Federated Neural Architecture Search for Medical Data Security

Xin Liu, Jianwei Zhao, Jie Li, Bin Cao, *Member, IEEE*, and Zhihan Lv, *Senior Member, IEEE*

***Abstract*—Medical data widely exist in the hospital and personal life, usually across institutions and regions. They have essential diagnostic value and therapeutic significance. The disclosure of patient information causes people's panic, therefore, medical data security solution is very crucial for intelligent health care. The emergence of federated learning (FL) provides an effective solution, which only transmits model parameters, breaking through the bottleneck of medical data sharing, protecting data security, and avoiding economic losses. Meanwhile, the neural architecture search (NAS) has become a popular method to automatically search the optimal neural architecture for solving complex practical problems. However, few papers have combined the FL and NAS for simultaneous privacy protection and model architecture selection. Convolutional neural network (CNN) has outstanding performance in the image recognition field. Combining CNN and fuzzy rough sets can effectively improve the interpretability of deep neural networks. This article aims to develop a multiobjective convolutional interval type-2 fuzzy rough FL model based on NAS (CIT2FR-FL-NAS) for medical data security with an improved multiobjective evolutionary algorithm. We test the proposed framework on the LC25000 lung and colon histopathological image dataset. Experimental verification demonstrates that the designed multiobjective CIT2FR-FL-NAS framework can achieve high accuracy superior to state-of-the-art models and reduce network complexity under the condition of protecting medical data security.**

***Index Terms*—Federated learning (FL), interval type-2 fuzzy rough neural network, medical data security, multiobjective evolution, neural architecture search (NAS).**

Manuscript received June 30, 2021; revised October 10, 2021 and December 15, 2021; accepted January 7, 2022. Date of publication January 19, 2022; date of current version May 6, 2022. This work was supported in part by the National Natural Science Foundation of China (NSFC) under Grant 61976242, in part by the Natural Science Fund of Hebei Province for Distinguished Young Scholars under Grant F2021202010, in part by the Natural Science Fund of Hebei Province under Grant G2019202350, in part by the Fundamental Scientific Research Funds for Interdisciplinary Team of Hebei University of Technology under Grant JBKYTD2002, and in part by the Guangdong Provincial Key Laboratory under Grant 2020B121201001. Paper no. TII-21-2760. *(Corresponding authors: Jie Li; Bin Cao.)*

Xin Liu and Jie Li are with the School of Economics and Management, Hebei University of Technology, Tianjin 300401, China, and also with the Guangdong Provincial Key Laboratory of Brain-Inspired Intelligent Computation, Southern University of Science and Technology, Shenzhen 518055, China (e-mail: 202011701002@stu.hebut.edu.cn; lijie@hebut.edu.cn).

Jianwei Zhao and Bin Cao are with the State Key Laboratory of Reliability and Intelligence of Electrical Equipment, Hebei University of Technology, Tianjin 300130, China, with the School of Artificial Intelligence, Hebei University of Technology, Tianjin 300401, China, and also with the Guangdong Provincial Key Laboratory of Brain-Inspired Intelligent Computation, Southern University of Science and Technology, Shenzhen 518055, China (e-mail: 201422102003@stu.hebut.edu.cn; caobin@scse.hebut.edu.cn).

Zhihan Lv is with the Uppsala University, 75105 Uppsala, Sweden (e-mail: lvzhihan@qdu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2022.3144016.

Digital Object Identifier 10.1109/TII.2022.3144016

I. Introduction

MEDICAL data have crucial diagnostic value and therapeutic significance, while private information disclosure can result in serious issues. Accordingly, the security and privacy issues of medical data have attracted more and more concern. Because of the high sensitivity characteristics of these biomedical data, data protection issues and privacy invasion risk also make these calculations subject to be strictly regulated. Meanwhile, data protection laws strictly control how data can be obtained, used, and stored.

Federated learning (FL) transmits only parameters but not data to overcome the difficulties of privacy protection. Deep learning collects large amounts of data for centralized training, leading to serious privacy threats [1], [2]. Distributed training can mitigate privacy threats among several participants [3]. FL is the model training with privacy protection in heterogeneously distributed networks. However, FL is different from distributed machine learning. FL application scenarios are more complex, focusing on the privacy of participants in addition to the goal of improving training efficiency and model accuracy [4].

FL provides a feasible direction to data security and data island. Google first proposed FL in 2016 as a solution to the problem of Android phone end users' updating their models locally [5]. Moreover, it breaks through data islands to achieve resource sharing. Past studies only concentrated on centralized algorithms, storing and processing all data on a central memory. However, because of the vast amount of biomedical data extensively distributed in hospitals and individuals, a distributed and computationally efficient approach is urgently needed. FL as a distributed machine learning technology has been applied to the health care field to improve people's health by making disease diagnoses under the condition of protecting privacy. The personal health train (PHT) has been designed to utilize and analyze data from different countries and constitutes, and it breaks the patient privacy barrier of data sharing [6]. Privacy-preserving FL was studied for monitoring heart activity data by wrist wearable devices in [7]. Fedhealth was proposed and applied to diagnose Parkinson's disease, and this learning framework improved the identification while protecting privacy [8]. FL has advantages

in biomedical data analysis [9]. It can be used for natural language processing, extracting unstructured text information from electronic medical records using multiple hospital clinical records, learning from patient representation, and phenotypic classification [10]. In [11], FL has been used to analyze the medical data from smart bracelets, aiming to screen out heart disease.

In FL, participants train the model using local data and transmit the relevant model or the updated parameters to the central server. However, the high network complexity can result in excessive model parameters and computational resources in FL. Manually designing models also requires a lot of time and cost, so it is vital for us to automatically search for the optimal network architecture with minimal complexity and manual intervention in FL. The method to lighten network structure is to design a concise and automatic network architecture optimization framework, reducing the complexity of the network [12].

Neural architecture search (NAS) can automatically find the best architecture and the related optimal parameters. It has been successfully applied in complex practical problems, such as image classification [13], especially in medical fields [14]. NAS includes search space, search strategies, and evaluation methods [15]. Evolutionary algorithms (EAs) can be used to continuous, discrete, or mixed search space for NAS. A two-layer surrogate-assisted evolutionary algorithm [16] was proposed to achieve automatic multiobjective NAS for difficult tasks. However, few papers have conducted NAS in FL. In this article, we combine NAS and FL for medical data security, which protects privacy and reduces communication costs.

Generally speaking, the structure and parameters of traditional deep neural networks are difficult to explain. For this issue, the integration of fuzzy rough sets provides an effective solution [17]. Moreover, the fuzzy neural network (FNN) combining fuzzy sets with the neural network (NN) is a powerful tool for analysis and optimization in medical diagnosis fields. In an FNN, input features are transformed to membership functions (MFs); then, via the fuzzy rule layer, "IF-THEN" rules can be formed to perform analysis. The interval type-2 MF (IT2MF) extends each membership degree to a more applicable degree range for real-world problems. Rough set theory is complementary to fuzzy sets; thus, by combining them, a rough set enhanced firefly algorithm with the IT-2 fuzzy logic system (IT2FLS) was proposed [18] for heart disease prediction. Sarkar *et al.* [19] proposed a rough type-2 fuzzy C-means clustering algorithm to process the soft-tissue classification for brain magnetic resonance images. A new fuzzy diagnosis method based on the type-2 fuzzy system can help doctors realize faster and more accurate diagnosis by changing the uncertainty level of the model [20]. Via mingling the IT-2 fuzzy rough set with the NN, the IT-2 fuzzy rough NN was proposed by Cao *et al.* [21] for time series prediction. However, no paper has combined IT-2 fuzzy rough NN with FL for medical image classification with emphasis on medical data security.

CNN is an effective tool in the image recognition field [22]. This article constructs a convolutional IT-2 fuzzy rough FL model based on NAS (CIT2FR-FL-NAS) for medical data security. As far as we know, it is the first application of such the CIT2FR-FL-NAS framework to medical image recognition concerning medical security. Furthermore, it also can develop an accurate, low-cost, and scalable model for image diagnosis and management of disease while protecting privacy. Clinical data show that lung and colon cancers are the first and third common malignant tumors, and the two common causes of human death and morbidity, seriously threatening people's health and safety. We test the LC25000 lung and colon histopathological image dataset, and the proposed framework achieves accurate classification effect under the condition of protecting medical data security.

The contributions can be summarized as follows.

1) For medical data security, we propose a multiobjective FL-NAS model. Each participant trains the model locally utilizing its own data, avoiding the privacy information disclosure of patients. Moreover, it automatically searches the optimal network architecture with minimal complexity and manual intervention.
2) A supernet CNN is designed to extract features from histopathological images, and by integrating the IT2FR set theory, a convolutional IT-2 fuzzy rough neural network (CIT2FRNN) model is proposed. This model can effectively increase the interpretability of the CNN.
3) An improved multiobjective evolutionary algorithm based on utility is proposed. Through experimentation, compared to the other state-of-the-art models, the CIT2FR-FL-NAS model can achieve high accuracy and reduce the network complexity under the condition of protecting privacy.

The rest of this article is organized as follows. Section II provides the preliminaries needed to understand this article. The proposed CIT2FR-FL-NAS model is presented in Section III. Section IV reports the case study. Finally, Section V concludes this article.

II. Preliminaries

A. Neural Architecture Search

NAS includes search space, search strategies, and performance evaluation [23]. The search space defined the basic architecture that needs to be estimated to construct NNs. Search strategies determine the way of searching basic architecture units for particular search tasks and confirm the way of connections inside the network. In this article, we mainly focus on the EA-based search.

EAs hardly depend on the attribute information of the optimization problem itself (e.g., differentiability) and have wide applications in NAS. EAs for NNs can be dated back to thirty years ago, which is called neuroevolution. We can reconstruct the architecture and generate the best model by inheriting the current knowledge [24]. EAs are proved to be a very effective and state-of-the-art NAS method [25]. In the work of [26], the authors designed an indirect encoding way to search the best architecture according to the characteristics of the NNs, and this method can make the evolutionary process more economical in terms of computation. For some historical reasons, there are few related works about multiobjective neuroevolution. With

respect to NAS, the computational resource consumption and the accuracy should be concerned. Thus the multiobjective neuroevolution has great research significance. In the work of [27], NSGA-II has been utilized to optimize conflicting objectives of the hardware efficiency and the network accuracy. The BioNet-Explorer framework [28] has been proposed to generate multiple DNN architectures for wearable devices systematically. EEEA-Nets [29] is a NAS framework to generate network architectures having minimal computational cost and prediction error, which can maintain the accuracy as well as reduce time and the number of parameters.

B. IT-2 Fuzzy Rough Set

Fuzzy logic is based on human linguistic information, which has some advantages, such as stability, free model, and robustness. Fuzzy logic combining NN method can be a practical solution for control, prediction, and classification fields [30].

Gaussian and Gaussian combination,[1] sigmoid, and other functions can be utilized as MFs. By using several MFs, an input feature value can be transformed to several different degree values. Therefore, MFs can describe the value distribution and characterize each input feature, which facilitates further processing.

A great deal of uncertainty exists in reality's available datasets, such as biomedical image data. Traditional type-1 fuzzy set is not practical enough to reflect fuzziness. Instead, uncertainty can be represented by higher-level type-2 fuzzy sets [31]. Moreover, an IT2MF converts a given input value to a degree range, which increases the practicability of complex problems [32].

Type-2 fuzzy sets (T2FSs) can strengthen model representation by fuzzification, then can effectively explain the fuzzy information. Fuzzy set theory utilizes fuzzy clusters that are represented as MFs to describe the input values as membership degrees and subsequently generate fuzzy rules. Rough set theory quantifies the connection with aforementioned fuzzy rules to a set of entities. It takes feature selection as the focus to transform fuzzy theory and realizes accurate biological image classification through the rough FNN [33]. By combining the IT-2 fuzzy set, the rough set theory, and the NN, an IT2FRNN was constructed [21].

C. Convolutional Fuzzy Rough Neural Network

CNN has been extensively applied to medical image learning [34]. Combining fuzzy rough sets and CNN can effectively reduce noise and data uncertainty. CNN is a feature extractor, which includes: local perception, weight sharing, and spatial down-sampling. This structure can effectively deal with noisy and distorted image information. Fuzzy rough sets can learn MFs, and then can generate fuzzy rules from amounts of data. It is a model approximation strategy. Moreover, it can reduce data uncertainty and solve complicated practical problems. Thus, we can better understand original data and the difficult classification task with data ambiguity and noise.

[1]See the MATLAB documentation and search for "Gaussian combination."

CNNs have high complexity and low interpretability, while fuzzy systems have natural interpretability. Combining CNNs with fuzzy rough sets is conducive to improving the interpretability of deep neural networks. Yegnejou *et al.* [17] proposed an interpretable deep convolutional fuzzy classifier, which first regards the CNN as an automatic feature extractor, and then uses the fuzzy clustering for further feature analysis. Although the utilization of fuzzy classifier reduces network performance slightly, an efficient interpretation mechanism is introduced. Hsu *et al.* [35] combined CNN and FNN, used the semi-connected layer, fuzzified the final feature maps generated by CNN, generated fuzzy rules, and finally obtained classification inference. Nguyen *et al.* [36] used the fuzzy layer to fuzzify the input, and then carried out a series of processing through the fuzzy convolution layer, pooling layer and full connection layer, and finally executed defuzzification and classification.

D. Federated Learning

FL [37] targets to construct an FL model on account of distributed data sets. It is an emerging distributed privacy protection technology. Every participant downloads the global model from the central equipment, then trains the model by using the local data, and transmits parameters to the central equipment to update the original model. Moreover, this cycle continues many times until the model convergence is recognized. Without exchanging and sharing data, every participant trains its model and parameters by local data. Thus, FL reduces the risk of privacy and sensitive data leakage. In other word, multiple participants (such as mobile devices or hospitals) collaborate to train the global model on a central server.

FL is the training of privacy-protection model in heterogeneous and distributed networks. However, FL differs from the traditional distributed machine learning. In the process of traditional distributed machine learning, the data of each participant is distributed independently and identically, and the data amount is similar. The central node has the access right to distributed nodes without considering the privacy issue. In the FL environment, the data of each FL participant is owned by itself, which is not necessarily independent and uniformly distributed. The data volume and data quality of each node can be significantly different. Each node has the autonomy of its own data, and the privacy issue needs to be fully considered.

III. Federated Neural Architecture Search Model

We construct a multiobjective convolutional IT-2 fuzzy rough FL framework based on NAS for medical data security, denoted as CIT2FR-FL-NAS. This model can automatically search optimal architectures for medical diagnostic problems with improving the interpretability of deep NNs by fusing fuzzy rough set theory. Moreover, it not only can attain high accuracy but also can reduce the network complexity under the condition of protecting privacy.

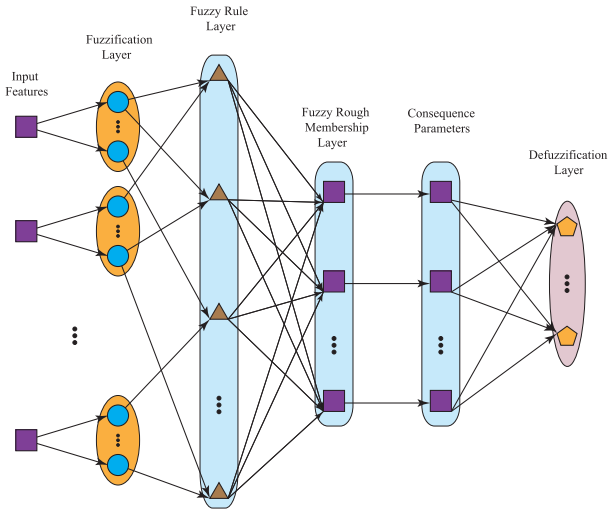


Fig. 1. Interval type-2 fuzzy rough neural network model.

A. Convolutional Interval Type-2 Fuzzy Rough Neural Network

As shown in Fig. 1, L_n denotes layer n, I_i denotes the input feature i, and O denotes the output. Specifically, by denoting layer n's output as O^n, the mechanism of the IT2FRNN can be detailed layer by layer as follows.

1) L_1

$$O_i^1 = I_i \tag{1}$$

where $i = 1, \ldots, IN$ denotes the index, and IN denotes the number of input features.

2) L_2

$$O_{i,j,l}^2 = \underline{f}_{i,j}^{\text{IT2}}\left(O_i^1\right) \tag{2}$$

$$O_{i,j,r}^2 = \overline{f}_{i,j}^{\text{IT2}}\left(O_i^1\right)$$

$$\text{s.t. } i = 1, \ldots, IN,\ j = 1, \ldots, N_i^{\text{mb}} \tag{3}$$

where l and r denote the lower and upper cases for the IT-2 fuzzy set, $[\underline{f}_{i,j}^{\text{IT2}}, \overline{f}_{i,j}^{\text{IT2}}]$ denotes the output of an IT-2 MF, and N_i^{mb} denotes the number of MFs for input i.

3) L_3

$$O_{i,l}^3 = \prod_{j=1}^{N_i^{\text{ir}}} O_{\text{ind4rule1}(i,j),\text{ind4rule2}(i,j),l}^2 \tag{4}$$

$$O_{i,r}^3 = \prod_{j=1}^{N_i^{\text{ir}}} O_{\text{ind4rule1}(i,j),\text{ind4rule2}(i,j),r}^2$$

$$\text{s.t. } i = 1, \ldots, N^{\text{rule}},\ j = 1, \ldots, N_i^{\text{ir}} \tag{5}$$

where $\text{ind4rule1}(i,j)$ and $\text{ind4rule2}(i,j)$ denote the indices of a MF in L_2 for input j of fuzzy rule i, N^{rule} denotes the number of fuzzy rules, and N_i^{ir} denotes the number of inputs for fuzzy rule i.

4) L_4

$$O_{i,l}^4 = \prod_{j=1}^{N^{\text{rule}}} O_{j,l}^3 w_{i,j}^4 c_{i,j}^4 \tag{6}$$

$$O_{i,r}^4 = \prod_{j=1}^{N^{\text{rule}}} O_{j,r}^3 w_{i,j}^4 c_{i,j}^4$$

$$\text{s.t. } i = 1, \ldots, N^{\text{rough}},\ j = 1, \ldots, N^{\text{rule}} \tag{7}$$

where $w_{i,j}^4$ denotes the connection weight between rough node i and fuzzy rule node j, $c_{i,j}^4$ denotes the connection status between rough node i and fuzzy rule node j, and N^{rough} denotes the number of rough nodes.

5) L_5

$$O_i^5 = a_{i,0}^5 + \sum_{j=1}^{IN} a_{i,j}^5 I_j$$

$$\text{s.t. } i = 1, \ldots, N^{\text{rough}},\ j = 1, \ldots, IN \tag{8}$$

where $a_{i,j}^5$ $(j = 0, 1, \ldots, IN)$ denotes parameters.

6) L_6

$$O^6 = \sum_{j=1}^{N^{\text{rough}}} \frac{O_j^5\left(O_{j,l}^4 + O_{j,r}^4\right)}{\sum_{j=1}^{N^{\text{rough}}}\left(O_{j,l}^4 + O_{j,r}^4\right)}$$

$$\text{s.t. } j = 1, \ldots, N^{\text{rough}}. \tag{9}$$

In summary, the procedure is as follows.

1) L_1: Layer 1 receives the input feature values of a sample.
2) L_2: For each input feature, layer 2 utilizes several MFs to transform each feature into a series of membership degrees.
3) L_3: By selecting several MFs and multiplying the corresponding membership degrees, each node in layer 3 determines the activation probability of a fuzzy rule.
4) L_4: In traditional FNNs, the next layer defuzzifies the fuzzy rules to generate the output. However, in the fuzzy rough neural network (FRNN), a rough layer is added to further arrange the fuzzy rules in the fuzzy layer. Each rough node associates several fuzzy rules with different degrees; these are referred to as fuzzy rough membership degrees. As a result, a large number of fuzzy rules can be reduced to a smaller number of fuzzy rough rule outputs, which increases the simplicity and interpretability of the system.
5) L_5: For each fuzzy rough rule, a consequence is generated via a linear transformation of the input features. Combined with the nonlinear rules and linear consequences, the IT2FRNN can fully utilize the input feature information.
6) L_6: Finally, the defuzzification in layer 6 produces the output based on the fuzzy rough rule probabilities and consequences.

The CIT2FRNN model is improved based on IT2FRNN, and is detailed as follows.

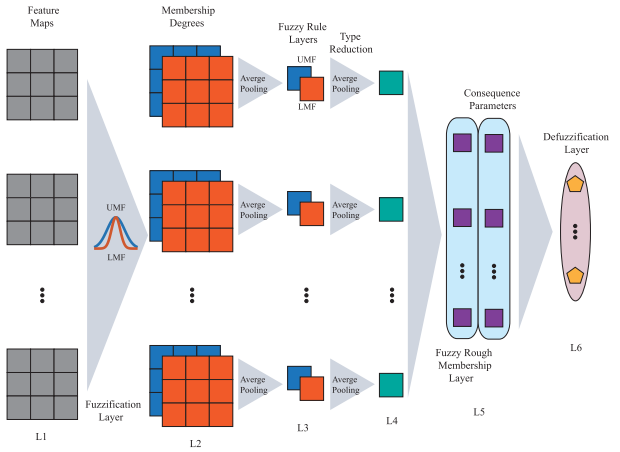


Fig. 2. Convolutional interval type-2 fuzzy rough structure.

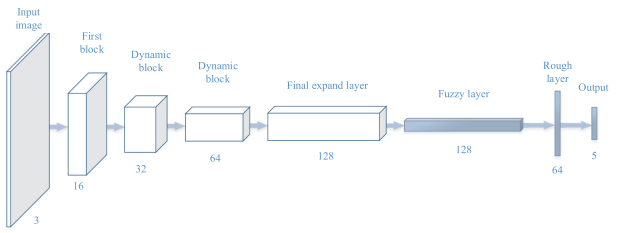


Fig. 3. Supernet structure.

1) As illustrated in Fig. 3, a supernet CNN is designed to transform the input image and obtain features for further process via the IT-2 fuzzy rough set as in Fig. 2. The supernet is a simplified version of that in [16] and [38], and the number of dynamic blocks is decreased from 5 to 2.
2) L_1: As the CNN is utilized to extract useful features, the inputs are several feature maps.
3) L_2: For fuzzification, the Gaussian interval type-2 membership function is utilized, formulated as follows:

$$\underline{f}^{IT2}(u) = e^{-(u-c)^2\times\left(2\underline{\sigma}^2+\varepsilon\right)} \tag{10}$$

$$\overline{f}^{IT2}(u) = e^{-(u-c)^2\times\left(2\overline{\sigma}^2+\varepsilon\right)}$$

$$\text{s.t.,}\ \underline{\sigma} < \overline{\sigma} \tag{11}$$

where u denotes the input value, c denotes the center parameter, $\underline{\sigma}$ and $\overline{\sigma}$ are scaling factors, and $\varepsilon = 10^{-6}$ denotes a small value. Via fuzzification, each input feature map will be transformed to a lower membership degree map and an upper membership degree map.
4) L_3: Simultaneously considering brevity and the characteristics of fuzzy rules, each membership degree map is averaged to one degree value via the average pooling. In this way, all membership degrees can be equally considered and the calculation is simple.
5) L_4: As aforementioned, in L_4 of the IT2FRNN, the upper and lower membership degrees are summarized separately, which are added together in L_6. Contrarily, each pair of lower and upper membership degrees can be averaged first to simplify the calculation, which can be achieved via average pooling, realizing type reduction. Then, these reduced membership degrees are connected to the rough nodes via a full connection layer.
6) L_5: For each rough node, this layer generates a consequence via the linear regression of all the original inputs, which can be realized by connecting the input values to consequence nodes via a full connection layer. As the elements in the input feature maps can be enormous, the parameter amount will be large. Accordingly, the consequence nodes can be removed, and only the degree values are utilized for classification.
7) L_6: This layer contains more than one node, each of which represents a class label. Full connections are utilized between the rough nodes and the output nodes, and the connection weights are to be optimized. Finally, the node with the maximum output value is obtained, and the corresponding label is the predicted class label.

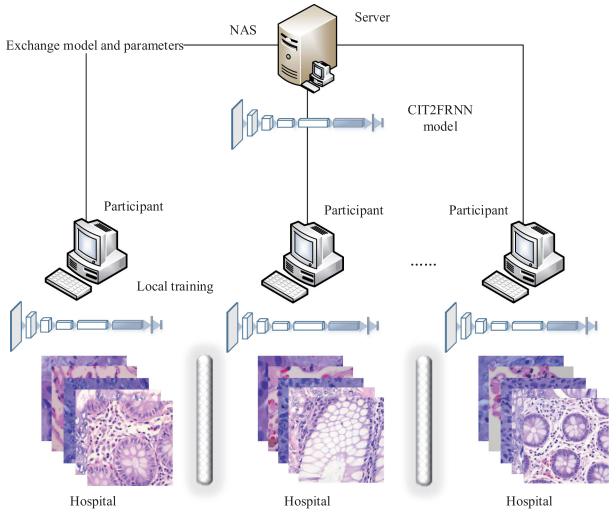
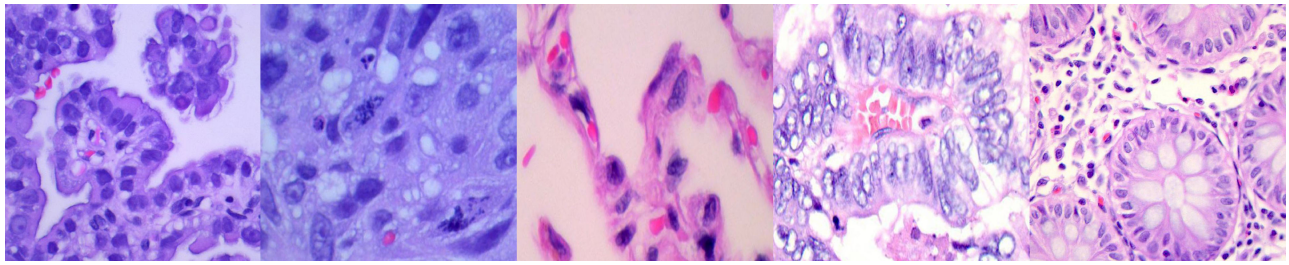


Fig. 4. FL framework.

B. Federated Learning Based on Neural Architecture Search

In this article, we proposed an FL framework as in Fig. 4. In this framework, we use Fed-Avg: the parameters of each participant's own training are transmitted to the server and averaged in each communication phase. The ultimate goal is to achieve medical image diagnosis of cancerous lesions under the condition of protecting privacy. The FL process is as follows. The participants download the global model, then train the model using the local data, and finally obtain new parameters. Every participant transmits the new network parameters to the central server, and the server averages the parameters and then updates the original model. Afterward, the new model with the parameters is transmitted to every participant. The above procedure is conducted for several rounds until the whole training process converges.

Following the procedure in [16] and [38], a supernet is required and trained. As the cancerous lesion diagnosis problem is



(a) (b) (c) (d) (e)

Fig. 5. Lung and colon medical images. (a) Lung adenocarcinoma. (b) Lung squamous cell carcinoma. (c) Benign lung tissue. (d) Colon adenocarcinoma. (e) Benign colonic tissue.

TABLE I
SEARCH SPACE

Variable	Implication	Value
N_{block}	Number of blocks	2
L_{kernel}	Kernel size	$\{3, 5, 7\}$
R_{expan}	Expansion rate	$\{1, 2, 3, 4\}$
D_{block}	Depth of each block	$\{1, 2, 3, 4\}$
L_{input}	Input image resolution	$\{128, 132, 136, \ldots, 256\}$
F_{fuzzy}	Flag of the fuzzy layer	$\{0, 1\}$

much more minor than the ImageNet, and to reduce the supernet complexity, a simplified supernet is constructed as in Fig. 3, in which the number of dynamic blocks is 2 instead of 5 and the channel numbers are also decreased. To protect data privacy, the supernet is trained under the FL framework.

After the trained supernet is generated, the NAS-based FL begins; thus, the searched network architecture is trained in the clients for one or more epochs based on the local data. The server gathers the model parameters to update the model and evaluate the architecture. The server is also responsible for exploring the network architecture space based on the multiobjective surrogate-enhanced neuroevolution [16] via simultaneously considering the network accuracy and complexity, and the search space is listed in Table I.

Finally, via combining proposed supernet CNN structure, the IT-2 fuzzy rough structure, and the FL based on NAS, we propose a CIT2FR-FL-NAS framework for feature exaction and classification of histopathological images, aiming to protect medical data security.

C. Improved Multiobjective Evolutionary Algorithm

In the original NSGANetV2 [16], NSGA-II [39] was utilized to evolve the CNN architecture. To improve search efficiency and performance, we utilize MOEA/D [40] and make several improvements. There are many variants of MOEA/D. Especially, for the decomposition, we utilized the normalized Chebyshev approach

$$v_{i,j}^{\text{fit}} = \max\left(\frac{y_{i,m} - v_m^{\text{ideal}}}{v_m^{\text{nadir}} - v_m^{\text{ideal}}} / w_{j,m}\right)$$
$$\sum_{m-1}^{M} w_{j,m} = 1 \quad \forall j \tag{12}$$

where $v_{i,j}^{\text{fit}}$ denotes the fitness value of individual i with respect to reference weight vector j, $y_{i,m}$ denotes the mth objective value of individual i, v_m^{ideal} (v_m^{nadir}) denotes the mth objective value of the ideal (nadir) point, $w_{j,m}$ denotes the mth value of weight vector j, and M denotes the number of objectives.

Based on this baseline MOEA/D, we improve the selection strategy, and introduce utility to quantify the probability of selecting parents in the neighborhood of a weight vector for exploration (while for a predefined small probability of 0.1, parents are selected among the whole population), which is updated as follows:

$$v_i^{\text{util}} = uti_i + \alpha^{\text{util}} \times v_i^{\text{util}} \tag{13}$$

where v_i^{util} denotes the utility value of weight vector i, uti_i denotes the average normalized network accuracy improvement of the offspring corresponding to weight vector i, and $\alpha^{\text{util}} = 0.99$ denotes the utility parameter.

IV. CASE STUDY

A. Data Description

The LC25000 lung and colon histopathological image dataset [41] is utilized for experimentation. The dataset contains 15 000 lung histopathological images with three categories: lung adenocarcinoma [see Fig. 5(a)], lung squamous cell carcinoma [see Fig. 5(b)], and benign lung tissue [see Fig. 5(c)], as well as 10 000 colon histopathological images with two categories: colon adenocarcinoma and benign colonic tissue, each of which includes 5000 images. The original image size is 768×768. The dataset is divided into the training, validation, and test dataset, and the split ratio is $3 : 1 : 1$.

B. Experimental Setting

For FL, three clients are established; accordingly, the training dataset is uniformly separated to all participants.

For the CIT2FRNN model, as illustrated in Fig. 3, two dynamic blocks are stacked, whose depths, as well as each layer's kernel size and expansion rate, are optimized. As in Fig. 3, for the first block, two dynamic blocks, the final expand layer, the fuzzy layer, and the rough layer, the numbers of channels are 16, 32, 64, 128, 128, and 64, respectively.

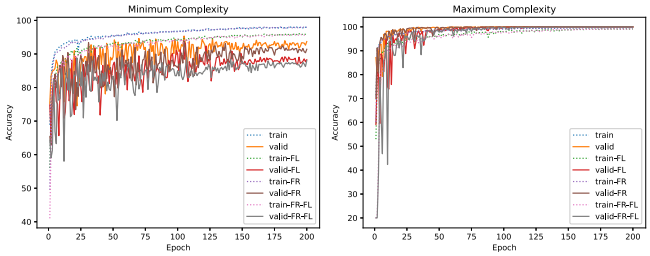


Fig. 6. Accuracy curves of the network architectures with the minimum and maximum complexities in the search space (i.e., Table I) during training. FR and FL denote the integrations of the interval type-2 fuzzy rough set and the FL, respectively.

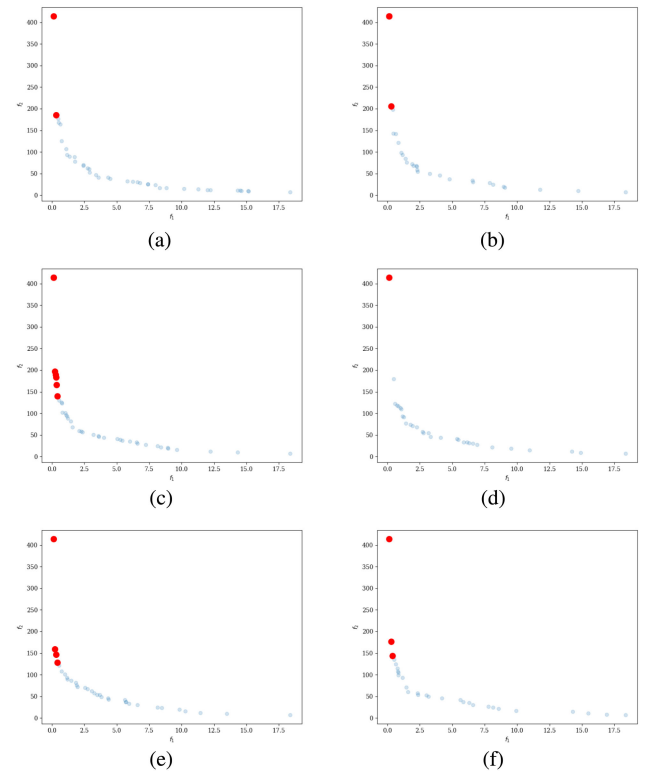


Fig. 7. Visualization of the performance of all explored architectures. (a) NSGA-II. (b) MOEA/D. (c) MOEA/D-1. (d) MOEA/D-2. (e) MOEA/D-3. (f) MOEA/D-4.

For the model training in the CIT2FR-FL-NAS framework, the SGD optimizer is utilized for optimization. The initial learning rate is 0.05, the Nesterov momentum with the factor of 0.9 is set up, and weight decay parameter is 4×10^{-5}. The number of epochs is 200 for the training of the supernet and 5 for the refinement during neuroevolution. Every one epoch, the clients upload the model parameters to the central server, then the central server averages all of the parameters and sends the updated model to the clients for further training.

C. Results and Analysis

1) Training of the Supernet: Fig. 6 illustrates the accuracy curves of various models. Two network architectures are trained for 200 epochs. For the architecture with the minimum complexity [see Fig. 6(a)], implementing the FL and FR will decrease the accuracy. For the network architecture with the maximum complexity [see Fig. 6(b)], the performance differences of various models are trivial. Table II lists the best accuracies and the corresponding epoch number of all models. Similar to Fig. 6, the architecture's performance with the minimum complexity is worse than that of the architecture with the maximum complexity. Table III lists the test accuracies of best models in Table II, and the increment of complexity contributes to the performance improvement. For the maximum-complexity network architecture, the accuracy obtained is 99.96% with FL and FR, 0.04% worse than the model with centralized learning. Though the FR has no contribution to the accuracy, it improves interpretability to the model. For the minimum-complexity network architecture, the result attained 92.98% for the model with FL and 89.24% for the model with FR and FL. The model with FR after centralized learning can attain the accuracy of 100.00%.

TABLE II
STATISTICS OF BEST ACCURACIES OF MODELS WITH THE MINIMUM AND MAXIMUM COMPLEXITIES

		train	valid	train-FL	valid-FL	train-FR	valid-FR	train-FR-FL	valid-FR-FL
Min Comp	acc	98.08	95.36	96.06	93.18	98.05	93.98	95.86	89.02
	epoch #	190	104	177	105	189	104	189	56
Max Comp	acc	99.76	100.00	99.25	99.96	99.75	100.00	99.22	99.98
	epoch #	190	92	195	124	198	86	185	167

TABLE III
STATISTICS OF TEST ACCURACIES OF MODELS

	min	min-FL	min-FR	min-FR-FL	max	max-FL	max-FR	max-FR-FL
Accuracy	95.94	92.98	94.02	89.24	100.00	99.96	100.00	99.96

Note: "min" and "max" denote the network architectures with the minimum and maximum complexities.

TABLE IV
TEST ACCURACIES OF OTHER RELATED MODELS

	DHS-CapsNet [42]	multi-input capsule network [43]	CNN model [44]
Accuracy	99.23	99.58	96.33

2) Discussion of FR: On the one hand, as listed in Table II, the addition of FR slightly decreases the average accuracy of the minimum-complexity architecture, but the difference is little for the maximum-complexity architecture. On the other hand, the feature maps are transformed to membership degrees in the fuzzy domain via adding the FR, increasing the interpretability. What should be mentioned is that, in the models after training, the parameters $\underline{\sigma}$ and $\overline{\sigma}$ in (10) and (11) tend to have quite similar absolute values. The reason may be that, via the average pooling, the same gradients forced the two parameters to converge to the same absolute value.

3) Comparison of the Acquired Results With Other Related Models: Table IV lists the performance of state-of-the-art deep learning models for comparison. Obviously, our proposed maximum-complexity model is better than the DHS-CapsNet [42], the CNN model in [44], and the multi-input capsule network [43]. Additionally, our proposed model with FR can add interpretability and privacy. Therefore, the model we proposed has excellent competitive advantages and realistic significance.

4) Multiobjective NAS: For the NAS in this part, the trained maximum-complexity architectures integrating FL (with and without FR) is employed as the supernets. Based on the supernets trained in Section IV-C1, the multiobjective NAS explores the search space as in Table I to sample network architectures via simultaneously considering the accuracy and FLOPs. Fig. 7 illustrates the objective values of all the obtained nondominated architectures after evolution of 30 generations for NSGA-II and various MOEA/D. The architectures with test accuracies not worse than the multi-input capsule network [43] (99.58%) are highlighted in red. MOEA/D in Fig. 7(b) denotes the baseline MOEA/D. MOEA/D-1 (MOEA/D-2) denotes MOEA/D with the initial utility values uniformly sampled from 0.1 (0.5) to 0.01 (0.05), and the better the accuracy, the larger the utility value. MOEA/D-3 (MOEA/D-4) denotes MOEA/D with initial utility values set to 0.1 (0.5). With respect to the number of highlighted architectures, MOEA/D-1 $>$ MOEA/D-3 $>$ MOEA/D-4 $>$ NSGA-II $=$ MOEA/D $>$ MOEA/D-2. With respect to the quality of highlighted architectures, MOEA/D-1, MOEA/D-3, and MOEA/D-4 dominate NSGA-II regardless of the maximum-complexity architecture. In conclusion, CIT2FR-FL-NAS model can attain high accuracy and reduce the amount of calculation and network complexity under the condition of protecting privacy.

V. Conclusion

This article proposed a CIT2FR-FL-NAS model for image classification with focusing on medical data security. As far as we know, this was the first application of combining the NAS and the IT-2 fuzzy rough set theory in FL for medical image diagnosis under the condition of protecting data security. The multiobjective CIT2FR-FL-NAS protected privacy as well as simultaneously reduced the computational burden and improved accuracy. We tested the proposed framework on the LC25000 lung and colon histopathological images. Experimental verification demonstrated that the generated CIT2FR-FL-NAS structure was compact and better than other related models. We conclude that our research contribution will be beneficial to medical image processing and security from these results. It helps medical practitioners make more accurate medical diagnoses while protecting data privacy with minimal manual intervention.

References

[1] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 4, pp. 870–885, Apr. 2019.

[2] S. Savazzi, M. Nicoli, M. Bennis, S. Kianoush, and L. Barbieri, "Opportunities of federated learning in connected, cooperative, and automated industrial systems," *IEEE Commun. Mag.*, vol. 59, no. 2, pp. 16–21, Feb. 2021.

[3] M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6532–6542, Oct. 2020.

[4] Y. Qian, L. Hub, J. Chen, X. Guan, M. M. Hassan, and A. Alelaiwi, "Privacy-aware service placement for mobile edge computing via federated learning," *Inf. Sci.*, vol. 505, pp. 562–570, Dec. 2019.

[5] H. B. Mcmahan, E. Moore, D. Ramage, and B. A. Y. Arcas, "Federated learning of deep networks using model averaging," 2016. [Online]. Available: https://arxiv.org/abs/1602.05629

[6] T. M. Deist, F. J. W. M. Dankers, and P. Ojha, "Distributed learning on 20 000 lung cancer patients - The personal health train," *Radiotherapy Oncol.*, vol. 144, pp. 189–200, Mar. 2020.

[7] Y. S. Can and C. Ersoy, "Privacy-preserving federated deep learning for wearable IoT-based biomedical monitoring," *ACM Trans. Internet Technol.*, vol. 21, no. 1, 2021, Art. no. 21.

[8] Y. Chen, X. Qin, J. Wang, C. Yu, and W. Gao, "Fedhealth: A federated transfer learning framework for wearable healthcare," *IEEE Intell. Syst.*, vol. 35, no. 4, pp. 83–93, Jul./Aug. 2020.

[9] J. Xu, B. S. Glicksberg, C. Su, P. Walker, J. Bian, and F. Wang, "Federated learning for healthcare informatics," *J. Healthcare Inform. Res.*, vol. 5, no. 1, pp. 1–19, Nov. 2020.

[10] D. Liu, D. Dligach, and T. Miller, "Two-stage federated phenotyping and patient representation learning," in *18th SIGBioMed Workshop Biomed. Natural Lang. Process.*, 2019, pp. 283–291, doi: 10.18653/v1/W19-5030.

[11] M. V. Perez, K. W. Mahaffey, H. Hedlin, J. S. Rumsfeld, and Garcia, "Large-scale assessment of a smartwatch to identify atrial fibrillation," *New England J. Med.*, vol. 381, no. 20, pp. 1909–1917, Nov. 2019.

[12] H. Zhu, H. Zhang, and Y. Jin, "From federated learning to federated neural architecture search: A survey," *Complex Intell. Syst.*, vol. 7, no. 2, pp. 639–657, Apr. 2021.

[13] F. Junior and G. G. Yen, "Particle swarm optimization of deep neural networks architectures for image classification," *Swarm Evol. Comput.*, vol. 49, pp. 62–74, 2019.

[14] Z. Yu, X. Li, X. Niu, J. Shi, and G. Zhao, "AutoHR: A strong end-to-end baseline for remote heart rate measurement with neural searching," *IEEE Signal Process. Lett.*, vol. 27, pp. 1245–1249, Jul. 2020, doi: 10.1109/LSP.2020.3007086.

[15] R. Pengzhen, X. Yun, and C. Xiaojun, "A comprehensive survey of neural architecture search: Challenges and solutions," *ACM Comput. Surv.*, vol. 54, no. 4, May 2021, Art. no. 76.

[16] Z. Lu, K. Deb, and E. Goodman, "NSGANetV2: Evolutionary multi-objective surrogate-assisted neural architecture search," in *Proc. 16th Eur. Conf. Comput. Vis.*, 2020, pp. 35–51.

[17] M. Yeganejou, S. Dick, and J. Miller, "Interpretable deep convolutional fuzzy classifier," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 77, pp. 1407–1419, Jul. 2020.

[18] N. C. Long, P. Meesad, and H. Unger, "A highly accurate firefly based algorithm for heart disease prediction," *Expert Syst. Appl.*, vol. 42, no. 21, pp. 8221–8231, Nov. 2015.

[19] J. P. Sarkar, I. Saha, and U. Maulik, "Rough possibilistic Type-2 fuzzy C-means clustering for MR brain image segmentation," *Appl. Soft Comput.*, vol. 46, pp. 527–536, Sep. 2016.

[20] E. Ontiveros, P. Melin, and O. Castillo, "Comparative study of interval Type-2 and general Type-2 fuzzy systems in medical diagnosis," *Inf. Sci.*, vol. 525, pp. 37–53, Jul. 2020.

[21] B. Cao, J. Zhao, Z. Lv, Y. Gu, P. Yang, and S. K. Halgamuge, "Multiobjective evolution of fuzzy rough neural network via distributed parallelism for stock prediction," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 5, pp. 939–952, May 2020.

[22] H. Yu, L. T. Yang, Q. Zhang, D. Armstrong, and M. J. Deen, "Convolutional neural networks for medical image analysis: State-of-the-art, comparisons, improvement and perspectives," *Neurocomputing*, vol. 444, pp. 92–110, Jul. 2021.

[23] T. Elsken, J. Metzen, and F. Hutter, "Neural architecture search: A survey," *J. Mach. Learn. Res.*, vol. 20, no. 55, pp. 1–21, Mar. 2019.

[24] Y. Chen, R. Gao, F. Liu, and D. Zhao, "ModuleNet: Knowledge-inherited neural architecture search," *IEEE Trans. Cybern.*, to be published, doi: 10.1109/TCYB.2021.3078573.

[25] E. Galvan and P. Mooney, "Neuroevolution in deep neural networks: Current trends and future challenges," *IEEE Trans. Artif. Intell.*, vol. 6, no. 2, pp. 476–493, Dec. 2021.

[26] J. Long, S. Zhang, and C. Li, "Evolving deep echo state networks for intelligent fault diagnosis," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4928–4937, Jul. 2020.

[27] A. Marchisio, A. Massa, V. Mrazek, B. Bussolino, M. Martina, and M. Shafique, "NASCaps: A framework for neural architecture search to optimize the accuracy and hardware efficiency of convolutional capsule networks," in *Proc. IEEE/ACM Int. Conf. Comput. Aided Des.*, 2020, pp. 1–9.

[28] B. S. Prabakaran, A. Akhtar, S. Rehman, O. Hasan, and M. Shafique, "BioNetExplorer: Architecture-space exploration of biosignal processing deep neural networks for wearables," *IEEE Internet Things J.*, vol. 8, no. 17, pp. 13251–13265, Sep. 2021.

[29] C. Termritthikun, Y. Jamtsho, J. Ieamsaard, P. Muneesawang, and I. Lee, "EEEA-Net: An early exit evolutionary neural architecture search," *Eng. Appl. Artif. Intell.*, vol. 104, Sep. 2021, Art. no. 104397.
[30] S. Aminikhanghahi, S. Shin, W. Wang, S. I. Jeon, and S. H. Son, "A new fuzzy Gaussian mixture model (FGMM) based algorithm for mammography tumor image classification," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 10191–10205, Apr. 2017.
[31] L. Zadeh, "The concept of a linguistic variable and its application to approximate reasoning-i," *Inf. Sci.*, vol. 8, no. 3, pp. 199–249, 1975. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0020025575900365
[32] M. Han, K. Zhong, T. Qiu, and B. Han, "Interval type-2 fuzzy neural networks for chaotic time series prediction: A concise overview," *IEEE Trans. Cybern.*, vol. 49, no. 7, pp. 2720–2731, Jul. 2019.
[33] C. Affonso, R. J. Sassi, and R. M. Barreiros, "Biological image classification using rough-fuzzy artificial neural network," *Expert Syst. Appl.*, vol. 42, no. 24, pp. 9482–9488, Dec. 2015.
[34] S. K. Zhou *et al.*, "A review of deep learning in medical imaging: Imaging traits, technology trends, case studies with progress highlights, and future promises," *Proc. IEEE*, vol. 109, no. 5, pp. 820–838, May 2021.
[35] M.-J. Hsu, Y.-H. Chien, W.-Y. Wang, and C.-C. Hsu, "A convolutional fuzzy neural network architecture for object classification with small training database," *Int. J. Fuzzy Syst.*, vol. 22, no. 11, pp. 1–10, Feb. 2020.
[36] T.-L. Nguyen, S. Kavuri, and M. Lee, "A multimodal convolutional neuro-fuzzy network for emotion understanding of movie clips," *Neural Netw.*, vol. 118, pp. 208–219, Oct. 2019.
[37] H. Zhu and Y. Jin, "Multi-objective evolutionary federated learning," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 4, pp. 1310–1322, Apr. 2020.
[38] H. Cai, C. Gan, T. Wang, Z. Zhang, and S. Han, "Once for all: Train one network and specialize it for efficient deployment," in *Proc. Int. Conf. Learn. Representations*, 2020, pp. 1–13. [Online]. Available: https://arxiv.org/pdf/1908.09791.pdf
[39] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II," *IEEE Trans. Evol. Comput.*, vol. 6, no. 2, pp. 182–197, Apr. 2002.
[40] Q. Zhang and H. Li, "MOEA/D: A multiobjective evolutionary algorithm based on decomposition," *IEEE Trans. Evol. Comput.*, vol. 11, no. 6, pp. 712–731, Dec. 2007.
[41] A. A. Borkowski, M. M. Bui, and Thomas., "Lung and colon cancer histopathological images | kaggle," 2019. Accessed: Jul. 16, 2020. [Online]. Available: https://www.kaggle.com/andrewmvd/lung-and-colon-cancer-histopathological-images
[42] K. Adu, Y. Yu, J. Cai, K. Owusu-Agyemang, B. A. Twumasi, and X. Wang, "DHS-CapsNet: Dual horizontal squash capsule networks for lung and colon cancer classification from whole slide histopathological images," *Int. J. Imag. Syst. Technol.*, vol. 31, no. 4, pp. 2075–2092, Mar. 2021.
[43] M. Ali and R. Ali, "Multi-input dual-stream capsule network for improved lung and colon cancer classification," *Diagnostics*, vol. 11, no. 8, Aug. 2021, Art. no. 1485.
[44] M. Masud, N. Sikder, A.-A. Nahid, A. K. Bairagi, and M. A. AlZain, "A machine learning approach to diagnosing lung and colon cancer using a deep learning-based classification framework," *Sensors*, vol. 21, no. 33, Jan. 2021, Art. no. 748.

Xin Liu received the master's degree in economics from Jilin University, Changchun, China, in 2012. She is currently working toward the Ph.D. degree in management science and engineering with the School of Economics and Management, Hebei University of Technology, Tianjin, China.

Her main research interests include intelligent computation, security and privacy protection, Big Data analytics with their applications to smart health care, and Internet of Things.

Jianwei Zhao received the master's degree in computer science and technology in 2018 from the Hebei University of Technology, Tianjin, China, where he is currently working toward the Ph.D. degree in control theory and control engineering with the School of Artificial Intelligence.

His main research interests include intelligent computation with its applications to cyber-physical system, Big Data, graphics and visual media, high performance computing, and cloud computing.

Jie Li received the Ph.D. degree in electrical engineering from the Hebei University of Technology, Tianjin, China, in 2002.

She is currently a Professor with the School of Economics and Management, Hebei University of Technology. Her research interests include Big Data analytics in smart health care, business, and finance.

Bin Cao (Member, IEEE) received the Ph.D. degree in computer application technology from Jilin University, Changchun, China, in 2012.

From 2012 to 2014, he was a Postdoc with the Department of Computer Science and Technology, Tsinghua University, Beijing, China. He is currently a Professor with the Hebei University of Technology, Tianjin, China. His research interests include intelligent computation with its applications to cyber-physical system, Big Data, graphics and visual media, high performance computing, and cloud computing.

Zhihan Lv (Senior Member, IEEE) received the Ph.D. degree in computer applied technology from the Ocean University of China, Qingdao, China, in 2012.

He is currently with Uppsala University, Uppsala, Sweden. He has completed several projects successfully on PC, website, smartphone, and smartglasses. His research interests include multimedia, Big Data analytics, computer vision, augmented reality, virtual reality, 3-D visualization, and graphics.