Application of Artificial Intelligence in Medical Imaging Diagnosis

Baoming Zhang1†, Weili Yue2, Qiang Liu3, Shimin Hu4

1Department of medical imaging, Hebei Eye Hospital, 478162333@qq.com
2Department of medical imaging, Hebei Eye Hospital, yueweili6014@163.com
3Department of medical imaging, Hebei Eye Hospital, 13933708000@139.com
4Department of medical imaging, Hebei Eye Hospital, 13903198136@139.com
† Corresponding author: BAOMING ZHANG

Abstract
The development of artificial intelligence promotes the great progress of medical imaging diagnosis. Based on this, this paper reviews and discusses the medical image diagnosis based on artificial intelligence in recent years, introduces the procedure of medical image diagnosis, the algorithms involved and the key progress, analyzes the shortcomings of the current technology, and the possible development direction in the future.

CCS CONCEPTS
Computing methodologies–Artificial intelligence–Philosophical/theoretical foundations of artificial intelligence–Cognitive science

Keywords
medical imaging diagnosis, image processing, artificial intelligence, deep learning;

1 INTRODUCTION
Medical imaging diagnosis is a non-invasive way for doctors to obtain internal tissue imaging data and then diagnose diseases with quantitative and qualitative methods. Clinically, the combination of medical imaging as well as the conventional disease examination has gradually become the important fundamental for doctors to make medical diagnoses. During this process, the interpretation of medical imaging data has become a complicated process. At present, the interpretation of medical imaging data is a very challenging important task for medical diagnosis.

Artificial intelligence technology consists of different fields such as machine learning, computer vision, and natural language processing, with the target of producing intelligent machines which are similar to human being. In recent years, with the rapid development of core algorithms, computing power and big data, the researchers have started to apply artificial intelligence technologies into medical image diagnosis, expecting to solve the problems exposed by manual image interpretation, assist or even replace doctors in the field of disease diagnosis. At present, the application of artificial intelligence technology (especially deep learning) has already reached a lot of progress in the direction of automatic analysis of medical images and assist doctors to make medical diagnosis. With the basis of the analysis and compilation of data, this paper will introduce the current research status of artificial intelligence technology in medical imaging diagnosis, summarize the existing problems as well as give an outlook.

2 COMPUTER AIDED DIAGNOSIS SYSTEM
There are normally two core parts involved into artificial intelligent medical diagnosis: medical image detection and medical image classification. Normally, in order to realize the intelligent diagnosis, there are three steps that the researchers should do: image database building, classification model training...
and classification model prediction. Among them, the main task of image database building is to extract suspected lesion areas from the original medical images as candidate images, and select some of them as training set and the rest as test set. In the training part, all images will be sequentially go through the whole or part procedures of image preprocessing, feature extraction as well as image annotation so that the original candidate images can be converted into a feature set of candidate images with lesion type labels. Later on, after the importing these candidate images in to a certain appropriate artificial intelligent image prediction model training , a medical image lesion prediction model with low training error will be obtained. This prediction model will be used to predict the type of candidate images in the test set, and the prediction results will be the type of lesion in the test set that the model thinks. A more intuitive flowchart can be seen in the Figure 1.

**Figure 1: The main procedure of CAD system**

### 2.1 Image preprocessing

The main target of medical image preprocessing is to remove a large number of irrelevant and redundant parts of medical images and highlight the interest regions. With the removing of differences between different types or sources of data, the later steps such as feature extraction and image classification will be promoted. The common medical image preprocessing tasks are image enhancement and image segmentation.

Image enhancement can improve the quality of medical images by means of reasonable selection of threshold values, data resampling, grayscale transformation enhancement, histogram enhancement, image smoothing, image sharpening, color enhancement, frequency domain enhancement and so on[1-3].

Image enhancement can even reduce or even remove image noise to improve image clarity and contrast, which will build a good basis for subsequent image lesion region segmentation quality and feature extraction.

For example, Papadopoulos et al [4] tested five methods of image contrast enhancement and demonstrated for the first time and proved that image preprocessing could indeed improve the performance of computer-aided diagnosis systems. In fact, the windowing technique commonly used in computed tomography (CT) imaging can be considered as a typical display technique based on grayscale transformation enhancement [5]. Continuous wavelet transform (CWT), which belongs to the frequency domain enhancement method, has been used in positron emission tomography, magnetic resonance imaging and mammography, achieved good results [6]. Ultrasound imaging can achieve image noise suppression and image sharpness enhancement by image smoothing, image sharpening and frequency domain enhancement [7]. Histogram enhancement has been used for computed radiography (CR) digital chest images [8] and mammogram images [9], respectively, and has been shown to help reduce unclear areas in the original image and suppress possible artifacts during the imaging process. Hsu and Chou [10] designed a special color enhancement method for ultrasound images of the prostate and retinal fundus vascular images. This method was proved to be really effective in helping medical personnel to improve the accuracy of image evaluation.

Image segmentation is mainly used to segment images into different anatomical regions by edge detection algorithms, region growing algorithms, and model-based algorithms and so on, so that the important interest regions can be detected, namely the suspected focal regions in the usual sense. As an example, Ng et al [11] used k-means clustering in cascade with level set algorithm, and this method achieved good segmentation results on brain MRI images. Zhang and Chen [12] modified the objective function in the traditional fuzzy C-mean algorithm by replacing the Euclidean distance in the traditional algorithm with the kernel-induced distance. At the same time, it also gained good results in brain MRI images. Pham et al [13] used split-merge segmentation to obtain the seed set of the highest probability region inside the abdominal CT images. Then, with the combination of the methodology of the region growth segmentation, the liver region was separated very well. Dehmeshki et al [14] used a modified version of the region-growth method to achieve accurate segmentation of nodal tissue within lung CT images. The doctors satisfaction level was 84% for the first given segmentation results, while the other remaining parts could also be reasonably solved with the usage of the alternative solutions proposed by this method. Bingli Zhu [15] proposed a Gauss-Laplacian operator based on the existing edge detection operator. The segmentation method based on it has reached a very good application results in the field of the CT images of the brain.

With the development of neural networks, deep neural network-based segmentation methods, relying on their better autonomous learning ability as well as the ability of extracting
more abstract high-level features, have dominated the medical imaging field in recent years. It covers almost all kinds of types of current medical imaging tasks. The earliest CNN-based medical image segmentation was the neuromfilm segmentation made by Ciresan et al [16]. They used convolutional neural networks for pixel by pixel classification, which reached the exceeded human levels segmentation results. However, the convolution process will inevitably result in the losses of image detail information, which will bring severe influences on the semantic segmentation for pixel-level classification. However, the fully convolutional network (FCN) has solved this problem very effectively. Ronneberger et al., with the basis of FCN proposed a network structure (U-Net, which was composed of mutually symmetric systolic path (convolutional layer, downsampling layer) and expansion path (upsampling layer, convolutional layer). Among them, the systolic path is used to obtain contextual information while the dilated path is used for precise positioning, so that the accurate segmentation based on a small number of electron microscopic cell images can be realized.

2.2 Feature Extraction

Feature extraction is the process of acquiring characteristic information in medical images by computer. Strictly speaking, it consists of two aspects namely the image feature extraction and the feature selection. Good feature extraction and selection can not only simplify the complexity of input sample images and reduce the complexity of feature selection but also reflect the structural information, visual characteristics and biological background knowledge of the case to be diagnosed. Therefore, even if only relative easy image prediction model training is adopted, the final model can achieve a desired good prediction results. The feature selection is normally used to solve two problems: the degradation of the subsequent algorithm performance due to high feature dimensionality as well as the increase of the generalization error of the prediction model resulting from the increase of the model complexity.

At present, there are two main categories of image classification methods, with the support of image feature extraction and feature selection to achieve better image classification.

One category is to use artificially defined image features, including position features, shape features, grayscale features and texture features, as well as wavelet transform, Gaussian transformed features, features obtained by local binary pattern (LBP), etc., combined with various feature selection and dimensionality reduction methods, including principal component analysis, combined decision tree methods, ANOVA, correlation metrics, etc., to finally achieve good image classification and recognition; literature [18,19] proposed texture features based on diversity index for computer-aided diagnosis system of breast lumps, and related experiments confirmed the effectiveness of this method in breast lump diagnosis tasks. In the literature [20,21], texture features were used in prostate tumor classification and thyroid cancer diagnosis systems with good results. Buciu and Gacsádi [22] were the first to extend Gabor transform features to a computer-aided diagnosis system based on breast images, but the results seemed to be limited. The spatial location feature in the literature [23] was obtained by processing the region of interest of the segmented lesion through polarized spatial pyramids. This feature can well express the location association information of the image before and after segmentation, and by combining it with the morphological features obtained by the statistical analysis method of image edges and importing the document topic generation model (latent dirichlet allocation, LDA), the performance of the computer-aided diagnosis system built with this breast mass image is outstanding.

The other category is the automatic feature extraction, selection as well as the classification with the usage of the neural network model. In order to automatic detect the lung nodules, ZHu et al [24] adapted the RCNN network into a 3D-based network, learning the nodule features effectively, which can obtain 92% sensitivity on lung image database consortium (LIDC). Kooi et al [25] provided extra 45,000 image acquisitions to train the classification model based on the original CNN network. Related experiments confirmed that the CNN network with the addition of acquisition information can obtain a better performance for breast image classification. Al-Masni et al., by using DL and CNN to extract mammography lesion image histology features, also achieved similarly good results. Shi et al [26] adopted deep polynomial network (DPN) to relearn texture features of ultrasound images to generate more representative features and get better classification result. This technology has gained competitive results in the field of the classification of ultrasound of prostate tumor small sample.

2.3 Prediction model training

The essence of the image prediction model training is the core of Artificial Intelligence Diagnosis. If feature extraction and feature selection determine the upper limit of an Artificial Intelligence diagnostic system, then the lower limit of the system performance is relying on how to choose the appropriate machine learning method at a certain degree. A medical image prediction model trained by a suitable machine learning method can greatly compensate for the lack of effect of feature extraction methods, or even skip feature extraction directly. At present, the common methods used for prediction models include Naive Bayesian algorithm, support vector machine, linear discriminant analysis, decision tree, random forest, artificial neural network and so on.

The Naive Bayesian algorithm originated from classical mathematical theory and is a machine learning method with a solid mathematical foundation and stable classification efficiency. It can calculate the conditional distribution of an attribute from the distribution of the sample and the prior distribution of that attribute under the condition that the sample is of different types. The Naive Bayesian algorithm model assumes that the attributes are independent of each other, which is often not valid in practical
applications and does not work well when the number of attributes is large or the correlation between attributes is large. Its application in cancer and spine pathology classification tasks [27] and breast images [28]. The core concept of linear discriminant analysis is to project high-dimensional samples into an optimal discriminant vector space, ensuring that the new samples are projected to satisfy the "minimum intra-class variance and maximum inter-class variance". Applications of linear discriminant analysis in computer-aided diagnostic systems include breast image tasks [29], lung nodule diagnosis [30], and others.

A decision tree is a predictive model, which represents a mapping relationship between object attributes and object values. Each node in the tree model represents an object, while each bifurcated path represents a possible attribute value, and each leaf node corresponds to the value of the object represented by the path experienced from the root node to that leaf node. This is currently applied to tumor classification in breast ultrasound imaging [31]. Support vector machine is a predictive modeling method which is designed specifically for binary classification tasks. Its core idea is to find a hyperplane in the sample space to partition the samples and to ensure that the interval between the hyperplane and each support vector is maximized. This means, at the time when the interval of objective function is maximized, the constraint is the classical convex quadratic programming problem in which the training samples are all correctly classified. Its application areas include thyroid disease diagnosis [32], Parkinson's disease diagnosis [33], breast cancer classification [34], and lung nodule classification [35,36].

An artificial neural network is a computational model that simulates the neuronal structure of the brain and consists of a large number of multilayer neurons interconnected with each other. Each neuron represents a specific excitation function, and the connection between any two nodes represents the weight of the signal passing through the connection. Depending on the network connections, weights and excitation functions, artificial neural networks can theoretically approximate any algorithm, function or logical strategy to better simulate the complex nonlinear relationships between network inputs and outputs in real tasks. Early research on artificial neural networks in computer-aided diagnostic systems involved three image diagnosis tasks for breast cancer, heart disease, and diabetes [37], as well as tasks related to the examination and classification of breast images [38].

The deep neural network technique was developed based on the earlier artificial neural networks, and the expressiveness and upper performance limits of the whole network were greatly improved by deeper neural network structures. The introduction of special Relu (rectified linear unit) excitation function solves the overfitting problem of shallow neural networks to a certain extent; gradient shearing and weight regularization avoid the phenomenon of "gradient explosion". The introduction of batch normalization and residual network further reduces the possibility of gradient dispersion. Nowadays, deep neural networks are widely used in various fields with overwhelming performance advantages and good reputation in the industry, and they have achieved good practical results.

3 CHALLENGES THAT NEED TO BE SOLVED

Although artificial intelligence has made numerous breakthroughs in medical image analysis, the application of artificial intelligence in clinics to support the accurate diagnosis and personalized treatment is still restricted by the following aspects.

3.1 Sample labeling

Most of the current artificial intelligence methods are based on supervised learning. An important prerequisite for such methods is that the number of samples for training predictive models is sufficient and they are all labeled with type. Due to objective reasons such as patient privacy, medical research communication, and acquisition costs, the number of high-quality samples available for experiments is still very limited, which is the origin of the so-called "medical information silo effect". In addition, medical image annotators need to have a certain medical background, and it is even more costly to obtain high-quality medical annotated images than the medical images themselves; according to the latest "Artificial Intelligence in Medicine White Paper" published by the Institute of Artificial Intelligence of Shanghai Jiao Tong University in 2019: as the most common problem in processing medical images, "low sample size, lack of labels" has become the primary obstacle to the development of AI technology in medical imaging. Therefore, there is an ongoing research focus on how to improve the accuracy of classification prediction using the ideas of weakly supervised, transfer learning and multi-task learning with only a small amount of labeled data.

3.2 Privacy Protection

Medical data involves the personal privacy of patients. China has issued the "Information Security Technology Personal Information Security Standard", which presents clear and specific regulations on the collection, storage, application and transmission of personal data. Test reports, medical orders, medication records and other records generated by individuals due to illness and medical treatment are classified as sensitive personal information. The collection, sharing and transfer of sensitive personal information require the agreement of the subject of the personal information. At present, there are no regulations and standards specifically made for the protection of medical information and personal health privacy. The lack of institutions and standards is easy to breed medical privacy trafficking as well as obstruct the development of the market.

According to the research from Tramèr et al [39], the current artificial intelligence models are vulnerable in preventing privacy disclosure. Malicious attackers could extrapolate patient information from published artificial intelligence models. As a
result, the privacy of the models has gained more and more concern.

Medical data are often characterized by small samples. The data from a single medical institution is sometimes difficult to support the effective training of AI models. This means the aggregation of data among different medical institutions is necessary, which, however, will increase the risk of privacy leakage at the same time. This phenomenon makes the centralization of medical data sometimes infeasible.

3.3 Interpretation of Results
At present, the deep learning algorithms widely applied in the field of artificial intelligence demand the construction of multi-hidden nerve networks. The prediction process is a computational process under the corresponding parameters, which is not transparent. Moreover, there is no corresponding theoretical supports. As a result, the prediction results are not interpretable. The incompleteness of the dataset relied by deep learning algorithm may result in the bias of the final "rule set" and form the phenomenon of "algorithmic discrimination". Therefore, the study of interpretable methods for deep learning models will become the hot research topic in the field of medical images.

3.4 Robustness
The existing deep learning models at present have only good results for single dataset. It can not be used to predict other datasets effectively when it is not trained before. Because of the different acquisition parameters, acquisition devices, and acquisition time, the performance of medical images can vary a lot for the same disease, which results in the poor robustness and generalization of the current existing models. Therefore, the performance of practical detection in highly complex clinical applications is not good enough. How to combine brain cognition to improve the model structure and the training methods as well as the enhancement of generalization ability of deep learning models will become the hot research topics in the future.

4 CONCLUSION
This paper has conducted a comprehensive analysis on the research and current situation of artificial intelligence technology in medical diagnosis domestic and abroad in recent years. Generally speaking:

(1) Medical diagnosis based on artificial intelligence is still at the preliminary clinical application phase. The detection and prediction effectiveness as well as the clinical application process are worthy for deep research. The application of artificial intelligence in medical field has provided new ideas and directions for solving many medical problems, which is one of the key directions for the future development. Besides, it is very likely to improve the efficiency of doctors as well as the quality of work in the future

(2) Most of the current research are focusing on proposing more efficient algorithms for classification, feature extraction, image segmentation and so on. However, many fundamental limitations problems are neglected, such as the difficulties of image acquisition, the poor quality of sample tagging, the high cost of sample acquisition and so on, which will be exactly the biggest barriers for the development of artificial intelligence in medicine. The future development of artificial intelligence in medicine may focus on semi-supervised or even unsupervised learning direction, while the direction of algorithm design will be transitioned and improved from "large-scale data tasks" to "low-cost tasks with smaller sample requirements and less labeling work". This will not only meet the actual task demands of hospitals and related research institutions, but also significantly reduce the overall technical implementation threshold. At the end, this will bring more convenience to medical workers, technical researchers as well as more benefits to patients.

In a word, the medical diagnosis based on artificial intelligence is an interdisciplinary research field. The actively promotion of the development of artificial intelligence in medical field will speed up the development of multiple fields and disciplines.

REFERENCES
[1] Kotkar V A, Gharda S S. Review of various image contrast enhancement techniques. Int J Innovat Res Sci, Eng Technol, 2013, 2: 2786–2793.
[2] Bedi S S, Khandelwal R. Various image enhancement techniques—A critical review. Int J Adv Res Comput Commun Eng, 2013, 2: 1605–1609.
[3] Chaudhary C, Patil M K. Review of image enhancement techniques using histogram equalization. Int J Appl Innov Eng Manag, 2013, 2: 343–349.
[4] Papadopoulos A, Fotiadis D I, Costarouda L. Improvement of microcalcification cluster detection in mammography utilizing image enhancement techniques. Comput Biol Med, 2008, 38: 1045–1055.
[5] Warren R C, Pandya V Y, Effect of window width and viewing distance in CT display. Br J Radiol, 1982, 55: 72–74.
[6] Unser M, Aldroubi A. A review of wavelets in biomedical applications. Proc IEEE, 1996, 84: 626–638.
[7] Contreras Ortiz S H, Chiu T, Fox M D. Ultrasound image enhancement: A review. Biomed Signal Proc Control, 2012, 7: 419–428.
[8] Sene M L, Teklap A M, Schaezing R. Automatic anatomically selective image enhancement in digital chest radiography. IEEE Trans Med Imag, 1989, 8: 154–162.
[9] Gowri D S, Amudha T. A review on mammogram image enhancement techniques for breast cancer detection. In: 2014 International Conference on Intelligent Computing Applications. Coimbatore. 2014. New York: IEEE, 2014, 47–51.
[10] Hsu W Y, Chou C Y. Medical image enhancement using modified color histogram equalization. J Med Biol Eng, 2015, 35: 580–584.
[11] Ng H P, Ong S H, Foong K W C, et al. Medical image segmentation using k-means clustering and improved watershed algorithm. In: 2006 IEEE Southwest Symposium on Image Analysis and Interpretation. Denver. 2006. New York: IEEE, 2006: 61–65.
[12] Zhang D Q, Chen S C. A novel kernelized fuzzy C-means algorithm with application in medical image segmentation. Artif Intell Med, 2004, 32: 37–50.
[13] Pham M, Susomboon R, Disney T, et al. A comparison of texture models for automatic liver segmentation. In: Medical Imaging 2007: Image Processing. Landsdale: International Society for Optics and Photonics, 2007. 6512: 65124E.
[14] Dehmeshki J, Amin H, Valdivieso M, et al. Segmentation of pulmonary nodules in thoracic CT scans: a region growing approach. IEEE Trans Med Imag, 2008, 27: 467–480.
[15] Zhu B L. Improving gauss-laplacian operator based on CT image of the brain [in Chinese]. J Chongqing Three Gorges Univ, 2011, 27: 78–80.
[16] Ciresan DC, Giusti A, Gambardella LM, et al. Deep neural networks segment
neuronal membranes in electron microscopy images [J]. Advances in Neural Information Processing Systems. 2012. 25: 2852–2860.

[17] Ronneberger O, U-net: convolutional networks for biomedical image segmentation[C]. 2015, 33: 234–241.

[18] Nguyen V D, Nguyen D T, Nguyen T D, et al. An automated method to segment and classify masses in mammograms. World Acad Sci, Eng Technol, 2009, 3: 761–766.

[19] Braz Junior G, da Rocha S V, Gattass M, et al. A mass classification using spatial diversity approaches in mammography images for false positive reduction. Expert Syst Appl, 2013, 40: 7534–7543.

[20] Doyle S, Hwang M, Shah K, et al. Automated grading of prostate cancer using architectural and textural image features. In: 2007 4th IEEE International Symposium on Biomedical Imaging: From Nano to Macro. Arlington. 2007. New York: IEEE, 2007. 1284–1287.

[21] Gompertz B, Shantti N. Computer-aided diagnosis system for classifying benign and malignant thyroid nodules in multi-stained FNAB cytological images. Australas Phys Eng Sci Med, 2013, 36: 219–230.

[22] Bucia I, Gacsadi A. Directional features for automatic tumor classification of mammogram images. Biomed Signal Proc Control, 2011, 6: 370–378.

[23] Wang Y, Li J, Gao X. Latent feature mining of spatial and marginal characteristics for mammographic mass classification. Neurocomputing, 2014, 144: 107–118.

[24] W. Zhu, C. Liu, W. Fan and X. Xie, “DeepLung: Deep 3D Dual Path Nets for Automated Pulmonary Nodule Detection and Classification,” 2018 IEEE Winter Conference on Applications of Computer Vision (WACV). Lake Tahoe, NV, 2018, pp. 673-681, doi: 10.1109/WACV.2018.00079.

[25] Kool T, Litjens G, van Ginneken B, et al. Large scale deep learning for computer aided detection of mammographic lesions. Med Image Anal, 2017, 35: 303–312.

[26] Shi J, Zhou S, Liu X, et al. Stacked deep polynomial network based representation learning for tumor classification with small ultrasound image dataset. Neurocomputing, 2016, 194: 87–94.

[27] Calle-Alonso F, Pérez C J, Ártae-Nicolás J P, et al. Computer-aided diagnosis system: A Bayesian hybrid classification method. Comput Methods Progr Biomed, 2013, 112: 104–113.

[28] Kahn Jr C E, Roberts L M, Shaffer K A, et al. Construction of a Bayesian network for mammographic diagnosis of breast cancer. Comput Biol Med, 1997, 27: 19–29.

[29] Bose C, Turi D, Williams A, et al. Web services for the DDSM and digital mammography research. In: International Workshop on Digital Mammography. Heidelberg: Springer, 2006. 376–383.

[30] Guceri M N, Sahiner B, Petrick N, et al. Lung nodule detection on thoracic CT images: Preliminary evaluation of a computer-aided diagnosis system. Med Phys, 2002, 29: 2552–2558.

[31] Kuo W J, Chang R F, Chen D R, et al. Data mining with decision trees for diagnosis of breast tumor in medical ultrasonic images. Breast Cancer Res Treat, 2001, 66: 51–57.

[32] Sarit F, Naim A A, Shoorehdeli M A, et al. Thyroid disease diagnosis based on genetic algorithms using PNN and SVM. In: 2009 3rd International Conference on Bioinformatics and Biomedical Engineering. Beijing. 2009. New York: IEEE, 2009. 1–4.

[33] Shetty S, Rao V S. SVM based machine learning approach to identify Parkinson's disease using gait analysis. In: 2016 International Conference on Inventive Computation Technologies (ICICT). Coimbatore. 2016. New York: IEEE, 2017. 1–5.

[34] de Oliveira F S S, de Carvalho Filho A O, Silva A C, et al. Classification of breast regions as mass and non-mass based on mammograms using taxonomic indexes and SVM. Comput Biol Med, 2015, 57: 42–53.

[35] Campadelli P, Casiraghi E, Valentini G. Support vector machines for candidate nodules classification. Neurocomputing, 2005, 68: 281–288.

[36] Zhu Y, Yan Y, Hua Y, et al. Feature selection and performance evaluation of support vector machine (SVM)-based classifier for differentiating benign and malignant pulmonary nodules by computed tomography. J Digit Imag, 2010, 23: 51–65.

[37] Ince T, Kiranyaz S, Pulkkinen J, et al. Evaluation of global and local training techniques over feed-forward neural network architecture spaces for computer-aided medical diagnosis. Expert Syst Appl, 2010, 37: 8450–846.

[38] Bellotti R, De Carlo F, Tangaro S, et al. A completely automated CAD system for mass detection in a large mammographic database. Med Phys, 2006, 33: 3066–3075.

[39] Tramèr F, Zhang F, Juels A, et al. Stealing machine learning models via prediction apis. In: 25th USENIX Security Symposium. Berkeley: USENIX Association, 2016. 601–618.