Application Research of Voiceprint Recognition Technology in Mobile E-commerce Security

Zhenkun Wu[1,2,a], Zhenlong Peng[1,2,*,b], Ting Yu[1,2,c]

[1] TSL Business School, Quanzhou Normal University
Quanzhou 362000, China
[2]High Educational Engineering Research Center of Fujian Province for E-Commerce Intelligent Based on Cloud Computing and Internet of Things
Quanzhou 362000, China
*Corresponding author

Abstract—**Security is an important factor restricting the development of mobile e-commerce. Establishing a secure business application environment is of great significance for promoting sound development of mobile e-commerce. In this paper, we first introduce related background of mobile e-commerce security, expounds related concepts of mobile e-commerce security, and analyzes the threats of mobile e-commerce security, security requirements and security technologies. We analyzed the working principle of voiceprint recognition technology and its main application in mobile electronic security. At the same time, the security model of voiceprint recognition technology in mobile e-commerce application is constructed, and the process of security model is described in detail. It provides a certain reference for the technical support of mobile e-commerce security services.**

Keywords—E-commerce; Mobile commerce; Mobile e-commerce security; Voiceprint recognition

I. INTRODUCTION

In recent years, with the continuous development of the Internet and the popularity of mobile smartphones, mobile e-commerce has developed rapidly, but security issues have become increasingly prominent. To ensure the security of mobile e-commerce, we should strengthen identity authentication, such as introducing biometric technology to make up for the defects in traditional identity authentication and increase the accuracy of identity authentication. Voiceprint recognition recognizes the identity by voice features, and the process is simple and difficult to imitate. Voiceprint recognition technology can make transaction more secure [1].

II. OVERVIEW OF MOBILE E-COMMERCE SECURITY

A. Status of mobile e-commerce development

Customers use mobile terminals such as mobile phones or handheld computers that can access the Internet to conduct mobile e-commerce activities. Mobile operators, e-commerce operators and mobile device manufacturers are the main players to participate in the mobile e-commerce behavior of consumers [2]. With the continuous increase in the number of mobile users in China, China's mobile e-commerce has entered a period of rapid development. According to the data released by the Ministry of Industry and Information Technology of China, as of the end of December 2017, the total number of mobile phone users of China's three basic tele-communications companies has

reached 1.41 billion, the details is shown in fig 1, which shows that the mobile e-commerce market space has large development space [3].
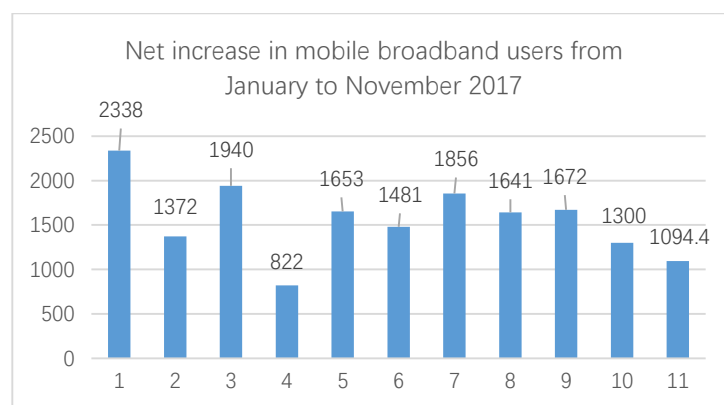

Fig. 1   Mobile broadband user number

B. The threats of mobile e-commerce security

1) Mobile terminal

Viruses are a major security threat to mobile terminals such as mobile phones. The way the virus spreads is mainly through text messages, emails, browsing websites and mobile phones. After the mobile phone is infected with a virus, the system may not work properly, and the mobile phone may automatically make a call, causing huge loss of telephone charges to the user. In addition, it is also possible to leak user passwords and private information, resulting in a capital security risk.

2) Network Service

The threats to the network service system are mainly: (1) unauthorized access. System intruders impersonate legitimate users by falsifying their identity and steal user data. (2) Integrity threats. If system information is illegally modified by intruders, which can cause damage to data integrity. (3) Refusal of service. The intruder sends a large amount of spam to the server, causing the server to fail to provide services to the user.

3) Privacy Security

Mobile e-commerce faces serious privacy security issues in the context of the 4G era, because 4g mobile networks are more open than the original wireless networks, so they are more likely to be targeted. Hackers steal personal privacy information from

users through network vulnerabilities and commit criminal activities such as fraud, which poses a great threat to users' personal and property security [4].

III. OVERVIEW OF VOICEPRINT RECOGNITION

A. Voiceprint recognition concept

Voiceprint recognition can be seen as a branch of Speech Recognition technology, which is in the range of speech signal processing, and both of them rely on the characteristics of the speech signal. The difference is that the purpose of speech recognition is only to identify the speech content in the speech signal, but not to identify the specific identity of the speaker, and the purpose of voiceprint recognition is to identify who the specific identity of the speaker is, in the speech signal. The semantic content is not concerned, emphasizing the difference between different speakers [5]. The most secure and reliable

identity authentication system usually introduces biometric technology, which greatly improves the security of the mobile e-commerce transaction process. Although voiceprint recognition technology is not the most widely used in many biometrics, it is undeniable that it has great potential application value. Compared with other biometrics, voiceprint recognition has many features such as low cost, fast recognition [6].

B. Classification of voiceprint recognition

Voiceprint recognition is divided into two categories, one is the speaker recognition, and the schematic diagram is shown in Figure 2. The other is the speaker confirmation, and the schematic diagram is shown in Figure 3. The former is to judge who is the sender of the voice among several people, and the latter is to confirm whether the voice is issued by the designated person.
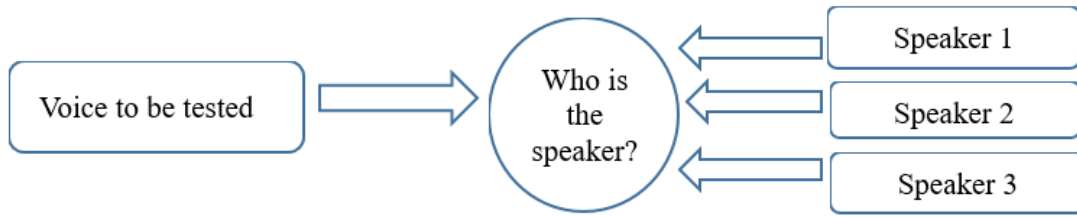

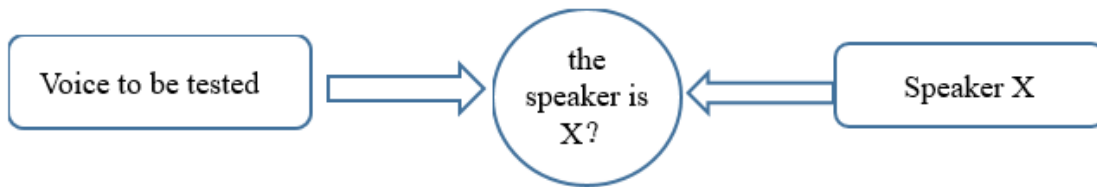Fig. 2   Diagram of speaker recognition

Fig. 3   Diagram of speaker confirmation

IV. APPLICATION OF VOICEPRINT RECOGNITION TECHNOLOGY IN MOBILE E-COMMERCE

In recent years, with the popularity of mobile communication technologies and smart phones, mobile e-commerce has developed rapidly. However, security issues have become more prominent. Some people have set passwords too simple for convenience, while too complicated passwords are easy to forget [7]. In contrast, voiceprint recognition is much simpler, and voiceprint recognition is not only convenient but also very secure. The uniqueness of the voiceprint makes everyone have a unique identity. If the user forgets the password,

he only needs to say a few words according to the system requirements to complete the authentication. As a result, the identity authentication process is greatly simplified. Users provide a more convenient service experience. In addition, combined with voiceprint recognition technology and digital encryption technology, transaction security can be improved greatly in mobile e-commerce transactions [8].

A. Introduction to voiceprint recognition process

The voiceprint recognition system is mainly composed of data preprocessing, voiceprint feature extraction, pattern matching and discrimination. The details can be shown in Fig.4.
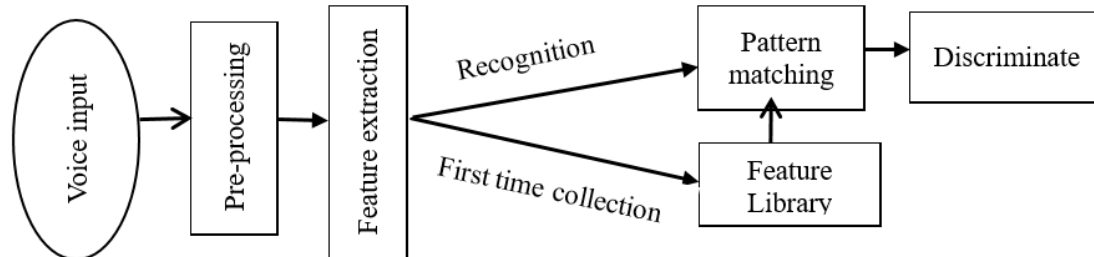

Fig. 4   Schematic of Voiceprint recognition system

1) Pretreatment

In fact, in a complete voiceprint recognition system, both the training process and the recognition process must pre-process original voice collected from the users, such as sampling, pre-emphasis, windowing etc. Sampling is the conversion of speech into computer-processable digitized signals. Pre-emphasis is a compensation technique that compensates for the loss of the speech signal during transmission. Windowing is to reduce the discontinuity of the signal at the beginning and end of the frame [9]. The pre-processing in the voiceprint system requires more high-frequency characteristics information to distinguish the speakers more accurately.

2) Feature extraction

The voiceprint feature value has a direct impact on the recognition effect. Although the current research has not fully understood which parameters are the best choice to reflect the speaker's personal characteristics, the best feature parameters can be found from two differences, one is the difference in the structure of each person's vocal organs, and the other is the different pronunciation habits of the speaker. The former difference appears as a static characteristic parameter in the speech spectral structure; the latter difference appears as a characteristic parameter that changes dynamically with time in the speech spectral structure. If you want to better reflect the speaker's speech characteristics, you can combine dynamic parameters and static parameters into composite feature parameters.

3) Pattern matching

After the feature is extracted, the next step is to choose the appropriate pattern matching method. The matching mode method can be roughly divided into two categories according to different recognition objects. One is text-related and the other is text-independent.(1) Text dependency method. The use of text-related methods to fully consider the meaning of speech and

speaker characteristics, so it is easier to implement. The main methods are dynamic time warping method (DTW) and hidden Markov model method (HMM). (2) Text-independent method. Text-independent is the focus of current voiceprint recognition technology. Although the implementation method of the method is relatively complicated because the speech content is uncertain, the flexibility is stronger because it does not require the user to pronounce according to the specific content. The main methods of text independence are probability statistics method, vector quantization method (CVQ) and artificial neural network method (ANN).

4) Discrimination

In the speaker recognition system for voiceprint recognition (as shown in Fig. 3), a multi-threshold decision method is generally employed. Threshold settings are very important for this type of system, not too high or too low, and just set it up. Because if the threshold is set too high, the real speaker may be refused, and if the threshold is set low and may receive people other than the speaker [9]. More advanced methods of differentiation often use machine learning algorithms to dynamically adjust for differential parameters.

V. MODEL AND PROCESS OF VOICEPRINT RECOGNITION IN MOBILE E-COMMERCE SECURITY

Alibaba launched the voiceprint-shopping feature, which allows users to complete their payment with their own voiceprints. Currently in China, Keda Xunfei and Deyi tong are at the forefront of research on voiceprint recognition technology. The voiceprint recognition system has a good application prospect in the real identity verification and payment of mobile e-commerce. The security model constructed in this paper applies voiceprint recognition technology to various activity processes of mobile e-commerce, which can improve the security of mobile e-commerce activities. The Basic security model diagram of Voiceprint recognition can be shown in Fig 5.
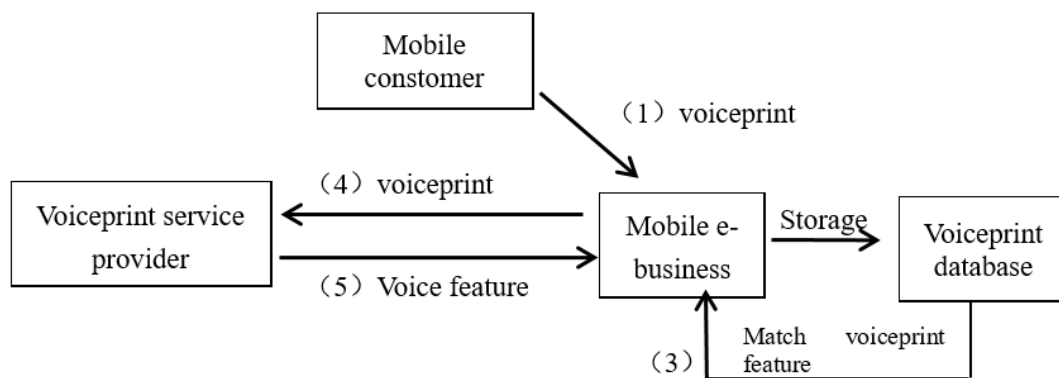

Fig. 5 Security model diagram of voiceprint recognition

The model is mainly created for mobile terminal users such as mobile phones in mobile e-commerce transactions, with the aim of ensuring the security of users in mobile e-commerce transactions. The participants in this model are mobile phone users, mobile e-commerce companies and voiceprint service providers. The users first transmit the voiceprint information to the mobile e-commerce enterprise through the client, then the mobile e-commerce enterprise transmits the voiceprint

information to the voiceprint service provider, and the provider extracts the voiceprint feature. Finally the voiceprint service provider returns the processed voiceprint to the mobile e-commerce business to confirm the identity of the user, thereby ensuring payment security. The main steps of this model are the extraction of voiceprint information, the storage of voiceprint information and the matching of voiceprints [10].

The basic process of the security model consists of three parts. The first is the extraction of voiceprint information. That is, the acquisition of the original data of the voiceprint, this step collects the voiceprint through the collector and formats and saves the collected data, and needs to pay attention to the protection of the integrity of the data information while performing data feature extraction. The second step is the storage of voiceprint information. The system needs to store the extracted voiceprint information features in the voiceprint database for use by mobile e-commerce enterprises. This process is often encrypted. The third step is the matching of voiceprints. After the mobile phone user inputs the voiceprint, the voiceprint will be sent to the mobile e-commerce enterprise in the form of "public key" encryption. After the mobile e-commerce enterprise receives the key, the voiceprint information is pre-processed and encrypted. After that, it is sent to the voiceprint service provider. The voiceprint service provider decrypts the user's voiceprint information by using the key and extracts the voiceprint information. The extracted voiceprint features are encrypted and then returned to the mobile e-commerce. Finally, the voiceprint features are stored in the user voiceprint database in the mobile e-commerce background to respond more quickly to user services.

VI. SUMMARY

Human biometrics are often unique and not easily counterfeited. The voiceprint feature has the characteristics of simple processing and high security level, and is very suitable for the application scenario of mobile electronic commerce, a lightweight intelligent terminal. We analyzed the basic characteristics of voiceprint recognition, and constructed a mobile e-commerce security model and analyzed its business process in detail. Our system fully utilizes the technical advantages of voiceprint recognition technology in the mobile e-commerce identity authentication system, thus effectively solving the troubles of user key management. We have reason to believe that voiceprint recognition technology will have greater development prospects in mobile e-commerce.

ACKNOWLEDGEMENT

REFERENCES

[1] Zhong Yuantao. Application of Mobile E-commerce Security to Speech Recognition Technology [J]. Modernization of Shopping Mall, 2015(03): 82.

[2] Wang Dafei. Mobile e-commerce security research [D]. Wuhan University of Technology, 2011:10-13.

[3] Ministry of Industry and Information Technology of the People's Republic of China. Economic Operation of the Communication Industry in November 2017 [EB/OL].[2017-12-19].http://www.miit.gov.cn/n1146312/n1146904/n1648372/c5967653/content.html

[4] Hu Ling, Quan Youqi, Hu Wei. The privacy and security of mobile e-commerce in 4G era [J]. Shopping mall modernization, 2017 (18): 37-38.

[5] Zhou Lei. Research on speaker identification method based on voiceprint recognition [D]. Shanghai Normal University, 2016: 3-4.

[6] Komal K. Kumbhare, K.V. Warkar. A Review on Noisy Password, Voiceprint Biometric and One-Time-Password [J]. Procedia Computer Science, 2016, 78: 382-383.

[7] Zheng Fang. Li Lantian, Zhang Hui, Eskar Meat. The voiceprint recognition technology and its application status [J]. Information Security Research, 2016, 2 (01): 49-50.

[8] Xia Biting, Qiu Tian. Voiceprint Identification and Its Application in Litigation [J]. Legal System and Society, 2014(34): 127-128.

[9] Peng Shiya. Research on identity authentication technology based on voiceprint recognition [D]. Nanjing University of Aeronautics and Astronautics, 2010: 9-13.

[10] Xu Xiaojuan. Application of fingerprint recognition technology in mobile e-commerce security [D]. Nanchang University, 2014: 23-27.