applied sciences

MDPI

Article

POMIC: Privacy-Preserving Outsourcing Medical Image Classification Based on Convolutional Neural Network to Cloud

Qing Yu[1], Hanlin Zhang [1,*], Hansong Xu [2] and Fanyu Kong [3]

[1] School of Computer Science and Technology, Qingdao University, Qingdao 266071, China
[2] Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[3] School of Software, Shandong University, Jinan 250100, China
* Correspondence: hanlin@qdu.edu.cn

Abstract: In the medical field, with the increasing number of medical images, medical image classification has become a hot spot. The convolutional neural network, a technology that can process more images and extract more accurate features with nonlinear models, has been widely used in this field. However, the classification process with model training with existing medical images needs a large number of samples, and the operation involves complex parameter computations, which puts forward higher requirements for users. Therefore, we propose a scheme for flexible privacy-preserving outsourcing medical image classification based on a convolutional neural network to the cloud. In this paper, three servers on the cloud platform can train the model with images from users, but they cannot obtain complete information on model parameters and user input. In practice, the scheme can not only reduce the computation and storage burdens on the user side but also ensure the security and efficiency of the system, which can be confirmed through the implementation of the experiment.

Keywords: cloud computing; secure outsourcing; privacy preservation; convolutional neural network; medical image classification

check for updates

Citation: Yu, Q.; Zhang, H.; Xu, H.; Kong, F. POMIC: Privacy-Preserving Outsourcing Medical Image Classification Based on Convolutional Neural Network to Cloud. *Appl. Sci.* **2023**, *13*, 3439. https://doi.org/10.3390/app13063439

Academic Editors: Jan Egger and Syoji Kobashi

Received: 20 December 2022
Revised: 23 February 2023
Accepted: 11 January 2023
Published: 8 March 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

In recent years, with the increasing complexity of medical images, it is difficult for radiologists and physicians to give an accurate diagnosis all the time. However, with the integration of various advanced computer technologies, such as artificial intelligence [1,2], Internet of Things [3], and cloud computing [4], medical image classification [5,6] is increasingly favored by researchers. Among them, the convolutional neural network, one of the core algorithms in image recognition, has an efficient and stable performance when performing medical image classification tasks [7,8].

For some users with limited computing resources (such as township clinics and community hospitals), it is difficult to train a model of a convolutional neural network with a large number of local medical records. Therefore, users prefer to upload medical data to the servers on the cloud platform [9]. Users can then obtain the classification results of medical images. However, it may raise some critical privacy issues that hinder the deployment of the envisioned service. The users' input contains sensitive personal health information which cannot be disclosed to the cloud in plaintext. At the same time, the model is considered intellectual property and embedded with trace data of (sensitive) training data. Therefore, how to protect the privacy of the input and the model becomes an issue.

The existing privacy-preserving schemes for the convolutional neural network are mainly based on homomorphic encryption [10] or differential privacy [11]. From a practical point of view, homomorphic encryption schemes [12] are limited to evaluating low-order polynomials on encrypted data. Otherwise, the computation of the encryption process is too large. The method of differential privacy is to add random noises to the data, which may lead to a decline in the availability of the data.

1.1. Related Work

In this section, we introduce some relevant knowledge of medical image classification, privacy-preserving outsourcing convolutional neural network to the cloud.

1.1.1. Medical Image Classification

Medical image classification, a subject integrating medical image technology and computer technology, has become a vital tool and technical means for medical research [13–15], disease diagnosis, and treatment. Recently, medical image classification based on deep learning [16] has become a hot research focus in the field of medical image research.

Arevalo et al. in [17] proposed an innovative representation learning framework for breast cancer diagnosis in mammography, which integrates deep learning technology to automatically identify features with the developed breast cancer benchmark dataset. The experimental results show that the proposed method has significantly improved the performance of the classification. Sun et al. in [18] developed a graph-based semi-supervised learning (SSL) scheme using a deep convolutional neural network (CNN) for breast cancer diagnosis. The accuracy was 0.8243 with mixed labeled and unlabeled data. Gao et al. in [19] extended the latest technology of CNN to help clinicians diagnose heart disease. It maintained the classification results of the eight view categories of echo video with 92.1% accuracy, while only a single spatial CNN network was used to achieve 89.5%. Jeyaraj et al. in [20] presented a new partition CNN structure, which had two partition layers to label regions of interest in multidimensional hyperspectral images and classify them. They obtained a classification accuracy of 91.4% with a sensitivity of 0.94 and a specificity of 0.91 for 100 image data sets training. For task classification of a cancerous tumor, normal tissue accuracy of 94.5% for 500 training patterns were obtained. Xu et al. in [21] proposed PPFDL, which is a joint privacy-preserving deep learning framework. Specifically, they designed a new solution to reduce the negative impact of irregular users on training accuracy. At the same time, Yao's garbled code circuit and homomorphic cryptosystem are used to ensure the confidentiality of all user-related information. A lot of experiments have proved its excellent performance in training accuracy, computation, and communication overhead.

In real life, for hospitals and clinics with limited computing resources, it is difficult to train and classify medical images on the local side. Therefore, based on the above work, we have achieved the outsourcing of the medical image classification task to the cloud service platform so as to reduce the computing burden at the local level and improve the efficiency of the task with high accuracy. The above CNN applications in medical image classification are summarized in Table 1.

Table 1. A summary of CNN applications in medical image classifcation.

References	Architecture	Dataset	Performance Metric	Computation Burden	Security
Arevalo et al. [17]	(Conv, ReLU, maxpool) × 2 + FC	Breast cancer benchmarking dataset	AUC 82.2%	Local side	✗
Sun et al. [18]	(Conv, maxpool) × 3, FC	Breast cancer benchmarking dataset	Accuracy 82.43%, AUC 88.18%	Local side	✗
Gao et al. [19]	Two path CNN of seven layers (conv, ReLU, maxpool) × 2, (conv, ReLU) × 2, (conv, ReLU, maxpool), (conv, dropout) × 2	Tsinghua University Hospital, Beijing and Fuzhou University Hospital, China	Accuracy 92.1%	Local side	✗
Jeyaraj et al. [20]	(Conv, ReLU, maxpool) × 2, FC	oral cancer in HSI image	Accuracy 91.4%	Local side	✗
Our scheme	(Conv, ReLU), (Conv, ReLU, maxpool) × 3, dropout, FC	Breast cancer benchmarking dataset	Accuracy 77.48%	Cloud servers	✓

1.1.2. Privacy-Preserving Outsourcing Convolutional Neural Network to Cloud

Outsourcing technology hands over the complex computation to the cloud so as to realize the rational allocation of resources and reduce the computing and storage burden on the local side. However, data and model information outsourced to the cloud may contain sensitive information. How to achieve privacy protection of sensitive information is a problem that is worth studying.

Li et al. in [22] proposed a CNN prediction scheme, which protects privacy in the outsourcing environment; that is, the model hosting server cannot learn results and models. By using two noncommunication servers with secret sharing and triplet generation and minimizing the use of heavyweight passwords, overall latency and accuracy are optimized. Zheng et al. in [23] proposed a secure cloud-based image service framework that allows privacy-preserving and effective image denoising in the cloud to generate high-quality images. It also shows how to make use of encryption technologies to support DNN image-de noising services. The security design can achieve the same denoising quality as plaintext with high efficiency locally and affordable cost in the cloud. Liu et al. in [24] present and evaluate a lightweight secure outsourcing neural network inference computation scheme, Sonic. It fully outsources the secure inference service to the cloud, freeing end devices and model owners from real-time online. A series of secure and effective function protocols using lightweight cryptography primitives are designed in Sonic to protect user input and model privacy in the whole inference service. A large number of evaluations show that sonic is more efficient than the existing technology in online phrases.

The above scheme uses garbled circuits (GC) and homomorphic encryption technologies [25] to realize outsourcing deep neural network models. However, they may bring a heavy computation burden. Therefore, we propose a lightweight cryptography privacy-preserving scheme with secret sharing to send the convolutional neural network model to the third-party cloud platform, which can save the computing resource [26] of users and servers. The comparison of different privacy-preserving outsourcing convolutional neural network schemes is shown in Table 2.

Table 2. The comparison of different privacy-preserving outsourcing convolutional neural network schemes.

Scheme	Security	Technology	Model	Domain	Efficiency
Zheng et al. [23]	Semi-honest and non-colluding	Yao's Garbled Circuits (GC)	Two parties	$\mathbb{Z}_{2^l}$	Medium
Li et al. [22]	Honest-but-curious and non-colluding	Homomorphic Encryption (HE) and Secret Sharing (SS)	Two parties	$\mathbb{Z}_{2^l}$	High
Liu et al. [24]	Semi-honest and non-colluding	Additive secret sharing (ASS)	Two parties	$\mathbb{Z}_{2^l}$	High
Our scheme	Semi-honest and non-colluding	Replicated Secret Sharing (RSS)	Three parties	$\mathbb{Z}_{2^l}$	High

1.2. Contribution

In this work, we propose a privacy-preserving outsourcing scheme of medical image classification based on a convolutional neural network to the cloud. It can reduce the computing burden of users by sending their medical images to the cloud service platform built with three servers. With lightweight cryptographic encryption technologies, the privacy of the input and the model can be protected. Our contribution can be summarized as follows:

- It achieves outsourcing medical image classification based on a convolutional neural network. Users can get the result of a medical image with a lower computing burden;
- For different protocol blocks in medical image classification based on a convolutional neural network, we provide privacy-preserving schemes utilizing lightweight cryptography primitives-secret sharing, which can not only ensure security but also improve the efficiency of service;

- A pathological section staining experiment with good accuracy is carried out, which proves the efficiency and security of the scheme in practice.

The rest of the paper is organized as follows. Section 2 introduces some preliminary knowledge. Section 3 describes the system model and threat model. Section 4 introduces some building blocks of privacy-preserving outsourcing schemes for medical image classification based on convolutional neural networks. Section 5 describes the detailed scheme. Section 6 introduces the experimental configuration and analyzes the practical experimental performance, and shows the experimental results. Finally, Section 7 draws a conclusion of the paper and introduces the future application of our scheme.

2. Preliminaries

In this section, we introduce some basic knowledge of a convolutional neural network and some cryptographic primitives.

2.1. Medical Image Classification

Medical image classification [27], a subject integrating medical image technology and computer technology, has become a vital tool and technical means for medical research, disease diagnosis, and treatment. Therefore, biomedical imaging plays an important role in medical disease diagnosis and treatment. There are several common medical imaging technologies, magnetic resonance imaging (MRI), positron emission tomography (PET) [28], computed tomography (CT), cone beam CT, and three-dimensional ultrasound imaging.

In recent years, with continuous improvement of computer technology and deep learning (DL), the convolutional neural network (CNN) has rapidly developed into a research hotspot of medical image analysis and classification. It is a machine learning model with multi hidden-layers that can learn more detailed characteristics and make more accurate classifications and predictions. With the deep learning method of artificial intelligence, finding methods for screening, diagnosis, and efficacy classification to process large-scale medical images is currently a major scientific issue and frontier research focus in the field of medical image analysis.

2.2. Convolutional Neural Network

As a typical algorithm of deep learning [29,30], a convolutional neural network (CNN) overcomes the disadvantages of a fully connected neural network, with more parameters and fewer layers. Furthermore, it can make full use of the connections between pixels to obtain important features. The CNN starts with the input layer, which corresponds to the pixels of the input picture, and ends with the probability value of the classification corresponding to the input picture. Its structure is composed of four common gadgets. The building blocks of a CNN are shown in Figure 1.

Convolution layer: Convolution layer can help to extract the features of the feeding layer. Learnable filter sets are the core of this layer, they are part of the parameters that make up the model. The computation in this layer is essentially a dot product of the weight vector and input vector of the feeding layer. The activation layer introduces nonlinear factors to neurons by using various activation functions, which can make the neural network approach any nonlinear function arbitrarily. Therefore, the neural network can be applied to many nonlinear systems. There are many activation functions, such as the Sigmoid function, Tanh function, Rectified Linear Unit (ReLU) function, etc. Among them, ReLU is the most popular activation function used in neural networks. Compared with sigmoid and tanh, the derivative of ReLU is easy to obtain, which means that the computation is simpler in the process of updating parameters with back-propagation. When the value is too large or too small, the derivative of sigmoid and tanh is close to 0, while ReLU can prevent the gradient from disappearing. Finally, the part less than 0 is 0, and the value greater than 0 is equal to itself, it can prevent over-fitting.

Pooling layer: A pooling layer is usually periodically inserted between successive convolution layers. The pooling layer aims to gradually reduce the spatial size of data so as

to reduce the number of parameters, which is conducive to reducing computing resources and controlling overfitting effectively. The average pooling layer and max-pooling layer are two common types of pooling layer functions. Between them, the max-pooling function is more widely used.

Fully connected layer: Fully connected layers (FC) play the role of "Classifier" in the whole convolutional neural network. The core operation of the fully connected layer is the matrix-vector product.

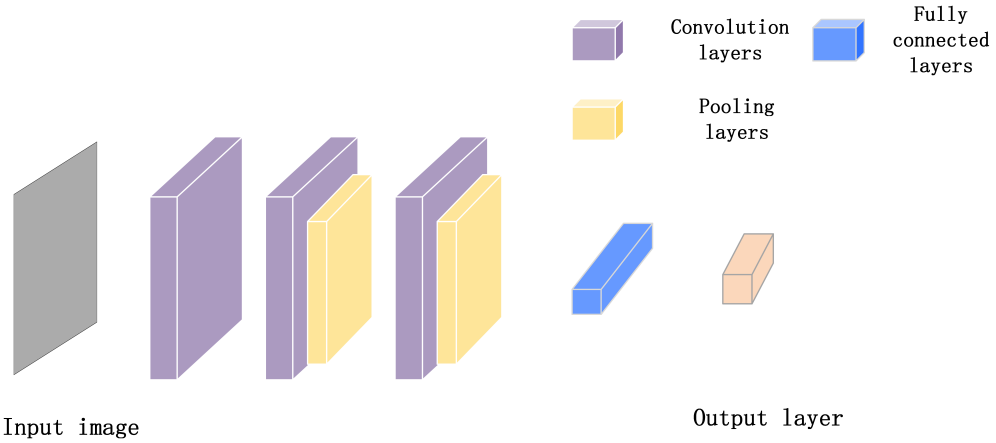


Figure 1. Building blocks of a CNN.

2.3. Secure Multi-Party Computation

Secure Multi-party Computation (MPC) is a term for a broad range of cryptographic techniques and protocols, which can enable a set of parties $P_1, ..., P_n$ to compute the function f with their private inputs $x_1, ..., x_n$ without anything beyond the output $f(x_1, ..., x_n)$ of the computation. Importantly, an actively misbehaving participant should not be able to bias the outcome of the computation (except by choosing their input) or learn anything about the inputs of the honest parties (except for what is leaked by the output itself). With the progress of technology and network equipment, MPC has become a practical science from a purely theoretical research field. More and more companies and researchers focus on this topic.

3. System Overview

In this section, we present the system model for the scheme and describe the threat model.

3.1. System Model

In this work, we provide a privacy-preserving outsourcing scheme for medical image classification based on a convolutional neural network in a three-server model. We model the problem as follows: In the so-called client-server scenario [31], the clients U_0 and U_1 (healthcare providers) want to execute medical image classification tasks with the help of a cloud platform. It can input data to the three servers P_0, P_1, and P_2 through secret sharing. The servers collectively run an interactive medical image classification task built on the framework of a convolutional neural network. In this process, the security requirement is that one server cannot learn any information about the others. In addition, the input and output are private from the servers. The detailed model architecture is shown in Figure 2.

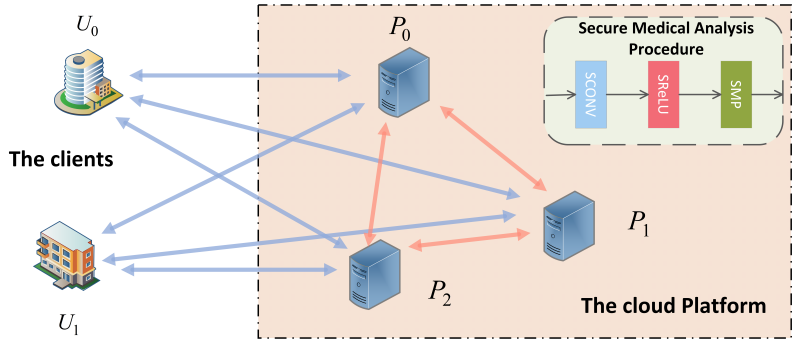


Figure 2. System Model.

3.2. Threat Model

We focus on the model of three-party servers with an honest majority, which has been used in different real-world applications [32]. In this system, two servers are expected to behave honestly, i.e., it means that they follow the protocol and keep the contents of the agreement strictly confidential, one party is expected to follow the protocol but might try to extract information. The major advantage of the honest majority setting is that protocols can be obtained only with light-weight arithmetic operations to provide securely outsourced computation and achieve information-theoretic security. However, the architecture information of the model, such as the size and number of layers of the weight, cannot be hidden.

4. Building Blocks

This section gives the building blocks for our privacy-preserving outsourcing medical image classification scheme.

4.1. Replicated Secret Sharing Technique

The 2-out-of-3 replicated secret sharing (RSS) was proposed by Araki et al [33] with high throughput and low latency. Let l be a general modulus, the method can work for arithmetic circuits over the ring modulo 2^l and Boolean circuits with $l = 1$. $\langle \cdot \rangle_i$ represents arithmetic sharing obtained by server P_i. $[\![\cdot]\!]_i$ represents boolean sharing in $\mathbb{Z}_2$ obtained by server P_i. The replicated secret sharing for three parties is described as follows:

- $\langle x \rangle \leftarrow share(x)$: For the secret value $x \in \mathbb{Z}_{2^l}$, the protocol samples three random values x_1, x_2, x_3 under the constraint that $x \equiv x_1 + x_2 + x_3 \bmod 2^l$. Each participant owns a portion. P_i $i \in 0, 1, 2$ gets (x_i, x_{i+1}). And it can be written as $\langle x \rangle := (x_1, x_2, x_3)$.
- $x \leftarrow reconstruct(\langle x \rangle)$: To reconstruct and reveal x, P_i sends x_i to P_{i+1}, each party can compute sum of $x_1, x_2, x_3 \in \mathbb{Z}_{2^l}$ locally, which means the secret value x is revealed to each party.

We also describe the addition and multiplication operations as follows:

The addition and subtraction operations between two shares can be computed locally with their linearity properties, which means we can get secret values $\langle x + y \rangle$ with two shares $\langle x \rangle = (x_1, x_2, x_3)$, $\langle y \rangle = (y_1, y_2, y_3)$. The secret value $(\langle x \rangle + c)$ is summed with the constant value c, it can obtain with $(\langle x \rangle + c := (x_1 + c, x_2), (x_2, x_3), (x_3, x_1 + c))$. Similarly, $\langle ax \pm by \pm c \rangle$ can be computed as $(ax_1 \pm by_1 \pm c, ax_2 \pm by_2, ax_3 \pm by_3)$ on the local side.

For the operation of multiplying two secret values $\langle xy \rangle$, P_1, P_2, P_3 first hold correlated randomness α, β, γ, respectively, whose detailed generation process can be seen in [33]. The correlate randomness meets $\alpha + \beta + \gamma = 0$. P_0 computes $z_0 = x_0y_0 + x_0y_1 + x_1y_0 + \alpha$ and sends it to P_1; P_1 computes $z_1 = x_1y_1 + x_1y_2 + x_2y_1 + \beta$ and sends it to P_2; P_2 computes $z_2 = x_2y_2 + x_2y_0 + x_0y_2 + \gamma$ and sends z_2 to P_1. The resharing process is performed for 2-out-of-3 sharing. P_i then sends z_i to P_{i+1}.

The protocol has very low communication: addition operation can be computed locally. For each multiplication gate, although parties need to interact to complete, RSS reduces half of the communication overhead compared with traditional ASS in the 3PC setting.

Note that decimals in the computation are unavoidable in the computation of a privacy-preserving outsourcing convolutional neural network, the truncation of the decimal fraction is necessary while secret sharing works on the integer values. The real data in the whole process of a neural network is rounded and scaled into $\mathbb{Z}_{2^l}$. For the real number x, y, assuming that the number of decimal places is q when the real numbers are multiplied, the length of the decimal part of the result is $2q$, which will exceed the length of l bits. We simply truncate the last q bits to ensure the numerical representation of length. This process will inevitably cause accuracy loss, but it is proven that the accuracy loss is within the reasonable range. The truncation technique of the decimal fraction is also introduced in [24].

4.2. Secure Comparison Protocol

In our scheme, the comparison operation is converted to binary sharing from arithmetic sharing to improve efficiency. As is introduced in [34], for the l-bit real number represented with binary stored in the computer, the sign of the number can be judged by getting the highest bit through computing the most significant bit MSB$(\cdot)$. When the highest bit is 1, which means that the number is negative, the lower $l-1$ bit represents the complement of the number. The highest bit is 0, which indicates that the number is positive. At this time, the lower $l-1$ bit represents the value of the number.

The most significant bit (MSB) denotes the sign of a ring element, which implies that the comparison operation can be converted into the MSB extraction of the difference between the two operands. Let $a = (x - y)$, then we can be computed comparisons b by extracting the most significant bit of a with $b = \text{MSB}(a)$. Because of $\langle a \rangle := (a_1, a_2, a_3)$ and $a \equiv a_1 + a_2 + a_3 \bmod 2^l$, b can be obtained by computing $b = \text{MSB}\ (a) = \text{MSB}\ (a_1) \oplus \text{MSB}\ (a_2) \oplus \text{MSB}\ (a_3) \oplus c$, where $c \in \{0, 1\}$ is a carry bit from $(l-2)$-th index. If $2^{l-1} \leq a_1 + a_2 + a_3 \leq 2^l$, the value of c is 1. Otherwise, $c = 0$.

To convert the arithmetic share into a binary sharing, $2l$ AND gates are needed for $\mathcal{O}(logl)$ rounds. For more details on the conversions of arithmetic and binary secret sharing, please refer to [35].

The secure comparison protocol is described in Algorithm 1.

Algorithm 1 SecureComparison $\Pi_{SC}\{P_0, P_1, P_2\}$

Require: The parties P_0, P_1, P_2 hold the arithmetic shares of x and y, $\langle x \rangle$ and $\langle y \rangle$ over $\mathbb{Z}_{2^l}$.

Ensure: The parties get the boolean share of bit $b = (x \overset{?}{<} y)$.

1: The parties compute the shares of a at local side, where $a = x - y$.
2: The parties compute the boolean share of bit c, where $c = a_1 + a_2 + a_3 \overset{?}{\geq} 2^{l-1}$.
3: The parties locally compute the boolean share of bit b, where $b = \text{MSB}\ (a_1) \oplus \text{MSB}\ (a_2) \oplus \text{MSB}\ (a_3) \oplus c$.
4: The parties output $[\![b]\!]$.

4.3. Division

In our privacy-preserving outsourcing medical image classification scheme, we implement division with a numerical method instead of invoking division using a garbled circuit protocol, which is one of the most common techniques for constructing a secure protocol based on secret sharing because of its efficiency. We also use the algorithm proposed by Goldschmid to implement division [36], which approximates the desired operation as a series of multiplications.

We define secure division protocol as follows:

Given secret shared value $\langle x \rangle$ and $\langle y \rangle$ with $y \in \mathbb{Z}^+$, the parties compute the share $\langle a \rangle$, such that $a = x/y$.

$$a = \frac{x}{y} = \frac{xw_0 ... w_{i-1}}{yw_0 ... w_{i-1}} \tag{1}$$

We define w_0 to be an initial approximation of $1/y$ with relative error $\varepsilon < 1$, and $x_0 = x$, $y_0 = y$, $x_i = x_{i-1}w_{i-1}$, $y_i = y_{i-1}w_{i-1}$, $w_i = 2 - y_i$. The relative error of the initial approximation can be updated as $\varepsilon = 1 - y_0 w_0 = 1 - y_1$. We can derivation $y_i = y_{i-1}w_{i-1} = y_{i-1}(2 - y_{i-1}) = 1 - (1 - y_{i-1})^2$. Therefore, $1 - y_i = (1 - y_{i-1})^2 = (1 - y_1)^{2^{i-1}} = \varepsilon^{2^{i-1}}$. If $\varepsilon < 1$ and y_i converges to 1, it can be concluded that x_i converges to the quotient a.

And we can refer to [37] for the details of the initial approximation in the algorithm.

5. Privacy-Preserving Outsourcing Medical Image Classification Based on Convolutional Neural Network

In this section, we introduce our proposed scheme for privacy-preserving outsourcing medical image classification to the cloud with the three-party model. In this process, the sensitive information in input and model can be protected with lightweight privacy-preserving protocols.

5.1. Linear Operations

In a convolutional neural network, matrix multiplication is the core operation. The forward and backward computation for both dense layers and convolutional layers are implemented as matrix multiplication, which in turn is based on dot products. Their output z_j can be computed through the formula

$$z_j = \sum_{k=1}^{n} w_k \cdot x_k + bias, j = 1, 2, ..., m \tag{2}$$

where m is the node number of output, n represents the size of the convolution kernel in the convolution operation, and the node number of input in a fully connected layer, w_k, x_k represents the kth values of weight and corresponding input while *bias* is the offset of the corresponding convolution kernel region or node, and the description of relevant formulas can be seen in [38].

Secure linear layers is a function that realizes secure computation of the linear computation described as Equation (1) [39]. It inputs secret shares of the vector $\langle x \rangle_i$ and weight vector $\langle w \rangle_i$ from the input layer or pooling layer and outputs the secret shares of result $\langle z_j \rangle_i$ for the subsequent computation of activation functions. Our scheme simply used replicated secret-sharing technology. The multiplication computing process of secure linear layers between the three servers P_0, P_1, P_2 is in Algorithm 2.

Algorithm 2 SecureLinear $\Pi_{SL}\{P_0, P_1, P_2\}$

Require: P_0 holds ($\langle x \rangle_0$,$\langle w \rangle_0$); P_1 holds ($\langle x \rangle_1$,$\langle w \rangle_1$), P_2 holds ($\langle x \rangle_2$,$\langle w \rangle_2$) resp. $r_{i,i+1}$ is generated with a pseudo-random generator using a key pre-shared between P_i and P_{i+1}.

Ensure: P_0, P_1,P_2 get $\langle x \cdot w \rangle_i$ ($i \in \{0, 1, 2\}$) resp.

1: P_i sends its sharing ($\langle x \rangle_i$, $\langle w \rangle_i$) to P_{i+1}. (If $i = 2, i + 1 = 0$) Therefore, P_0 has the pairs ($\langle x \rangle_0$, $\langle x \rangle_3$) and ($\langle w \rangle_0$, $\langle w \rangle_3$), P_1 has the pairs ($\langle x \rangle_0$, $\langle x \rangle_1$) and ($\langle w \rangle_0$, $\langle w \rangle_1$), P_2 has the pairs ($\langle x \rangle_1$, $\langle x \rangle_2$) and ($\langle w \rangle_1$, $\langle w \rangle_2$).

2: P_i computes $x_i \cdot w_i + x_i \cdot w_{i+1} + x_{i+1} \cdot w_i$ locally, which means P_0 obtains $x_0 \cdot w_0 + x_0 \cdot w_2 + x_2 \cdot w_0$, P_1 obtains $x_1 \cdot w_1 + x_0 \cdot w_1 + x_1 \cdot w_0$, P_2 obtains $x_2 \cdot w_2 + x_1 \cdot w_2 + x_2 \cdot w_1$.

3: P_i can obtain $\langle x \cdot w \rangle_i = x_i \cdot w_i + x_{i-1} \cdot w_i + x_i \cdot w_{i-1} + r_{i,i+1} - r_{i,i-1}$ with $x \cdot w = (x_0 + x_1 + x_2)(w_0 + w_1 + w_2) = (x_0 \cdot w_0 + x_0 \cdot w_2 + x_2 \cdot w_0) + (x_1 \cdot y_0 + x_0 \cdot y_1 + x_1 \cdot y_1) + (x_2 \cdot w_2 + x_2 \cdot w_1 + x_1 \cdot w_2) + r_{0,1} - r_{0,2} + r_{1,2} - r_{1,0} + r_{1,0} + r_{2,0} - r_{2,1}$

In practical experiments, we use a dedicated infrastructure that computes all dot products for matrix multiplication in a single batch of communication to reduce the number of communication rounds.

5.2. Nonlinear Operation

Both rectified linear unit (ReLU) and max-pooling are regarded as non-linear operations that are based on comparison followed by oblivious selection.

Rectified linear unit (ReLU) : The ReLU is a nonlinear function that can be expressed by $\mathrm{ReLU}(x) = max(0, x)$. And the result z of $\mathrm{ReLU}(x)$ can be obtained by simply computing

$$z = max(0, x) \rightarrow (x > 0) \cdot x. \tag{3}$$

Secure ReLU function aims to compute nonlinear activation function $\mathrm{ReLU}(x)$ securely. It inputs the secret shares of input value $\langle x \rangle$ from the convolution layer or full connection layer and outputs the secret shares of results $\langle z \rangle$; we can refer to [13] for a detailed description.

$$z = [\![x > 0]\!] \cdot \langle x \rangle \rightarrow \neg MSB(x) \cdot \langle x \rangle. \tag{4}$$

According to Equation (4), the secure ReLU function includes two parts, secure $\mathrm{MSB}(\cdot)$ operation, and secure multiplication operation. Among them, secure $\mathrm{MSB}(\cdot)$ operation uses the arithmetic secret shares $\langle x \rangle$ as input and outputs the Boolean secret shares of the highest bit $[\![a_{l-1}]\!]$. Suppose there is a l-bit secret value x, $\langle x \rangle_0^A$, $\langle x \rangle_1^A$ are secret shares of it. Let $x = x_{l-1}, ..., x_0$, $a = a_{l-1}, ..., a_0$, $b = b_{l-1}, ..., b_0$ and $c = c_{l-1}, ..., c_0$ denote x, $\langle x \rangle_0^A$, $\langle x \rangle_1^A$ and $\langle x \rangle_2^A$ with their corresponding bit strings respectively, and they meet $x = a + b + c \ (mod\ 2^l)$. The difference between the sum $(+)$ of bit strings of a, b and the bitwise-XOR $(\oplus)$ of the bit strings of a, b is equal to the carry bits $c_{l-1}, ..., c_0$, Then, $\mathrm{MSB}(x)$ can be obtained by computing $x_{l-1} = c_{l-1} + a_{l-1} + b_{l-1}$, and s converted to compute the carry c_{l-1} via an l-bit full adder.

The computation process of the secure ReLU function between the two servers P_0, P_1, P_2 is as shown in Algorithm 3.

Algorithm 3 SecureReLU $\Pi_{SR}\{P_0, P_1, P_2\}$

Require: P_0, P_1 and P_2 hold $\langle x \rangle_0$, $\langle x \rangle_1$ and $\langle x \rangle_2$, respectively.
Ensure: P_0, P_1 and P_2 get $\langle z \rangle_0 = \langle \mathrm{ReLU}(x) \rangle_0$, $\langle z \rangle_1 = \langle \mathrm{ReLU}(x) \rangle_1$ and $\langle z \rangle_2 = \langle \mathrm{ReLU}(x) \rangle_2$.
1: P_0 , P_1 and P_2 get $[\![a_{l-1}]\!]$ by run secure $\mathrm{MSB}(x)$.
2: P_i set $[\![\bar{a}_{l-1}]\!] = [\![a_{l-1}]\!] + i$ to get NOT $\mathrm{MSB}(x)$.
3: P_i changes boolean sharing $[\![\bar{a}_{l-1}]\!]$ to arithmetic shares $\langle \bar{a}_{l-1} \rangle$ using the term mixed-circuit computation for any technique that works over both computation domains [40].
4: S_0 and S_1 compute $\langle z \rangle = \langle \bar{a}_{l-1} \rangle \cdot \langle x \rangle$ according to the SecureLinear algorithm mentioned above.

Secure Max Pooling Layer: The max pooling layer reduces the spatial size of the data by selecting the max value in the window. Therefore, we can obtain the max value by comparing the larger of the two numbers many times.

The Secure Max Pooling Layer inputs a set of secret shares $\langle x_1 \rangle, \langle x_2 \rangle, ..., \langle x_{N_{max}} \rangle$ and outputs the secret shares of results $\langle z \rangle$.

$$max(a_1, a_2) = a_1 + b \cdot (a_2 - a_1) \tag{5}$$

where $b = \mathrm{MSB}(a_1 - a_2)$.

According to Equation (5), secure max pooling layer involves *secure* $\mathrm{MSB}(\cdot)$ *operation* and secure multiplication operation.

The computing process of the secure max pooling layer between the two servers P_0, P_1, P_2 is shown in Algorithm 4.

Algorithm 4 SecureMaxPooling $\Pi_{SMP}\{P_0, P_1, P_2\}$

Require: P_0, P_1 and P_2 hold the secret shares of input features within the pooling window $\langle x_1\rangle_0, ..., \langle x_{N_{max}}\rangle_0$ and $\langle x_1\rangle_1, ..., \langle x_{N_{max}}\rangle_1$ respectively.
Ensure: P_0, P_1 and P_2 obtain $\langle z\rangle_0 = \langle max(x_1, ..., x_{N_{max}})\rangle_0$, $\langle z\rangle_1 = \langle max(x_1, ..., x_{N_{max}})\rangle_1$ and $\langle z\rangle_2 = \langle max(x_1, ..., x_{N_{max}})\rangle_2$.
1: **For** each k from 1 to N_{max} **do**
2: P_i sets $\langle a_1\rangle_i = \langle x_k\rangle_i$, $\langle a_2\rangle_i = \langle x_{k+1}\rangle_i$.
3: P_0 , P_1 and P_1 compute secure MSB$(\langle a_1\rangle - \langle a_2\rangle)$ to get the comparison bit $[\![a_{l-1}]\!]$.
4: P_i changes boolean sharing$[\![\bar{a}_{l-1}]\!]$ to arithmetic shares $\langle \bar{a}_{l-1}\rangle$, it means P_i get $\langle b\rangle$.
5: P_0 , P_1 and P_1 set $\langle v\rangle = (i - \langle b\rangle) \cdot \langle a_1\rangle + \langle b\rangle \cdot \langle a_2\rangle$. P_i sets $\langle x_{k+1}\rangle_i = \langle v\rangle_i$.
6: **EndFor**
7: P_i output $\langle z\rangle_i = \langle max(x_1, ..., x_{N_{max}})\rangle_i = \langle x_{N_{max}}\rangle_i$.

For two-dimensional max pooling over a window, it needs to perform three comparison operations in order to obtain the max value. To reduce the time cost, it can be obtained by computing the maximum of two pairs of values followed by the maximum of the two results.

5.3. Complexity Analysis

When computing a privacy-preserving outsourcing medical image classification based on a convolutional neural network, we should consider the full process of training and inference since back-propagation is used in training, which mainly includes division. In our work, the division operation is achieved with the Goldschmidt method, which computes multiplications. Assuming the number of parameter nodes of the convolution layer and full connection layer is n_1 and n_2, therefore, the communication complexity of the training is $\mathcal{O}(n_1 + n_2)$ bit. In the process of inference, each round contains a series of time-consuming multiplication operations, which amount to $\mathcal{O}(n_1 + n_2)$ bit, the communication complexity of $\mathcal{O}(n_1 + n_2)$. As for the m comparison operations in max-pooling layer and Relu function, the round complexity of them are $\mathcal{O}(mlogl)$ and $\mathcal{O}(mlogl)$. For linear operation, suppose the stride is 1, the number of padding p, and the sizes of input tensor, kernel, and output tensor of the secure convolutional layer are $c_1 \times n_1 \times n_1$, $c_1 \times c_2 \times n \times n$ and $c_2 \times n_2 \times n_2$ respectively; and the sizes of the input vector and output vector of the fully-connected layer are c_1, c_2 respectively. As defined, the bit length of an additive secret share is l, and the max pooling window size is s (e.g., $s = 4$ if the pooling window is 2×2), and Table 3 shows the detailed communication complexity analysis.

Table 3. Communication Complexity Analysis of Secure.

Secure Function	Communication	Round Complexity
SReLU	$30l - 24$	$logl + 2$
SMP	$(n-1)(36l - 24)$	$(n-1)(logl + 2)$
SD	$k[6lnc_1c_2(n_1 - n + p + 1)^2 + 4lnc_1c_2]$	k
SCONV	$6lnc_1c_2(n_1 - n + p + 1)^2$	$2nc_2(n_1 - n + p + 1)$
SFC	$4lnc_1c_2$	c_2n

6. Experimental Setup and Results

6.1. Experimental Setup

We run our benchmarks on a commodity desktop equipped with Intel (R) Core i7-11700K CPU @ 3.60GHz × 4 running Ubuntu 20.04 on a VMware Workstation allocated with 16 GB memory. The samples are trained and tested with a latency of 88.5 ms and a bandwidth of 220 Mbps. We build our implementation on the MP-SPDZ [41]. MP-SPDZ

is a high-level library, which not only implements a series of MPC protocols, but also contains building blocks. We write code with Python and compile it into specific bytes. This code can be executed by the virtual machine to form the actual secure computing. This process allows optimization in the MPC context. The framework also has clear and precise computations that can be performed securely. This allows us to lower the cost in the next part. As for the public parameters, we set bit-length $l = 64$, fixed-point precision $q = 13$.

Accurate identification and classification of breast cancer subtypes is an important clinical task. The evaluation of invasive breast cancer can be conducted from three aspects: the proportion of glandular tube formation, nuclear polymorphism, and mitotic count. The traditional method, judging by the naked eye, may make mistakes with lower efficiency. Therefore, according to our proposed scheme, we carried out the inference experiment on breast cancer. The three servers on the cloud platform trained the samples preprocessed on the local sides to obtain the model, which could be used to infer images from multiple users.

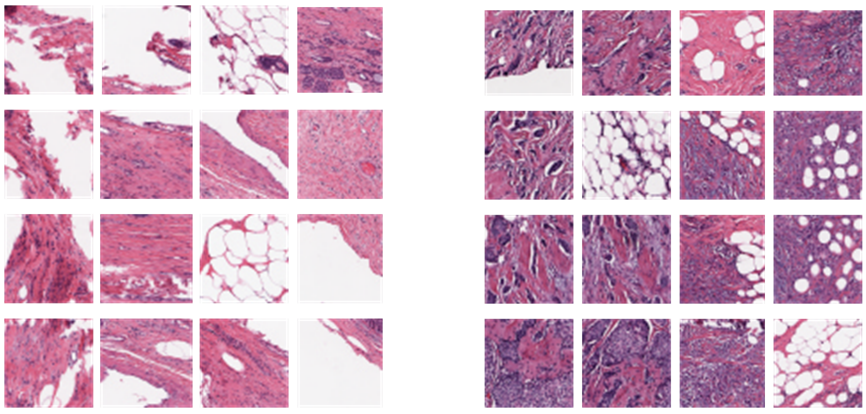
As for the hyperparameter settings in the training processing, it is given in Table 4.

Table 4. Hyperparameter Settings.

Parameters	Value
Number of epochs	15 epochs
Early stop	No
Mini-batch size	The size of 128
Reshuffling training samples	Fisher-Yates shuffle with MP-SPDZ's internal pseudo-random number generator as randomness source
Learning rate	0.01 for SGD
Learning rate decay/schedule	No
Random initialization	Independent random initialization by design

Samples : As for the dataset in our experiment, it consists of normal breast cells and breast cancer (BCa) specimens at 40×, which is shown in Figure 3. Each image is preprocessed to the size of 50×50 on the local sides. And we get different results by changing the number of images in different experiments.

Model: The convolutional neural network model is generally composed of 4 *Conv2D* layers, 3 *MaxPooling2D* layers, and 1 *Dense* layer. The model structure is obtained with previous work and experiments debugging parameters. The detailed structure is shown in Figure 4 below, which is formatted in Keras.



(a) The normal breast specimens (b) The cancer breast specimens

Figure 3. The experimental samples for classification.

```
♯ 1st Convolutional Layer
tf.keras.layers.Conv2D(16, 3, 1, 'same', activation='relu'),

♯2nd Convolutional Layer
tf.keras.layers.Conv2D(16, 3, 1, 'same', activation='relu'),
tf.keras.layers.MaxPooling2D(2),

♯3rd Convolutional Layer
tf.keras.layers.Conv2D(16, 3, 1, 'same', activation='relu'),
tf.keras.layers.MaxPooling2D(2),

♯4th Convolutional Layer
tf.keras.layers.Conv2D(16, 3, 1, 'same', activation='relu'),
tf.keras.layers.MaxPooling2D(2),

tf.keras.layers.Dropout(0.5),
tf.keras.layers.Flatten(),

♯Fully Connected Layer
tf.keras.layers.Dense(2, activation='softmax')
```

Figure 4. The CNN model used in the experiment.

The workflow of our privacy-preserving outsourcing medical image classification is shown in Figure 5.

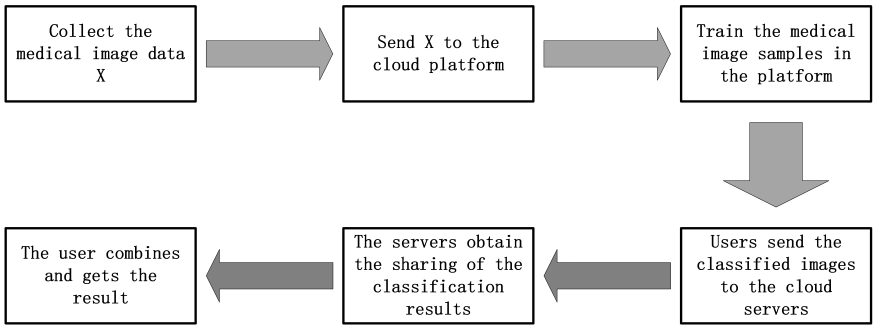


Figure 5. The workflow of our privacy-preserving outsourcing medical image classification.

6.2. Experimental Results

Figure 6 shows the comparison of training accuracy between the method of computing in plaintext on the local side and our privacy-preserving outsourcing scheme. We select 15 epochs as a sample with obvious fluctuations. The training acc of the direct method in plaintext on the local side is 0.5751, 0.7273, 0.7566, 0.7598, 0.7658, 0.7757, 0.7861, 0.7951, 0.7977, 0.7958, 0.8001, 0.7961, 0.7951, 0.7979, and 0.7977. The training acc of privacy-preserving outsourcing scheme is 0.684966, 0.750844, 0.75475, 0.769214, 0.769214, 0.771536, 0.772698, 0.778715, 0.772381, 0.773753, 0.778351, 0.780012, 0.774281, 0.785893, and 0.782164. Our MPC implementation has gained similar training acc performance compared with the cleartext counterpart. Among them, the training accuracy of privacy-preserving outsourcing can reach 0.773753.

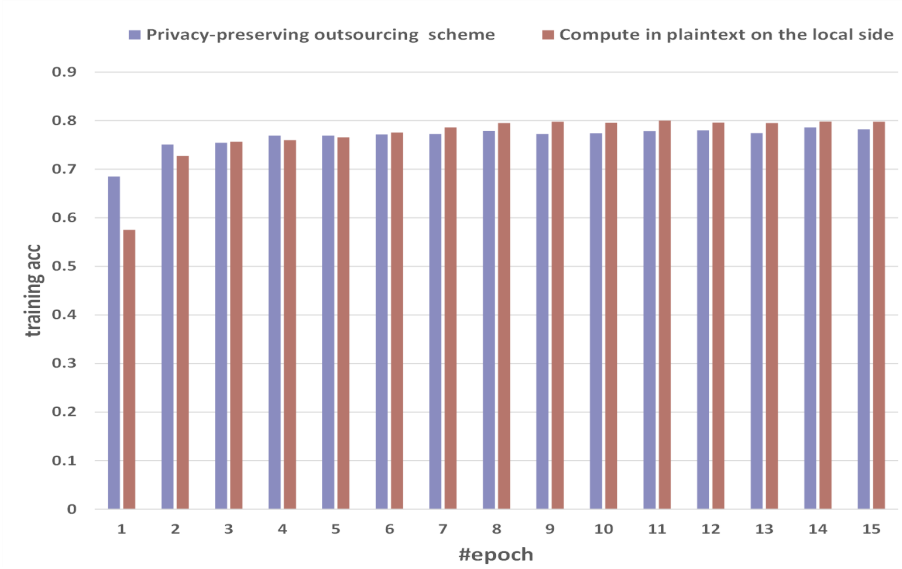


Figure 6. Comparison of training accuracy between the method of computing in plaintext on the local side and our scheme.

Figure 7 shows the comparison of training losses between the method of computing in plaintext on the local side and our privacy-preserving outsourcing scheme. We select 15 epochs as a sample with obvious fluctuations. We will find that with the increase of epochs, the gap of training loss between the method of computing in plaintext on the local side and our privacy-preserving outsourcing scheme is gradually narrowing. The losses computed at the user end are 0.6745, 0.5068, 0.4862, 0.4783, 0.4897, 0.4634, 0.4744, 0.4589, 0.4707, 0.4529, 0.4438, 0.4407, 0.4255, 0.4471, and 0.4254. The losses with the privacy-preserving outsourcing scheme are 1.25377, 1.17591, 0.82434, 0.82974, 0.73277, 0.77912, 0.65382, 0.57706, 0.52082, 0.53453, 0.52147, 0.53012, 0.52364, 0.53101, and 0.53214. With the increase of epochs, the loss gradually decreases, which shows the correctness and rationality of our experiment.

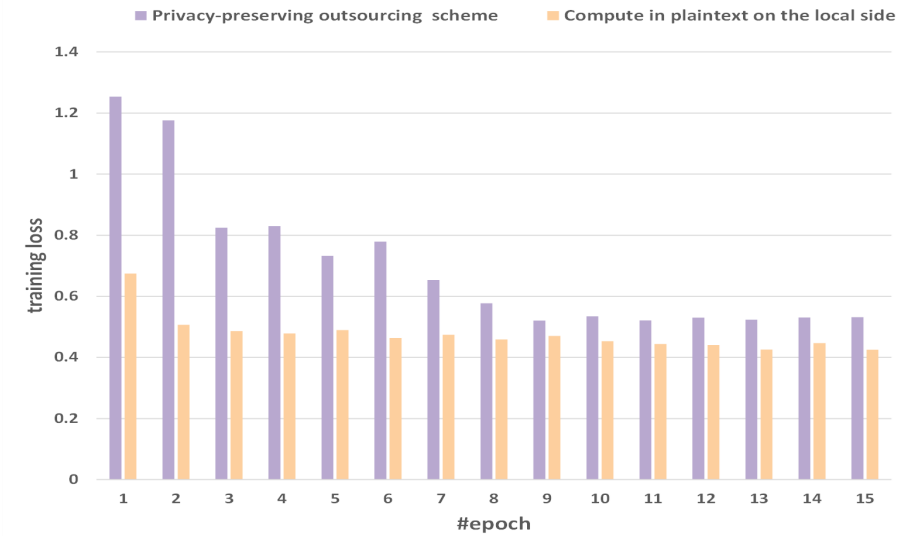


Figure 7. Comparison of training loss between the method of computing in plaintext on the local side and our scheme.

Figure 8 shows the comparison of test accuracy between the method of computing in plaintext on the local side and our privacy-preserving outsourcing scheme. We select 15 epochs as a sample with obvious fluctuations. The test acc of the direct method in plaintext

on the local side is 0.6812, 0.6797, 0.6774, 0.6787, 0.6727, 0.6784, 0.6809, 0.6779, 0.6745, 0.6745, 0.6777, 0.6844, 0.6737, 0.6839, and 0.6789. The training acc of privacy-preserving outsourcing scheme is 0.660925, 0.661776, 0.671921, 0.670179, 0.672472, 0.671423, 0.670179, 0.675153, 0.670729, 0.683268, 0.672917, 0.673121, 0.686854, 0.671286, and 0.674231. Our MPC implementation has gained similar training acc performance compared with the cleartext counterpart. Among them, the test accuracy of privacy-preserving outsourcing can reach 0.68113.

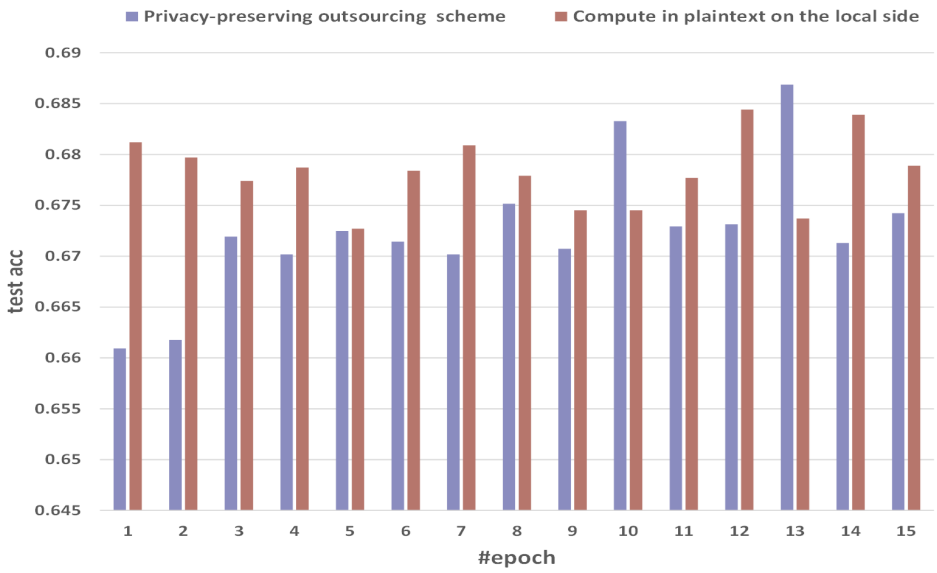


Figure 8. Comparison of test accuracy between the method of computing in plaintext on the local side and our scheme.

Figure 9 shows the comparison of test loss between the method of computing in plaintext on the local side and our privacy-preserving outsourcing scheme. We select 15 epochs as a sample with obvious fluctuations. We will find that with the increase in epochs, the gap of test loss between the method of computing in plaintext on the local side and our privacy-preserving outsourcing scheme is gradually narrowing. The losses computing at the user end are 0.6332, 0.6568, 0.6545, 0.6765, 0.6625, 0.6514, 0.6601, 0.6618, 0.6624, 0.6498, 0.6331, 0.6367, 0.6223, 0.6354, and 0.6182. The losses with privacy-preserving outsourcing scheme are 1.05377, 1.07591, 1.02434, 1.02974, 1.03277, 0.879127, 0.853824, 0.77706, 0.778715, 0.702974, 0.76854, 0.753241, 0.777706, 0.767706, and 0.762706. With the increase of epochs, the loss gradually decreases, which shows the correctness and rationality of our experiment.

Figure 10 shows the local time cost of the direct method and our scheme. In our experiment, samples were divided into training and test data sets in a ratio of 7:3. It could be inferred that the local cost of both direct computation and our scheme increased with the increase of samples. However, when the sample was fixed, the burden of the local end-performing privacy-preserving outsourcing scheme was far less than that of the direct computation, which also confirmed the superiority that it could greatly reduce the computing burden of users when completing the medical image classification.

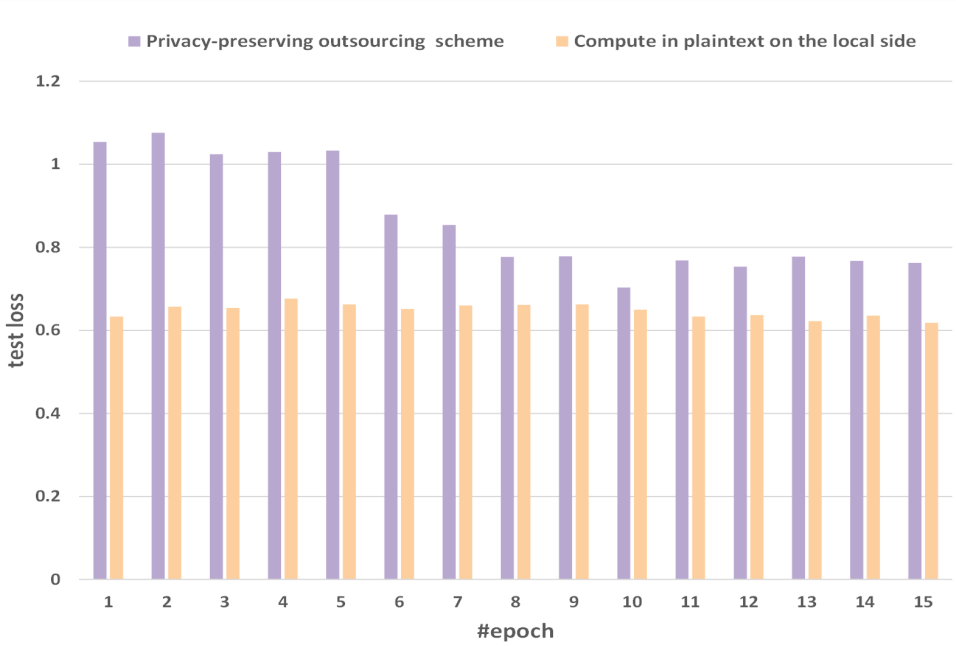


Figure 9. Comparison of test loss between the method of computing in plaintext on the local side and our scheme.

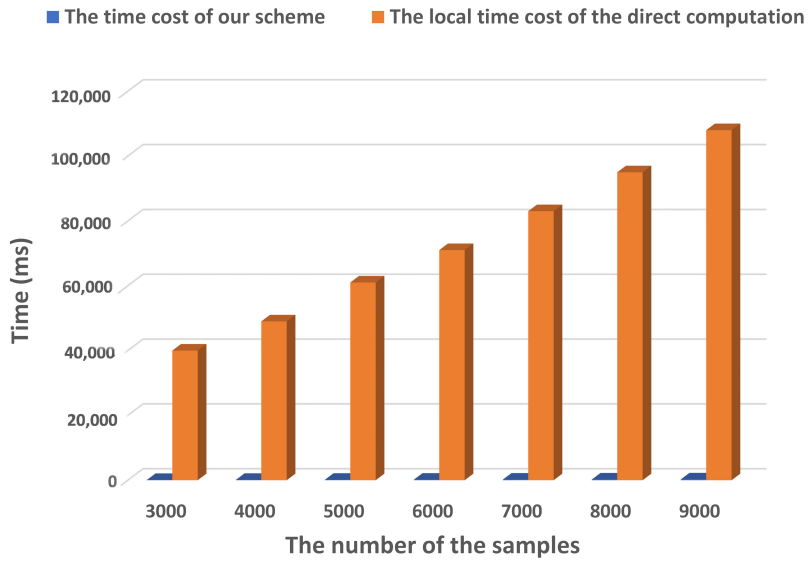


Figure 10. The local time cost of the direct method and our scheme.

7. Conclusions and Future Work

In this paper, we propose a scheme for privacy-preserving outsourcing medical image classification, which is the first attempt to outsource a specific medical application based on a convolutional neural network. In practice, it reduces the computing and storage burden on the user side. Combining the knowledge of cloud computing with cryptography, the sensitive information to protect the privacy of the input and the model information can be hidden in the whole scheme. We also carried out a pathological section staining experiment, which proved the efficiency of scheme.

The system proposed in the paper is for privacy-preserving outsourcing medical image classification in a semi-honest and non-colluding threat model, which means that we can widely implement medical image classification outsourcing based on a convolutional neural network. Further, we will explore how to achieve new general privacy-preserving

schemes for a malicious model in the future. Additionally, we will conduct research on other complex machine-learning algorithms in the future. For example, the training process of a decision tree often contains thousands of parameters, which is very time-consuming, and the data involved usually contains some private information. Therefore, it is necessary to design a privacy-preserving scheme for the process.

Author Contributions: Methodology, writing—review and editing, conceptualization, Q.Y. and H.Z.; validation, formal analysis, H.X.; investigation, software, F.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the National Natural Science Foundation of China (62102212), the Youth Program of Natural Science Foundation of Shandong Province (ZR202102190210), the Key Research and Development Project of Qingdao (21-1-2-21-XX) and the Shandong Provincial Youth Innovation Team (2022KJ296).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Secinaro, S.; Calandra, D.; Secinaro, A.; Muthurangu, V.; Biancone, P. The role of artificial intelligence in healthcare: A structured literature review. *BMC Med. Inform. Decis. Mak.* **2021**, *21*, 1–23. [CrossRef]
2. Mirbabaie, M.; Stieglitz, S.; Frick, N.R. Artificial intelligence in disease diagnostics: A critical review and classification on the current state of research guiding future direction. *Health Technol.* **2021**, *11*, 693–731. [CrossRef]
3. Chowdhury, S.; Mayilvahanan, P.; Govindaraj, R. Optimal feature extraction and classification-oriented medical insurance prediction model: Machine learning integrated with the internet of things. *Int. J. Comput. Appl.* **2022**, *44*, 278–290. [CrossRef]
4. Deepika, J.; Rajan, C.; Senthil, T. Security and privacy of cloud-and IoT-based medical image diagnosis using fuzzy convolutional neural network. *Comput. Intell. Neurosci.* **2021**, *2021*, 1–17. [CrossRef]
5. Cheng, J.; Tian, S.; Yu, L.; Gao, C.; Kang, X.; Ma, X.; Wu, W.; Liu, S.; Lu, H. ResGANet: Residual group attention network for medical image classification and segmentation. *Med. Image Anal.* **2022**, *76*, 102313. [CrossRef]
6. Ziller, A.; Usynin, D.; Braren, R.; Makowski, M.; Rueckert, D.; Kaissis, G. Medical imaging deep learning with differential privacy. *Sci. Rep.* **2021**, *11*, 1–8
7. Tripathi, M. Analysis of convolutional neural network based image classification techniques. *J. Innov. Image Process. (JIIP)* **2021**, *3*, 100–117. [CrossRef]
8. Salvi, M.; Acharya, U.R.; Molinari, F.; Meiburger, K.M. The impact of pre-and post-image processing techniques on deep learning frameworks: A comprehensive review for digital pathology image analysis. *Comput. Biol. Med.* **2021**, *128*, 104129. [CrossRef] [PubMed]
9. Benil, T.; Jasper, J. Cloud based security on outsourcing using blockchain in E-health systems. *Comput. Netw.* **2020**, *178*, 107344. [CrossRef]
10. Pulido-Gaytan, B.; Tchernykh, A.; Cortés-Mendoza, J.M.; Babenko, M.; Radchenko, G.; Avetisyan, A.; Drozdov, A.Y. Privacy-preserving neural networks with Homomorphic encryption: Challenges and opportunities. *Peer- Netw. Appl.* **2021**, *14*, 1666–1691. [CrossRef]
11. Li, Q.; Wen, Z.; Wu, Z.; Hu, S.; Wang, N.; Li, Y.; Liu, X.; He, B. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Trans. Knowl. Data Eng.* **2021**. [CrossRef]
12. Onoufriou, G.; Mayfield, P.; Leontidis, G. Fully homomorphically encrypted deep learning as a service. *Mach. Learn. Knowl. Extr.* **2021**, *3*, 819–834. [CrossRef]
13. Lim, J.S.; Hong, M.; Lam, W.S.; Zhang, Z.; Teo, Z.L.; Liu, Y.; Ng, W.Y.; Foo, L.L.; Ting, D.S. Novel technical and privacy-preserving technology for artificial intelligence in ophthalmology. *Curr. Opin. Ophthalmol.* **2022**, *33*, 174–187. [CrossRef] [PubMed]
14. Heidari, A.; Toumaj, S.; Navimipour, N.J.; Unal, M. A privacy-aware method for COVID-19 detection in chest CT images using lightweight deep conventional neural network and blockchain. *Comput. Biol. Med.* **2022**, *145*, 105461. [CrossRef] [PubMed]
15. Rehman, M.U.; Shafique, A.; Ghadi, Y.Y.; Boulila, W.; Jan, S.U.; Gadekallu, T.R.; Driss, M.; Ahmad, J. A Novel Chaos-Based Privacy-Preserving Deep Learning Model for Cancer Diagnosis. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 4322–4337. [CrossRef]
16. Huang, Q.X.; Yap, W.L.; Chiu, M.Y.; Sun, H.M. Privacy-Preserving Deep Learning With Learnable Image Encryption on Medical Images. *IEEE Access.* **2022**, *10*, 66345–66355. [CrossRef]

17. Arevalo, J.; González, F.A.; Ramos-Pollán, R.; Oliveira, J.L.; Lopez, M.A.G. Representation learning for mammography mass lesion classification with convolutional neural networks. *Comput. Methods Programs Biomed.* **2016**, *127*, 248–257. [CrossRef] [PubMed]
18. Sun, W.; Tseng, T.L.B.; Zhang, J.; Qian, W. Enhancing deep convolutional neural network scheme for breast cancer diagnosis with unlabeled data. *Comput. Med Imaging Graph.* **2017**, *57*, 4–9. [CrossRef]
19. Gao, X.; Li, W.; Loomes, M.; Wang, L. A fused deep learning architecture for viewpoint classification of echocardiography. *Inf. Fusion* **2017**, *36*, 103–113. [CrossRef]
20. Jeyaraj, P.R.; Samuel Nadar, E.R. Computer-assisted medical image classification for early diagnosis of oral cancer employing deep learning algorithm. *J. Cancer Res. Clin. Oncol.* **2019**, *145*, 829–837. [CrossRef]
21. Xu, G.; Li, H.; Zhang, Y.; Xu, S.; Ning, J.; Deng, R.H. Privacy-preserving federated deep learning with irregular users. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 1364–1381. [CrossRef]
22. Li, M.; Chow, S.S.; Hu, S.; Yan, Y.; Shen, C.; Wang, Q. Optimizing privacy-preserving outsourced convolutional neural network predictions. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 1592–1604. [CrossRef]
23. 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.* **2019**, *18*, 1261–1275. [CrossRef]
24. Liu, X.; Zheng, Y.; Yuan, X.; Yi, X. Securely Outsourcing Neural Network Inference to the Cloud with Lightweight Techniques. *IEEE Trans. Dependable Secur. Comput.* **2022**, *20*, 620–636. [CrossRef]
25. Falcetta, A.; Roveri, M. Privacy-preserving deep learning with homomorphic encryption: An introduction. *IEEE Comput. Intell. Mag.* **2022**, *17*, 14–25. [CrossRef]
26. Shen, W.; Yu, J.; Yang, M.; Hu, J. Efficient Identity-Based Data Integrity Auditing with Key-Exposure Resistance for Cloud Storage. *IEEE Trans. Dependable Secur. Comput.* **2022**. [CrossRef]
27. Yao, X.; Wang, X.; Wang, S.H.; Zhang, Y.D. A comprehensive survey on convolutional neural network in medical image analysis. *Multimed. Tools Appl.* **2022**, *81*, 41361–41405. [CrossRef]
28. Lee, J.S. A review of deep-learning-based approaches for attenuation correction in positron emission tomography. *IEEE Trans. Radiat. Plasma Med. Sci.* **2020**, *5*, 160–184. [CrossRef]
29. Dargan, S.; Kumar, M.; Ayyagari, M.R.; Kumar, G. A survey of deep learning and its applications: A new paradigm to machine learning. *Arch. Comput. Methods Eng.* **2020**, *27*, 1071–1092. [CrossRef]
30. Basha, S.S.; Dubey, S.R.; Pulabaigari, V.; Mukherjee, S. Impact of fully connected layers on performance of convolutional neural networks for image classification. *Neurocomputing* **2020**, *378*, 112–119. [CrossRef]
31. Braeken, A. Public key versus symmetric key cryptography in client–server authentication protocols. *Int. J. Inf. Secur.* **2022**, *21*, 103–114. [CrossRef]
32. Wei, W.; Tang, C.; Chen, Y. Efficient Privacy-Preserving K-Means Clustering from Secret-Sharing-Based Secure Three-Party Computation. *Entropy* **2022**, *24*, 1145. [CrossRef] [PubMed]
33. Araki, T.; Furukawa, J.; Lindell, Y.; Nof, A.; Ohara, K. High-throughput semi-honest secure three-party computation with an honest majority. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 805–817.
34. Keller, M.; Sun, K. Secure quantized training for deep learning. In Proceedings of the International Conference on Machine Learning, Seoul, Republic of Korea, 17–23 July 2022; pp. 10912–10938.
35. Mohassel, P.; Rindal, P. ABY3: A mixed protocol framework for machine learning. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Toronto, ON, Canada, 15–19 October 2018; pp. 35–52.
36. Goldschmidt, R.E. Applications of Division by Convergence. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 1964.
37. Catrina, O.; Saxena, A. Secure computation with fixed-point numbers. In *Financial Cryptography and Data Security, In Proceedings of the 14th International Conference, FC 2010, Tenerife, Canary Islands, 25–28 January 2010*; Revised Selected Papers 14; Springer: Berlin/Heidelberg, Germany, 2010; pp. 35–50.
38. Dong, Y.; Liu, Q.; Du, B.; Zhang, L. Weighted feature fusion of convolutional neural network and graph attention network for hyperspectral image classification. *IEEE Trans. Image Process.* **2022**, *31*, 1559–1572. [CrossRef]
39. Tanwar, V.K.; Raman, B.; Rajput, A.S.; Bhargava, R. SecureDL: A privacy preserving deep learning model for image recognition over cloud. *J. Vis. Commun. Image Represent.* **2022**, *86*, 103503. [CrossRef]
40. Rotaru, D.; Wood, T. Marbled circuits: Mixing arithmetic and boolean circuits with active security. In Proceedings of the International Conference on Cryptology in India, Hyderabad, India, 15–18 December 2019; pp. 227–249.
41. Keller, M. MP-SPDZ: A versatile framework for multi-party computation. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Los Angeles, CA, USA, 9–13 November 2020; pp. 1575–1590.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.