Journal of Computer and Communications, 2022, 10, 90-102
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Identity Authentication Based on Sensors of Smartphone and Neural Networks

Jingyong Zhu, Hanbing Fan, Yichen Huang, Miaomiao Lin, Tao Xu, Junqiang Cai, Zhengjie Wang*

College of Electronic and Information Engineering, Shandong University of Science and Technology, Qingdao, China
Email: 202001100737@sdust.edu.cn, 3406016832@qq.com, 1925582189@qq.com, 1925582189@qq.com, 3112152401@qq.com, 1742154051@qq.com, *cieewangzj@163.com

How to cite this paper: Zhu, J.Y., Fan, H.B., Huang, Y.C., Lin, M.M., Xu, T., Cai, J.Q. and Wang, Z.J. (2022) Identity Authentication Based on Sensors of Smartphone and Neural Networks. *Journal of Computer and Communications*, **10**, 90-102.
https://doi.org/10.4236/jcc.2022.107006

Received: July 4, 2022
Accepted: July 26, 2022
Published: July 29, 2022

Abstract

The smartphone has become an indispensable electric device for most people since it can assist us in finishing many tasks such as paying and reading. Therefore, the security of smartphones is the most crucial issue to illegal users who cannot access legal users' privacy information. This paper studies identity authentication using user action. This scheme does not rely on the password or biometric identification. It checks user identity just by user action features. We utilize sensors installed in smartphones and collect their data when the user waves the phone. We collect these data, process them and feed them into neural networks to realize identity recognition. We invited 13 participants and collected about 350 samples for each person. The sampling frequency is set at 200 Hz, and DenseNet is chosen as the neural network to validate system performance. The result shows that the neural network can effectively recognize user identity and achieve an authentication accuracy of 96.69 percent.

Keywords

Identity Authentication, Smartphone, Motion Sensor, Neural Network

1. Introduction

With the popularity and rapid development of science and technology, the smartphone has become an indispensable daily tool for many users. The smartphone is becoming a powerful assistant to help us finish much work, such as shopping, paying and reading. Besides, it is gradually becoming the core of the Internet of things. Therefore, its security is becoming a hot research topic since it is the premise of normal smartphone usage. Traditional authentication schemes, such as passwords or patterns, may be vulnerable to shoulder peeping and guessing

attacks by malicious people [1]. Due to the defects of traditional unlocking methods, researchers consider the biological feature as a new way to solve these problems. Among biological feature recognition approaches, iris recognition [2], fingerprint recognition [3], and face recognition [4] [5] achieve better effects, but they also have certain shortcomings. For example, the copied iris image can successfully cheat the iris reader. When we wear gloves or our hands with water, fingerprint recognition will also fail. Besides, fingerprint features can be easily copied using tape. Although 3D face recognition has higher security, the related attack technique has been proposed.

Currently, the performance of the smartphone is becoming more and more powerful. These smartphones contain many sensors with high precision, such as acceleration sensors, gyroscopes, gravity sensors, GPS modules, etc. These motion sensors can record the motion information of mobile phones. As a result, most behavior states can be captured when users use mobile phones, such as gait features or motion features. Therefore, we can utilize these features to realize identity authentication. Effectively extracting features from smartphones and making correct classification become a crucial problem. Deep learning technology has been widely used in computer vision, natural language processing, automatic driving, etc. In this paper, we employ a neural network to implement identity authentication for smartphone users by using built-in motion sensors of the smartphone. The neural network can analyze the differences between different people from the same behavior, improving security compared with physiological feature recognition. This scheme makes it possible to use the built-in sensor of the mobile phone for authentication by using human waving action.

1.1. Physiological Feature Recognition

In recent years, the research on identity authentication using the physiological feature is becoming a hot research topic. As an important identity feature, the iris has the advantages of uniqueness, invariance and collectability. Everyone's iris structure is unique and stable, and it will not change with the increase of people's age. Because of the above characteristics, the iris has become the most secure authentication method. At present, the iris acquisition mainly uses a CCD lens, which is large in size and high cost. Therefore, this scheme is not suitable for installation on mobile phones. And in the case of poor external lighting conditions, the accuracy of iris recognition will decrease seriously.

In addition, as the earliest physiological feature, the fingerprint identity recognition system has become increasingly mature. Fingerprint features are easier to extract than iris recognition, and the recognition accuracy is satisfied. However, verification of fingerprints requires dry fingers. In many cases, it is not convenient to unlock the mobile phone for this condition. Moreover, the fingerprint verification method has certain risks. Fingerprint features can be easily obtained from the door handle, mouse and water cup, which may lead to the leakage of user information.

With the development of deep learning and neural network, the effect of face recognition technology has reached a new level. Compared with fingerprint recognition and iris recognition, there is no additional hardware requirement because we can utilize the camera of mobile phones. However, face recognition technology also has its own defects. Face recognition technology has some error risks. When multiple faces have high similarity, the accuracy of recognition may decrease. Besides, the face information is open to the public. A photo can extract most of the features of the face, leading to the disclosure of user information.

To sum up, biological physiological feature recognition provides convenience and brings unsafe factors. Therefore, some researchers turn their attention to human behavior characteristics, especially gesture characteristics.

1.2. Behavior Feature Recognition

Human motion behavior characteristics can be applied in many fields, including gesture behavior [6], gait signal [7] [8] and keystroke dynamics [9] [10]. These behavior features can be used in identity authentication since they can represent the unique feature of each person. Compared with physiological features, it is more difficult for human behavior characteristics to be stolen, which can protect users' privacy more effectively.

1) Gesture behavior characteristics

Modern smartphones have integrated high-precision motion sensors, making it more feasible to study identity recognition using gesture behavior. When the user waves the mobile phone, the data generated by shaking the mobile phone, such as angular velocity and angular acceleration, they will be recorded by the internal motion sensor of the mobile phone, and the identity will be verified by comparing with the gesture characteristics inputted by the user.

2) Gait signal features

Every person has unique body characteristics, including limb muscle strength, bone density and center of gravity. The human motion model built by these features can be used to identify a person. The study [11] utilizes Kinect sensors to recognize user identity using gait features. Only gait features may not be enough if the environment is very complex or there are many persons in the test scenario because the noise and interference are very serious and cause feature extraction failure.

3) Keystroke dynamic characteristics

The human hand can finish complied activities. Therefore, the hand motion feature can be used to identify user identity. Specifically, dynamic keystroke features can be utilized for identity authentication because the keystroke habits of users can contain unique information using measurement data [12]. The studies [13] employ XGBoost algorithm implementation identity authentication based on differential classification learning and keystroke dynamics and achieve an accuracy of 90.91% in identity authentication.

Although many research results have been achieved, some issues must be solved. 1) The biometric information has more recognition accuracy, but the

acquisition of it may leak persons' privacy and require more hardware devices, leading to cost increases for mobile phone. 2) Behavior features do not involve personal privacy, but the recognition accuracy or response time may not be satisfactory. Therefore, the study of identity authentication for smartphones is an important problem for persons' information security.

Based on the studies of identity authentication of the smartphone, it is crucial that a user can implement identity recognition by using a simple action since this method can work under various scenarios. It can solve many existing problems requesting strict environmental conditions. Therefore, we propose a simple and effective identity authentication approach that requires a smartphone user to draw a circle in the air. The system recognizes the user using the motion feature from the smartphone's motion sensor and deep neural network. The contributions of this paper are summarized as follows. Firstly, we propose a smartphone identity authentication system using user waving action and a neural network. It achieves the recognition accuracy of 96.46 percent for 13 persons. Specifically, we utilize the smartphone's built-in motion sensors to collect data and feed the data into a neural network to implement identity authentication. We employ DenseNet to classify user identity. Secondly, we compare the recognition accuracy with other typical neural networks, including SqueezeNet and AlexNet. In addition, we analyze the effect of recognition accuracy with the training epoch. The results show that neural networks can be utilized as tools to implement identity recognition for user waving action. It also proves that the behavior feature of using a smartphone can be used to check user legal.

2. Background and Knowledge

This paper studied identity authentication using smartphones and neural networks. It collected motion data from the smartphone's built-in sensors and recognized user identity by training a neural network model. In this section, we introduced the background and knowledge of the system. It mainly included two parts, motion sensors and some related neural network models.

2.1. Motion Sensors

We utilized the human motion feature to implement identity recognition. Therefore, motion data play a great role in the system. These data come from the sensors built-in smartphone. So, the performance of these sensors is important for the system. In this system, motion sensors were chosen, including accelerometers, gyroscopes, direction sensors, gravity sensors and angular accelerometers. They can provide a vector of three-dimensional values and give us more information.

2.2. Neural Network

The neural network has been studied for many years. It has revitalized after the deep learning concept is proposed. Currently, deep learning and neural network

have been applied in many scenarios, including computer vision, natural language processing, intellectual driving, etc. [14]. Deep learning utilizes neural network models to implement abstract feature extraction and hidden feature representation. It can finish classification, regression and generation tasks and achieve perfect performance, especially for artificial intelligence applications [15]. We introduced some typical neural networks that had been applied successfully in other scenarios. We explained typical convolutional neural network (CNN), including AlexNet, SqueezeNet, and DenseNet. They are typical CNN and are widely applied in computer vision scenarios. We considered the motion sensor information as two-dimension matrix and classified the user identity using CNN.

1) AlexNet

AlexNet [16] is a classic convolution neural network, and it proposes many useful concepts that have been widely applied to other deep learning algorithms. The convolution operation is the core operation of deep learning since it can find abstract and hidden features. AlexNet includes many layers that implement different operations and functions, as shown in **Figure 1**. Specifically, it contains the input layer, convolution layer, pool layer, full connection layer and output layer. The basic working steps can be described as follows. Firstly, the input layer processes multidimensional data. Secondly, the convolution layer calculates convolution on the input data, and then the activation function is used for nonlinear mapping. Thirdly, the pooling layer extracts valuable features to reduce parameters. Finally, the final classification results will be calculated through the softmax function.

2) DenseNet

DenseNet [17] is another typical convolution network. It uses a dense connection mechanism to strengthen feature extraction. In other words, each layer is connected to all previous layers with the same channel size for feature reuse. It alleviates the problem of gradient disappearance. **Figure 2** is a typical density network consisting of many density blocks. There is a transition layer connection between each two adjacent density blocks. The transition layer uses convolution

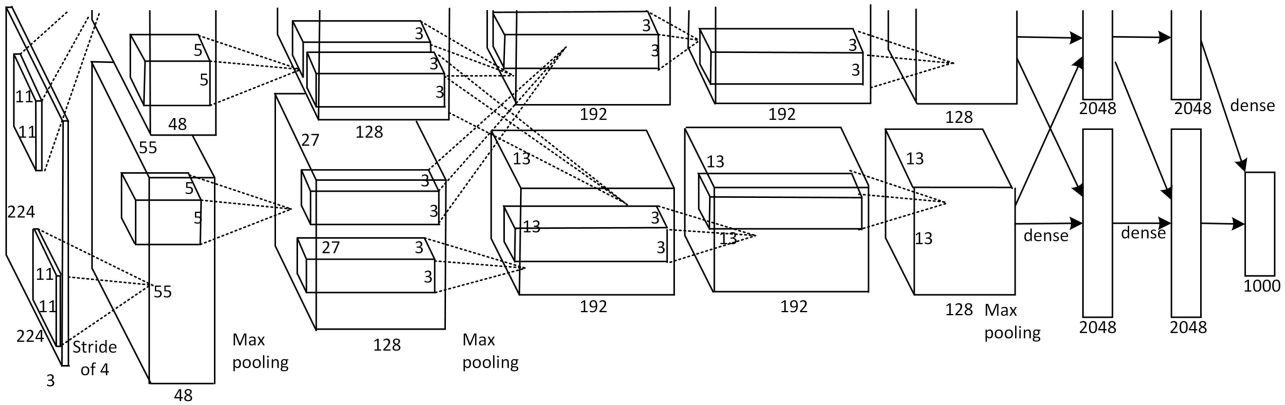

Figure 1. Typical principles of AlexNet [16].

and pool operations to reduce the size of the feature map. In addition, dense connections greatly reduce the number of parameters and retain many low-dimensional features.

3) SqueezeNet

SqueezeNet [18] is a very typical convolution network that is smaller than AlexNet and has a similar recognition accuracy. The key to it is to decrease the number of network parameters and calculation costs. Its crucial can be explained as follows. SqueezeNet utilities 1 * 1 convolution kernel, decreases the number of channels and moves downsample late in the network. It can be described in **Figure 3**.

3. System Framework

The system aimed to recognize user identity by utilizing user motion characteristics. The system framework contained four parts: signal collection, data preprocessing, neural network training, and identity authentication, as shown in **Figure 4**. The procedure of the system could be described as follows. Firstly, the user waved the smartphone, and the motion sensors' data were recorded. Secondly, the data was normalized to balance the difference among the different motion sensors. At the same time, we split the data into even lengths and resized them into standard shapes to feed them into the neural network. Thirdly, we input the samples to neural network and train network parameters. After the training process, the model parameters were stored. Finally, the identity was validated, and performance was analyzed.

The details of the system could be explained as follows. We designed an Android APP to collect motion sensor data, including accelerometers, gyroscopes, and direction sensors at three dimension spaces. We set the sampling frequency at 200Hz. We collected about three hundred fifty samples for each participant. We made a two-second timer to conduct an action, drawing a circle in space. We recorded the data and partitioned them into samples to validate the system. Then, we normalized the data into the same range to decrease the effect of different sensor values. We reshaped the sample into 224 * 224 to feed them into the neural network. We split all samples into 8:1:1 for training, validating and testing to evaluate system performance.

4. Performance Evaluation

We invite 13 participants to conduct a waving action by drawing a circle. Specifically, each user waves smartphone and the motion sensors in the smartphone record the motion data at 200 Hz. We analyze the data of accelerometers, gyroscopes, and direction sensors at three dimension spaces. We collect more four thousand four hundred samples to validate the system performance. Besides Android APP, we design three neural networks to validate system performance. We select DenseNet as the neural network model and set AlexNet and SqeezeNet as a comparison. We evaluate the system performance by analyzing the confusion

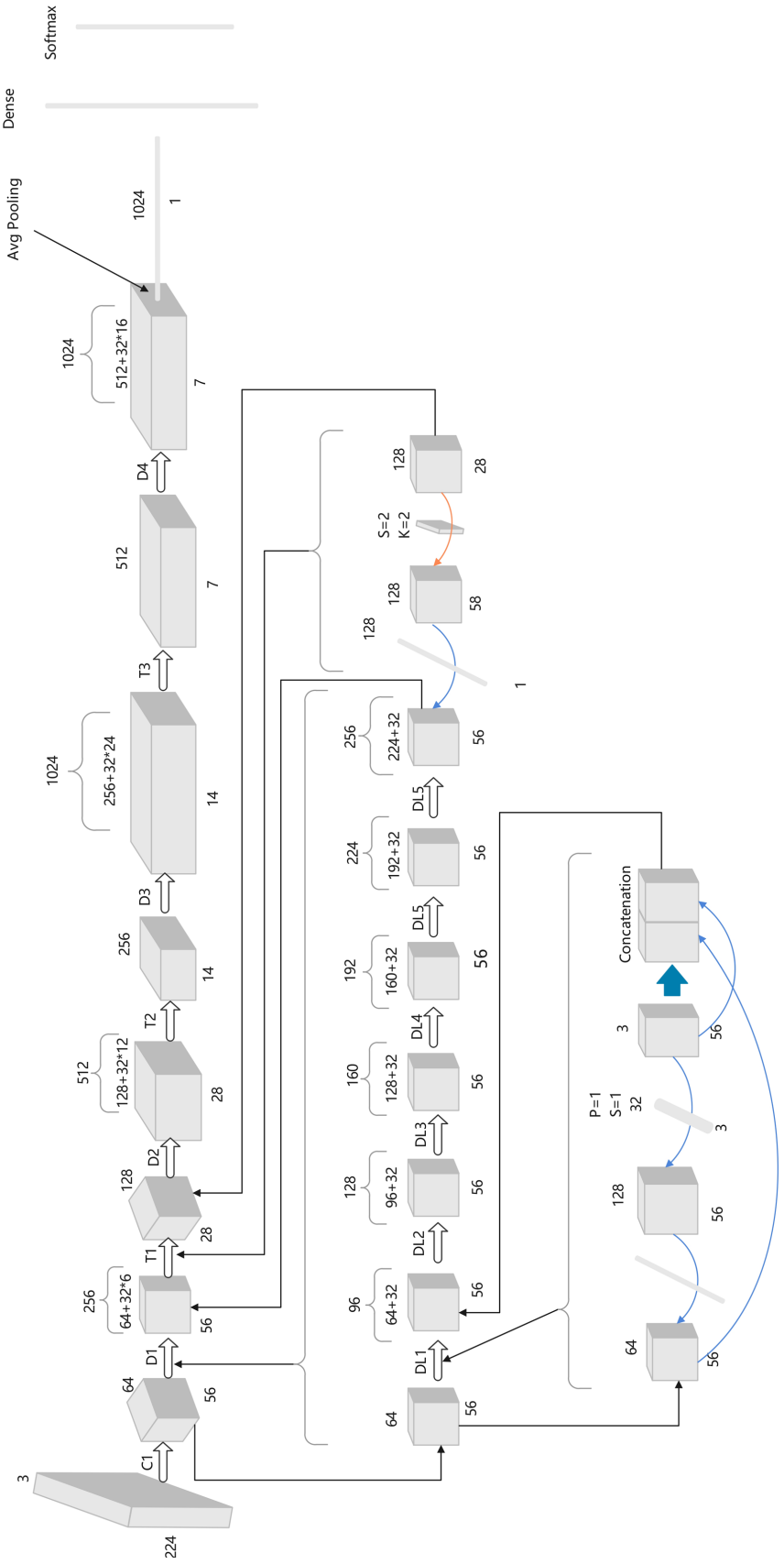

Figure 2. Typical principles of DenseNet [17].

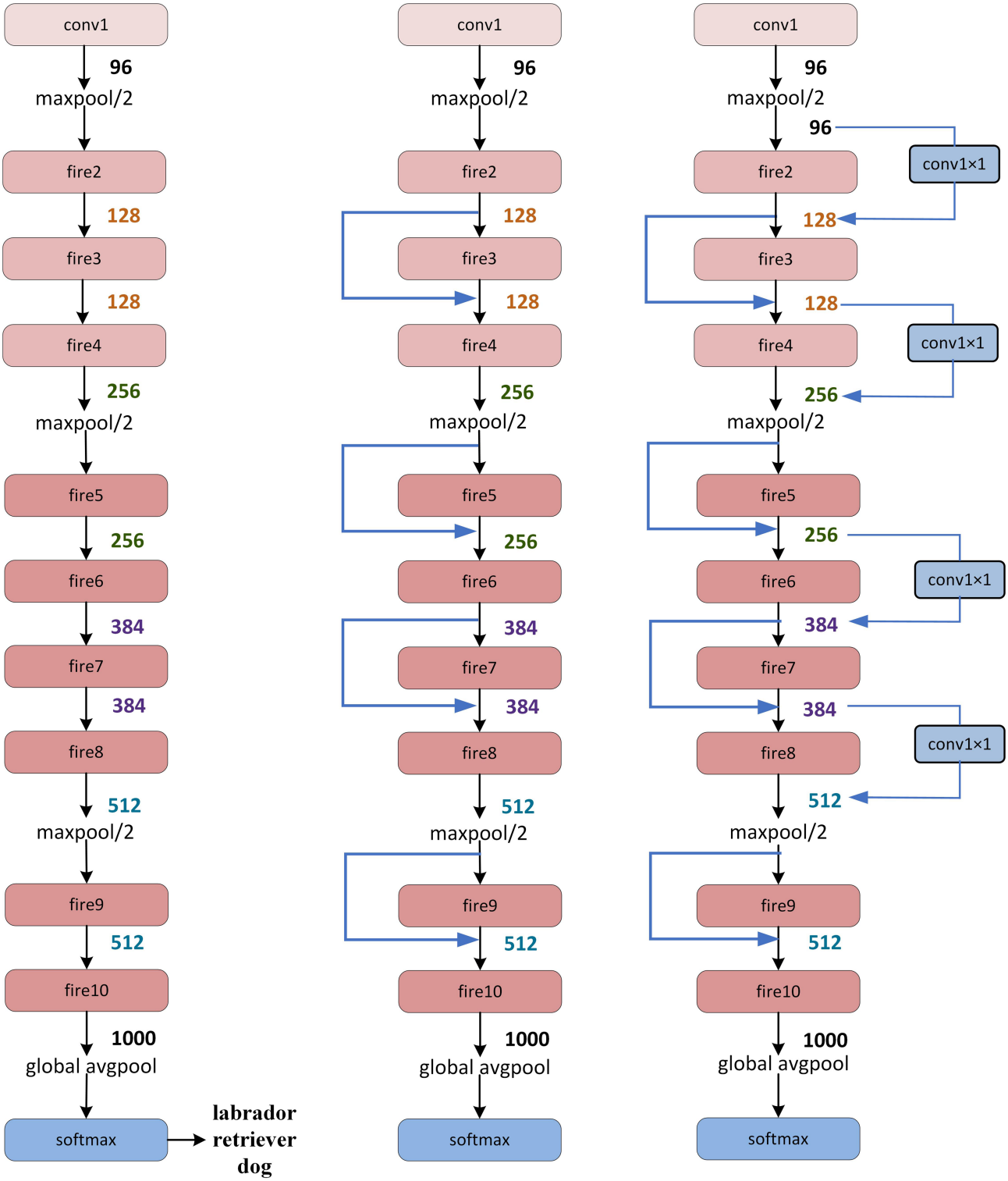

Figure 3. The structure of SqueezeNet and its changes [18].

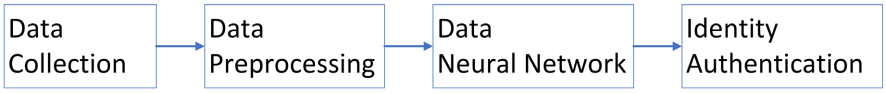

Figure 4. The system framework.

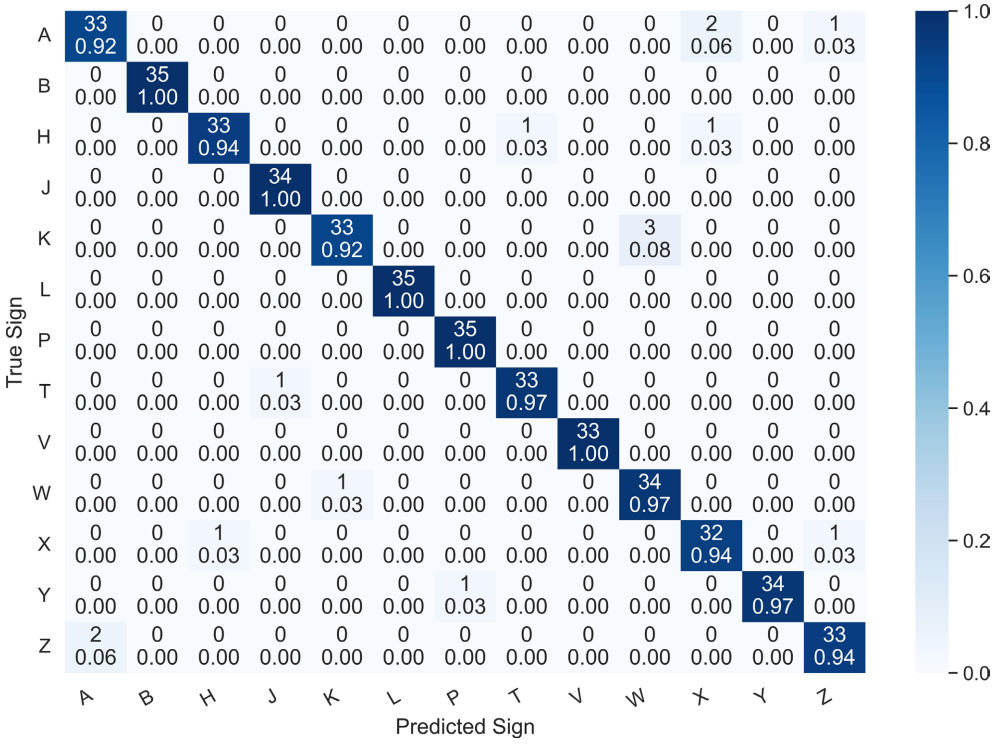

Figure 5. The fusion of the system.

matrix and error change with the training epoch.

Firstly, we analyze the system performance according to the confusion matrix, as shown in **Figure 5**. The results show that the average authentication accuracy is 96.15 percent. We can find that all 13 user authentication is above 92 percent, and these are satisfactory accuracy. Besides, five-person authentication is 100 percent, and three persons' accuracy is 97 percent, which shows the system has good identity accuracy.

Then, we analyze the effect of epoch on the training loss and training accuracy. We can see the training loss and training accuracy keep stable after 10 epochs, as shown in **Figure 6**. The result shows that we just can achieve good authentication accuracy by using 10 epochs. It proves that the DenseNet can effectively finish identity authentication using motion sensors of smartphones using a little training cost.

Next, we compare the performance of two neural networks, including AlexNet and SqueezeNet. The results show that the authentication accuracy decreases. The accuracy of AlexNet is 92.15 percent and the accuracy of SqueezeNet is 93.07 percent, as shown in **Figure 7**. This figure also proves that DenseNet holds the best recognition accuracy for all users compared with the other neural networks. The results indicate that the recognition accuracy of DenseNet is independent of users and reals satisfactory performance.

DenseNet has satisfactory recognition accuracy compared with the other neural networks. The reason can be explained as follows. The DenseNet utilizes densely connected convolutional networks to implement feature reuse and feature passing

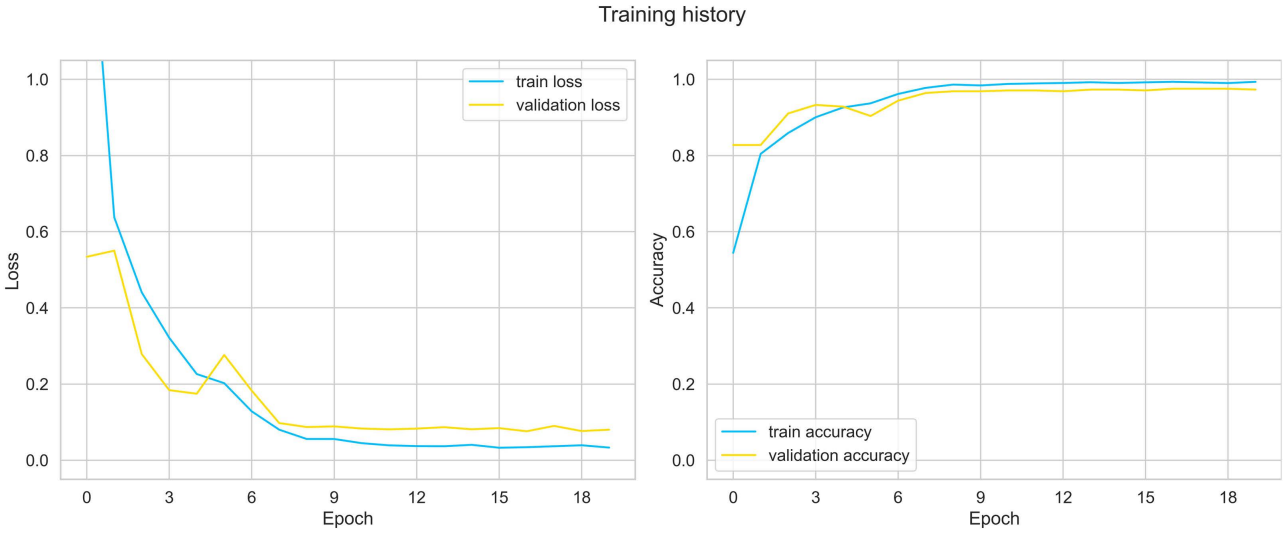

Figure 6. The accuracy and loss with epochs.

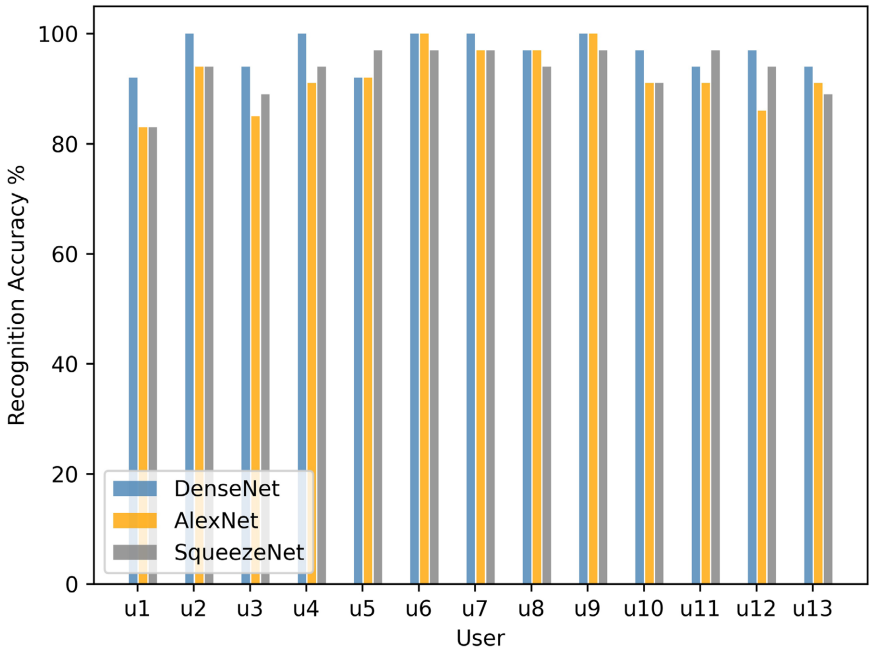

Figure 7. The comparison of different neural networks.

using DenseBlock. This method alleviates the vanishing-gradient problem and decreases the number of parameters. Therefore, it can effectively extract valuable features and real better classification results. As a result, it achieves better authentication accuracy than traditional neural networks.

We compare the results with the system of Waving Authentication (WA) proposed in [19]. The WA recognizes eight users with 92.83 percent using the SVM classification approach. Our system has better recognition results from the number of participants and recognition accuracy. The results indicate that neural networks have better recognition performance than traditional smartphone identity authentication methods.

5. Conclusions

At present, the smartphone has become the most crucial electric device for a lot of people. It can be used as a mobile computer to help us finish many work and entertainment, such as shopping, paying, and reading. Therefore, identity authentication is a crucial problem for smartphone users because the device stores much important information, especially including person's identity and digital wallet. The authorization for the legal user is the premise for the security usage of smartphones since it will refuse illegal users to access the data in the smartphone. This paper studies identity authentication for smartphone users using the internal sensors of smartphones and neural networks. Specifically, we collect sensor data when a user waves a smartphone and draws a circle, then process the data by normalizing them and feeding them into neural networks. We build DenseNet to validate the legal users. In addition, we choose another two neural networks, including SqueezeNet and AlexNet to compare the identity effect. The result shows that DenseNet achieves the best authentication accuracy. This neural network can be used to implement identity authentication for the smartphone.

Although we validate the effectiveness of DenseNet for smartphone identity authentication, we have some challenges with this application. Firstly, we can choose more brands and types of phone to validate the algorithm. Secondly, we may choose more neural networks to obtain more authentication results. Thirdly, more actions may be considered to evaluate the relationship between action and authentication accuracy. To sum up, we may build more experiment scenarios to evaluate the authentication scheme for smartphone applications.

Acknowledgements

The work is funded by the foundation of the Innovation and Entrepreneurship Training Program for College Students (S202110424011).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Roth, V. Richter, K., Freidinger, R. (2004) A PIN-Entry Method Resilient Against Shoulder Surfing. *Proceedings of the* 11*th ACM Conference on Computer and Communications Security*, Washington DC, 25-29 October 2004, 236-245. https://doi.org/10.1145/1030083.1030116

[2] Shelke, R. and Bagal, S.B. (2017) Iris Recognition System: A Novel Approach for Biometric Authentication. 2017 *International Conference on Computing, Communication, Control and Automation* (*ICCUBEA*), Pune, 17-18 August 2017, 1-5. https://doi.org/10.1109/ICCUBEA.2017.8463819

[3] Rahmawati, E., *et al.* (2017) Digital Signature on File Using Biometric Fingerprint with Fingerprint Sensor on Smartphone. 2017 *International Electronics Symposium*

on Engineering Technology and Applications (*IES-ETA*), Surabaya, 26-27 September 2017, 234-238. https://doi.org/10.1109/ELECSYM.2017.8240409

[4] Chen, L.W. and Ho, Y.F. (2016) A Face-Based Signage Interacting System for Mobile Users Using Smartphones. 2016 *IEEE Conference on Computer Communications Workshops* (*INFOCOM WKSHPS*), San Francisco, 10-14 April 2016, 1033-1034. https://doi.org/10.1109/INFCOMW.2016.7562239

[5] Wasnik, P., Raja, K.B. Ramachandra, R. and Busch, C. (2017) Assessing Face Image Quality for Smartphone Based Face Recognition System. 2017 5*th International Workshop on Biometrics and Forensics* (*IWBF*), Coventry, 4-5 April 2017, 1-6. https://doi.org/10.1109/IWBF.2017.7935089

[6] Rehman, A.U., Awais, M. and Shah, M.A. (2017) Authentication Analysis Using Input Gestures in Touch-Based Mobile Devices. 2017 23*rd International Conference on Automation and Computing* (*ICAC*), Huddersfield, 7-8 September 2017, 1-5. https://doi.org/10.23919/IConAC.2017.8082062

[7] Iuzbashev, A.V., Filippov, A.I. and Kogos, K.G. (2018) Continuous User Authentication in Mobile Phone Browser Based on Gesture Characteristics. 2018 *Second World Conference on Smart Trends in Systems, Security and Sustainability* (*WorldS4*), London, 30-31 October 2018, 90-95. https://doi.org/10.1109/WorldS4.2018.8611589

[8] Mufandaidza, M.P., Ramotsoela, T.D. and Hancke, G.P. (2018) Continuous User Authentication in Smartphones Using Gait Analysis. *IECON* 2018—44*th Annual Conference of the IEEE Industrial Electronics Society*, Omni Shoreham Hotel, Washington DC, 21-23 October 2018, 4656-4661. https://doi.org/10.1109/IECON.2018.8591193

[9] Roh, J.-h., Lee,S.-H. and Kim, S. (2016) Keystroke Dynamics for Authentication in Smartphone. 2016 *International Conference on Information and Communication Technology Convergence* (*ICTC*), Jeju, 19-21 October 2016, 1155-1159. https://doi.org/10.1109/ICTC.2016.7763394

[10] Cilia, D. and Inguanez, F. (2018) Multi-Model Authentication Using Keystroke Dynamics for Smartphones. 2018 *IEEE* 8*th International Conference on Consumer Electronics—Berlin* (*ICCE-Berlin*), Berlin, 2-5 September 2018, 1-6. https://doi.org/10.1109/ICCE-Berlin.2018.8576226

[11] Zeng, Y., Wu, L. and Xie, D. (2021) Gait Analysis Based on Azure Kinect 3D Human Skeleton. 2021 *International Conference on Computer Information Science and Artificial Intelligence* (*CISAI*), Kunming, 17-19 September 2021, 1059-1062. https://doi.org/10.1109/CISAI54367.2021.00212

[12] Li, F., Wang, X., Chen, H., Sharif, K. and Wang, Y. (2017) ClickLeak: Keystroke Leaks Through Multimodal Sensors in Cyber-Physical Social Networks. *Institute of Electrical and Electronics Engineers Access,* **5**, 27311-27321. https://doi.org/10.1109/ACCESS.2017.2776527

[13] Daribay, A., Obaidat, M.S. and Krishna, P.V. (2019) Analysis of Authentication System Based on Keystroke Dynamics. 2019 *International Conference on Computer, Information and Telecommunication Systems* (*CITS*), Beijing, 28-31 August 2019, 1-6. https://doi.org/10.1109/CITS.2019.8862068

[14] LeCun, Y., Bengio, Y. and Hinton, G. (2015) Deep learning. *Nature*, **521**, 436-444. https://doi.org/10.1038/nature14539

[15] Bengio, Y., Lecun, Y. and Hinton, G. (2021) Deep learning for AI. *Communications of the ACM*, **64**, 58-65. https://doi.org/10.1145/3448250

[16] Krizhevsky, A., Sutskever, I. and Hinton, G.E. (2017) ImageNet Classification with Deep Convolutional Neural Networks. *Communications of the ACM*, **60**, 84-90.

https://doi.org/10.1145/3065386

[17] Huang, G., Liu, Zhuang., van der Maaten, L., Weinberger, K.Q. (2017) Densely Connected Convolutional Networks. 2017 *IEEE Conference on Computer Vision and Pattern Recognition* (*CVPR*), Honolulu, 21-26 July 2017, 4700-4708. https://doi.org/10.1109/CVPR.2017.243

[18] Qiang, B., Zhai, Y., Zhou, M., Yang, X., Peng, B., Wang Y. and Pang, Y. (2021) SqueezeNet and Fusion Network-Based Accurate Fast Fully Convolutional Network for Hand Detection and Gesture Recognition. *IEEE Access*, **9**, 77661-77674. https://doi.org/10.1109/ACCESS.2021.3079337

[19] Hong, F., Wei, M., You, S., Feng, Y. and Guo, Z. (2015) Waving Authentication: Your Smartphone Authenticate You on Motion Gesture. *Presented at the Proceedings of the* 33*rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, Seoul, 18 April 2015, 263-266. https://doi.org/10.1145/2702613.2725444