# 基于智能手表PPG传感器的用户认证方案

谭智豪[1]，黄勤龙[1]，杨义先[1]

[1] 北京邮电大学网络空间安全学院，北京 100876

**摘要：**随着智能手表的迅速普及，安全方便的用户认证方案成为人们的需要。作为被广泛部署在智能手表上的生物电信号传感器，PPG传感器展现了其在用户身份验证领域的潜力。现有的认证方案通常有一些限制，需要用户提供比较多的注册数据以充分地反映用户的身份特征，这可能会影响到用户的使用体验。本文提出了一种利用智能手表PPG传感器的用户认证方案。通过使用孪生网络从用户手指级手势的PPG信号中提取特征，对用户的身份进行认证。本文通过实验对方案的性能进行了评估，认证的平均准确率为92%。此外，本文所提出的方案可以在少量的用户注册数据下实现较高的认证准确率。

**关键词：**用户认证，智能手表，PPG传感器，孪生网络

**中图分类号：** TP309

# User Authentication from Smartwatch Photoplethysmography sensor

TAN ZhiHao[1], HUANG Qinlong[1], YANG Yixian[1]

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876

**Abstract:** With the rapid proliferation of smartwatch, a secure and convenient smartwatch-based user authentication scheme are desired. As the widely deployed bioelectrical signal sensor in smartwatch, Photoplethysmography (PPG) sensors have shown potentials for authentication. Existing authentication solutions usually have some limitations. They require the user to provide an amount of registration data from user to reflect the profile of user, which may impact the experience of user. In this paper, we propose a PPG-based smartwatch authentication scheme. We leverage the Siamese Network to extract the feature of user from the PPG signal affected by the finger-level gesture for authentication. We conduct some experiments to evaluate the performance of the scheme. The experiment results show that our model has an average accuracy rate of 92.43%. In addition, the authentication model can achieve high authentication accuracy with a small amount of user registration data.

**Key words:** User authentication, smartwatch, PPG sensor,siamese network

---

Foundations: National Natural Science Foundation of China Foundation (No. 61572080)

Author Introduction: Tan Zhihao(1996- ), female, student, major research direction: security authentication, Email: jylytzh@bupt.edu.cn. Huang Qinlong(1988- ), male, associate professor, major research direction：data security, and mobile cloud security, E-mail:longsec@bupt.edu.cn. Correspondence author：Yang Yixian (1961-), male, professor, major research direction：cryptography, information and network security, E-mail:yxyang@bupt.edu.cn.

# 0 Introduction

As the wearable device market continues to growth rapidly, smartwatches are gradually integrated into our daily life. To provide different kinds of application, smartwatches are equipped with a variety of sensors to collect our personal information, such as voice, GPS and health physiological information. While the smart wearable devices provide users convenience, they also attract the attention of attacker [1]. Therefore, it is necessary to provide a secure user authentication scheme for smartwatch.

Existing commercial smartwatches mainly use PIN-based passcodes and pattern-based passcodes to verify the legitimacy of user [2]. However, user trends to disable this knowledge-based security authentication mechanism since the inconvenience of typing on the small-sized screen of smartwatch [3][4]. On the other hand, this method is not secure. It may be attacked by smudges [5], shoulder-surfing [6] and sensor-based inference[7],which have been proven to be effective on smartphones. Moreover, it is difficult to migrate some mature authentication technologies from smartphone, such as iris and fingerprints, due to the limitations of power consumption and sensor size.

In order to solve this problem, many authentication schemes were proposed for wearable device by taking advantage of user's behavior patterns and motion habits, such as gait [3], handwrite [8], keystroke [9] and touch [10]. Among these behaviors, gesture is considered as a promising biometric in the field of behavior-based authentication. In recent years, some work [11][12][13] has demonstrated the potential of using gesture for authentication on wrist wearable devices. We can leverage the sensors of smartwatches, such as accelerometer, gyroscope and PPG sensors, to measure the gesture behavior for authentication.

However, in order to learn the gesture behavior of users, most existing behavior-based authentication schemes require users to repeat the behavior many times for registration. This is not convenient for users. Furthermore, the existing authentication schemes of smart devices mostly identify a user from an existing user group. They required the data both genuine users and impostors to train the authentication model, which is impractical.

Considering the disadvantages of existing schemes, we propose a smartwatch authentication scheme based on siamese network, which utilizes the PPG signals influenced by finger-level gesture behaviors for authentication. We first use the gesture data of volunteers to train a general behavior authentication model based on the siamese network. This model can distinguish different users effectively, even if they did not participate in training. The user registered a gesture as the profile for initialization. When authenticating, the user is asked to perform the same gesture selected in the registration. The PPG signal fragments of gestures were extracted and input into the model with the registered sample for comparison. If the average distance between the new gesture and registered sample is less than the pre-defined threshold, the user passes the authentication. The experiment including 40 participants is conducted to evalu-

ate the effectively of scheme. The experiment results show that our scheme can achieve an authentication accuracy above 90% with only a single prior instance.

## 1 Related Works

To address the limitations of existing authentication methods for smart devices, researchers have begun to analyze sensors data of device, to extracted human behavior habits [14][15], physical characteristics [16][17], or their combinations [3][10], for protect the mobile devices. One thread of authentication research is to measures the behavioral patterns by the inertial measurement unit (IMU) for smart devices. Zou et al. [18] proposed a deep-learning structure for gait authentication, which collects users' inertial-based gait data in unconstrained conditions by the accelerometer of smartphone. Yu et al. [12] proposed a user authentication system based on tiny gestures, which collects tiny gesture signal by the IMU sensor of smartwatch. Their efforts show that motion sensors on mobile device have potential for behavior authentication. However, according to recent studies [19], the motion sensor of smartphone can be used to eavesdrop the speech privacy. Users may be more sensitive to the use of IMU sensors in the future.

Another thread of authentication research is to use the physical characteristics of the human. As PPG sensors are widely deployed in wrist wearable device, PPG-based authentication has drawn great attention in academia. Cao et al. [20] proposed a two-factor authentication system in wearable devices, call PPGPass, which collects wrist PPG signals in three conditions (signatures writing, passwords inputs, and patterns inputs). Zhao et al. [21] built a continuous authentication system in wrist-worn devices, called TrueHeart, which exploit the PPG signals after the mitigate processing of Motion artifacts. These efforts illustrate the potential of PPG sensor for authentication on wrist wearables. However, their schemes can only identify users participating in the training, which reduce the feasibility of scheme in the wrist devices.

The neural network has achieved the great success in the fields of image classification, natural language processing and activity recognition. They can extract features from the dataset based on the defined label automatically. Researchers have proposed many structures of network to satisfy the requirements of different tasks. siamese network first proposed by [22] to solve the problem of signature verification, is widely used to solve the problem of Few-shot learning. Recently, researchers leverage the siamese network to process time sequence of sensor for authentication. Xu et al. [17] proposed a smartphone authentication system, TouchPass, which leverage IMU sensor to collect active vibration signals affected by touching fingers. They construct a siamese convolution network to extract behavior-independent feature. Fan et al. [23] proposed an electromyography (EMG)-based user authentication system, called EmgAuth, which leverages Myo armband to record the EMG signals during user picking up the phone.

They used the raw EMG signal to train the Siamese convolution Network for authentication.

# 2 Preliminaries

## 2.1 PPG Sensor

The PPG sensor is mainly used to estimate the heart rate and the blood pressure by detecting the pattern of blood flow changes. A PPG sensor includes at least one light-emitting diode (LED) as the light emitter and one photodiode (PD) as the light receiver. The light emitter uses the green light or red light to illuminate the skin. The light receiver measures the intensity of light that is either transmitted or reflected. The light will be absorbed by biological tissues when it travels through the human body. Since different blood volumes have different absorptivities of light, the wearables infer the changes of blood flow in the wrist area based on the intensity changes of the light received by the PD.

## 2.2 Independence Component Analysis

The basic task of blind source separation (BSS) algorithm is estimating parts of source signals that are combined in observations. Independence Component Analysis (ICA) is a special BSS algorithm. It assumes that the source signals are nongaussian and mutually independent. The observational signal can be regarded as a linear combination of a smaller number of independent component sources. The source signal is defined a $n$-dimensional vector $S(t) = [s_1(t), s_2(t), ..., s_n(t)]^T$. The observational signal is defined a $m$-dimensional vector $X(t) = [x_1(t), x_2(t), ..., x_n(t)]^T$, where $m$ is required to be larger than $n$. The mathematical model of the ICA algorithm is described as follows:

$$X(t) = A^T S(t) \tag{1}$$

where $A$ is a mixing matrix of $m*n$ that indicates how the source signal vector $S$ are linearly combined to build the observational signal $X$. The ICA algorithm can obtain a separation matrix $B$ of $n * m$ by the Maximum Likelihood Estimation even the $A$ and $S$ is unknown. By transforming the observational signal $X$, the separation signal $Q$ can as close as possible to the real source signal $S$. The function is defined as follows:

$$Q = BX \tag{2}$$

# 3 Overview

## 3.1 Key insights and Design goal

Currently, some studies use PPG sensor of wrist devices for both gesture recognition [24] and authentication [4][11]. The gesture behavior involves a series of sophisticated muscle movement. Due to the wrist vessels are compressed to varying degree, these movements have a noticeable effect on the flow of blood even the finger-level gestures. The PPG sensor detects the changes of blood flow, which can be used to extract the behavioral patterns of gesture. In addition, the muscle movements of human body are controlled by the subconscious, which is difficult to modify consciously. Even if the same gesture performed by different people, the behavioral patterns of muscle movements are distinguishable[12]. Therefore, we leverage the biological information and behavioral patterns contained in PPG signals for authentication.

Our scheme is designed to ensure the information security of smartwatch while increase the convenience of user, through accurately authenticating the user by the pre-selected gesture. In general, the design goals for our scheme are:

- Tiny gesture: Our scheme can authenticate user by finger-level gesture behavior, because sophisticated gesture may inconvenient due to the environment constraints.
- Accurate: Our scheme needs to extract consistent and distinguishable biometrical from PPG signals of gesture, to authenticate the user accurately.
- Rapid Registration: The process of user enrollment should be easy and fast.
- Offline: Our authentication scheme should work on device even without network access.

## 3.2 Architecture

The architecture of our scheme is shown in Fig.1. It can be divided into the preparation phase and the application phase.

**Preparation phase**. In the preparation phase, we collected data from volunteers to train the siamese network model. The volunteers were asked to wear smartwatch and perform the gesture. We take as inputs the PPG measurement from smartwatch's PPG sensors. The gesture-related PPG signals were preprocessed to extract the gesture fragments. For each PPG segment, we used ICA algorithm to separate gesture signals, and detect the start point and the end point of gesture behavior fragment by the energy stream of gesture signals. The fragments of gesture patterns in the PPG signal are extracted to generate training pairs. According the labels of training pair, the siamese network train the neural subnetwork which can extra the features to distinguish different users and recognize the same user. By calculating the distance

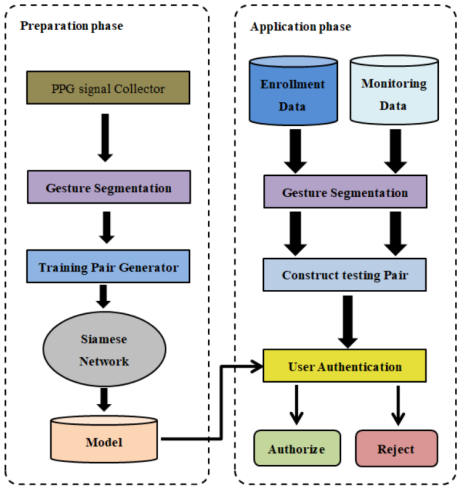


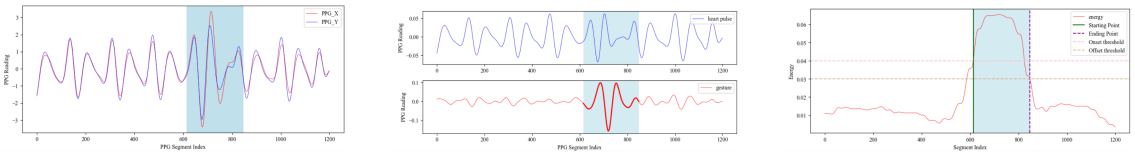

图 1: The architecture of our scheme

between the features of the input signal, the model can output the degree of different between gesture segments.

**Application phase**. In the application phase, we used the trained siamese network model to provide authentication service. The user is first required to select a gesture to register. The system performs the gesture extraction algorithm to extract the gesture fragments from the PPG signals recorded in the registration, and store the PPG signal fragments of gesture behaviors in the database as user's profile. When authenticating, the smartwatch activates the PPG sensor to collect the data of user's gesture behavior. The new PPG signal fragments of gesture behavior are extraced by the same extraction algorithm from the new PPG signals. The new PPG fragment and the registered PPG fragment of gesture are used to construct testing pair and fed into the siamese network that we train in the preparation phase. The siamese network calculates the distance of the input PPG signal test pair. If the average of the distance is within the pre-defined threshold, the current user's identity is considered legitimate, otherwise the user's access will be denied.

# 4 Gesture Segmentation

To extract the PPG signal fragments of gesture intuitively, we established a third-order Butterworth bandpass filter with a bandwidth of 2-10 Hz. It mitigates the noise caused by the breathing and power-line, and remains the high-frequency part of the pulse signal and the gesture-related signal that is easy to analyze. The filtered signal is further normalized by means and variance. Specifically, the filter is only used for the gesture segmentation phase, because the filter removes some semantic information of the signal at other frequencies, which negatively



(a) The gesture related PPG signal (b) The result of ICA separating (c) The Energy stream of gesture

图 2: Example of gesture segmentation

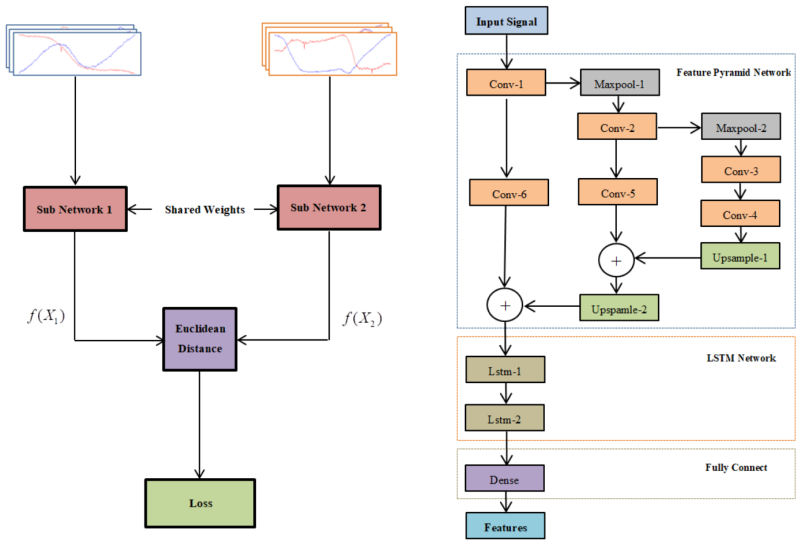
impact the authentication accuracy.

Due to the heartbeat pulse are constantly impact the measurements of PPG sensor, it is hard to characterize the starting and the ending points of the gesture behavior fragment based on the observed PPG signal without removing the influence of the heartbeat pulse. Inspired by [20], the observed PPG signal segment can be considered as a linear combination of heartbeat pulse signal and gesture signal. We use a blind source separation algorithm based on independent component analysis to recover the source signal affected by gesture.

In this paper, the gesture-related PPG signal segments collected by two adjacent PPG sensors on the smartwatch are used as the input of the blind source separation algorithm, which are shown in Fig.2a. The results of signal separation are shown in Fig.2b. It can be observed that there is a regular signal and an irregular signal. We consider the former is a heartbeat pulse signal and the latter is a gesture signal. Because gesture related signal has the higher skewness and kurtosis[25], we select the best output data as the gesture signals by comparing the skewness and kurtosis. We found that the selected gesture signal has obvious fluctuation during the gesture. We applied a sliding window with a length of 1 second, and calculated the standard deviation of the signal within each window as the energy feature to measure the fluctuation of the gesture signal, as shown in Fig.2c. We design an energy-based double threshold principle to detect the start point and the end point of gesture. The energy stream rises above the onset threshold denotes the start point, and it falls down the offset threshold denotes the end point of the active segments. The fragments of gesture behavior are extracted from the raw PPG signal and interpolate into the same length of 200 as the input of siamese network.

## 5 Design of siamese network

Fig.3a shows the architecture of siamese network in our scheme. The siamese network consists of two identical subnetworks,which shared the same structure and weight. The interpolated raw PPG gesture fragment are used as the input of subnetwork. Specially, we design a neural subnetwork to extract the feature of gesture. The architecture of the proposed subnetwork is shown in Fig.3b. The subnetwork is composed of three parts: feature pyramid network




(a) The architecture of siamese network (b) Subnetwork Design

图 3: siamese network architecture

module, LSTM network module and fully connect Module. First, a three-level feature pyramid convolutional networks are used to extract the spatial information of gesture. Then, we connect a 2-layer LSTM network after the output of the feature pyramid network layer to extract the temporal information of gesture behavior. Finally, we adopt a full connection layer to take the output of previous network into account. This subnetwork can synthesize the spatial and temporal information of gesture behavior to extract feature of user. The siamese network extracts the features of two input samples through the subnetwork, and calculates Euclidean distance between the features as the output. In this work, the loss function is defined as follow:

$$Loss = Yd^2 + (1 - Y)\{max(0, m - d)\}^2 \tag{3}$$

where $Y$ is a binary label of the input vector pairs. When the input vector $X_1$ and $X_2$ belongs to the same person, $Y$ is 1, on the other hand, $Y$ is 0. The pair generating algorithm is shown as Algorithm 1. $m$ is the margin of distance that is set to 1 in this work, $d$ is Euclidean distance that represents the difference between input samples. If the two input samples are from the same people, the *Loss* is monotonically increasing by $d$. If the two input samples are from the different users, the *Loss* is monotonically decreasing by $d$. The target of siamese network is to minimizing the *Loss* by the gradient descent algorithm. It can minimize the pair distance of the same user and maximize the pair distance of different users. When a user tries to log in, the authentication is performed based on the gesture behavior templates of the registered user. The behavior feature of the newly recorded gesture is combined with the registered template to generate the testing pairs. The testing pairs are fed into the siamese network to compute the

Euclidean distance $d_w$ of the output vectors. If $d_w$ is smaller than a pre-determined threshold, the gesture behavior is authenticated as coming from the legitimate user.

**Algorithm 1** Generating Training Pairs

**Input:** *Data*

```
Len=length(Data)
for p in (0,...,Len) do
    N=length(Data[p])
    for i in (0,...,(N − 1)) do
        for j in (i,...,N) do
            Pair[1] = [Data[p][i], Data[p][j]]
            Label[1] = 1
            diff_person = (p + Random(1, Len))%Len
            Index=Random(0,length(Data[diff_person]))
            Pair[2] = [Data[p][i], Data[diff_person][Index]]
            Label[2] = 0
            Pair[3] = [Data[p][j], Data[diff_person][Index]]
            Label[3] = 0
            TrainData.append(Pair, Label)
        end for
    end for
end for
return TrainData
```

# 6 Evaluation

## 6.1 Experimental Setting

To validate the feasibility of our scheme, we develop an android program to collect PPG data at the frequency of 200hz on smartwatch. The smartwatch was a Ticwatch pro with the system of Wear os by Google 2.18. We use *getSensorList()* to get the type number of PPG sensor on the smartwatch, and register it in *registerListener()* to get the reading of PPG sensors. The raw data is recorded as a CSV file and stored locally on the smartwatch. The data is transmitted to the GPU server for data analysis. Our experimental uses TensorFlow and Keras to train the proposed neural network model for authentication. The experiment is the Window 10 operation system running on a server with an Intel(R) Core i7-6700hq CPU at 2.60 GHz and an NVIDIA GeForce GTX 1060.

In order to train an authentication model, we recruited 40 Volunteers, 20 females and 20


图 4: Nine finger-level Chinese Sign Language gesture

males, with the age range from 20 to 25, to build a gesture signal dataset. The volunteers wore the smartwatch on their left wrist and made gestures according to the instruction of software. As shown in Fig 4, we selected nine figer-level Chinese Sign Language gestures as research example. The volunteers were asked to perform the gestures in sequence with 30 repetitions per gesture. In total, we collect 10800 PPG sensor signals segments for the experimental evaluation.

## 6.2 Evaluation Metrics

We are using widely accepted metrics to evaluate the performance of scheme. These metrics include Accuracy rate (ACC), False-acceptance rate (FAR) and False-rejection rate (FRR). The Accuracy rate (ACC) is showing the overall performance of the authentication system. The False-acceptance rate (FAR) is the measure of the likelihood that the authentication system will incorrectly accept access attempts from unauthorized users. The False-rejection rate (FRR) reflects the proportion of positive that are incorrectly identified by authentication system.

## 6.3 Accuracy

### 6.3.1 Authentication Performance

To evaluate the performance of siamese network systematically, we divided the data set into training set and test set according to the label of user. Specifically, we randomly selected 8 out of 40 participants' data as the testing dataset, and the remaining data was used to construct training dataset. Then, we constructed training pairs set and testing pairs set according to algorithm 1 respectively. To avoid the deviation by data drift and overfitting, we repeat such cross validation mechanisms for 10 iterations and averaged the experimental results.

Table.1 shows the results of 10 repeats of the experiment. The experiment result shows that the average accuracy of the 10 repeats was 92.43%, with a 7.29% FAR and 8.1% FRR. The accuracy of the third can reach the accuracy of 96.54%. However, the accuracy of experiment in group 6 and group 7 was less than 90%, which was significantly lower than the average accuracy, and the performance of other metrics was also terrible. We investigated the reasons for the corresponding data. There are three reason may lead to this situation. Firstly, the gesture

表 1: The Result of Cross-Validation

| index | Test set | ACC(%) | FAR(%) | FRR(%) |
|---|---|---|---|---|
| 1 | 9, 36, 4, 1, 13, 26, 34, 25 | 92.71 | 7.04 | 7.77 |
| 2 | 26, 1, 15, 3, 32, 33, 36, 4 | 94.17 | 5.54 | 6.37 |
| 3 | 38, 13, 32, 33, 19, 20, 25, 3 | 96.54 | 3.22 | 3.92 |
| 4 | 38, 2, 27, 33, 21, 31, 9, 26 | 94.59 | 5.11 | 5.98 |
| 5 | 32, 5, 36, 34, 21, 16, 3, 30 | 96.17 | 3.55 | 4.38 |
| 6 | 28, 27, 18, 12, 30, 8, 21, 32 | 85.9 | 13.79 | 14.67 |
| 7 | 37, 19, 15, 22, 17, 9, 27, 2 | 91.43 | 8.29 | 9.09 |
| 8 | 31, 2, 14, 18, 29, 16, 24, 1 | 86.79 | 12.95 | 13.7 |
| 9 | 24, 38, 34, 20, 15, 9, 29, 21 | 93.52 | 6.16 | 7.09 |
| 10 | 34, 30, 2, 9, 5, 6, 14, 25 | 92.49 | 7.23 | 8.02 |
| mean | | 92.43 | 7.29 | 8.1 |

detection algorithm may misidentify the PPG signal segments affected by other body movement as gesture. The wrong signal segments are fused into the pair data, which misleads the authentication model. Secondly, in the process of data collection, some volunteers' unnatural performance may produce unqualified data, which will negatively impact the performance of the authentication model. Finally, the siamese networks trained with the data of different users have different attention in feature extraction, which leads to differences in the generalization of authentication models.

### 6.3.2 The Influence of Registration Data Size

The size of registration data is the number of gestures for user in the initialization. We expect to minimize the size of the registration data to reduce the time and cost of the register process. On the other hand, the registration data should fully reflect the profile of user to allow the model make an accuracy authentication. Therefore, we conduct the experiment to evaluate the impact of different sizes of registration data. In addition, we compare the siamese networks with traditional machine learning algorithm to verify the effectiveness of model in reducing user registration efforts. According to the work of [24], we extracted the feature of gesture in Time domain, Frequency domain and Time-frequency domain. We use the Gradient Boosting Tree (GBT) and Support Vector Machine (SVM) algorithm to build multi-user classifier respectively. As shown in Fig.5, the siamese network model achieve a decent performance even the size of the registration data is small. Specifically, siamese network can reach a 93% average accuracy for using 3 registration samples. The performance of Gradient Boosting Tree (GBT) and Support Vector Machine (SVM) increases to a stable level with the increase in the size of registration data. The highest average accuracy of SVM is still below 90%. The result shows that the siamese network model can reduce the requirement of registration data for authentication. The prediction accuracy of siamese network is better than other models among different size of

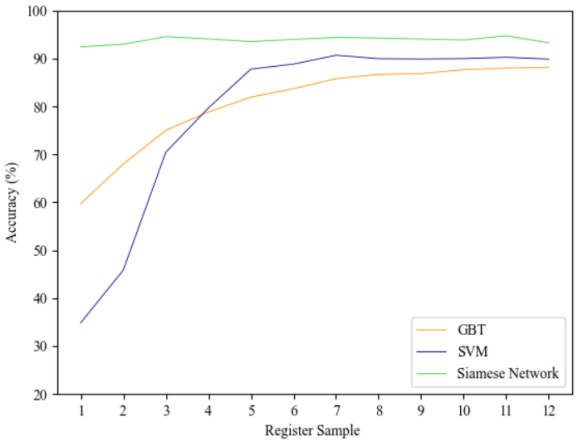



图 5: The architecture of our scheme

registration data. It indicates the siamese network can extract the feature of different users more efficiently for authentication.

## 7 Conclusion

In this paper, we present a smartwatch authentication scheme, which leverage PPG signals of finger-level gesture and siamese network to verify user. We analyze the gesture-related PPG signal, and use blind source separation algorithm to extract the PPG signal fragments of gesture. The siamese network are used to extract unique representation from the PPG signal fragments of gesture to authenticates user accurately. We conduct an experiment with 40 participants and build a dateset of 9 finger-level sign language gestures. The results show that our scheme is capable of authenticating users accurately, with an average accuracy of 92.43% . In addition, our scheme can reduce the effort of user in the registration stage. Compared with traditional machine learning algorithm, our scheme can achieve the accuracy above 90% by one registration sample.

## 参考文献（References）

[1] Ching K W, Singh M M. Wearable technology devices security and privacy vulnerability analysis[J]. International Journal of Network Security & Its Applications, 2016, 8(3): 19-30.

[2] Nguyen T, Memon N D. Smartwatches Locking Methods: A Comparative Study[C]. SOUPS. 2017.

[3] Vhaduri S, Poellabauer C. Multi-modal biometric-based implicit authentication of wearable device users[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(12): 3116-3125.

[4] Shang J, Wu J. A Usable Authentication System Using Wrist-worn Photoplethysmography Sensors on Smartwatches[C]. 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019: 1-9.

[5] Aviv A J, Gibson K L, Mossop E, et al. Smudge attacks on smartphone touch screens[J]. Woot, 2010, 10: 1-7.

[6] Zakaria N H, Griffiths D, Brostoff S, et al. Shoulder surfing defence for recall-based graphical passwords[C]. Proceedings of the seventh symposium on usable privacy and security. 2011: 1-12.

[7] Xu Z, Bai K, Zhu S. Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors[C]. Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks. 2012: 113-124.

[8] Griswold-Steiner I, Matovu R, Serwadda A. Wearables-driven freeform handwriting authentication[J]. IEEE Transactions on Biometrics, Behavior, and Identity Science, 2019, 1(3): 152-164.

[9] Acar A, Aksu H, Uluagac A S, et al. A Usable and Robust Continuous Authentication Framework using Wearables[J]. IEEE Transactions on Mobile Computing, 2020.

[10] Peng G, Zhou G, Nguyen D T, et al. Continuous authentication with touch behavioral biometrics and voice on wearable glasses[J]. IEEE transactions on human-machine systems, 2016, 47(3): 404-416.

[11] Ohtsuki T, Kamoi H. Biometrie authentication using hand movement information from wrist-worn PPG sensors[C]. 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC). IEEE, 2016: 1-5.

[12] Yu X, Zhou Z, Xu M, et al. Thumbup: Identification and authentication by smartwatch using simple hand gestures[C]. 2020 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE Computer Society, 2020: 1-10.

[13] Li Y, Xie M. Understanding secure and usable gestures for realtime motion based authentication[C]. IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2018: 13-20.

[14] Sanchez S H, Pozo R F, Gomez L A H. Driver Identification and Verification From Smartphone Accelerometers Using Deep Neural Networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020.

[15] Lee W H, Liu X, Shen Y, et al. Secure pick up: Implicit authentication when you start using the smartphone[C]. Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies. 2017: 67-78.

[16] Lu L, Mao J, Wang W, et al. A Study of Personal Recognition Method Based on EMG Signal[J]. IEEE Transactions on Biomedical Circuits and Systems, 2020, 14(4): 681-691.

[17] Xu X, Yu J, Chen Y, et al. TouchPass: towards behavior-irrelevant on-touch user authentication on smartphones leveraging vibrations[C]. Proceedings of the 26th Annual International Conference on Mobile Computing and Networking. 2020: 1-13.

[18] Zou Q, Wang Y, Wang Q, et al. Deep learning-based gait recognition using smartphones in the wild[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 3197-3212.

[19] Ba Z, Zheng T, Zhang X, et al. Learning-based practical smartphone eavesdropping with built-in accelerometer[C]. Proceedings of the Network and Distributed Systems Security (NDSS) Symposium. 2020: 23-26.

[20] Cao Y, Zhang Q, Li F, et al. PPGPass: Nonintrusive and Secure Mobile Two-Factor Authentication via Wearables[C]. IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020: 1917-1926.

[21] Zhao T, Wang Y, Liu J, et al. Trueheart: Continuous authentication on wrist-worn wearables using ppg-based biometrics[C]. IEEE INFOCOM 2020-IEEE Conference on Computer Communications. IEEE, 2020: 30-39.

[22] Bromley J, Guyon I, LeCun Y, et al. Signature verification using a" siamese" time delay neural network[J]. Advances in neural information processing systems, 1994: 737-737.

[23] Fan B, Liu X, Su X, et al. Emgauth: An emg-based smartphone unlocking system using siamese network[C]. 2020 IEEE International Conference on Pervasive Computing and Communications (PerCom). IEEE, 2020: 1-10.

[24] Zhao T, Liu J, Wang Y, et al. Towards Low-cost Sign Language Gesture Recognition Leveraging Wearables[J]. IEEE Transactions on Mobile Computing, 2019.

[25] Selvaraj N, Mendelson Y, Shelley K H, et al. Statistical approach for the detection of motion/noise artifacts in Photoplethysmogram[C]. 2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society. IEEE, 2011: 4972-4975.