Hindawi
Security and Communication Networks
Volume 2020, Article ID 6626471, 10 pages
https://doi.org/10.1155/2020/6626471

Research Article

Fed-SCNN: A Federated Shallow-CNN Recognition Framework for Distracted Driving

Yaojie Wang,[1] Xiaolong Cui,[1] Zhiqiang Gao,[1] and Bo Gan[2]

[1] *Counter-Terrorism Command Information Engineering Research Team, Engineering University of PAP, Xi'an 710086, China*
[2] *School of Information Engineering, Engineering University of PAP, Xi'an 710086, China*

Correspondence should be addressed to Yaojie Wang; wangyaojie0313@126.com

Received 19 October 2020; Revised 4 November 2020; Accepted 9 November 2020; Published 21 November 2020

Academic Editor: Nanrun Zhou

Although distracted driving recognition is of great significance to traffic safety, drivers are reluctant to provide their own personalized driving data to machine learning because of privacy protection. How to improve the accuracy of distracted driving recognition on the basis of ensuring privacy protection? To address the issue, we proposed the federated shallow-CNN recognition framework (Fed-SCNN). Firstly, a hybrid model is established on the user-side through DNN and shallow-CNN, which recognizes the data of the in-vehicle images and uploads the encrypted parameters to the cloud. Secondly, the cloud server performs federated learning on major parameters through DNN to build a global cloud model. Finally, The DNN is updated in the user-side to further optimize the hybrid model. The above three steps are cycled to iterate the local hybrid model continuously. The Fed-SCNN framework is a dynamic learning process that addresses the two major issues of data isolation and privacy protection. Compared with the existing machine learning method, Fed-SCNN has great advantages in accuracy, safety, and efficiency and has important application value in the field of safe driving.

1. Introduction

With the rapid development of the economy, the frequency of traffic accidents is increasing year by year. Distracted driving is one of the main causes of traffic accidents [1]. Recognition based on distracted driving is a problem that needs to be solved urgently. Distracted driving is driving while doing another activity that takes your attention away from driving, such as editing SMS and calling, which seriously threatens traffic safety. According to the National Highway Traffic Safety Administration (NHTSA), nearly 30% of traffic accidents in the United States are related to driving distraction [2]. Due to the fast speed of the car, when the driver edits WeChat while driving, his sight will leave the road for about 4 seconds, almost covering the length of the football field at 60 mph.

With the indepth study of machine learning (ML), the classification algorithms represented by SVM [3, 4], AdaBoost [5], and Bayesian networks [6, 7] are widely used in the field of distracted driving, the core of which is to extract latent association features to identify distracted driving. Although the simulation experiment has achieved good results, it is limited by various conditions, and the actual effect is poor [8]. Therefore, the recognition of distracted driving still faces two major challenges [9]:

Driving behavior data involve personal privacy issues, which often exist in the form of islands, and a large number of data owners are reluctant to share

The large amount of data produced by users each day is limited by the environment of mobile driving, resulting in poor interactivity and hindered data communication.

Based on the above two challenges, the recognition of distracted driving cannot obtain the data of a large number of users in practical applications, which seriously restricts the development of this research.

With the promulgation of the General Data Protection Regulation (GDPR) [10] in EU, the traditional method of sharing private data was banned, and a large amount of isolated data could not fully enjoy the dividends brought by big data and cloud computing, which caused a great waste of resources. Fortunately, federated learning (FL) [11], a new distributed ML framework, was proposed by Google, which not only meets the needs of privacy protection but also fully participates in large-scale machine learning. Since then, many research institutions have also begun to study FL [12–14], especially in the fields of finance, medical care, and advertising, which have achieved many impressive achievements.

Based on this, a federated shallow-CNN [15] recognition framework for distracted driving (Fed-SCNN) is proposed. Firstly, a hybrid model is established on the user-side through deep neural networks (DNN) [16] and shallow-CNN, which recognizes the data of the in-vehicle images and uploads the encrypted parameters to the cloud. Secondly, the cloud server performs FL on major parameters through DNN to build a global model. Finally, the DNN is updated in the user-side to further optimize the hybrid model. The above three steps are cycled to iterate the local hybrid model continuously. Fed-SCNN can not only protect personal privacy and effectively solve the problem of data islands but also have higher recognition accuracy, which has important application value in the field of safe driving, which provides a new idea for distracted driving. The framework proposed in this paper is a dynamic learning process, which not only continuously enhances the recognition ability of distracted driving on the basis of privacy protection but also can support users to join friendly, which has better scalability.

2. Related Work

2.1. Overview of Federated Learning. Federated learning is an emerging technology of ML, which was first proposed by Google in 2016. The key idea is to protect user data during the process [12]. As a distributed ML method, it supports model training on large corpus distributed data. The training process is to fit the global optimal statistical model through the combination of training parameters, which can be expressed as minimizing the following objective function:

$$\min_{w} F(w),\quad \text{where } F(w) \coloneqq \sum_{k=1}^{m} p_k F_k(w), \tag{1}$$

where m is the total number of devices, $p_k \geq 0$, and the sum of p_k is 1; $F_k(.)$ is the objective function of the k-th device. The local objective function is often defined as empirical risks related to local data, i.e., cross-entropy. Federated learning is expected to become the basis for the next generation of collaborative computing [13]. Since the advent of federated learning, a variety of research studies based on FL have emerged, e.g., privacy-preserving ML [17], federated multitask learning [18], as well as personalized federated learning [19]. The scene containing two data owners (e.g., enterprises A and B) is taken as an example to introduce the architecture of federated learning. The specific architecture principle is shown in Figure 1.

The advantage of federated learning is that private data never leave the local area, which meets the needs of user privacy protection. At the same time, it can take advantage of big data to effectively solve the problem of data islands, which guarantees that federated models are better than isolated models in machine recognition.

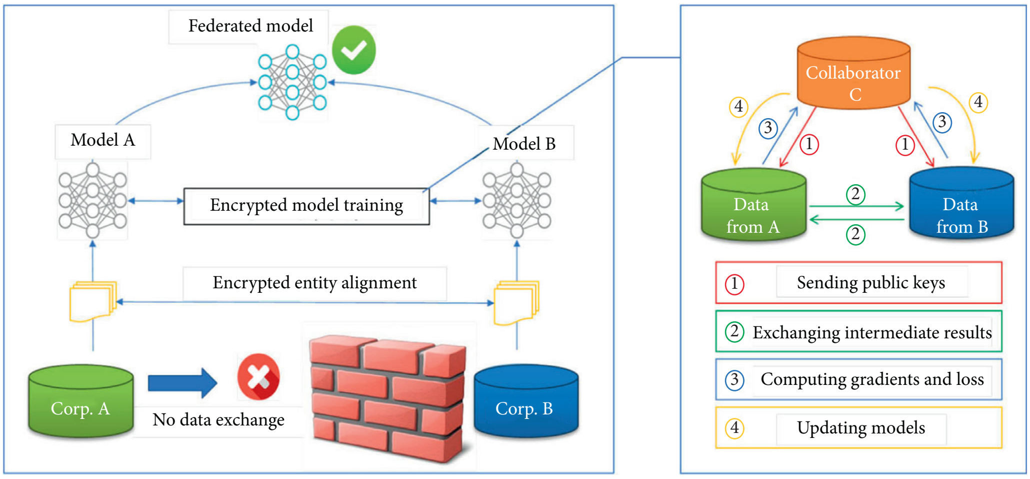
According to the distribution of user data dimensions, Yang et al. [13] divided federated learning into three categories: horizontal federated learning (HFL), vertical federated learning (VFL), and federated transfer learning (FTL). Fed-SCNN belongs to federated transfer learning category. It is the first of its kind tailored for distracted driving.

2.2. Recognition of Distracted Driving. Rao et al. defined the distracted driving as a dangerous behavior in which drivers turn their attention to the activities unrelated to driving tasks, resulting in the decline in drivers' vision, consciousness, decision-making, and operational ability [20]. Distracted driving has a serious negative impact on normal driving, which leads to a large number of vicious traffic accidents every year. There are three main types of distraction [21]:

Visual: taking your eyes off the road
Manual: taking your hands off the wheel
Cognitive: taking your mind off of driving

Many experts and scholars have conducted lots of studies on the recognition of distracted driving. Yang et al. [22] used the vehicle motion parameters collected by the on-board GPS and established a Gaussian mixture model (GMM) to identify whether the driver was distracted. Jin et al. [23] collected vehicle data in the driving state through CAN and established a recognition model through SVM; Tango and Botta collected detailed operating dynamic parameters in the cab and used a variety of machine learning methods to identify distracted driving; Liang and Lee [24] found that distracted driving is highly time-dependent and proposed a dynamic Bayesian Network cognitive distraction detection model. Wollmer et al. [25] proposed an online driver distraction detection model, which utilizes long short-term memory neural network (LSTM-NN) to detect distraction status.

However, these studies are based on data collected under limited driving conditions or simulated driving environments, which leads to certain limitations. More seriously, the current research mainly considers the accuracy and efficiency of distracted driving recognition, but they ignore privacy protection, especially uploading personal privacy to the cloud, which also brings serious security risks [26]. For example, private data stored in the cloud may be stolen by cloud providers and other cloud clients. Therefore, this paper takes smart-mobile driving as the research background and fully considers the actual communication capabilities. It aims to solve the protection of personal privacy in the cloud environment through federated learning. At the same time, the shallow hybrid model is adopted by the user-side to identify whether the driver is distracted, which gives



(a)

(b)

Figure 1: The example of vertical federated learning architecture [13].

the necessary warning to prevent the potential risk of traffic accidents.

3. The Proposed Framework of Fed-SCNN

3.1. Overall Design of Fed-SCNN. In response to the two major challenges faced by distracted driving recognition, a federated shallow-CNN recognition framework for distracted driving (Fed-SCNN) was proposed. The proposed framework mainly includes two machine learning techniques: federated learning and shallow-CNN (SCNN). The former mainly uses distributed data to build a global statistical model through DNN to improve the recognition accuracy, and at the same time, upload the major parameters under the homomorphic encryption condition. Convolutional neural network (CNN) [27], which has the advantage of image feature extraction, is responsible for extracting user-side differentiated features, that is, the personalization of the local model. In order to take into account the loT hardware level, we decided to use SCNN to meet the needs of the current cab, which can improve the efficiency of recognition. The overall framework design is shown in Figure 2, which briefly expresses the process of Fed-SCNN.

During driving, the RGB image of the driver as the subject object, which is obtained through the built-in HD camera probe, is used as the input of the hybrid model. At the same time, it is assumed that the Internet of Vehicles can communicate with the cloud normally. The framework of Fed-SCNN is a dynamic process, the core of which is summarized in five steps:

(1) Local users independently perform recognition learning tasks through local DNN and SCNN

(2) Transmit the parameters of the local DNN model to the cloud in homomorphic encryption

(3) Establish a global cloud model in the cloud through federated learning

(4) Update local DNN parameters when requested by local users

(5) The fully connected layer of local DNN and SCNN is fused, and the final hybrid model is established after adjusting the parameters

The above is a brief introduction to Fed-SCNN for distracted driving. According to actual needs, it may be considered to regularly update the parameters of the DNN model, e.g., updating the major parameters once every night. The operation process is shown in Algorithm 1.

3.2. Federated Model. Inspired by the research of Rao et al. [20], this paper also focused on distracted driving recognition based on images of driving behavior. However, the current research studies mainly consider the accuracy of recognition and do not pay attention to privacy protection, especially uploading personal privacy to the cloud, which brings serious security problems. Therefore, the framework of Fed-SCNN performs the training and sharing of encryption model through federated learning. The key entities are mainly divided into the cloud and a large number of user-side. Major parameter information can be transmitted between the cloud and the user in encrypted form, while any information is not transmitted between the users, which leads to the phenomenon of data islands.

In this paper, we use deep neural networks to learn cloud models and user-side DNN models. DNN, which is essentially multiple linear regression, performs end-to-end feature learning and classifier training by inputting the user's original data. Considering the characteristics of federated learning, this paper makes significant improvements to local DNN network, that is, the major parameters before the last hidden layer are shared, and the parameters between the last hidden layer and the output layer are not shared. The detailed reasons are explained in the following section.

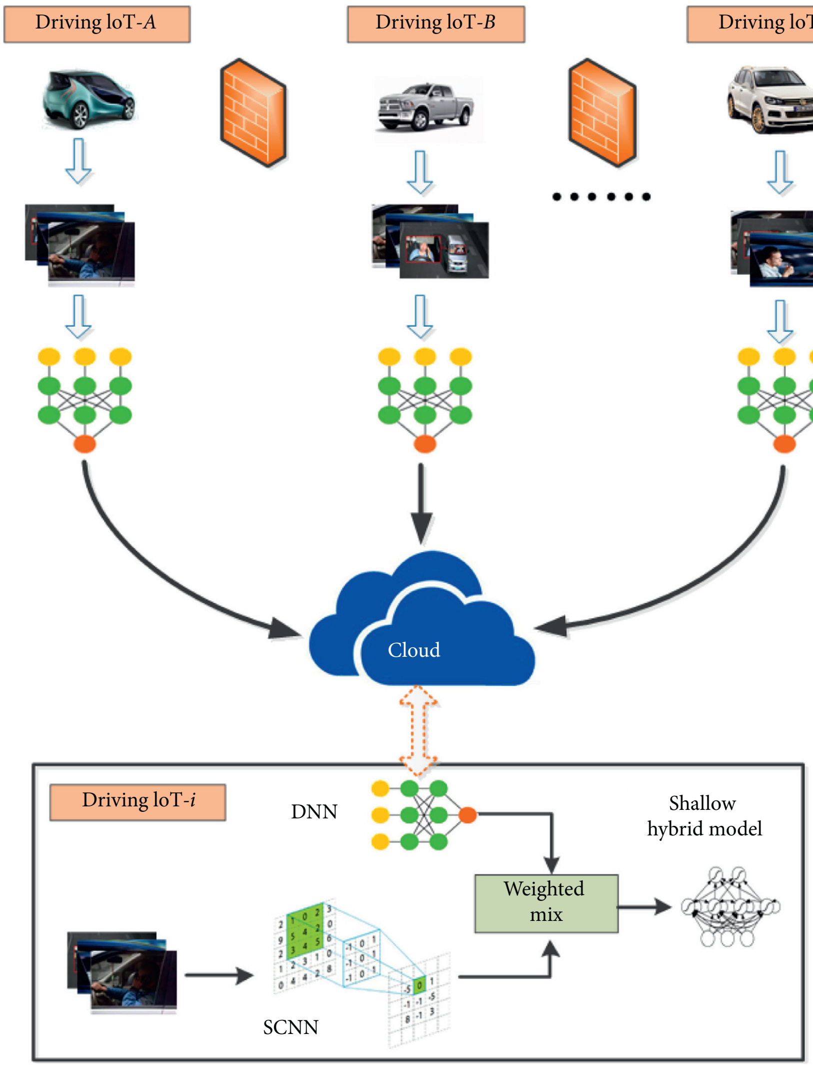


Figure 2: The overall framework design of Fed-SCNN.

3.2.1. Cloud Model. The cloud server uses public data and the parameters uploaded by the user to establish a global cloud model f_s. The objective optimization process during training can be expressed as

$$\arg\min_{\Theta} L = \sum_{i=1}^{n} l\left(y_i, f_s\left(x_i\right)\right), \qquad (2)$$

where $l(\cdot,\cdot)$ denotes the loss function of the training model, e.g., cross-entropy loss function. $\{x_i, y_i\}$ represents sample x_i, and the corresponding label y_i, n, denotes the sample size of public data. Θ represents the parameter matrix that needs to be learned, including the weights and bias of the hidden layers (the parameters between the last hidden layer and the output layer are not included). After the cloud model is established, the parameter Θ is distributed to all users.

3.2.2. User-Side DNN Model. The user also builds a local DNN model like the cloud model. The training process remains basically the same, except that the sample data are relatively small and belong to personal privacy data. For any user u, the local DNN model is expressed as f_u, and the objective function can be expressed as

$$\arg\min_{\Theta^u} L = \sum_{i=1}^{n} l\left(y_i^u, f_u\left(x_i^u\right)\right). \qquad (3)$$

As an important parameter of local DNN, Θ^u is uploaded to the cloud in the encrypted form. The cloud trains the parameter set $\{\Theta^1, \Theta^2, \ldots, \Theta^n\}$, to update the global cloud model and the parameter Θ, and then distributes the updated parameter Θ to all users. According to actual needs, local parameters can be updated regularly, such as daily updated once a night. The whole process above is a dynamic process of iterative optimization, which continuously improves the recognition ability of the model.

In addition, the parameter Θ in the communication process can avoid information leakage through homomorphic encryption [28]. Homomorphic encryption can operate in the ciphertext domain, which is suitable for cloud computing. This paper briefly introduces the addition homomorphism as an example, which is defined as follows.

```
    Initialize local DNN and the final model with random weights $\theta$ of DNN. Local SCNN has been trained;
Input: $n$: number of driving loT; $f$: update frequency
    while cloud server is running do
        $\theta_{nt} \leftarrow$ driving loT-$n$ performs DNN
        if $t\% \ f == 0$ then
            for $i = 0$; $i < n$; $i{+}{+}$ do
                Send $\theta_{it}$ to the cloud;
            end
            labels = Fed ($\theta_{1t}, \theta_{2t}, \ldots, \theta_{nt}$)
        end
        if service request = True then
            Generate $\theta_{\text{cloud}}$ base on labels; send $\theta_{\text{cloud}}$ to local users;
            $\theta_{\text{local}}$ = transfer ($\theta_{\text{cloud}}$)
        update DNN with $\theta_{\text{local}}$
            Final Model = mix{DNN, SCNN}
        end
    end
```

Algorithm 1: Processing algorithm in Fed-SCNN.

Definition 1 (addition homomorphism). The encryption function E satisfies

$$E(x+y) = E(x) \oplus E(y), \tag{4}$$

where x and y are not leaked in the whole process, so the algorithm $\oplus$ is homomorphic addition [29].

According to the characteristics of Definition 1, the weight matrix and the bias vector are operated in the encrypted, so that the original data will not be leaked, which meets the needs of Fed-SCNN.

3.3. Shallow Hybrid Model. Due to the limited driving environment, federated learning can effectively solve the problem of data islands to build a general model. But for distracted driving, another important issue is personalization. Even if we can use the global model through the cloud, its performance on specific users is still very poor because there is a distribution difference between any user and cloud data. At the same time, DDN can only learn common features, but it fails in learning the fine-grained information on a particular user.

For personalized difference learning, convolutional neural networks (CNN) can learn higher-level features in learning tasks, that is, personalized features can be learned on the basis of a general model. This method greatly improves the recognition accuracy at the expense of a small amount of computational efficiency, which can more accurately predict distracted driving.

Taking into account the hardware conditions of the loT, we decided to adopt a shallow-CNN (SCNN), which can reduce the dependence on high-performance hardware. As an important part of the shallow hybrid model, SCNN mainly extracts high-level features to make up for the shortcomings of the local DNN model. The following structural block of SCNN is represented by C2D-BN-LR: conv2d ⟶ batch normalization ⟶ leaky ReLU. The specific network structure of SCNN is: HPF ⟶ two C2D-BN-LR layers ⟶ one fully connected layer ⟶ sigmoid function.

After updating the local DNN model, the two networks are merged to obtain a shallow hybrid model, as shown in Figure 3. The last hidden layer in the local DNN is merged with the fully connected layer of the local SCNN, and then the output layer is connected. Through the fusion of the two models, we continually iteratively optimize and finally achieve local optimal prediction. For any user u, the objective function optimization process of the local mixed model can be expressed as

$$\begin{aligned} f_u\left(x_i^u\right) &= \text{soft}\max\left\{\langle \text{DNN}|t\text{SCNN}\rangle * \lambda_i\right\}_{\left(x_i^u\right)}, \\ \arg\min_{\lambda^u} L &= \sum_{i=1}^{n} l\left(y_i^u, f_u\left(x_i^u\right)\right), \end{aligned} \tag{5}$$

where softmax $\{\cdot\}$ is used as the output operation and $\langle\cdot|\cdot\rangle$ denotes the network fusion layer. It should be noted that λ represents the parameter matrix to be learned between the network fusion layer and the output layer. Through proper training and optimization of the shallow hybrid model, the final local recognition model can be obtained.

4. Experiment Analysis

4.1. Dataset. At present, there are few open source datasets for distracted driving, and the annotation quality of the datasets is poor [30]. Therefore, the simulation experiment in this paper first built its own dataset, which mainly includes three key steps: (1) collection of images set related to the recognition of the driver distraction behavior; (2) preprocessing images in the dataset; and (3) classification of data and marking. The experimental data mainly come from open source datasets such as ImageNet [31] and Open Images [32]. To prevent overfitting, we perform preprocessing operations on the data set, such as rotation, translation, and scaling, while the image size is cropped to 224 × 224 to reduce redundant data, which facilitates SCNN

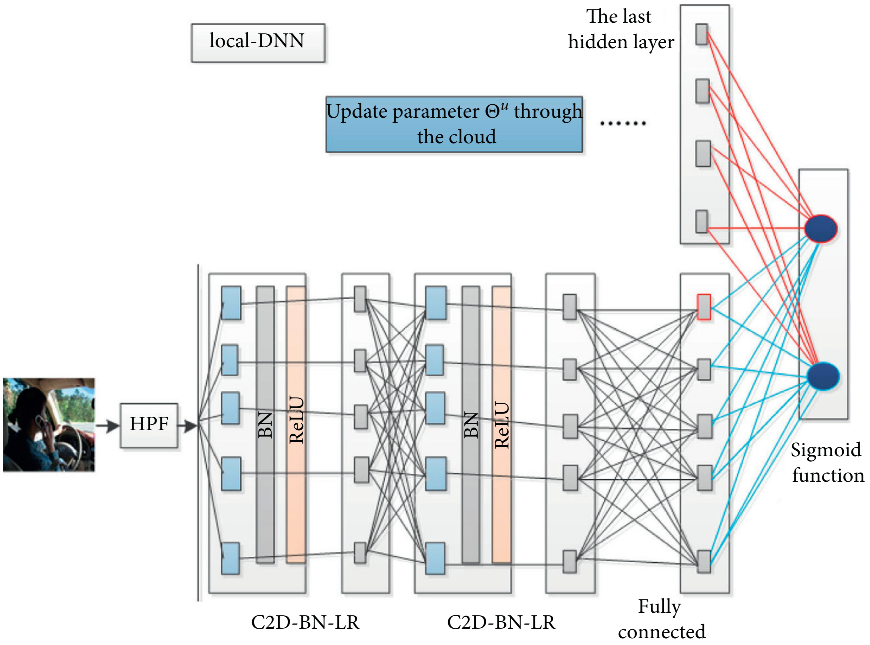


Figure 3: The principle structure of the shallow hybrid model.

analysis. The self-built data, a total of 4233 pictures, are divided into twelve different behavior categories, as shown in Table 1.

In general, each image corresponds to only one category. Figure 4 is an example of dataset classification. It should be noted that some sample images may also have multiple labels, for example, the driver makes a phone call with his right hand and leaves the steering wheel with left hand, which belongs to both $C3$ and $C12$. At the same time, in order to verify the experiment, the dataset is randomly divided into two parts, the training data occupies 90%, and the rest is used for testing.

4.2. Experimental Setup. In this experiment, both cloud and user perform DNN based on TensorFlow Federated Framework (TFF) [33]. At the same time, for users, SCNN is implemented through TensorFlow. The hardware environment is shown in Table 2.

For the local SCNN model, the optimization algorithm based on Adam is adopted, the learning rate is 0.0002, and the loss function is expressed in binary cross-entropy. Stochastic gradient descent (SGD) is used to iterate continuously during training samples. After the completion of the model, the test set is used to compare the recognition accuracy of shallow hybrid model, SCNN, and local DNN model.

4.3. Recognition Accuracy. Our results are shown in Figure 5. With the increase of training epochs, we compare the change of recognition accuracy of local DNN, SCNN, and hybrid model. The accuracy of the above three models is proportional to the iteration within a certain range. Figure 6(a) shows that when the epochs are greater than 130, the average accuracy of the local DNN reaches 67.5%. When it exceeds 169 epochs, the accuracy rate will not increase. The recognition accuracy of local DNN is still poor, but it has made progress compared with traditional decision trees and SVM. Figure 6(b) shows that the average accuracy of SCNN reaches 80.2% when the epoch is greater than 20. After more than 40 epochs, the accuracy rate of SCNN fluctuated slightly at 81%, which exceeded the local DNN model by nearly 14%.

Based on the above two independent experiments, the hybrid model is tested. Assuming that the parameters learned by FL in the local DNN are unchanged under 150 epochs, and based on the parameters learned by SCNN in 30 epochs, the results are shown in Figure 6(c). Over 5 epochs, the accuracy rate of Fed-SCNN can exceed 93%, and the average accuracy rate can basically maintain 95.3% after 15 epochs. In addition, the average detection time of each frame in Fed-SCNN is 597 ms, which has a high detection rate and meets the real-time requirements of risk warnings.

Furthermore, the parameters are optimized. On the basis of multiple experiments and debugging, the parameters are kept learned by FL in the local DNN which are unchanged under 150 epochs, and based on the parameters learned by SCNN in 50 epochs, after 18 epochs, the recognition accuracy of shallow hybrid model reaches 98.73%, as shown in Figure 5.

4.4. Algorithm Comparison. In order to verify the superiority of Fed-SCNN, the algorithm in this paper is compared with the traditional ML algorithm [20]. As shown in Figure 7, the accuracy of classic classification algorithms does not exceed 60%, such as decision trees, SVM, Naive Bayes, and MLP. The accuracy of CNN can reach 97%, but it depends on high-performance hardware. However, the accuracy of Fed-SCNN is far more than 95% under the condition of low

Table 1: Twelve categories of self-built dataset.

Category	Activity	Sample proportion (%)
$C1$	Safe driving	13.7
$C2$	Texting—right	12.5
$C3$	Right-hand call	14.5
$C4$	Texting—left	12.3
$C5$	Left-hand call	11.7
$C6$	Adjust automobile console	12.1
$C7$	Drinking	5.2
$C8$	Taking the back seat items	2.7
$C9$	Hair and makeup	6.7
$C10$	Talking to passenger	8.5
$C11$	Smoking	5.7
$C12$	Keeping your hands off the wheel	4.2

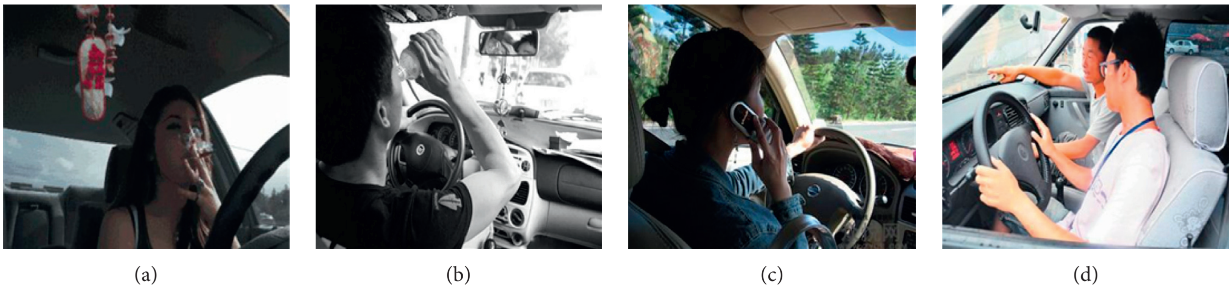

(a) (b) (c) (d)

Figure 4: The example of dataset classification: (a) smoking, (b) drinking, (c) right-hand call, and (d) talking to passenger.

Table 2: Experimental environment of software and hardware.

Cloud-server (one device)	Software platform	TensorFlow federated
	CPU	i7-8250U 3.2 GHz
	RAM	16 GB DDR4 1600 MHz
	GPU	NVIDIA 1080
User-side (three device)	Software platform	TensorFlow v 0.12
	CPU	i5-7500 1.8 GHz
	RAM	8 GB DDR4 1600 MHz
	GPU	NVIDIA 1080

hardware requirements. On the basis of 150 epochs of local DNN and 50 epochs of SCNN, the accuracy of the shallow hybrid model can reach 98.73% after 18 epochs, which fully reflects the advantages of Fed-SCNN in distracted driving recognition.

Under the condition of ensuring high accuracy, the training efficiency of Fed-SCNN and CNN scheme are compared. As shown in Figure 8, the average accuracy of Fed-SCNN quickly reached 95%, while the accuracy of CNN only reached 95% after 190 minutes of training. Therefore, it can be shown that Fed-SCNN is superior to the CNN scheme in terms of efficiency, which is more suitable for mobile driving hardware environment.

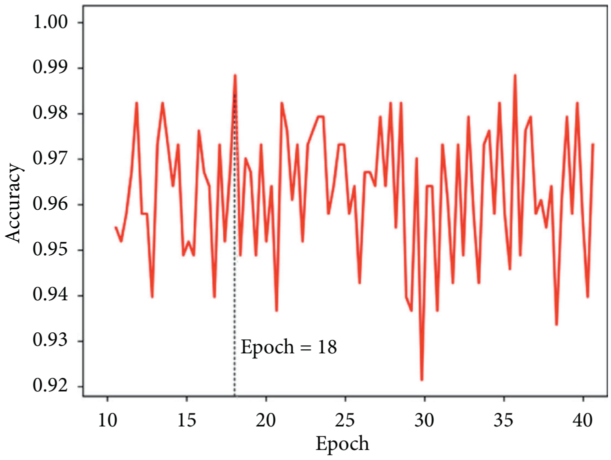


Figure 5: The change in the recognition accuracy rate of the shallow hybrid model after optimization.

4.5. Security Analysis. The security of Fed-SCNN is mainly based on two aspects:

(1) *Homomorphic Encryption*. The security of this paper is based on the privacy protection mechanism of federated learning. There are three main methods of privacy protection in federated learning: differential privacy, homomorphic encryption, and secure multiparty computing. Among them, homomorphic encryption

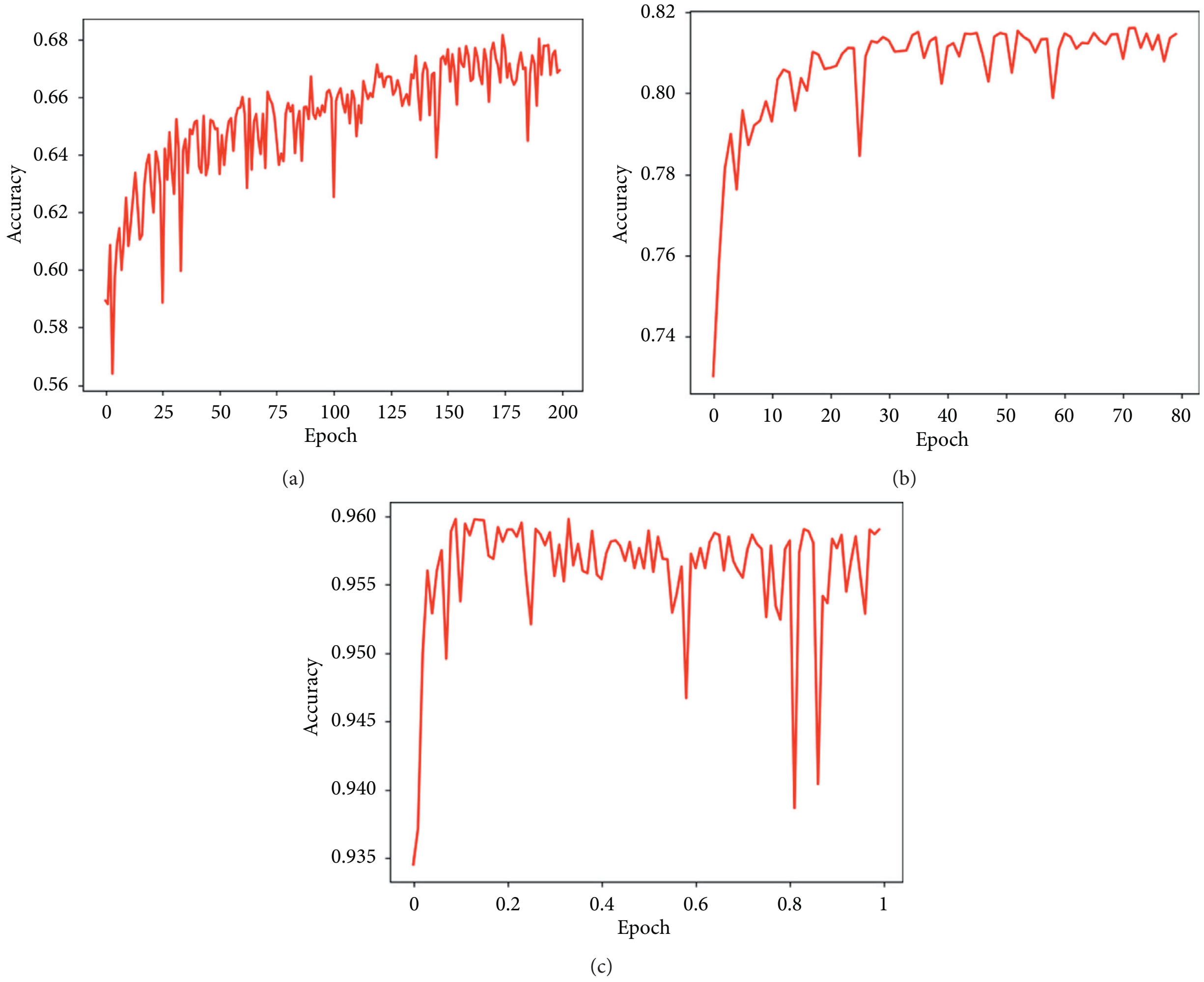
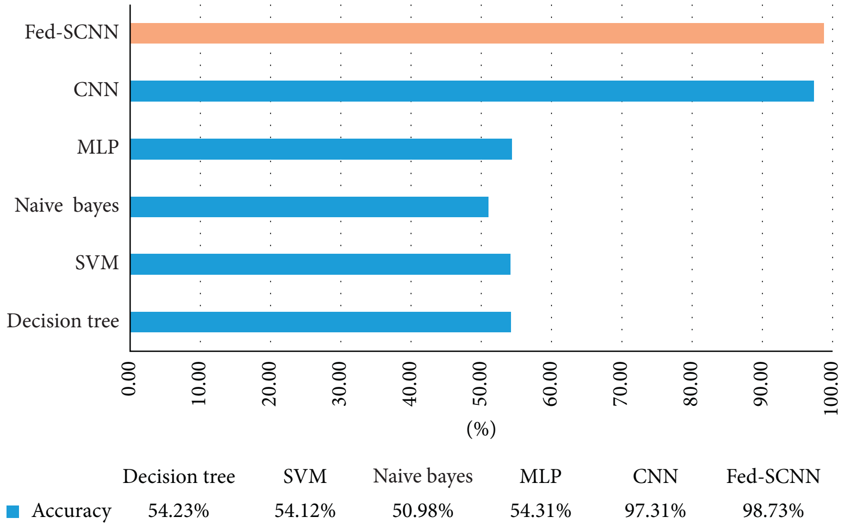


Figure 6: The relationship between recognition accuracy rate and epoch of three models: (a) local DNN, (b) SCNN, and (c) shallow hybrid model.



	Decision tree	SVM	Naive bayes	MLP	CNN	Fed-SCNN
🟦 Accuracy	54.23%	54.12%	50.98%	54.31%	97.31%	98.73%

Figure 7: The comparison of recognition accuracy between Fed-SCNN and other traditional ML algorithm [20].

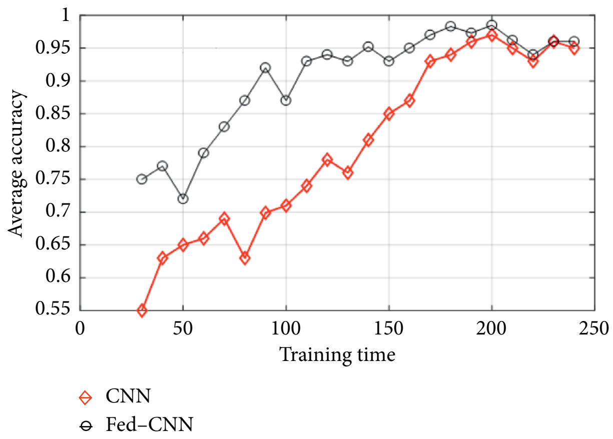


Figure 8: The efficiency of Fed-SCNN and CNN model training.

has the highest security. In this paper, the major parameters passed between the cloud and users are encrypted using additive homomorphism, that is, the security of the system depends on the confidentiality of the key, which fully complies with Kerckhoffs' principle [34].

(2) The data do not leave the local area, which is another advantage of federated learning, and meet the GDPR Act Requirements. In the communication process, only the important parameters of training are passed, e.g., gradient parameters. It is difficult to recover the original data by inverse operation under the existing technical conditions, which improves the safety of the data to a certain extent.

5. Conclusions

In this paper, a federated shallow-CNN recognition framework for distracted driving is proposed. For distracted driving, we innovatively propose a recognition method based on federated learning, which provides a new research idea for distracted driving recognition. The framework of Fed-SCNN is a dynamic learning process, which can solve the two major problems of data island and privacy protection. Compared with the existing ML methods, the recognition accuracy is higher. The experimental results show that Fed-SCNN has great advantages in accuracy, safety, and efficiency and has important application value in the field of safe driving.

On the basis of ensuring the accuracy of recognition, how to reduce the amount of calculation and improve the recognition efficiency of Fed-SCNN is the key research direction in the future.

Data Availability

The datasets used in this paper are mainly obtained through open source channels, such as ImageNet and open images, and downloaded from the dataset website: https://www.kaggle.com/c/state-farm-distracted-driver-detection.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (grant nos. U1603261 and U1636114), National Key R&D Program of China (grant no. 2017YFB0802000), and Natural Science Foundation Project of Xinjiang Province of China (grant no. 2016D01A080).

References

[1] K. J. Parnell, J. Rand, and K. L. Plant, "A diary study of distracted driving behaviours," *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 74, pp. 1–14, 2020.

[2] D. Ascone, T. Lindsey, and C. Varghese, "An examination of driver distraction as recorded in NHTSA databases," in *Traffic Safety Facts—Research Note,* NHTSA's National Center for Statistics and Analysis, Washington, DC, USA, 2009.

[3] Y. X. Wang, X. Z. Li, and Z. Y. Wang, "Parameters optimization of SVM based on the swarm intelligence," *Journal of Physics: Conference Series*, vol. 1437, Article ID 012005, 2020.

[4] L. Xin, "The research of intrusion detection of college room based on SVM," *Bulletin of Ence and Technology*, vol. 36, no. 10, pp. 85–91, 2012.

[5] Z. Z. Li, Q. H. Zeng, X. D. Li, and Y. Yu, "Face detection technology based on combining skin color model with improved adaboost algorithm," in *Proceedings of the IEEE 4th International Conference on Signal and Image Processing (ICSIP)*, Wuxi, China, July 2019.

[6] L. F. Gutiérrez, J. B. Bekios-Calfa, and B. K. Keith, "A review on Bayesian networks for sentiment analysis," in *Proceedings of the 7th International Conference on Software Process Improvement*, Guanajuato, Mexico, October 2019.

[7] D. Heckerman, "A tutorial on learning with Bayesian networks," in *Learning in Graphical Models,* MIT Press, Cambridge, MA, USA, 1999.

[8] F. A. Wilson and J. P. Stimpson, "Trends in fatalities from distracted driving in the United States, 1999 to 2008," *American Journal of Public Health*, vol. 100, no. 11, pp. 2213–2219, 2010.

[9] https://www.cdc.gov/motorvehiclesafety/distracted_driving/.

[10] K. A. Houser and W. Gregory Voss, "GDPR: the end of google and facebook or a new paradigm in data privacy?" *SSRN Electronic Journal*, vol. 56, no. 1, pp. 151–167, 2019.

[11] H. B. Mcmahan, E. Moore, D. Ramage, and B. A. Arcas, "Communication-efficient learning of deep networks from decentralized data," 2016, https://arxiv.org/abs/602.05629v3.

[12] J. Konečný, H. Brendan McMahan, F. X. Yu, P. Richtárik, A. T. Suresh, and D. Bacon, "Federated learning: strategies for improving communication efficiency," 2019, https://arxiv.org/abs/1610.05492.

[13] Q. Yang, Y. Liu, T. J. Chen, and Y. Tong, "Federated machine learning: concept and applications," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 2, pp. 1–19, 2019.

[14] K. Cheng, T. Fan, Y. Jin et al., "Secureboost: a lossless federated learning framework," 2019, https://arxiv.org/abs/1901.08755.

[15] S. Xu, Z. Lin, G. Zhang, T. Liu, and X. Yang, "A fast yet reliable noise level estimation algorithm using shallow CNN-based noise separator and BP network," *Signal Image and Video Processing*, vol. 14, no. 1, pp. 1–8, 2019.

[16] O. Abdel-Hamid, A. R. Mohamed, H. Jiang, L. Deng, G. Penn, and D. Yu, "Convolutional neural networks for speech

recognition," *IEEE/ACM Transactions on Audio, Speech, and Language Processing*, vol. 22, no. 10, pp. 1533–1545, 2014.

[17] Y. Chen, F. Luo, T. Li et al., "A training-integrity privacy-preserving federated learning scheme with trusted execution environment," *Information Sciences*, vol. 522, pp. 69–79, 2020.

[18] V. Smith, C. K. Chiang, M. Sanjabi, and A. S. Talwalker, "Federated multi-task learning," in *Proceedings of the Advances in Neural Information Processing Systems 30 (NIPS 2017)*, Long Beach, CA, USA, December 2017.

[19] R. Hu, Y. Guo, H. Li, Q. Pei, and Y. Gong, "Personalized federated learning with differential privacy," *IEEE Internet of Things Journal*, vol. 7, no. 10, p. 1, 2020.

[20] X. Rao, F. Lin, Z. Chen, and J. Zhao, "Distracted driving recognition method based on deep convolutional neural network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 8, pp. 1736–1746, 2019.

[21] https://www.nhtsa.gov/risky-driving/distracted-driving.

[22] J. Yang, T. Chang, and E. Hou, "Driver distraction detection for vehicular monitoring," in *Proceedings of the 36th Annual Conference on IEEE Industrial Electronics Society*, pp. 108–113, Glendale, AZ, USA, November 2010.

[23] L. Jin, Q. Niu, H. Hou, H. Xian, Y. Wang, and D. Shi, "Driver cognitive distraction detection using driving performance measures," *Discrete Dynamics in Nature and Society*, vol. 2012, Article ID 432634, 12 pages, 2012.

[24] Y. Liang and J. D. Lee, "A hybrid Bayesian Network approach to detect driver cognitive distraction," *Transportation Research Part C: Emerging Technologies*, vol. 38, no. 1, pp. 146–155, 2014.

[25] M. Wollmer, C. Blaschke, T. Schindl et al., "Online driver distraction detection using long short-term memory," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 2, pp. 574–582, 2011.

[26] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the Advances in Cryptology—EUROCRYPT 1999*, pp. 223–238, Prague, Czech Republic, May 1999.

[27] S. Lawrence and C. L. Giles, "Face recognition: a convolutional neural network approach," *IEEE Transactions on Neural Networks*, vol. 8, no. 1, pp. 98–113, 2002.

[28] T. Ristenpart, E. Tromer, H. Shacham et al., "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 199–212, Chicago, IL, USA, January 2009.

[29] A. López-alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*, pp. 1219–1234, New York, NY, USA, May 2012.

[30] S. Diegelmann, K. Ninaus, and R. Terlutter, "Distracted driving prevention: an analysis of recent UK campaigns," *Journal of Social Marketing*, vol. 10, no. 2, ahead-of-print (ahead-of-print), 2020.

[31] J. Deng, W. Dong, R. Socher et al., "ImageNet: a large-scale hierarchical image database," in *Proceedings of the Computer Vision and Pattern Recognition*, pp. 248–255, Miami, FL, USA, June 2009.

[32] A. Kuznetsova, H. Rom, N. Alldrin et al., "The open images dataset V4: unified image classification, object detection, and visual relationship detection at scale," *International Journal of Computer Vision*, vol. 128, pp. 1956–1981, 2018.

[33] https://tensorflow.google.cn/federated.

[34] http://www.crypto-it.net/eng/theory/kerckhoffs.html.