ATLANTIS PRESS

Advances in Engineering Research, volume 120

International Forum on Energy, Environment Science and Materials (IFEESM 2017)

Design of NFC Mobile Payment System Based On Fingerprint Identification

Xueyi Zhang[1, a], Shuangle Zhao[2,b]

[1]Electronic Information College, Tianjin University of Science & Technology, Tianjin 300222 China

[2]Electronic Information College, Tianjin University of Science &Technology, Tianjin 300222 China

[a]zhangxueyi@tust.edu.cn, [b]zhsl@tust.edu.cn

Key words: NFC Payment; Fingerprint Identification; ActiveX; LabVIEW; Access

Abstract: In order to avoid unauthorized payment of various stolen NFC terminal and to ensure convenient payment process, NFC Secure Payment System Based On Fingerprint Identification is designed, the fingerprint image collection module and the NFC reader are connected on the system server，the system software is developed in LabVIEW Programming environment. It includes User's Interfaces and Service's Application, the storage and identification of personal data, such as NFC card number and fingerprint information and so on, are achieved by managing Access database. When payment is made, the user fingerprint verification is performed first on the server. The system test results are as follows: the payment time is less than 1S, the payment distance is less than 10cm, and the fingerprint storage capacity is more than 4000. The system is accurate, reliable and stable. The intelligent payment system can be used in consuming place of campus as well as enterprise, and also provides reference value for security applications such as identity identification.

Introduction

Near Field Communication (NFC) technology, as a short-range wireless communication technology，has the characteristics of natural security, simple payment process, and fluent user experience. Furthermore, the payment terminals need no networks (WiFi and mobile network) or power supply. Mobile payment, as an offline payment method, is executed through the Non-contact approach between NFC mobile phone and receiving terminal (such as POS machine embedded NFC module). NFC payment is a mature technology in Japan and South Korea. NFC has been applied in small-amount consumption areas such as traffic, shopping, and entertainment, etc in Europe and America. At present, China's NFC payment services such as Unionpay "quick pass" business and China Mobile "and" business are developing rapidly. NFC Mobile phone quantities are becoming increasingly rich, and wearable devices such as NFC wristbands and NFC rings also have been reported in recent news.

Thanks to the short communication distance of the NFC, the common security threats, such as intermediate attacks and the third eavesdropping can be greatly reduced or be solved by encryption, SSL and, other technologies. However, once the NFC terminal is lost, it will lead to the unauthorized payment, information leakage, and other security threats. Therefore, it is necessary to verify the identity, legality, authenticity, and uniqueness of the user. At present, NFC card terminals is mainly applied to small-amount payments, with anonymous and non-loss-reporting methods, and the identity authentication is still based on WPKI, that is, passwords and digital signatures and other authentication methods. Liu [1] proposed a mobile payment identity authentication protocol, which is based on the combination of mobile token and PIN code. Chang Liu [2] proposed an identity authentication system with dynamic password. Password authentication increases the bur-

den of NFC payment obviously , it isn't a quick and convenient way of mobile payment.

The current challenges of NFC, without increasing the costing of terminal, are to prevent unauthorized payment, break the limit of small-amount payment, and improve the user experience. However, little literature has been reported. Abu-Saymeh [3] proposed an authentication framework based on gesture recognition and language recognition, a third-party monitoring software for monitoring all NFC applications was proposed in Ref [3]. However, as the security of the monitoring software affects the security of the NFC application, the security protection of the monitoring software is significant. The fingerprint identification is suitable for the quick payment due to its uniqueness and efficiency. This paper proposes a design of the fingerprint verification provided by the business acceptor and a NFC security payment system that authenticate the identification on the server side. The system is suitable for various NFC terminals.

System composition and working principle

The system includes NFC terminal, NFC card reader (such as POS machine), fingerprint collection module, computer, etc. Block diagram of system composition is shown in Figure 1.

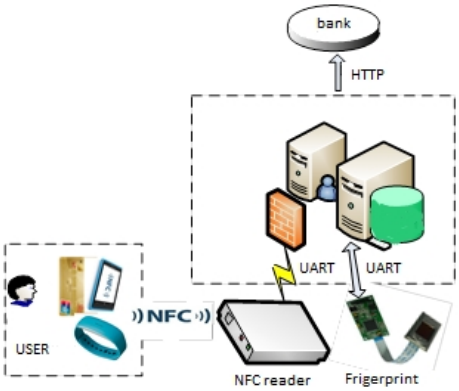

Fig. 1 block diagram of system composition

The system initiates the fingerprint acquisition module and the NFC card reader when the NFC card is detected. Then the system collects the current input fingerprint and generating the signature and sends the NFC card number to the host computer. The application program accesses the host computer fingerprint database according to the unique NFC card number, and reads the registered fingerprint features associated with the card number. The data is sent to the fingerprint module to make the alignment and to produce the results of comparison. The host computer examines the results of the corresponding processing: If the input fingerprint matched with the registered fingerprint, identity authentication is successful; if not, the certification failed. The system implements the authentication to guarantee payment is done by the authorized user.

Hardware Design of the System

The system consists of upper computer and lower computer, the upper computer (PC) is based on LabVIEW to register and store the fingerprint data collected by the fingerprint module to form the fingerprint library. At the same time, the input fingerprint and the registered fingerprint are compared by upper computer. The lower computer includes the fingerprint acquisition module, the NFC terminal and the NFC card reader module. The upper computer and the lower computer make a real-time communication through the USB bus interface, hardware circuit block diagram is shown in Figure 2.

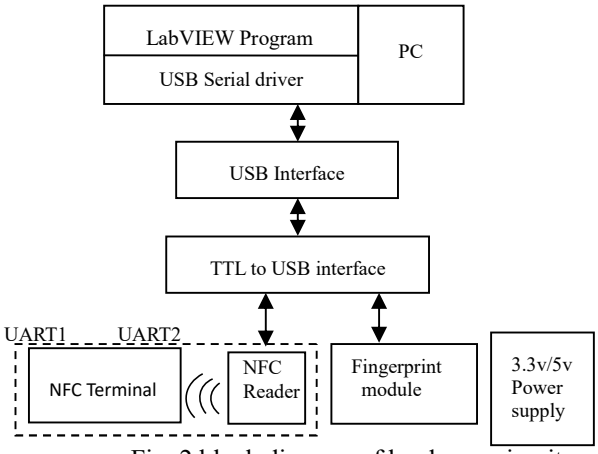

Fig. 2 block diagram of hardware circuit

Fingerprint acquisition module

In order to improve the accuracy and reliability of the system's fingerprint verification, the fingerprint acquisition module is selected with FPM20A which is capacitive and high-resolution. The hardware components include sensor FPC1011F and processor DSP, which support the Biokey algorithm. The algorithm is a fast and accurate 1: 1 fingerprint recognition algorithm, which can realize fingerprint acquisition, preprocessing, feature extraction and fast fingerprint matching. The FPM20A module uses the standard UART serial port to output 32-byte fingerprint feature points. The baud rate is optional, and the default baud rate is 57600 bps. The format of the transmitted frame is 10 bits and there is no parity bit.

NFC card reader module

The NFC card reader module uses ZLG600A-T2 with built-in NFC chip PN532, the module is developed based on the Arduino platform and it can read and write 13.56MHz smart card which is accord with non-contact card protocol(ISO14443-4 A / B) (like a variety of public transport RFID card) [4]. ZLG600A-T2 can generate interruption when a card is detected, the data type and output mode of card number can be set by modifying the firmware[4]. After the serial port conversion, ZLG600A-T2 will transmit the data of card number to the host computer database through the USB interface. The circuit block diagram is shown in figure 3.

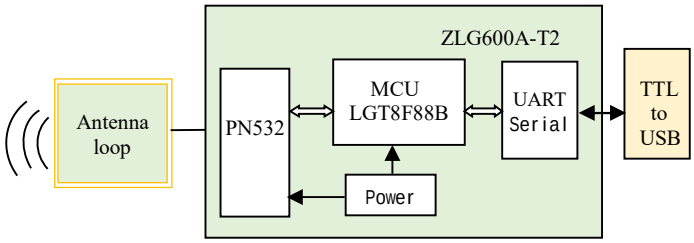

Fig. 3 circuit block diagram of NFC card reader module

NFC card terminal module

The NFC card is a user- oriented terminals of the mobile payment system, held and used by the consumer. According to the NFC communication standard, NFC card operating modes can be divided into card mode, card reader mode and point to point mode. Therefore, NFC card and card reader are NFC devices with built-in NFC chip. Since the NFC standard is compatible with the RFID ISO14443-4 A /B protocol, the NFC terminal does not need to be designed separately. It can be a common RFID IC card or a mobile phone that supports NFC functionality and has configured for card mode. The NFC card power is powered by the non-contact card reader RF field and remains active when the NFC card terminal is not powered, namely a passive IC card.

Serial communication module

Both the card reader module ZLG600A-T2 and the fingerprint acquisition module FPM20A

use the standard UART serial port as output port, which need level conversion module to achieve communicate with PC. The conversion process is simple and does not elaborate.

System Software Design

The lower-level computer's software include NFC Arduino card reader communication module, fingerprint communication command debugging module; PC software is developed by LabVIEW, through LabVIEW access to the database to achieve personal information management and smart card recharge & consumption management, is the server software of the payment system.

NFC Arduino card reader communication

NFC Arduino card reader module is used to achieve the near-field communication between the card reader module and the NFC card terminal to obtain NFC card number and send them to the host computer. By updating the firmware, once it has detected the card, ZLG600A-T2 can generates interruption to read out continuously the card number, the UART output baud rate is 57600Kbps.The firmware update process involves several aspects: (1) Install the IDE chip patch in the standard Arduino IDE programming software environment; 2) Write a new firmware code; 3) Firmware updating[5-6]. The program codes are not listed due to the limited space.

Fingerprint module and host computer communication data format testing

In order to ensure the control instructions are accurate when LabVIEW sends them to the FPM20A module and to get the response results of the module, Gussie serial assistant software is selected to test the format of the data packets between FPM20A module and the host computer, the software supports hexadecimal. For example, when the host computer sends directive of fingerprint image entry, corresponding command and module response data packets format in the agreement are shown in Table 1[7], the data packets format tested with Gussie software is shown in the Figure 4. The command code issued by the host computer serial assistant is "01H", and the confirmation code "00H" returned by the response data packets indicate that the fingerprint image entry is successful. In addition, generating fingerprint image features, uploading fingerprint features and matching fingerprint features such as the instructions were all tested. The instruction & response data packets format of the above test commands are shown in table 2.

Table 1 instruction &response data packets format of inputting fingerprint image

data packets bytes	2bytes	4bytes	1bytes	2bytes	1bytes	bytes
data packets contents	headers	addresses	identifier	length	instruction/confir-mation code	checksum
instruction packets	0xEF01	XXXX	01H	03H	01H	05H
response packets	0xEF01	XXXX	07H	03H	XXH	Sum

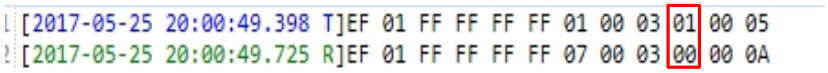

Figure. 4 data packets format tested with Gussie software

Table 2 instruction & response data packets format of the above test commands

No.	function	instruction data packets	response data packets
1	entry fingerprint image	0xEF01 FFFFH 01H 0003H 01H 0005H	0xEF01 FFFFH 07H 0003H XXH SUM
2	generating fingerprint features	0xEF01 FFFFH 01H 0004H 02H ID SUM	0xEF01 FFFFH 07H 0003H XXH SUM
3	uploading fingerprint features	0xEF01 FFFFH 01H 0004H 08H ID SUM	0xEF01 FFFFH 07H 0003H XXH SUM
4	matching fingerprint features	0xEF01 FFFFH 01H 0003H 03H 0007H	0xEF01 FFFFH 07H 0005H XXH SUM

ID means BufferID, it refers to the number of buffers in the module that store fingerprint features, such as CharBuffer1 and CharBuffer2, and their BufferID are 01H and 02H respectively. Only the confirmation code "00H" returned by all of the response packet indicates that the instructions had successfully executed, otherwise they are failed.

Host computer software

The LabVIEW software is composed of two parts: the front panel and the block diagram program. The software includes personal information management module and recharge & consumption module.

Front panel interface of personal information management

Based on the input and output functions of the design controls, the front panel interface is shown in figure 5, it includes functions such as fingerprint signature, display, input for NFC card number and user ID number and NFC card reading, and information input status indication. The program can create, delete, update and query personal information, the creation of the personal information is presented in the following sections.

Figure. 5 front panel interface of personal information management

Program design of information creation

Although fingerprint module FPM20A has fingerprint storage and matching function, the storage capacity is limited. This paper designs the database registration fingerprint feature separately. The module will collect and process the fingerprints which are allowed or authorized, and upload fingerprint features to the host computer by the serial port, through LabVIEW connection, read and edit the fingerprint database. The program uses modular design ideas, including VISA access, fingerprint collection and registration, NFC card number entry and database management modules.

VISA access

LabVIEW uses the VISA node to implement serial communication with the fingerprint module. When the system is working, the module is initialized by the VISA Configure Serial Port. When the fingerprint is collected, the switching value is sent to the FPM20A through the serial port to control its startup fingerprint acquisition and processing program, and then call the serial read function (VISA Read) to read the fingerprint feature.

Fingerprint registration module

This module is to register the new fingerprint features in the host computer to form the fingerprint library. The LabVIEW program issues directives to FPM20A module for fingerprint image collection and fingerprint feature codes creation, and completes the fingerprint feature codes storage by database accessing. The fingerprint registration flow chart is shown in Figure 6.

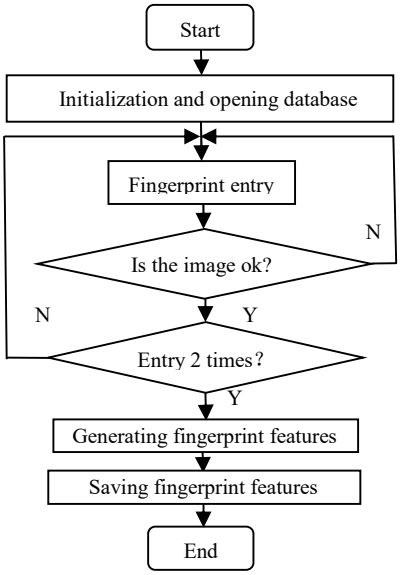

Figure. 6 flow chart of the fingerprint registration

As it requires LabVIEW to edit the database to achieve the new fingerprint registration and NFC card number entry, therefore the specific database operation is unified (see section 3.3.2.4).

NFC card number entry

ZLG600A-T2 is the active mode, once the RF domain detects the NFC card, it will send 10 decimal NFC card number to the host computer through the serial. LabVIEW uses VISA serial read function to read the card number, and write them to the database, if the card number has been registered, then the error returned; Conversely, to the database to add card number.

Database management

This article uses Microsoft Access as a system database to store and manage the fingerprints and NFC card number and other important data. The Access property is rich and flexible for use. First, a database file named Fingerprint.mdb needs to be established in Access. Then, according to the system needs, a fingerprint feature table, user information table, transaction records and NFC card table, user request table, etc. are needed to be created. Each line of these tables is a record and user information table is the core table. UserID is used as the index field links to the other tables of the respective UserID fields. Next, a data source named DSN (Data Source Names) named Finger needs to be created. The fingerprint feature table is shown in table 3, the user information table is shown in table 4.

Table 3 fingerprint feature table in access database

fingerprint feature table		
ID	**User name**	**fingerprint feature codes**
1	LU	EF01FFFF0703003CA13D4F5G6H39C32D6E19B70B7789EF3453 C4D5C65DC33C4C2D34D6A3C6D3D5DC46D3D4CA7D3C4D
2	JIN	EF01FFFF5D4F3D4D51D3D4DBD3D32D4D5D8907C4C3C2C13D4A 6A7A8A9A070702D837D370A0D0F9323DF489D3C4A5AC
3	ZHAO	EF01FFFF5E5A6D7F8C9D00800D3D1D2D4D68D90DD1A2A3A4A5 A6A7A800897782453C0C98C7C5D5434B8B9FC339A5D4
4	W ANG	EF01FFFF4A5D67F8C9C0329C7C6C32100000CCB7B2B3B5B3B1 B6B8C7C54CDC23D4A6A789A62A6A7D8C9A97D6A7D8C9

Table 4 user information table in access database

User Information Table				
ID	**User name**	**NFC coding**	**Student ID**	**balance**
1	LU	5845020336	13212101	100
2	JIN	2158354625	13212102	50
3	ZHAO	4836220402	13212103	80
4	WANG	5621952868	13112104	60

After completing the database and table creation, LabVIEW can access the database. The commonly used access tools are SQL Toolkit, ADO control and LABSQL toolkit [5]. This article calls the Microsoft ADO control using the LABVIEW ActiveX function. The SQL language is used for Read &Write operations of the fingerprint database. Limited by the space, only the methods to open database, to add new fingerprints and NFC card number are introduced in the followings.

(1) Opening database

Using SubVI of opening Database, the Refnum input to open the Automation function node is provided by the Automation Refnum control, and you need to select Microsoft Access from the Object Type Library in the Selecting the ActiveX Class window, then the object Application is created at the top of Access ActiveX Sever and it connects with the opening automation node, Refnum output of the opening automation node is Application Refnum[8].

(2) Adding new fingerprint features

Block diagram of Personal Information Registration Program is shown in Figure 9, for user fingerprints, NFC card number and user ID and other data preservation, each fingerprint has a unique user ID. The database is operated by running Execute Function of the CurrentDb, Execute method is made by conveying the pointer to the database, the use of Execute method has a unique input Query, which performs a valid SQL Query expression. SQL statements include INSERT INTO, SELECT, CREAT TABLE and other instructions, INSERT INTO command is used to store the fingerprint feature codes, and write them to the fingerprint table, the command syntax is: (field1, field2, ...) VALUES ('data1', ' data2 ', ...). Similarly, you can use INSERT INTO to implement card numbers and other data add to the database. After the end of the database operation, you can use the Closing method of Connection object to close the database[9], it is not introduced. User fingerprints and other personal information registration program block diagram as shown in figure 7.

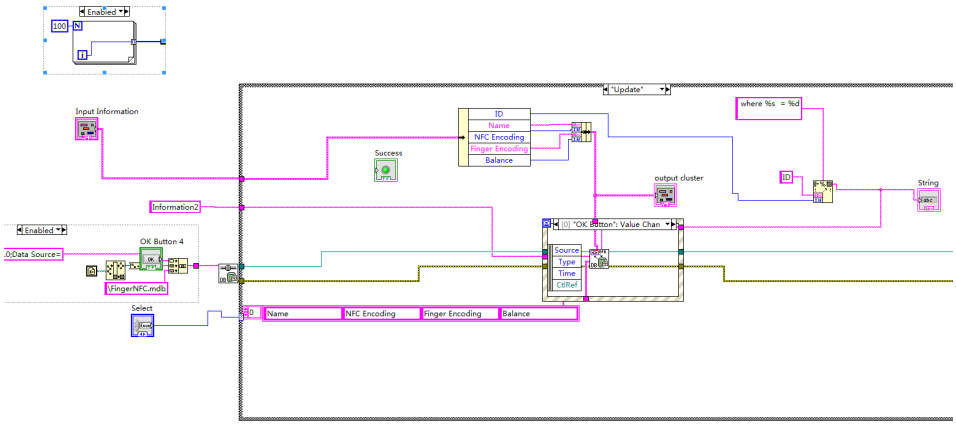

Figure.7 block diagram of personal information registration program

Front Panel Interface of NFC Payment System

Front Panel Interface of NFC Payment System is shown in figure 8 with two parts of Recharge

and Consumption. It shows Consumption Amount, fingerprint verification images and match results, etc. The amount of recharge input, card balance can also be seen in Recharge interface.

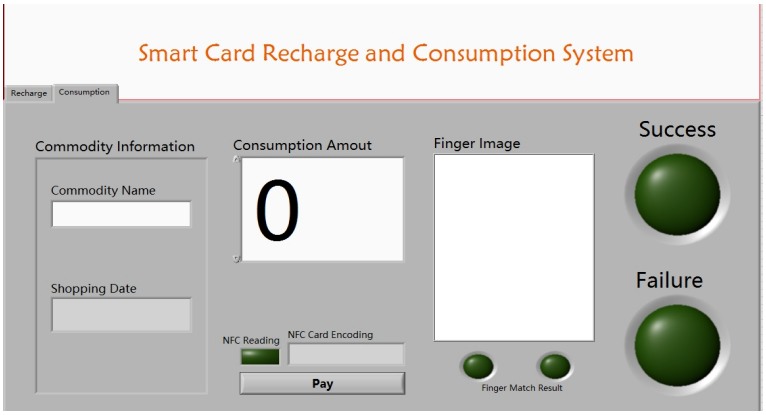

Figure.8 front panel interface of NFC payment system

Program design of NFC fingerprint verification payment

The algorithm of fingerprint identification determines the operating time of the payment system, FPM20A supports 1: 1 fingerprint identification algorithm, therefore, the rapid fingerprint verification is realized by means of fingerprint matching within the module and uploading the results to the upper computer. The fingerprint verification payment is the key part of the system. After the system inputs the consumption amount of money and detects the NFC card, it accesses the user information table in access database, as shown in Table 4. The system gets the NFC card balance and determines whether it is available for the payment, if the balance is insufficient, the charge is not successful. If the balance is sufficient, The LabVIEW program sends the instructions to the fingerprint module for entry fingerprint image and fingerprint feature codes creation， it also accesses the fingerprint library to read the fingerprint codes of the current NFC card holder and sent them to FPM20A module through the VISA function. The system makes difference response according the matching result from FPM20A, if they are equally matched , the system charges, and updates the database balance, if not, the system pay is failed and it exits after two times of mismatching. The system fingerprint verification payment flow is shown in figure 9.

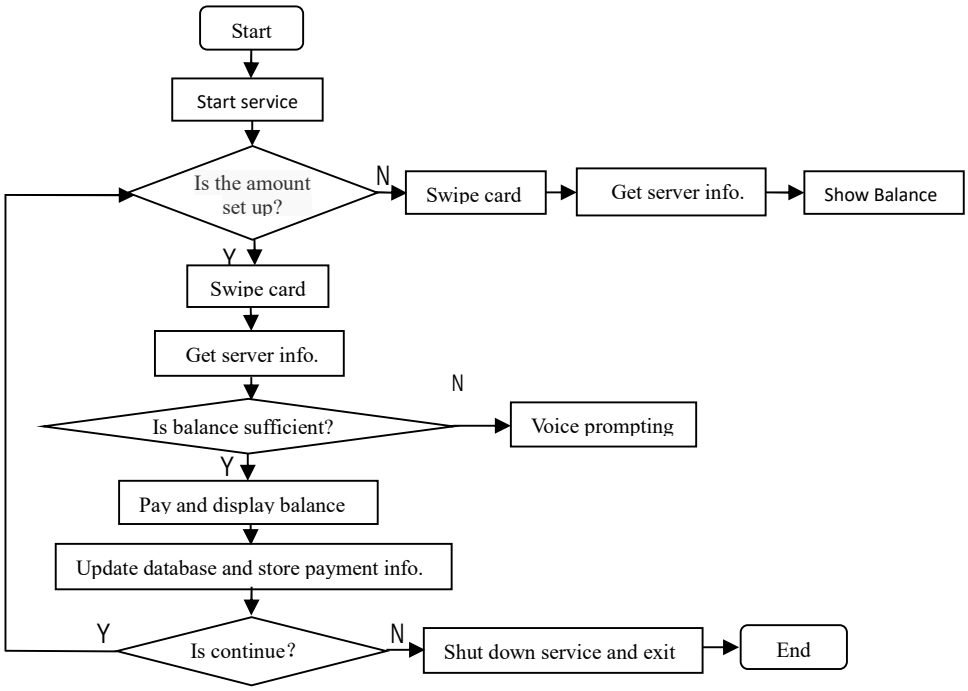

Figure .9 program flow of the system fingerprint verification payment program flow

Trough subVI program creation, the program implements the NFC card number query and can read the value of the specified field of the query record, including the name and balance, the implementation of this function is achieved through a data query subVI program, it opens the NFC card table of the current database and returns the records that match the criteria. The balance in the record is compared with the amount of setting consumption, if the balance is insufficient, the program exits the database, If it is sufficient, the program use the SQL statement to query the record based on the index name (user NFC card number) and to obtain the specified fingerprint feature fields; then the field value is read by use of Property Node 1, Invoke Node 2 and Property Node 3. The three Automation Close Nodes function of Close Property, Close Fields and Close item is to turn off the corresponding database to release the memory. The system fingerprint verification payment program block diagram is shown in figure 10.

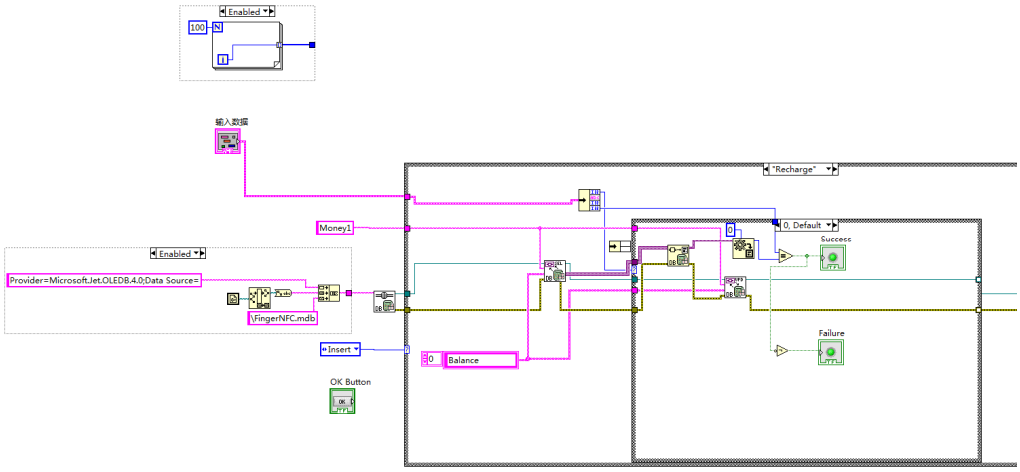

Figure.10 fingerprint verification payment system program block diagram

System Performance Testing

In order to verify the performance and reliability of the NFC security payment system, functional testing is carried out. The system collects 6 fingerprints successfully before NFC payment testing, when the NFC card closes to the antenna of the NFC reader, the number of the card was read out successfully, after setting the amount of consumption is 25yuan, the system waited entry of the fingerprint, its image displayed in the front panel window with lighting up the lamp, the testing of NFC payment is successfully.

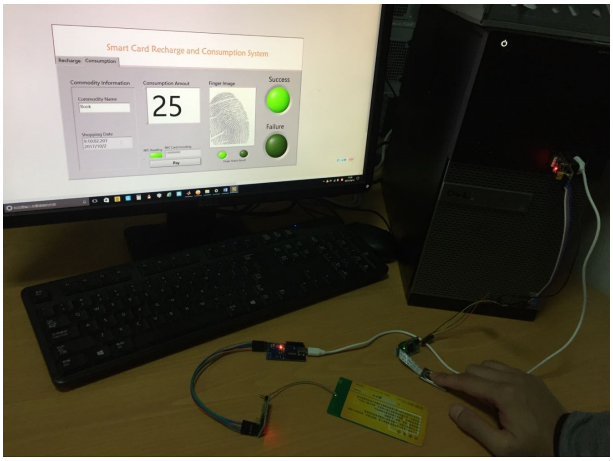

Figure.11 fingerprint verification payment system program block diagram

Conclusion

(1) A NFC secure payment system based on fingerprint identification is designed in this paper, the payment time of the system is less than 1S and its distance is less than 10cm, the fingerprint storage capacity is more than 4000. The system can prevent the payment terminal from being stolen, and ensure the friendly user experience. The system does not increase the payment security.
(2) The system software is based on LabVIEW environment development, through the link of Access database to achieve fingerprint acquisition, entry and recognition. It provides new concepts and methods of fingerprint verification system developing which is different from the system developing in Android platform and embedded platform, the new system is more concise, more efficient. The system capacity and scalability are stronger than previous one.
(3) The design of the system is flexible and practical. If the fingerprint fails to pay, the system can collect the same user's new fingerprints and re-register. The system test results show that the security payment system is stable and reliable, especially for the One-Card system of campus, business and other application occasions, it also provides a reference for identification and other security applications.
(4) The system software store and manage the transaction information and user data information. The further work includes the development server for the user's client. The user can query card balance, recharge records and manage the transaction records by logging the server.

References

[1] Liu Mingda, pick Juan, Zhao Bo, Li Yifan. A mobile payment authentication protocol based on mobile token [J].Wuhan Journal of Science (SCIENCE EDITION),2016，62(2):110－116．
[2] Liu Chang, Li Xiaodong, Bi Yunfeng. Design of fingerprint identification alarm system based on LABVIEW virtual instrument technology [J]. modern electronic technology2012，35(4):187－190．
[3] Dirar Abu-Saymeh, Dhiah el Diehn I. Abou-Tair, Ahmad Zmily “An Application Security Framework for Near Field Communication” 2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.
[4] Tom Igoe, Don Coleman. NFC Arduino、Android and PhoneGap NFC[M]. Publishing House of Electronics Industry，2014.
[5] Wikipedia. Arduino UNO Introduction. http://kb.open.eefocus.com.
[6] Information on http://dzzone.taobao.com/
[7] Information on http://www.zlg.cn/
[8] LabVIEW User nanual．National Instruments Corporation．(2015)
[9]Database ConnectivityToolset UserManual．National Instruments Corporation．(2015)