PULMONARY FUNCTION MONITORING USING PORTABLE ULTRASONOGRAPHY AND PRIVACY-PRESERVING LEARNING ARCHITECTURE

by

MENGHAN LIU

Submitted in partial fulfillment of the requirements

For the degree of Master of Science

Thesis Adviser: Dr. Ming-Chun Huang

Department of Electrical Engineering and Computer Science

CASE WESTERN RESERVE UNIVERSITY

January, 2017
Pulmonary Function Monitoring Using Portable Ultrasonography and
Privacy-preserving Learning Architecture

Case Western Reserve University
Case School of Graduate Studies

We hereby approve the thesis of

MENGHAN LIU

for the degree of

Master of Science

Dr. Ming-Chun Huang
Committee Chair, Adviser
Department of Electrical Engineering and Computer Science

Dr. Daniel G. Saab
Committee Member
Department of Electrical Engineering and Computer Science

Dr. Soumyajit Mandal
Committee Member
Department of Electrical Engineering and Computer Science

1We certify that written approval has been obtained for any proprietary material contained therein.
Table of Contents

List of Tables v
List of Figures vi
Acknowledgements ix
Acknowledgements ix
Abstract x
Abstract x

Chapter 1. Introduction 1
  Pulmonary Monitoring Using Ultrasound Imaging System 2
  Data Analysis Using Privacy-preserving Deep Learning 4
  Privacy-preserving Pulmonary Monitoring System 6

Chapter 2. Related Works 8
  Respiratory Measurements Researches 9
  Privacy-preserving Learning Methods 10

Chapter 3. Methods 14
  Ultrasound Image Processing Module 14
  Privacy-preserving Deep Learning Module 23

Chapter 4. Experimental and Results 27
  Respiratory Indexes Measurement 27
  Performance of Privacy-preserving Deep Learning Module 35

Chapter 5. Discussion 42
### List of Tables

<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Technical specifications of Interson ultrasound imaging probe</td>
<td>17</td>
</tr>
<tr>
<td>4.1</td>
<td>Information of the public dataset</td>
<td>28</td>
</tr>
<tr>
<td>4.2</td>
<td>Accuracy of Diaphragm Detection</td>
<td>29</td>
</tr>
<tr>
<td>4.3</td>
<td>Computational results and the ground truth</td>
<td>32</td>
</tr>
<tr>
<td>4.4</td>
<td>Prediction Error using 3 Heuristic methods (L)</td>
<td>34</td>
</tr>
</tbody>
</table>
# List of Figures

1.1 The privacy-preserving health monitoring architecture contains a global server and several local sites. Each local site is a potable ultrasound-based device, which contains image processing module and deep learning module. 6

3.1 Flowchart of image processing module. It contains algorithms of diaphragm detection, segmentation and mutual information. Respiratory rate is measured by counting peaks and tidal volume is estimated from diaphragm excursion. 16

3.2 A prototype overview. A spirometer device and an ultrasound device are connected to the tablet while collecting training dataset. After training the predict model, the spirometer could be removed. Only using the tablet and an ultrasound probe to detect breathing information. 16

3.3 (A) Airflow Rate waveform. (B) Tidal volume waveform is computed by airflow rate integral. Difference between valley and peak is tidal volume for one inspiration. 17

3.4 Curve $C = (x, y) : \phi(x, y) =$ propagation in normal direction 20

3.5 The left figure shows how to locate the center of circle arc using principal directions. The right figure shows the minimum-area-rectangle of a diaphragm and its center. 23

3.6 Architecture overview of the proposed collaborative privacy-preserving deep learning system. Each portable device servers as a local site and the remote XMPP server is used as global server. 24
4.1 Comparison of Results. (a) is the segmentation by Chan-Vese algorithm; (b) is the segmentation by Adaptive Thresholding algorithm; (c) is the segmentation by Fuzzy c means algorithm; (d) is the segmentation by EM/MPM algorithm.

4.2 The clear respiratory MI signal for 2000 frames of volunteer02: the average breathing period is 3.30s and the respiration rate is 18.2 times/minute.

4.3 (A) Regression of Run 1. (B) Regression of Run 2. 'a' stands for slope; 'b' stands for intercept on excursion axis.

4.4 (A) Regression of Run 1 and Run 2. (B) Comparison between real tidal volume and predicted value of test dataset.

4.5 (A) Comparison of three heuristic methods when diaphragm is incomplete. (B) Incompleteness of diaphragm caused by brightness.

4.6 The left sub-figure is CNN architecture with 12 layers; The left sub-figure is MLP architecture with 10 layers.

4.7 Reconstruct rate of decentralized MLP and CNN containing 3, 5, 7 local participants. The legends are different update orders. 'Centralized mini-batch' means each SGD batch is pooled from all training data.

4.8 Five local participants training with 4 different combination of deep learning algorithm and parameter exchange protocol.

4.9 Five local participants training in CNN with different selection fraction.
5.1 Typical detection failures. (A) Non-detection; partial diaphragm appears, but it is too small and omitted by the detector. (B) Mis-detection; cause by tissue or organ similar to diaphragm in shape and brightness. (C) Combination of both non-detection and mis-detection; the small piece of diaphragm is omitted, so the similar tissue is detected.

5.2 (A) The location of diaphragm at the end of inspiration in test 1. (B) The location of diaphragm at the end of expiration in test 1. (C) A combination of (A) and (B), which s the locations of diaphragm at one end of inspiration and the following end of expiration; this image shows an excursion distance in test 1. (D) The location of diaphragm at the end of inspiration in train 1. (E) The location of diaphragm at the end of expiration in train 1. (F) A combination of (D) and (E), which shows the locations of diaphragm at one end of inspiration and the following end of expiration; this image shows an excursion distance in train 1.

5.3 The tidal-volume of User 4. The fluctuation is smaller than the real condition because the air breathed out was leaked when using by the spirometer.

6.1 Ultrasound images of diaphragm and heart. (A) Ultrasound diaphragm. (B) Ultrasound heart in parasternal short axis view. (C) Ultrasound heart in parasternal long axis view. (D) Ultrasound heart in apical view.
Acknowledgements

0.1 Acknowledgements

I would first like to thank my thesis advisor, Professor Ming-Chun Huang of the Electrical Engineering and Computer Science Department at Case Western Reserve University. He's the finest advisor and one of the most creative and most hardworking people I know. He always provides insightful discussions about the research. Under his supervision, I learned how to define a research problem, find a solution to it, and finally publish the results. He provided valuable guidance whenever I meet with trouble and steered me in the right direction of research. To summarize, he is my best mentor in my life.

I would also like to acknowledge Professor Daniel G. Saab and Professor Soumyajit Mandal of the Electrical Engineering and Computer Science Department at Case Western Reserve University as the committee members of my Master defense. I am gratefully indebted to their help and time.

I would also like to thank my lab mates also friends who were involved in research projects related to this thesis: Haotian Jiang, Jia Chen, James Starkman, and Alaa Badokhon. They are excellent teammates with strong research skills and knowledges. We have worked together and encouraged each other to overcome obstacles in research.

Finally, I must express my very profound gratitude to my parents for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Author

Menghan Liu
Abstract

Pulmonary Function Monitoring Using Portable Ultrasonography and Privacy-preserving Learning Architecture

Abstract

by

MENGHAN LIU

0.2 Abstract

Personal health monitoring system in home environment has gained more and more attention. In the personal data transmission and analysis, privacy is an important concern. In this thesis, I present a privacy-preserving health monitoring architecture, which can extract respiratory signs from ultrasound images and collaboratively build deep learning model for classifying health status. The architecture contains a global server and several local sites. Each local site consists of an ultrasound probe and a tablet. Performance of the system is evaluated with several experiments. The error of respiratory rate measurement is less than 0.5 time/minute, and the average error of tidal volume estimation is about 0.1 L. Performance of privacy-preserving deep learning architecture is tested using a human activity recognition dataset. The reconstructed rate could keep 90% in different scenarios. In conclusion, the proposed monitoring system is feasible for personal health monitoring.
1 Introduction

With the explosion of portable biosensor systems, personal healthcare device has garnered lots of attention in the scientific community and the industry in the last years. It plays a significant role in reducing hospitalization, burden of medical staff, consultation time, waiting lists and overall healthcare costs. The idea behind small portable gadgets that monitor our life signs is that a person can collect health information on a regular basis, monitor changes and at times consult a doctor. These systems can comprise various types of small physiological sensors, transmission modules and processing capabilities, and can thus facilitate low-cost wearable unobtrusive solutions for continuous all-day and any-place health, mental and activity status monitoring. Personal portable devices for health monitoring help users to become active participants in their own care. Users can check health condition more frequently and conveniently.

A variety of sensors are integrated as part of a portable health-monitoring system, such as skin/chest electrodes, temperature probe, piezoelectric sensor, accelerometer, ultrasound probe and so on. Using these sensors, vital biosignals can be detected, such as Electrocardiogram(ECG), skin temperature, respiration rate, body movements, organ/tissue images et al\textsuperscript{1}. The data collected by personal portable devices is personal
Introduction

health record (PHR) which individuals can access, manage and share with other authorized users in a private, secure, and confidential environment. Many of the devices are connected wirelessly to a centralized system which collects and monitors data, and, if needed, alerts a medical professional. However, the personal information leak during transmission is a big concern. As the computational ability of portable devices increase, some analysis tasks can be shifted from central server to devices.

1.1 Pulmonary Monitoring Using Ultrasound Imaging System

Lung conditions usually are classified as obstructive lung disease and restrictive lung disease. People with obstructive disease have shortness of breath due to difficulty exhaling all the air from lungs. People with restrictive lung disease cannot fully fill their lungs with air. The most common disease are asthma and chronic obstructive pulmonary disease (COPD). Hundreds of millions of people are burdened with chronic respiratory conditions. Four million people die prematurely from chronic respiratory diseases each year, which is the 4th leading cause of death worldwide. In the USA, more than 12 million Americans are known to have COPD and it is the third most common cause of death. In 2010, the cost of COPD in the USA is approximately US $50 billion. Asthma is also very severe. In 2011, 235 million people have been diagnosed with asthma and asthma attack caused 250,000 deaths globally. This number increased to 334 million in 2014. Meanwhile, in the United States, asthma prevalence increased from 7.3 % in 2001 to 8.4% in 2010. 25.7 million persons had asthma in 2010, that means one of 12 people had asthma. Asthma results in a high cost for individuals and the nation. In the United
States, every person with asthma spent 3,300 dollars each year from 2002-2007 in medical expenses and the overall nation-wide expense is about 56 billions for medical costs, lost school, work days, and early deaths in 2007\(^6\). Long-term monitoring patients with lung disease is very significant to anticipate exacerbations and allow early therapeutic intervention. Usually, restrictive and obstructive lung diseases are identified using pulmonary function tests. Patients have to take test with an interval of at least 2 to 3 months between visits. Therefore, portable respiratory testing devices for monitoring lung functions in home environment has been getting increasingly attention. They will release patients from periodic examine in hospital and allow patients to get day-to-day care.

Vital roles for monitoring pulmonary function are respiration rate, tidal volume, lung capacity and so on. Respiratory rate can be measured automatically using piezoelectric sensor (PZO), laser doppler vibrometer (LDVi), and pyroelectric sensor. Spirometer is the most common standard tidal volume measurement, which has been designed to be portable and can be used in home environment. However, it still has limitation. Patients place the device in mouth and use a nose clip to guarantee that breathing flow is only through mouth. This a volitional tests which require patient’s understanding and cooperation. Therefore, spirometer can be problematic and unsuitable for measuring tidal volume in infant or children, heavily sedated or unconscious patients, or patient who cannot control muscles around mouth. Non-volitional techniques work fine in these situations, which can measure respiratory parameters based on other body movements. Camera-based and Doppler radar based methods detect chest motion. However, they could not provide the information of inside respiratory muscles. Many restrictive lung disease is mainly related to respiratory muscle deficiency\(^7\). Ultrasound will be a good solution. It does not require patient’s operation. Other people could help them to measure
breathe. It also allows directive visualization of muscles movement in human breathing and collection of image sequence of respiratory muscles. These additional information will assist doctor to make more efficient diagnosis and treatment. Non-invasive, point-of-care, ultrasound-based portable system that monitors respiratory status of patients in home environment is needed, feasible and promising\textsuperscript{8}.

1.2 Data Analysis Using Privacy-preserving Deep Learning

Health monitoring system not only can collect health data, but also have ability of pattern recognition and anomaly detection using data analysis and machine learning. In recent years, deep learning has gaining an increasing popularity among machine learning practitioners and researchers. It attempts to model high-level abstraction in data by using model architectures composed of multiple non-linear transformations, which has the wide applicability in all aspects of life, such as computer vision, audio and video processing, information retrieval, natural language processing and understanding, biometrics, and robotics. Recently, more and more researches applied deep learning technology in analytics of Electronic Health Records (EHR)\textsuperscript{9,10} and diagnosis of health state\textsuperscript{11–13}. Instead of using historical, empirical, clinically driven descriptions of disease, these techniques allow the data to speak for themselves. Researchers could discover deep properties and features of disease from quantitative medical data collected from patients or laboratory experiments. Furthermore, once the computer learn the medical model, it could be used for automatic long-term monitoring, which can release patients from periodic clinical examinations, offer innumerable opportunities to create efficient
health solutions out of clinical environment, and drive healthcare towards personalized medicine.

When we considering to apply deep learning in health monitoring system, one of the biggest risks is associated with the privacy of patients and their data. With the development of medical examination device and database system, more and more data from hospitals, health organization, and patient at home is collected and maintained in a large data warehouse. Customers or users no longer physically possess the storage of their data and cannot control the way of personal data being used. In addition, severe data leakage may happens once the data warehouse is attacked by hacker. Therefore, how to efficiently verify the correct usage and privacy of the user data becomes a big challenge in deep learning. The methods of data mining for privacy protection usually based on data distortion, perturbation, anonymity, and secure multiparty computing (SMC)\(^1\)\(^4\). Among these popular methods, SMC is practical compared to other solutions that change raw data and affect training results\(^1\)\(^5\). A collaborative learning framework commonly contains multiple sites with training capability and each site has its local dataset. Only releasing local trained model could well protect privacy, because no raw data will be shared. Another benefit is that the parallelizing computation in local site could reduce the burden of central server and runtime of training. Many researchers have made efforts in implementing distributed collaborative protocols. The architecture of distributed learning are implemented in different machine learning methods, such as SVM\(^1\)\(^6\), Logistic Regression\(^1\)\(^5\), and Neural Network\(^1\)\(^7\). Dean et al.\(^1\)\(^8\) proposed a distributed deep learning algorithm to accelerate the training of deep neural network, and proved that asynchronous Stochastic Gradient Descent (SGD) works very well with
deep neural networks. Shokri et al.\textsuperscript{19} proposed a privacy-preserving deep learning protocol and claimed that the promising accuracy of this privacy-preserving deep learning protocol indicates that Distributed Selected SGD (DSSGD) works well. Nowadays, personal healthcare devices are more and more popular in home environment. Once adding a computational module to personal device, each family could be a local site for collecting personal health record and training local deep learning model.

1.3 Privacy-preserving Pulmonary Monitoring System

Figure 1.1. The privacy-preserving health monitoring architecture contains a global server and several local sites. Each local site is a potable ultrasound-based device, which contains image processing module and deep learning module.
I aim to design a privacy-preserving health monitoring architecture, which can extract respiratory signs from ultrasound devices and build deep learning model for classifying health status, as shown in 1.1. Patients could use it to examine lung health status day to day. Health organization and hospital could also utilize the local data to train deep learning neural network for health status classification and data analysis, but they don't need to collect patient's raw data. The architecture implements a collaborative learning scheme to enable multiple local sites to one learn deep learning model together without releasing personal data. It contains a global server and several local sites (portable ultrasound-based devices). Global server could be a XMPP server or HPC cluster. Each portable ultrasound device used in home environment is a local site, containing an ultrasound probe and a tablet. While performing ultrasound exam, a series of ultrasound images are collected and processed to extract respiratory information in image processing module. Diaphragm is the major muscle responsible for breathing. Therefore, we can estimate breath information from movement of diaphragm. The implemented algorithms are designed to analyze diaphragm movement and measure respiratory rate and tidal volume. Then, the extracted respiratory signals and raw images can be used as the input of deep learning module. The output is parameters of neural network, which will be shared with other local sites through global server. In the future research, we will work on extract more vital signs, such as heart rate, from ultrasound image. Then, the privacy-preserving collaborative deep learning architecture could be used for monitoring other disease.
2 Related Works

Studies on health monitoring systems include wearable health monitoring system (WHMS), mobile health monitoring system (MHMS), and remote health monitoring system (RHMS). These systems obtain vital signs using various sensors, such as electrocardiogram (ECG), oxygen saturation (SpO₂), heart rate (HR), photoplethysmography (PPG), blood glucose (BG), respiratory rate (RR), and blood pressure (BP), to perform a variety of the smart tasks\(^{20}\). The tasks not only include traditional pattern recognition and anomaly detection but also building subject specific models and personalization. ARVmobile v1.0 is a multi-platform mobile personal health monitoring application proposed by Mena et al., which consists of an ABP sensor to detect BP and HR signals and smartphone receivers\(^{20}\). Based on the collected information, it performs early detection and intervention of hypertension, potential abnormal BP and HR levels for medical feedback. Baig et al. developed vital signs monitoring and interpretation system for older adults caring. HR, BP, pulse rate, SpO₂, and temperature are collected by wireless medical devices and transmitted in real-time to a laptop\(^{21}\). Then, authorized nurses could perform manual readings of collected data and Family members could be alerted when abnormality is detected by fuzzy logic model. Another m-health platform called
SHARE is developed for automatic cardiovascular and fall risk assessment in hypertensive patients. Heart Rate Variability (HRV) features are extracted from ECG data and classified off-line using data-mining approaches.

Most health monitoring systems implement 1-D signal collecting sensors, however 2D image sensor could provide more information and more clear observation of organs and tissues. Therefore, I mainly study on developing a HMS with image-based sensor for monitoring patients with respiratory failures. In HMS, a lot of challenges need to be studied, such as traffic and data communication, data processing, security and privacy, real-time and emergency handling, failure detection and handling, scalability, accuracy and so on. Privacy of personal data is an important concern in many studies.

### 2.1 Respiratory Measurements Researches

Diaphragmatic ultrasound has a wide range of applications in respiratory measurement and breathing activity monitoring. The study of Xirouchaki et al. has shown that in mechanically ventilated critically ill patients, lung ultrasound has a significant impact on decision making in the process of addressing specific clinical questions. Many related researches have been conducted to assess respiratory functions. Some researchers validated the relationship of diaphragmatic excursion using M-mode and B-mode examinations. Cohen et al. found a linear relation between diaphragmatic excursion and Tidal volume by M-mode ultrasonography. Ultrasonic measurement of diaphragmatic excursion during quiet breathing, voluntary sniffing, and forced breathing were conducted on patients referred for pulmonary function testing. B-mode is another
commonly used method. The linear relation between inspired volume and hemidiaphragmatic movement also be proved by B-mode. Samantha et al. implement diaphragm ultrasonography for pulmonary function testing by measuring excursion and velocity. However, the excursion distance is measured manually by placing a cranio-caudal displacement line. Therefore, an automatically computation method is necessary to save human effort and time.

Diaphragm thickness and respiratory rate can be measured from ultrasound image and are significant indications of respiratory diseases. An ultrasonography-based method was proposed to evaluate diaphragm thicknesses during respiration and compared with conventional measurements of respiratory functions in patients with amyotrophic lateral sclerosis (ALS). An ultrasound system was implemented to accurately record respiration rate and four types of respiratory template are identified for asthma. Umbrello et al. evaluated the performance of ultrasonographic indices of diaphragm contractile activity (respiratory excursion and thickening) in comparison to traditional indices of inspiratory muscle effort during assisted mechanical ventilation. Chrysostomou et al. performed qualitative analysis of diaphragmatic motion to indicate diaphragmatic weakness.

2.2 Privacy-preserving Learning Methods

Diagnostic of lung function using automatic methods could detect abnormal status timely and conveniently. There are many researches are involved with data analysis of COPD and asthma using machine learning algorithms. Amaral et al. developed a clinical decision support system for the categorization of airway obstruction level in patients with
COPD using forced oscillation (FO) measurement\textsuperscript{3}. Different supervised machine learning (ML) techniques were investigated in order to the search for the best classifier, including k-nearest neighbour (KNN), random forest (RF) and support vector machines with linear (SVML) and radial basis function kernels (SVMR). The study in\textsuperscript{31} utilized RF machine learning algorithm to determine factors that predict risk of multiple COPD exacerbations in a single year. Prasad et al. gathered the clinical signs and symptoms of asthma and analyzed data using machine learning algorithms such as Auto-associative memory neural networks, Bayesian network, ID3 and C4.5\textsuperscript{32}. As illustrated in Section 1.2, such traditional machine learning methods usually collect all data before training, which is not safe for personal privacy. Therefore, distributed learning framework is needed for privacy-preserving.

There are plenty of approaches focused on privacy preserving distributed learning framework. Differential privacy and security multi-party computation are wildly used in these frameworks. Hamm et al.\textsuperscript{33} proposed a framework named as Crowd-ML, which can collect and analysis data from smart devices. It labeled auxiliary data from local classifiers collected by trusted entity and then used labeled auxiliary data to find its empirical risk minimizer and trained global \( \hat{\theta} \)-differentially private classifier. Some frameworks do not want to take third party into account. Phan et al.\textsuperscript{34} proposed deep private auto-encoder (dPA), which implements \( \epsilon \)-differential privacy on objective functions. Sensitivity analysis and noise insertion are used on data reconstruction and cross-entropy error objective functions. Wang et al.\textsuperscript{15} proposed that a model offers on-line model learning, called EXpectation Propagation LOgistic REgRession (EXPLORER), which is a Bayesian alternative for the distributed frequentist logistic regression model. They
enhanced the confidentiality of EXPLORER by a Secured Intermediate Information Exchange (SINE) protocol. The work of Barni et al.\textsuperscript{35} is based on the assumption that users and the service provider are distrust to each other. Their framework consists 3 security levels. Level 1 using a protocol, Privacy-Preserving Scalar Product (PPSP), to protect the weighted sum of input. In level 2, oblivious polynomials evaluation protocol is used to avoid oblivious function evaluation problem. In level 3, fake neurons are added to protect the knowledge embedded within the neural network. Therefore, this framework not only protected users private information, but also the knowledge of the service providers. The algorithm proposed by Shokri et al.\textsuperscript{19} using distributed selective Stochastic gradient descent (SGD) allows the participants to train their models independently using their own data, and then share their key parameters selectively. It provides effective confidentiality with very low costs. Danner et al.\textsuperscript{36} also used SGD, however, tree topology and homomorphic encryption are applied to its protect privacy. There are plenty of approaches focused on privacy preserving distributed learning framework. Differential privacy and security multi-party computation are wildly used in these frameworks. Hamm et al.\textsuperscript{33} proposed a framework named as Crowd-ML, which can collect and analysis data from smart devices. It labeled auxiliary data from local classifiers collected by trusted entity and then used labeled auxiliary data to find its empirical risk minimizer and trained global \( \hat{\theta} \)-differentially private classifier. Some frameworks do not want to take third party into account. Phan et al.\textsuperscript{34} proposed deep private auto-encoder (DPA), which implements \( \varepsilon \)-differential privacy on objective functions. Sensitivity analysis and noise insertion are used on data reconstruction and cross-entropy error objective functions. Wang et al.\textsuperscript{15} proposed that a model offers on-line model learning, called EXpectation Propagation LOgistic REgRession (EXPLORER), which is a Bayesian
alternative for the distributed frequentist logistic regression model. They enhanced the confidentiality of EXPLORER by a Secured Intermediate Information Exchange (SINE) protocol. The work of Barni et al.\textsuperscript{35} is based on the assumption that users and the service provider are distrust to each other. Their framework consists 3 security levels. Level 1 using a protocol, Privacy-Preserving Scalar Product (PPSP), to protect the weighted sum of input. In level 2, oblivious polynomials evaluation protocol is used to avoid oblivious function evaluation problem. In level 3, fake neurons are added to protect the knowledge embedded within the neural network. Therefore, this framework not only protected users’ private information, but also the knowledge of the service providers. The algorithm proposed by Shokri et al.\textsuperscript{19} using distributed selective Stochastic gradient descent (SGD) allows the participants to train their models independently using their own data, and then share their key parameters selectively. It provides effective confidentiality with very low costs. Danner et al.\textsuperscript{36} also used SGD, however, tree topology and homomorphic encryption are applied to its protect privacy.
3 Methods

The privacy-preserving pulmonary monitoring system contains a global server and several local sites. Each local site mainly contains two parts: image processing module and privacy-preserving deep learning module. First of all, the collected ultrasound image sequence of diaphragm is processed to estimate respiratory information: respiratory rate and tidal volume. Then, the information is fed into privacy-preserving deep learning module to train deep learning model. The global server maintains a global deep learning neural network by integrating parameters uploaded from local sites.

3.1 Ultrasound Image Processing Module

The flowchart of image processing module is shown in Figure 3.1. The breathing information is extracted by analyzing diaphragm movement. An ultrasound probe is placed on the right lower rib cage of a volunteer. First of all, diaphragm area is detected from each ultrasound image frame using Histogram of Oriented Gradient (HOG) features and Viola-Jones. Then we segment out diaphragm using Chan-Vese algorithm and compute mutual information (MI) to reflect relation among consecutive ultrasound image sequence. Segmentation is only conducted in detected area instead of the whole
frame, which has three advantages. First, the runtime of segmentation decreases. Second, the detected area can be used as initial curve to avoid select seed manually. Third, segmentation in detected area ensures the segmented diaphragm does not contain redundant organs and tissue. It is helpful to improve accuracy of diaphragm excursion measurement. In the 1D MI waveform, from one peak to next peak is one respiratory cycle. Therefore, the respiratory rate is measured by counting respiratory cycles. The image frames at peaks and valleys are the key frames. The diaphragm excursion from peak to valley has linear relation with tidal volume. Therefore, the tidal volume is estimated based on diaphragm excursion. Three heuristic methods are implemented to measure diaphragm excursion in one respiratory cycle: principle component analysis, minimum-area-rectangle, and centroid of mass. The ground true for training estimation parameters is collected by spirometer sensor. Parameters of the linear relationship are trained using measured diaphragm excursion and spirometer data. After obtaining the trained parameters, users can measure tidal volume only using ultrasound image and linear relation parameters.

### 3.1.1 Ultrasound-spirometer System Setup

Both the ultrasound device and spirometer device used in this system can be connected to a tablet (Figure 3.2), which makes the proposed system potable. Each volunteer was simultaneously assessed with ultrasound probe and spirometer in sitting position. In the proposed system, ultrasound examinations were performed with Interson 'Seemore', a portable ultrasound probe. The pulse frequency is set as 5MHz and scan depth is 15cm. Diaphragm excursions on successive respiratory cycles were recorded at a rate of 12 frames/s. More details of probe specifications are in Table 3.1Continuous spirometric
Figure 3.1. Flowchart of image processing module. It contains algorithms of diaphragm detection, segmentation and mutual information. Respiratory rate is measured by counting peaks and tidal volume is estimated from diaphragm excursion.

measurements were made with vernier spirometer. It can be connected to 'Intel Edison' development board as a sensor and send data to a computer. The raw data collected from the spirometer sensor is airflow rate, as shown in Figure 3.3(A). Tidal volume was measured by integrating airflow rate, shown as in Figure 3.3(B). Peaks in Figure 3.3(B)

Figure 3.2. A prototype overview. A spirometer device and an ultrasound device are connected to the tablet while collecting training dataset. After training the predict model, the spirometer could be removed. Only using the tablet and an ultrasound probe to detect breathing information.
Methods

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Depth Range</td>
<td>2-15 cm</td>
</tr>
<tr>
<td>Pulse Frequency</td>
<td>3.5-5MHz</td>
</tr>
<tr>
<td>Frame Rate</td>
<td>12 fps</td>
</tr>
<tr>
<td>Scan Angle</td>
<td>60 degrees</td>
</tr>
<tr>
<td>Image Format</td>
<td>Jpeg</td>
</tr>
<tr>
<td>Image Size</td>
<td>$1024 \times 600$</td>
</tr>
<tr>
<td>Gray Scale</td>
<td>256 shades</td>
</tr>
<tr>
<td>Scanning Mode</td>
<td>B-mode</td>
</tr>
</tbody>
</table>

Table 3.1. Technical specifications of Interson ultrasound imaging probe

represent the end of inspiration and the valleys are the start. Difference between valley and peak is the tidal volume of the corresponding breathing cycle.

![Airflow Rate and Tidal Volume Waveforms](image)

Figure 3.3. (A) Airflow Rate waveform. (B) Tidal volume waveform is computed by airflow rate integral. Difference between valley and peak is tidal volume for one inspiration.

3.1.2 Diaphragm Detection and Segmentation

In ultrasound image, the gray pattern of diaphragm and illumination are not very obvious. It is more appropriate to detect diaphragm based on special arc shape of diaphragm. Therefore, HOG features are implemented to detect diaphragm location.
HOG is a local statistic of the orientations of image gradients, which has been applied in object detection and pedestrian. Because local object appearance and shape can be characterized very well by the distribution of local intensity gradients or edge directions. To train diaphragm detector, 10% ultrasound images are selected from full dataset and used as training data, which contains positive and negative instances. The positive instances contain diaphragm area and negative instances do not have or have very small part of diaphragm. For each positive image, we record the position information of the rectangular area which is the minimum rectangle to envelop diaphragm. Next, each training image is divided into many cells. In each cell, HOG computes the gradient magnitude and orientation around keypoints to construct a histogram. The magnitude is given by:

\[ |\nabla I(x, y)| = \sqrt{G_x^2 + G_y^2} \]  

(3.1)

while gradient is given by:

\[ \theta(x, y) = \arctan \left( \frac{G_x}{G_y} \right) \]  

(3.2)

where, \( G_x \) and \( G_y \) are the derivative in horizontal and vertical directions. Then, orientations are quantized into a number of bins and magnitudes for identical orientations are accumulated into a histogram. For each histogram bin, histogram value is the sum of all the magnitudes having that particular orientation. For better invariance to illumination and noise, the histogram values are normalized by the total energy of all orientations to obtain values between 0 and 1. A common normalization scheme is implemented and computed as:

\[ V_n = \frac{V}{\sqrt{||V||^2 + \epsilon^2}} \]  

(3.3)
Methods

After feature extraction, a huge number of feature vectors are obtained for each ultrasound image. However, using the total number of features to carry out a classification is inadequate in terms of computing time and the robustness, since many of these features contain irrelevant information (noise). Viola-Jones algorithm uses AdaBoost to select feature. AdaBoost is a machine learning boosting algorithm that constructs a strong classifier through a weighted combination of weak classifiers. A template histogram over all training dataset is computed which is the mean histogram of all training positive instances. HOG weak classifiers classify positive and negative according to the distance between histogram of an input image and the template histogram. The weak classifier is defined as:

$$u = \begin{cases} 
1, & \text{if } d(h_j, m_j) < \theta_j \\
0, & \text{otherwise}
\end{cases}$$

(3.4)

Then the strong classifier is:

$$G = \begin{cases} 
1, & \sum_{n=1}^{N} \alpha_n g_n \geq \frac{1}{2} \sum_{n=1}^{N} \alpha_n = T \\
0, & \text{otherwise}
\end{cases}$$

(3.5)

where $G$ and $g$ are the strong classifiers and weak classifiers. $T$ is the strong classifier threshold.

In detection of positive area, the algorithm takes advantage of cascading to discard negative area. The image will be scanned with sub-windows in different size. When sub-windows contains some percentage of having positive area, these regions are passed to next cascade stage, otherwise, are discarded. Finally, a detector is trained and saved as an ‘xml’ file. In this system, we trained a diaphragm detector with 5 stages. The file contains the parameters of weak classifiers in each stage, such as threshold and weight.
Methods

Figure 3.4. Curve $C = (x, y): \phi(x, y) = \text{propagation in normal direction}$

To segment diaphragm area, an active contour algorithms is implemented to find region of interest (ROI). It shows great performance on ultrasound image segmentation, even if ultrasound images have some undesired properties, such as gray-scale, attenuation, speckle, blurred boundaries, and low contrast between ROI. The basic idea of this model is that starting with a curve around the objects, the curve extends or shrinks toward its interior normal, and stops when touch the boundary of the objects. Given an image $u_0$, the goal is to look for the best approximation $u$ of $u_0$ by minimizing an energy function $F(c_1, c_2, C)$. $u$ is the segmented result and it takes two values:

$$u = \begin{cases} 
\text{average}(u_0), & \text{inside } C \\
\text{average}(u_0), & \text{outside } C 
\end{cases}$$

(3.6)

Notations are illustrated in Figure 3.4. The energy function $F(c_1, c_2, C)$ is defined by

$$F(c_1, c_2, C) = \mu \int_{\Omega} \delta(\phi(x, y)) |\nabla \phi(x, y)| dxdy + \nu \int_{\Omega} H(\phi(x, y)) dxdy$$

$$+ \lambda_1 \int_{\Omega} |u_0(x, y) - c_1|^2 H(\phi(x, y)) dxdy + \lambda_2 \int_{\Omega} |u_0(x, y) - c_2|^2$$

$$+ (1 - H(\phi(x, y))) dxdy$$
where \( C \) is an arbitrary variable curve, and constants \( c_1, c_2, \) depending on \( C, \) are averages of \( u_0 \) inside \( C \) and respectively outside \( C. \mu \geq 0, \nu \geq 0, \lambda_1, \lambda_2 \geq 0 \) are fixed parameters and function \( H \) is the Heaviside function, defined by:

\[
H(z) = \begin{cases} 
1, & \text{if } z \geq 0 \\
0, & \text{if } z \leq 0 
\end{cases}
\]  

(3.7)

In this equation, the first item is the length of curve and the second item is the area of the region inside. They are the regularizing items. Primary steps of the algorithm are shown in Algorithm 1.

**Algorithm 1** Chan-Vese active contour algorithm

```plaintext
/* Initialization */
Step 1: \( \phi^0 \leftarrow \phi_0, n \leftarrow 0. 
/* Iteration */
Step 2: Compute \( c_1(\phi^n) \) and \( c_2(\phi^n). 
Step 3: Solve the PDE in \( \phi \) to obtain \( \phi^{n+1}. 
Step 4: Reinitialize \( \phi \) locally to the signed distance function to the curve (this step is optional).
Step 5: If the solution is stationary, stop, otherwise go to Step 2.
```

### 3.1.3 Key Frame Detection

Mutual information (MI) is computed to form a 1D signal. MI measures statistical dependence of two images and is defined by

\[
MI(A, B) = H(A) + H(B) - H(A, B) = \sum_{ab} p(a, b) \log \frac{p(a, b)}{p(a)p(b)}
\]  

(3.8)

where, \( A \) and \( B \) are ROI from two consecutive image frames. \( H(A), H(B), \) and \( H(A, B) \) are the entropies of \( A \) and \( B, \) and their joint entropy respectively. \( p(a, b), p(a) \) and \( p(b) \)
are the joint probability distribution of \( a \) and \( b \), and their individual probability distributions, where \( a \) and \( b \) are the pixel values in \( A \) and \( B \). An image at the end of inspiration is selected as a reference image. MI between this frame and all other segmented image frames were computed. Large MI value occurs when diaphragm is close to the reference frame, i.e. the end of inspirations. On the contrary, small MI value occurs when the diaphragm motion is far away from the reference. Thus 1D signal’s magnitude and phrase are related to respiration. The corresponding images at peaks and valleys are key frames.

3.1.4 Diaphragm Excursion Measurement

When diaphragm moves, its shape, size, and position change. However, these changes are not common image transform, such as affine, projective, rotation, and scale. Therefore, it is necessary to represent diaphragm with one center point. The excursion distance between two key frames in one respiratory cycles is measured by computing the distance between centers of two diaphragm areas. I apply three heuristic methods to represent diaphragm location. In the first method, we defined a center in the coordinate of principle direction. To simplify the question, the shape of segmented diaphragm area is approximately considered as an arc of circle. The way to find the center of an arc circle is defined in the left figure of Figure 3.5. Principal component analysis is applied on a circle arc to find its principal directions, then the arc is mapped to the two principal directions separately. Midpoints of each mapping is defined as the coordinate of circle arc center. In this heuristic method, the diaphragm excursion is represented by the distance on ‘\( x_1 \)’ direction, which can tolerate the incompleteness of diaphragm. In the rest two methods, the diaphragm excursion is Euclidean distance. In the second method, we use the center of the minimum-area-rectangle as the center of diaphragm area, as
Methods

shown in the right figure of Figure 3.5. To find the minimum-area-rectangle, first of all, we need to compute the convex hull of diaphragm. Then for each edge of the convex hull, it computes the edge orientation and the area of bounding rectangle on that orientation. Finally, the center of rectangle with the minimum area represents the diaphragm location. The third method implements the centroid of mass as the representation of a diaphragm.

Figure 3.5. The left figure shows how to locate the center of circle arc using principal directions. The right figure shows the minimum-area-rectangle of a diaphragm and its center.

3.2 Privacy-preserving Deep Learning Module

Figure 3.6 illustrates the main components and protocols of the proposed collaborative privacy-preserving deep learning architecture (CPDL) in distributed mobile environment. The assumption behind our solution is that all of the $N$ local sites agree with a common deep learning objective and each of them has a local private dataset available for training. The basic elements in CPDL are a global server implemented on remote XMPP server, which is responsible for updating/downloading the parameters, and several local sites implemented on tablets. Before uploading, the trained parameters will
be selected. With parameter exchange protocol, local participants can share information during training, which is helpful for avoiding local optimum.

**Figure 3.6.** Architecture overview of the proposed collaborative privacy-preserving deep learning system. Each portable device servers as a local site and the remote XMPP server is used as global server.

### 3.2.1 Parameters Selection

There are many ways to select parameters. An magnitude based criterion for selecting uploaded parameters is implemented. In a nutshell, at each iteration, a fraction of weights are updated by equation 3.9. These weights are the ones associated with the largest gradients.

\[
W_i(n+1) = \begin{cases} 
W_i(n) - \alpha \frac{\partial E}{\partial W_i(n)}, & \text{if } \frac{\partial E}{\partial W_i(n)} > \text{thres} \\
W_i(n), & \text{otherwise}
\end{cases}
\]  

(3.9)

where the \text{thres} is computed by sorting the gradient and \( E \) is the cost function. With this gradient-based partial update scheme, less information of the local participant is
shared. Since each local only share small fraction of the gradients to the server at each round, it is more difficult for the attacker to eavesdrop intact personal information.

### 3.2.2 Parameter Exchange Protocols

In our system, we mainly considered two different parameter exchange protocols: round robin and asynchronous. For both round robin and asynchronous scenarios, in each training epoch, each local participant will download the most updated parameters from the global server, runs the local training using local dataset, and uploads selected gradients to the global server. With round robin, all the local participants run selective SGD one by one in a fixed order. The next local participant will not be activated until the current local participant completely finishes a mini-batch training. However, with asynchronous scenario, each local participant does their own job independently. When one local participant is training the local model, others may upload the gradients to the server or download the parameters from global server.

**Round Robin Exchange Protocol.** To train the neural network with round robin, a weight matrix $W^G$ and learning rate are initialized on the global server. Then, global server will actively distribute the initial weight to the first local participant and wait for the selected gradients. After receiving the selected gradients from current active local participant, the global server updates the stored parameter and distribute the most updated weights to the next local participant. Ultimately, the global server hold the well-trained model which is the collaborative learning result.

On the local site, it replaces the old weight parameters with the latest ones downloaded from global server. Then, the local participant runs the standard SGD algorithm with a self-defined learning rate, mini-batch size and number of epoch. After that, the
local participant selects the gradients $\Delta W$ with top $\theta$ fraction largest magnitude, and upload the selected gradient $\Delta W_s$ to the server. This fraction of gradient represents the most important set of changes in local parameter. The selection criteria is unchanged for the entire training process.

**Blocking Asynchronous Exchange Protocol.** Different from round robin, global server in asynchronous scenario needs to handle more conflicts. In this paper, a kind of blocking asynchronous logic is implemented. Beside weight and learning rate initialization, the global server also needs to set a boolean flag variable 'Free' to indicate the current status of the server. At the beginning, the flag is true. If the server is accepting the new selected gradients from one of the local participants or updating its parameters, the flag will become false and the server will block all of the remaining request temporarily. In blocking asynchronous, local participants can join in the training process whenever they want without any coordination. The global server always waiting for the weight request from local. Once receiving the request, the server will send the current weights to the corresponding local site.

On the local site, since there is no fixed order in asynchronous scenario, whenever a local participant wants to join in the training, it sends a request for downloading the most newest weights from the server. Once receiving the weights, the local site does the same things in round robin scenario. The only difference is that before uploading $\Delta W_s$ to global server, the local needs to check the 'Free' status of the global server first. If the server is free, the local uploads the gradients immediately. Otherwise, the local has to wait until the server is not busy.
4 Experimental and Results

We designed several experiments to evaluate the performance of image processing module and privacy-preserving deep learning module. CWRU Institutional Review Board has approved the human subjects’ experiments and the approval is appended.

4.1 Respiratory Indexes Measurement

In this section, we conducted experiments to test the performance of image processing module. To evaluate the accuracy of respiratory rate, a public dataset and our own dataset are both used. The public dataset is from Petrusca et al.\textsuperscript{42}, which can be downloaded from "https://www.vision.ee.ethz.ch/datasets/index.en.html". It contains videos of diaphragm movement from 9 volunteers. Each volunteer performed regular breath for five and half minutes. The ultrasound device is Antares (Siemens Medical Solutions). Sample rate is from 15 to 25 frames per second and center frequency of ultrasound is about 2 MHz. This dataset is used for evaluating the performance of image segmentation and computed respiration rate. More details about the dataset are in Table 4.1. 'V01', 'V02', ..., 'V09' are the numbers of volunteers. To collect real dataset, volunteers' diaphragm is imaged with a USB ultrasound probe in B-mode. The probe is adjusted to 5 MHz and placed inferior of the rib cage with the fan direction aligned approximately
in parallel to the lowest rib. Five volunteers are asked to breathe normally for 5 minutes and the ultrasound image sequences are collected as normal breathing dataset, named as 'Real01', 'Real02',..., 'Real05'. They are used for verifying the accuracy of the segmentation algorithms. At the same time, we record the number of breathing cycles as ground truth.

Table 4.1. Information of the public dataset

<table>
<thead>
<tr>
<th>Number</th>
<th>Spatial Resolution</th>
<th>Sample rate (fps)</th>
<th>Center frequency (MHz)</th>
<th>Data size (GB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V01</td>
<td>640 × 480</td>
<td>25</td>
<td>2.22</td>
<td>1.92</td>
</tr>
<tr>
<td>V02</td>
<td>712 × 480</td>
<td>16</td>
<td>2.00</td>
<td>1.79</td>
</tr>
<tr>
<td>V03</td>
<td>712 × 480</td>
<td>17</td>
<td>1.82</td>
<td>1.87</td>
</tr>
<tr>
<td>V04</td>
<td>720 × 540</td>
<td>15</td>
<td>2.22</td>
<td>1.91</td>
</tr>
<tr>
<td>V05</td>
<td>720 × 540</td>
<td>15</td>
<td>2.22</td>
<td>1.87</td>
</tr>
<tr>
<td>V06</td>
<td>720 × 540</td>
<td>17</td>
<td>1.82</td>
<td>1.80</td>
</tr>
<tr>
<td>V07</td>
<td>500 × 480</td>
<td>14</td>
<td>2.22</td>
<td>1.10</td>
</tr>
<tr>
<td>V08</td>
<td>700 × 480</td>
<td>17</td>
<td>1.82</td>
<td>1.87</td>
</tr>
<tr>
<td>V09</td>
<td>700 × 480</td>
<td>16</td>
<td>1.82</td>
<td>1.64</td>
</tr>
</tbody>
</table>

Four volunteers participated in the tidal volume experiments. An over one-minute ultrasound video and corresponding spirometer sensor data were collected when user breaths. This process was repeated six times by each volunteer. In the first time, volunteer performed normal breath. Then the volunteer performed deep breath without detaching ultrasound probe. The first two times was combined as Run 1. The third and forth times as Run 2 repeated the former two, but the probe is detached for a while and put back. In the last two times, volunteer breath for 1 minute deep or normal as they preferred. Run 1 and Run 2 are used as train datasets. The rest two times are used as test datasets.
4.1.1 Diaphragm Detection Performance

Detector was trained using images selected in training datasets. To test the accuracy of diaphragm detection, we picked one ultrasound video from each volunteer’s six videos and detected diaphragm in each frame of the video using the method discussed in section III. Accuracy of the detection is shown in Table 4.2, ranging from 96.33% to 100%. The accuracy is slightly influenced by the quality of ultrasound video. The details will be discussed in section V.

Table 4.2. Accuracy of Diaphragm Detection

<table>
<thead>
<tr>
<th>User No.</th>
<th>Total Frames</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>791</td>
<td>96.33%</td>
</tr>
<tr>
<td>2</td>
<td>685</td>
<td>100%</td>
</tr>
<tr>
<td>3</td>
<td>662</td>
<td>97.13%</td>
</tr>
<tr>
<td>4</td>
<td>719</td>
<td>98.89%</td>
</tr>
</tbody>
</table>

4.1.2 Diaphragm Segmentation Performance

The predominant motion in image is a two-dimensional profile of the diaphragm which follows the breathing cycle of the volunteers. Voluteer02’s image is used as example to compare four segmentation algorithms. The segmentation result using Chan-Vese is a binary image, as shown in Figure 4.1(a). The white arc is the diaphragm and the black part is other tissues and organs. Compared with the original image, shape and location of segmented areas are matched with expectation. There are some small spots above the arc of diaphragm which are the tissues of the liver. When the contour shrinks or extends around diaphragm, liver tissues are also segmented out, because it is very close to the diaphragm, lighter than background, and also in our rectangular seed. The contraction and relaxation of diaphragm force the liver to move. Movement of spots and diaphragm
are in the same phase, and these spots does not affect the 1D respiration signal. In order to verify segmentation accuracy of Chan-Vese, we also do segmentation with other three algorithms as comparison: Adaptive thresholding\textsuperscript{43}, EM/MPM algorithm\textsuperscript{44} and Fuzzy c-means (FCM)\textsuperscript{45}. Results are in Figure 4.1(b)-(d). These three algorithms segment out diaphragm as well as the upper white area which has the similar gray value as diaphragm area. EM/MPM result is worse. The extracted diaphragm by EM/MPN is wider than real one. Compared with these three algorithms, Chan-Vese has the advantage that it can exclude the light areas and extract the diaphragm area only. Therefore, performance of Chan-Vese in our dataset is superior.

Figure 4.1. Comparison of Results. (a) is the segmentation by Chan-Vese algorithm; (b) is the segmentation by Adaptive Thresholding algorithm; (c) is the segmentation by Fuzzy c-means algorithm; (d) is the segmentation by EM/MPM algorithm.
4.1.3 Respiratory Rate Measurement

An example of computed MI waveform is shown in Figure 4.2. There are 38 peaks and 38 valleys in the 2000 frames. Respiration rate is 18.2 times/minute. To verify the computed result, we record the number of respiration cycles in the corresponding volunteer's video. There are 38 such cycles in this video clip and one cycle is approximately 3s, which corresponds to $3 \times \text{SampleRate}$ frames in the video file. The measured respiratory rate and corresponding ground truth of all volunteers are listed in Table 4.3. By comparison, the computational results are very close to ground truth.

Figure 4.2. The clear respiratory MI signal for 2000 frames of volunteer02: the average breathing period is 3.30s and the respiration rate is 18.2 times/minute.

4.1.4 Tidal Volume Prediction

Diaphragm excursion is measured with the three heuristic methods mentioned above. The result of principle direction method of User 2 is used as example in the following discussion. The diaphragm excursion computed from ultrasound images and real tidal volume from spirometer sensor are plotted in Figure 4.3. We implemented regression to find the fitted line. Linear relation between diaphragm excursion and tidal volume is
Table 4.3. Computational results and the ground truth

<table>
<thead>
<tr>
<th>Number</th>
<th>Computational Respiratory Rate (times/minute)</th>
<th>Ground truth (times/minute)</th>
<th>Time for one cycle (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V01</td>
<td>17.1</td>
<td>17</td>
<td>3.51</td>
</tr>
<tr>
<td>V02</td>
<td>18.2</td>
<td>18</td>
<td>3.30</td>
</tr>
<tr>
<td>V03</td>
<td>17.3</td>
<td>17</td>
<td>3.47</td>
</tr>
<tr>
<td>V04</td>
<td>15.5</td>
<td>15</td>
<td>3.87</td>
</tr>
<tr>
<td>V05</td>
<td>15.3</td>
<td>15</td>
<td>3.92</td>
</tr>
<tr>
<td>V06</td>
<td>17.8</td>
<td>18</td>
<td>3.37</td>
</tr>
<tr>
<td>V07</td>
<td>16.3</td>
<td>16</td>
<td>3.75</td>
</tr>
<tr>
<td>V08</td>
<td>17.2</td>
<td>17</td>
<td>3.49</td>
</tr>
<tr>
<td>V09</td>
<td>16.3</td>
<td>16</td>
<td>3.57</td>
</tr>
<tr>
<td>Real1</td>
<td>18.2</td>
<td>18</td>
<td>3.30</td>
</tr>
<tr>
<td>Real2</td>
<td>19.2</td>
<td>19</td>
<td>3.15</td>
</tr>
<tr>
<td>Real3</td>
<td>19.3</td>
<td>19</td>
<td>3.11</td>
</tr>
<tr>
<td>Real4</td>
<td>19.8</td>
<td>20</td>
<td>3.03</td>
</tr>
<tr>
<td>Real5</td>
<td>19.0</td>
<td>19</td>
<td>3.16</td>
</tr>
</tbody>
</table>

observed. Regression parameters of two runs are slightly different, which is caused by detaching. Although we tried to put the ultrasound back to the same place, it cannot be the exactly same. In addition, the ultrasound probe rotation and angle change also cause the difference.

Then we compute a global regression over all train data, as shown in Figure 4.4(A) and plot it and test data in Figure 4.4(B) to observe its performance. The regression line closely fits to the test data. The average error between the measured tidal volume from ultrasound images and the ground truth from spirometer is 0.1032L. The evaluation of prediction using three methods is list in Table 4.4. In a healthy, young human adult, tidal volume is approximately 0.5L per inspiration. The prediction error of User 1 and 2 are about 0.1L using principle direction method. However, the prediction error of User 3 and 4 are higher. The higher error of User 3 is caused by probe position and angle. The
higher error of User is 4 caused by spirometer measurement error. The low quality of data will affect the accuracy of tidal volume measurement. More discussion is in Section V. If the images which contain the impact of probe position and angle are eliminated, the error of User 3 will be 0.1177L, 0.1293L, and 0.1270L for Principle direction, Centroid of mass, and Minimum-area-rectangle, respectively. The performance of principle direction method is the most outstanding one. This is because the distance computation of principle direction compute can tolerate the incompleteness of diaphragm. As shown in 4.5(B), a brightness area covers partial diaphragm. This results in the incompleteness of diaphragm in 4.5(A). The arc center 'a' is supposed to move to point 'b' when the user breath in. However, based on the detected image, the calculated distance is from point 'a' to point 'b' and it is longer than the distance from point 'a' to point 'b'. This will affect training and test results. Principle direction method computes the distance on 'x1' direction. Therefore, the measured distance are same when diaphragm is complete and incomplete.

Figure 4.3. (A) Regression of Run 1. (B) Regression of Run 2. 'a' stands for slope; 'b' stands for intercept on excursion axis.
Figure 4.4. (A) Regression of Run 1 and Run 2. (B) Comparison between real tidal volume and predicted value of test dataset.

Table 4.4. Prediction Error using 3 Heuristic methods (L)

<table>
<thead>
<tr>
<th>Heuristic methods</th>
<th>User 1</th>
<th>User 2</th>
<th>User 3</th>
<th>User 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principle direction</td>
<td>0.0794</td>
<td>0.1032</td>
<td>0.1852</td>
<td>0.1471</td>
</tr>
<tr>
<td>Centroid of mass</td>
<td>0.1110</td>
<td>0.1223</td>
<td>0.1737</td>
<td>0.1624</td>
</tr>
<tr>
<td>Minimum-area-rectangle</td>
<td>0.1007</td>
<td>0.1672</td>
<td>0.1571</td>
<td>0.1770</td>
</tr>
</tbody>
</table>

Figure 4.5. (A) Comparison of three heuristic methods when diaphragm is incomplete. (B) Incompleteness of diaphragm caused by brightness.
4.2 Performance of Privacy-preserving Deep Learning Module

4.2.1 Dataset

A Human Activity Recognition dataset is used to evaluate the proposed system. The dataset contains recordings of 30 volunteers performing activities of daily living (ADL) while carrying a waist-mounted smartphone with embedded inertial sensors. The activities are composed of six basic activities (standing, sitting, lying, walking, walking downstairs, and walking upstairs) and six postural transitions that occurred between the static postures (stand-to-sit, sit-to-stand, sit-to-lie, lie-to-sit, stand-to-lie, and lie-to-stand). There are 10299 samples in the dataset and these samples are randomly partitioned into two parts, where 70% are training data and 30% are the test data. The raw data is sampled with a slide window of 50% overlap. In each window, 561 features are extracted.

4.2.2 Experiment Setup

The distributed architecture is implemented with Torch7 on a XMPP (global server) and several mobile devices (local sites). The mobile device can be smartphones, tablets, or any computing modules as long as they support Torch7. In this paper, local deep learning training algorithm is run on surface book. The global server is implemented on a XMPP server. Experiments in the scenarios with 3, 5 and 7 local devices are performed for different combinations of deep learning algorithms (CNN and MLP) and parameter exchange protocols (round robin and asynchronous). The training dataset is split into \( n \) parts as the local dataset. \( n \) is the number of local sites.
We verify two deep neural network algorithms (CNN and MPL) in the collaborative privacy-preserving architecture. Architectures of the two deep neural networks are designed with Torch7 nn package and shown in Figure 4.6. The input is processed data with 561 features and the output is predicted labels of 12 activities. The networks are trained by SGD. The mini-batch size is 100. In the following experiments, we evaluated the performance of proposed CPDL in two aspects: reconstructed rate with different fraction of parameter selection and network traffic. The centralized deep learning trained by mini-batch SGD on entire dataset is used as baseline. We compare the results of centralized and decentralized learning to verify how privacy preserving mechanism affects deep learning performance. The network traffic is monitored with one of the most popular network security analysis tool: wireshark. The network traffic is measured by summing up the length of captured packets.

We proposed a metric, reconstruction rate, to compare the performance of learned classifiers in centralized and decentralized architectures, which is different from accuracy. Accuracy is computed based on predicted result and real labels (ground truth). However, it cannot well reflect how decentralized architecture and parameter selection

Figure 4.6. The left sub-figure is CNN architecture with 12 layers; The left sub-figure is MLP architecture with 10 layers.
mechanism affect the performance compared with centralized learning. Reconstruct rate is defined by equation 4.1

\[
\text{reconstructRate} = \frac{\text{number}(\{x : x \in T_d \cap x \in T_c\} \cup \{x : x \in F_d \cap x \in F_c\})}{\text{number}(S)}
\]  

(4.1)

where \(T_d\) is the set of instances correctly classified by decentralized learning scheme, while \(T_c\) is the set of instances correctly classified by centralized learning scheme. \(F_d\) is the set of instances incorrectly classified by decentralized learning scheme, while \(F_c\) is the set of instances incorrectly classified by centralized learning scheme. \(S\) is the whole dataset. \(\text{number()}\) is the function, which gives the total number of elements in a set. Higher reconstruct rate indicates that the privacy-preserving decentralized deep learning architecture works better.

### 4.2.3 Parameter Exchange Sequence

In our experiment, we evaluated the parameter exchange sequence sequentially and asynchronously. For each update order, two deep learning algorithms, CNN and MLP, are implemented. In this experiment, reconstructed rate are used to show the performance of CPDL compared with centralized training.

Figure 4.7 shows the reconstruction rates at different fraction of selected parameter for sharing when the decentralized architecture contains several local sites. The fractions are chosen at 0.0001, 0.001, 0.01, 0.1, and 1. Figures on the left show the results of CNN algorithm and those on the right are the results of MLP algorithm. The experiments are repeated using the decentralized architecture containing 3 local sites, 5 local sites, and 7 local sites. The results of centralized SGD mini-batch training for CNN and
MLP are used as baseline. When the fraction is 1, the reconstruction rate of decentralize training using Round Robin is 100%, which means that when every participants upload all their results sequentially, the MLP and CNN models trained in distributed system is exactly the same with the models trained in centralized system. The results of round robin and asynchronous are very similar. Furthermore, the figure shows that performance of decentralized system does not decrease too much when the sharing fraction decreases. The reconstruct rate stays around or above 90% when select fraction varies from 0.01 to 1 and starts decreasing from 0.01 to 0.0001. Finally, by comparing MLP and CNN, it is found that the fraction of parameter selection has greater impact on the performance of MLP than CNN. At fraction 0.0001, reconstruct rate of MLP decreases by 20%, however, CNN only decreases by 10%.

4.2.4 Network Traffic

While collaboratively training activity classifier, the transmitted packets between global server and local sites is captured using wireshark. The transferred data includes weight parameters of neural network, gradients, and messages for checking status of global server and local sites. The network traffic of different learning architectures are measured by cumulating the length of packets. The traffic cost in distributed system with 5 local sites is an example to show the results (see Figure 4.8). The selected fraction is 100%. 'x axis' shows the percentage of finished job. 'y axis' is the amount of cumulative transmitted data when $n\%$ of training jobs are finished. In this experiments, four combinations of deep learning algorithms and parameter exchange protocol are evaluated: distributed MLP trained in round robin order, distributed MLP trained in asynchronous order, distributed CNN trained in round robin order, and distributed CNN trained in
Figure 4.7. Reconstruct rate of decentralized MLP and CNN containing 3, 5, 7 local participants. The legends are different update orders. 'Centralized mini-batch' means each SGD batch is pooled from all training data.

asynchronous order. For the four combinations, the amount of cumulative transmitted data keeps increasing. The black dash line in Figure 4.8 shows the amount of data
transform for uploading all training data from all locals to global for one time. In our case, training a deep learning model using decentralized way causes more data transmission than centralized method. The reason is that the amount of one mini-batch data is smaller than the amount of weight parameters and computed gradients transferred during training one mini-batch data. If we increase the number of samples in one mini-batch or we use larger input, such as images or videos, the black dash line will go up. Decentralized method will cause less data transmission. Therefore, we cannot tell which method has lower burden on Internet network. It depends the size of min-batch and size of each training sample.

The figure also shows that the network traffic of MLP (the blue line and the red line) is larger than CNN (the yellow line and purple line). This is because the designed deep learning architectures of MLP have more parameters to train than CNN, thus more data need be exchanged in each round (downloading from global server to a local site and uploading that local site to global server). Furthermore, deep learning models trained in asynchronous order (the red line and purple line) have higher network traffic than it in round robin order (the blue line and yellow line), which is caused by our communication mechanism between global server and local sites. In asynchronous uploading order, before uploading newly trained gradients, local site will send some messages to check the free status of server and server will send responses. This step causes extra data transmission. Therefore, the network traffic of CPDL depends on the architecture of network and extra communication between local site & server.

If CPDL only transfers partial parameters, the network traffic will reduce. Therefore, we also evaluate the affect of parameter selection on network traffic, and results
Figure 4.8. Five local participants training with 4 different combination of deep learning algorithm and parameter exchange protocol.

are shown in Figure 4.9. It can be observed that the lower fraction of parameter selection is, the less traffic the training process generates. The amount of transferred data at 'Fraction=1' is the largest (blue line), and the amount at 'Fraction=0.0001' is the smallest (green line). Therefore, parameter selection does not only have benefit for preserving privacy of personal data, but also can reduce traffic load on Internet.

Figure 4.9. Five local participants training in CNN with different selection fraction.
5 Discussion

5.1 Imaging Processing Module

The experiments demonstrate feasibility and accuracy of the tidal volume estimation system and three heuristic methods that automatically compute diaphragm excursion. The quality of ultrasound videos affects diaphragm detection.

During the measurement, users might record videos contain irrelevant tissue and organ around diaphragm, and unwanted brightness caused by partial detachment of the ultrasound probe. For the diaphragm detection, there are 3 typical kinds of failures: mis-detection, non-detection, and combination of both. Non-detection is caused by the incompleteness of diaphragm image. Figure 5.1(A) shows an example of non-prediction, the bright area covers the diaphragm and only a small portion of it appears in the image (where the arrow points), which makes it unable to be detected. In this case, nothing is detected in the image. Mis-detection is usually caused by the tissue or organ that has similar shape to diaphragm (Figure 5.1(B)). Figure 5.1(C) is the combination situation. The diaphragm is incomplete because of the coverage of the brightness, so it is not detected. However, there is a white curve similar to the diaphragm in shape, so it is detected.
Moreover, different location and angle where the probe is placed influence the average error between the predicted tidal volume and the record of spirometer greatly. For example, the average error of User 3 was larger than the errors of User 1 and 2. In the first test ultrasound video (test 1) of User 3, the location of diaphragm between two adjacent key frames are generally longer than the distances in other videos, while the tidal volume does not change largely. This is because the probe was shifted or the angle of the probe was changed when collecting test1 comparing with the setting in collecting other videos. Figure 5.2 shows the distance of diaphragm between two adjacent key frames of two videos. Images in the first line are from the test 1 and images in the second line are from one of the videos in train dataset, train 1. Figure 5.2(A) and Figure 5.2(D) are the end of inspirations, Figure 5.2(B) and Figure 5.2(E) are the end of expirations. Figure 5.2(C) and Figure 5.2(F) shows movement distances. Based on the spirometer records, the user inspired about 0.83L air from a to b and 0.82L air from d to e. However, it is obvious that the distance between two adjacent key frames in Figure 5.2(C) and Figure 5.2(F) are different. The excursion distance from a to b in Figure 5.2(C) is 144.5 pixels, while the distance from d to e based on Figure 5.2(F) is 23.99 pixels. For further study, as
mentioned in Capriglione’s research\textsuperscript{50}, probe position tracking system and angle management system, consists of different kinds of accelerators, can be added on the probe to assistant the data collection. For each user, based on the position and angle the probe was placed, different regression models can be build to improve accuracy.

![Image](image_url)

Figure 5.2. (A) The location of diaphragm at the end of inspiration in test 1. (B) The location of diaphragm at the end of expiration in test 1. (C) A combination of (A) and (B), which s the locations of diaphragm at one end of inspiration and the following end of expiration; this image shows an excursion distance in test 1. (D) The location of diaphragm at the end of inspiration in train 1. (E) The location of diaphragm at the end of expiration in train 1. (F) A combination of (D) and (E), which shows the locations of diaphragm at one end of inspiration and the following end of expiration; this image shows an excursion distance in train 1.

Finally, the failure in using spirometer might also reducing the accuracy of prediction results. For example, when User 4 was measuring his/her tidal volume by spirometer, some air breathed out was leaked. Therefore, the recorded volume was smaller than the real volume, as shown in Figure 5.3. Therefore, the result is not as good as the rest of the Users.
Figure 5.3. The tidal-volume of User 4. The fluctuation is smaller than the real condition because the air breathed out was leaked when using by the spirometer.

5.2 Privacy-preserving Deep Learning Module

In the proposed system, mini-batch SGD is performed, which is much faster than batch gradient descent. However, frequent updates with a high variance may cause the objective function to fluctuate. During performing experiments, we found that the classifying results and trained parameters are slightly different when the initial parameters and input sequence change. The accuracy will fluctuate with a small range [-1%,+1%]. We also find that the line of reconstruct rate for each parameter exchange protocols is not monotone decreasing alone with the decreasing of selected fraction. The figure of "7 Local sites using MLP" on the lower right corner of Figure 4.7 is an example. The red line shows the results in asynchronous scenario. The reconstruct rate at 0.1 is higher than it at 1. This is because the global model with selected mechanism can converge to a point around minimum. This point is more closed to global minimum than the model trained without weight selection. Therefore, we cannot tell the model at fraction 1 must be better than it at fraction 0.1 and 0.01.
Another observation is that only using very small fraction of gradient to update parameters, the performance still can be guaranteed. This is because that different weight has different sensitivity to the cost function. The sensitivity of the cost function with respect to a individual weight at each iteration depends on two factors: the shape of the mean-square error (MSE) surface and the location of that weight at that distance relative to the bottom of the MSE surface. This sensitivity is reflected in the steepness of the gradient vector components. Those weights with large gradient on the error surface result in considerably large contribution to the reduction of the overall mean square error. Therefore, when the sensitivity of a particular weight is smaller than a pre-defined threshold, we think this weight is not important and can be ignored. We filter out gradients with very small contribution for reducing the error, which won't affect the accuracy very much.
6 Future Research

I explored a personal health monitoring system based on ultrasound devices and collaborative deep learning architecture. It still has space to improve the work in the following parts.

First of all, as discussed in Section V, the location and angle of probe can influence the quality of diaphragm image. A well-trained user can easily find the right place to detect a complete and clear diaphragm. However, in home environment, user usually does not have too much experience. A instructing mechanism for probe adjustment is needed. As mentioned in Capriglione’s research, probe position tracking system and angle management system, consists of different kinds of accelerators, can be added on the probe to assistant the data collection. In the future, based on the position and angle the probe was placed, different regression models can be built to improve accuracy. The detected position and angle also can assist user to find clear diaphragm image in good quality. When the user put the ultrasound probe inappropriately, the system could provide instructions, such as ‘move to the right’ and ‘move to the left’.

Furthermore, ultrasound could be used to visualize heart movement. We can explore algorithms to process heart ultrasound image and extract hear information, such as heart beat. The more information we have, the more health status can be monitored.
and more disease can be detected using privacy-preserving deep learning architecture. However, heart detection is much difficult than diaphragm detection. As shown in Figure 6.1, the shape of heart is more complicated and vague than the shape of diaphragm which is an arc. In addition, The shape of heart varies a lot from different position and angle of probe, as shown in Figure 6.1 (B), (C), and (D). Therefore, a more powerful image processing algorithm is need. We will try to improve Chan-Vese or figure out a new one which can deal with complex and various shape.

![Figure 6.1. Ultrasound images of diaphragm and heart. (A) Ultrasound diaphragm. (B) Ultrasound heart in parasternal short axis view. (C) Ultrasound heart in parasternal long axis view. (D) Ultrasound heart in apical view.](image)

Finally, CNN and MLP deep learning algorithm is usually used to deal with data that each training sample is independent. They are not suitable for time-series data. For example, time-series data is collected while performing activities. The way used currently is using a slide window and feature extraction computation to convert a piece of time-series data into one independent sample. One drawback of this way is that the relation
information between frames or samples in raw data cannot be effectively used. Recurrent neural network (RNN)\textsuperscript{53} and long short term memory (LSTM)\textsuperscript{54–56} might be good solutions. They are networks with loops in them, allowing information of previous data to persist. Besides the network parameters, RNN and LSTM also keep a hidden state. They pass a hidden state between timesteps, so at each interval they produce an output based on the input at that timestep and the state at the previous timestep. Implement RNN and LSTM in the privacy-preserving deep learning architecture could be the next step of research, which might deal with time-series data more effectively.
7 Conclusions

In this thesis, I studied on an ultrasound based home monitoring system with privacy-preserving deep learning architecture. The accuracy of diaphragm detection, respiratory rate measurement, and tidal volume estimation was evaluated using three experiments. The error between computed respiration rate and ground truth is less than 0.5 times/minute. The accuracy of diaphragm detection is over 96%, and the error of predicted tidal volume is about 0.1L compared with results measured by spirometer. In the proposed architecture, privacy of user is protected from two levels. First, local data is not collected in one large data warehouse. Second, only very small fraction of information of local deep learning model is shared using parameter selection. To evaluate the performance of the proposed architecture, we conducted two experiments. The results show the proposed architecture performs well in different scenarios. The reconstruction rate could keep around 90% compared with centralized training. We also measured the network burden and analyze the factors that may cause high network traffic. These results verify the feasibility of applying collaborative learning in distributed personal healthcare environment.
**NOTICE OF APPROVAL**

CWRU IRB Protocol Number: IRB-2016-1504  
Protocol Title: *Skin Condition Profiling and Physiological Traits Measurement for Evidence-based Wound Care*  
Responsible Investigator (RI): Ming-Chun Huang  
Co-Investigator (CI): Soumyajit Mandal, Ph.D.  
RI Department: Case Western Reserve University IBC and SBER IRB - ENG - Electrical Engineering and Computer Science  
Type of Review: Expedited  
Risk Level: Minimal  
Vulnerable Population(s): None  
Approval Date: 04/22/2016  
CONTINUING REVIEW DEADLINE: 04/07/2017  
EXPIRATION DATE: 04/21/2017

The CWRU Institutional Review Board (IRB) has approved the above new protocol through the **EXPEDITED** review process.

When conducting Human Subjects’ Research, your responsibilities include the following:

1. Report all adverse events and unanticipated problems involving human subjects to the IRB Office, located in the Office of Research Administration (ORA), within three (3) business days of your knowledge of the occurrence.
2. Provide the IRB with a complete Continuing Review form (available in our electronic application system at [http://sberirb-app.case.edu](http://sberirb-app.case.edu), or from the ORA) by the continuing review deadline noted above, and when the study is to be terminated.
3. Submit all proposed changes to the protocol to the IRB and wait for IRB approval before implementing any protocol change or modification.
4. Keep all research data and original consent documents in your possession for at least three (3) years after the study is terminated.
5. Note that completely de-identified data can be kept and used for research indefinitely. The IRB is primarily concerned about identifiers/identifiable data.  If you want to terminate your study, identifiers/identifiable data must be destroyed.  This includes paper or electronic master lists, contact lists, codes/codebooks, transcripts containing identifiers and video and audio recordings.
6. If applicable, please use the most current IRB-approved consent forms.  Feel free to use copies of these forms as long as they are identical to what was originally IRB approved.  If you wish to change the forms or any other part of the study, you must submit an addendum request/protocol modification with revised copy(ies) of the relevant document(s) and wait for IRB approval before a modification can be implemented.
7. **Discontinue all work pertaining to this protocol if a continuing review approval is NOT finalized by the expiration date noted above.**  No further work on this protocol is allowable until the proper continuing review materials or required revisions are approved by the IRB.
   a. Please note that, if the continuing review materials or required revisions are not received by the expiration date, the RI and this study would be automatically placed on Administrative Hold for 30 days.  This means that the RI loses their IRB privileges and research from this study must cease.
   b. If after 30 days, the CWRU IRB still does not have the protocol for processing, this protocol will be administratively terminated and your IRB privileges will be revoked for all your protocols.

Thank you for your attention to this matter. Please contact the IRB office at 216-368-6993 if we can be of further assistance.
Complete References


