; Ruiz, M.T.; Shen, C.-W. Transfer Learning-Based Multi-Scale Denoising Convolutional Neural Network for Prostate Cancer Detection. *Cancers* **2022**, *14*, 3687. [CrossRef] [PubMed]

125. Stroke Prediction. Available online: https://kaggle.com/code/swatis1/stroke-prediction (accessed on 4 July 2023).

126. GitHub—UCSD-AI4H/COVID-CT: COVID-CT-Dataset: A CT Scan Dataset about COVID-19. Available online: https://github.com/UCSD-AI4H/COVID-CT (accessed on 3 July 2023).

127. Chest X-ray Images (Pneumonia). Available online: https://www.kaggle.com/datasets/paultimothymooney/chest-xray-pneumonia (accessed on 4 July 2023).

128. El-Shafai, W.; Abd El-Samie, F.E. Extensive COVID-19 X-ray and CT Chest Images Dataset. *Mendeley Data* **2020**, *3*. [CrossRef]

129. Kurdziel, K.A.; Shih, J.H.; Apolo, A.B.; Lindenberg, L.; Mena, E.; McKinney, Y.Y.; Adler, S.S.; Turkbey, B.; Dahut, W.; Gulley, J.L.; et al. The Kinetics and Reproducibility of 18F-Sodium Fluoride for Oncology Using Current PET Camera Technology. *J. Nucl. Med.* **2012**, *53*, 1175–1184. [CrossRef]

130. TCGA-PRAD—Dataportal. Asia. Available online: https://dataportal.asia/dataset/212601019_tcgaprad (accessed on 4 July 2023).

131. Litjens, G.; Futterer, J.; Huisman, H. Data from Prostate-3T. *Cancer Imaging Arch.* **2015**. [CrossRef]

132. Bloch, B.N.; Jain, A.; Jaffe, C.C. Data from PROSTATE-DIAGNOSIS. *Cancer Imaging Arch.* **2015**. [CrossRef]

133. Maffre, G.P.; Gervais, G.; Bruno, L.; Julien, R.; Damien, E.; Mélanie, F.; Arthur, D.; Hugo Messidor-2. ADCIS. Available online: https://www.adcis.net/en/third-party/messidor2/ (accessed on 14 June 2023).

134. Liu, Y.; Ma, Z.; Liu, X.; Ma, S.; Ren, K. Privacy-Preserving Object Detection for Medical Images with Faster R-CNN. *IEEE Trans. Inf. Forensics Secur.* **2022**, *17*, 69–84. [CrossRef]

135. Usman, O.L.; Muniyandi, R.C. CryptoDL: Predicting Dyslexia Biomarkers from Encrypted Neuroimaging Dataset Using Energy-Efficient Residue Number System and Deep Convolutional Neural Network. *Symmetry* **2020**, *12*, 836. [CrossRef]

136. Usman, O.L.; Muniyandi, R.C.; Omar, K.; Mohamad, M. Privacy-Preserving Classification Method for Neural-Biomarkers Using Homomorphic Residue Number System CNN: HoRNS-CNN. In Proceedings of the 2022 International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 16–17 February 2022; pp. 1–8.

137. Brown, J.M.; Campbell, J.P.; Beers, A.; Chang, K.; Ostmo, S.; Chan, R.V.P.; Dy, J.; Erdogmus, D.; Ioannidis, S.; Kalpathy-Cramer, J.; et al. Automated Diagnosis of Plus Disease in Retinopathy of Prematurity Using Deep Convolutional Neural Networks. *JAMA Ophthalmol.* **2018**, *136*, 803–810. [CrossRef]

138. Data | Free Full-Text | Indian Diabetic Retinopathy Image Dataset (IDRiD): A Database for Diabetic Retinopathy Screening Research. Available online: https://www.mdpi.com/2306-5729/3/3/25 (accessed on 3 July 2023).

139. Data Sets | ImageCLEF/LifeCLEF—Multimedia Retrieval in CLEF. Available online: https://www.imageclef.org/datasets (accessed on 4 July 2023).

140. Ahmad, I.; Shin, S. A Perceptual Encryption-Based Image Communication System for Deep Learning-Based Tuberculosis Diagnosis Using Healthcare Cloud Services. *Electronics* **2022**, *11*, 2514. [CrossRef]

141. MediSecFed: Private and Secure Medical Image Classification in the Presence of Malicious Clients | IEEE Journals & Magazine | IEEE Xplore. Available online: https://ieeexplore.ieee.org/abstract/document/9664357 (accessed on 11 June 2023).

142. Hajjaji, M.A.; Dridi, M.; Mtibaa, A. A Medical Image Crypto-Compression Algorithm Based on Neural Network and PWLCM. *Multimed Tools Appl.* **2019**, *78*, 14379–14396. [CrossRef]

143. Jaeger, S.; Candemir, S.; Antani, S.; Wáng, Y.-X.J.; Lu, P.-X.; Thoma, G. Two Public Chest X-ray Datasets for Computer-Aided Screening of Pulmonary Diseases. *Quant. Imaging Med. Surg.* **2014**, *4*, 475–477. [CrossRef]

144. Krishna, A.A.; Arikutharam, V.; Ramnan, K.V.; Bharathi, H.; Chandar, T.S. Dynamic Image Encryption Using Neural Networks for Medical Images. In Proceedings of the 2022 IEEE IAS Global Conference on Emerging Technologies (GlobConET), Arad, Romania, 20–22 May 2022; pp. 739–745.

145. Ultrasound Nerve Segmentation. Available online: https://kaggle.com/competitions/ultrasound-nerve-segmentation (accessed on 3 July 2023).

146. The Wide Trail Design Strategy | SpringerLink. Available online: https://link.springer.com/chapter/10.1007/3-540-45325-3_20 (accessed on 3 July 2023).

147. Panwar, K.; Singh, A.; Kukreja, S.; Singh, K.K.; Shakhovska, N.; Boichuk, A. Encipher GAN: An End-to-End Color Image Encryption System Using a Deep Generative Model. *Systems* **2023**, *11*, 36. [CrossRef]

148. Gaudio, A.; Smailagic, A.; Faloutsos, C.; Mohan, S.; Johnson, E.; Liu, Y.; Costa, P.; Campilho, A. DeepFixCX: Explainable Privacy-Preserving Image Compression for Medical Image Analysis. *WIREs Data Min. Knowl. Discov.* **2023**, *13*, e1495. [CrossRef]

149. Zhu, L.; Qu, W.; Wen, X.; Zhu, C. FEDResNet: A Flexible Image Encryption and Decryption Scheme Based on End-to-End Image Diffusion with Dilated ResNet. *Appl. Opt.* **2022**, *61*, 9124–9134. [CrossRef]

150. Pati, S.; Thakur, S.P.; Hamamcı, İ.E.; Baid, U.; Baheti, B.; Bhalerao, M.; Güley, O.; Mouchtaris, S.; Lang, D.; Thermos, S.; et al. GaNDLF: A Generally Nuanced Deep Learning Framework for Scalable End-to-End Clinical Workflows in Medical Imaging. *Commun. Eng.* **2023**, *2*, 23. [CrossRef]

151. Ding, Y.; Zhang, C.; Cao, M.; Wang, Y.; Chen, D.; Zhang, N.; Qin, Z. ToStaGAN: An End-to-End Two-Stage Generative Adversarial Network for Brain Tumor Segmentation. *Neurocomputing* **2021**, *462*, 141–153. [CrossRef]

152. BRATS—SICAS Medical Image Repository. Available online: https://www.smir.ch/BRATS/Start2015 (accessed on 5 July 2023).

153. Codella, N.; Rotemberg, V.; Tschandl, P.; Celebi, M.E.; Dusza, S.; Gutman, D.; Helba, B.; Kalloo, A.; Liopyris, K.; Marchetti, M.; et al. Skin Lesion Analysis toward Melanoma Detection 2018: A Challenge Hosted by the International Skin Imaging Collaboration (ISIC). *arXiv* **2019**, arXiv:1902.03368.

154. Irvin, J.; Rajpurkar, P.; Ko, M.; Yu, Y.; Ciurea-Ilcus, S.; Chute, C.; Marklund, H.; Haghgoo, B.; Ball, R.; Shpanskaya, K.; et al. CheXpert: A Large Chest Radiograph Dataset with Uncertainty Labels and Expert Comparison. *Proc. AAAI Conf. Artif. Intell.* **2019**, *33*, 590–597. [CrossRef]

155. Intel & MobileODT Cervical Cancer Screening. Available online: https://kaggle.com/competitions/intel-mobileodt-cervical-cancer-screening (accessed on 5 July 2023).

156. Ahn, J.M.; Kim, S.; Ahn, K.-S.; Cho, S.-H.; Lee, K.B.; Kim, U.S. A Deep Learning Model for the Detection of Both Advanced and Early Glaucoma Using Fundus Photography. *PLoS ONE* **2018**, *13*, e0207982. [CrossRef] [PubMed]

157. Dou, Q.; Yu, L.; Chen, H.; Jin, Y.; Yang, X.; Qin, J.; Heng, P.-A. 3D Deeply Supervised Network for Automated Segmentation of Volumetric Medical Images. *Med. Image Anal.* **2017**, *41*, 40–54. [CrossRef] [PubMed]

158. Shen, D.; Wu, G.; Suk, H.-I. Deep Learning in Medical Image Analysis. *Annu. Rev. Biomed. Eng.* **2017**, *19*, 221–248. [CrossRef] [PubMed]

159. Medical Image Segmentation Using Deep Learning: A Survey—Wang—2022—IET Image Processing—Wiley Online Library. Available online: https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/ipr2.12419 (accessed on 4 June 2023).

160. Kim, K.; Jung, I.Y. Secure Object Detection Based on Deep Learning. *J. Inf. Process. Syst.* **2021**, *17*, 571–585. [CrossRef]

161. Ding, Y.; Wu, G.; Chen, D.; Zhang, N.; Gong, L.; Cao, M.; Qin, Z. DeepEDN: A Deep Learning-Based Image Encryption and Decryption Network for Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 1504–1518. [CrossRef]

162. Shin, H.-C.; Roth, H.R.; Gao, M.; Lu, L.; Xu, Z.; Nogues, I.; Yao, J.; Mollura, D.; Summers, R.M. Deep Convolutional Neural Networks for Computer-Aided Detection: CNN Architectures, Dataset Characteristics and Transfer Learning. *IEEE Trans. Med. Imaging* **2016**, *35*, 1285–1298. [CrossRef]