The Principle and Design of Separate Fingerprint Identification System

Meng-meng Liu(✉)

School of Teacher Education, Anqing Normal University, Anqing, China
Liumm@aqnu.edu.cn

Abstract. Separate fingerprint identification system (SFIS) is composed of high-speed DSP (digital signal processor), SRAM and Flash chip, whose modules include fingerprint entry, image processing, fingerprint contrasting, fingerprint searching and module storing. SFIS can be an integrated outer equipment with the help of corresponding fingerprint sensor.

Keywords: Separate fingerprint identification system (SFIS) · Upper computer · DSP (digital signal processor)

1 Introduction

1.1 Working Principle

As shown in Fig. 1, Fingerprint processing basically includes two parts: fingerprint logging process and fingerprint matching process. Fingerprint matching includes fingerprint contrasting (1:1) and fingerprint searching (1:N).

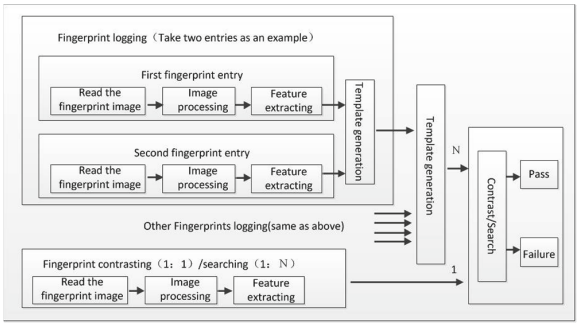

Fig. 1. Working principle diagram.

In the course of fingerprint logging, via fingerprint sensor, the module will record every fingerprint several times. Three times by default, but can be modified into two times at command mode by the corresponding instruction. The

X. B. Zhai et al. (Eds.): MLICOM 2019, LNICST 294, pp. 32–41, 2019.
https://doi.org/10.1007/978-3-030-32388-2_3

following step are processing the recorded image and extracting the features of the image. The distinctive data extracted from the image every time will be first temporarily put in the buffer and then processed. As a result, a group of data representing fingerprint features, which is the template of the fingerprint, can be attained. These data are the basis of fingerprint matching and are stored in the buffer. Finally, the template is stored in the Flash ROM of the module.

In the course of fingerprint matching, module records fingerprint image which requires testing via fingerprint sensor. The feature of the fingerprint image will be extracted. The distinctive data are stored in the buffer, and then will be contrasted with the template generated in the course of fingerprint logging, which will be called 1:1 fingerprint contrasting if the distinctive data are contrasted with one template, or 1:N fingerprint searching if contrasted with several templates.

There are two contrasting results: passing and failure. When the contrasting result is passing, the corresponding template storing serial numbers will be obtained (ID number).

1.2 Main Characters

DSP is the processing center of the fingerprint identifying module. It basically integrates all aspects of fingerprint processing. The advantages are as follows:

(1) Independence: the function of fingerprint entry, image processing, feature extracting, template generating, template storing, fingerprint contracting and fingerprint searching will be finished separately without the control of the upper computer.
(2) Widespread applications: providing two working modes (i.e. Command and Separate) and two module control ports. Four combination states, which are command, contrast, record and delete, appear when the module control ports are powered up. There exist two modes of application scope separate mode application scope, including simple safe box and door lock, and command mode application scope, including more complicated door control, fingerprint IC card terminal, PC online fingerprint recognition and authentication system.
(3) High security: The storage area of fingerprint template in different modes is separated physically and logically. Separate mode is protected by super fingerprint, and command mode by verifying equipment password.

2 Working Mode

There are two working modes of fingerprint identification module: separate mode and command mode. Which mode will be chosen depends on working environment.

2.1 Separate Mode

Separate mode refers to a separate working style of the modules, by which the simple operations, such as fingerprint logging, deleting and contrasting, can be finished. There are three states in separate working mode: logging, fingerprint searching and template deleting.

Fingerprint Logging
Fingerprint logging refers to the process of recording the same fingerprint image several times, generating fingerprint template and storing into module sequentially. If you want to enter one template, you should input fingerprint image three times by default, which means you have to press your finger for three times. But under command mode, you can use system setting command to modify it into two times. As a security measure, the earliest four module logging fingerprints are set as super fingerprints. If there is at least one super fingerprint in the module, fingerprint logging again requires verifying super fingerprint before following fingerprints are entered. The capacity of fingerprint database is 64 fingerprints in separate working mode. When the database is full, new fingerprint will cover the last template and the next direction is given.

Fingerprint Searching
Fingerprint searching refers to recording a fingerprint image that will then be processed and contrasted with all fingerprint templates stored in the module, after which two contrasting results (passing and failure) will be generated. At the fingerprint searching state, the module has dormancy function: if waiting time exceeds 14 s, the module will go into hibernation state. Users can wake up the module by pressing the waking-up pin in the users interface.

Template Deleting
Template deleting refers to deleting thoroughly all fingerprint templates, including super fingerprints in the module. Under the separate working mode, deleting template requires verifying the super fingerprint. After that, the module deletes template and gives direction.

2.2 Command Mode

In the relatively complicated application system, separate working mode can't meet the requirement already. Fingerprint identification modules can work in command working mode. When there is a upper computer (single chip or PC) or network, fingerprint identification and identity authentication management can be finished. Command mode refers to module linking with a upper computer via communication ports, and can finish relatively complicated and complete fingerprint identification management under the control of the upper computers command. Fingerprint identification integrates 28 basic instructions. Combining these basic instructions can satisfy all fingerprint management function in practical applications. The database capacity in command working mode is 512 fingerprints, which are divided into high-end and low-end, with each 256 fingerprints. In the command mode, upper computer should first send a command

to the module to verify the equipment password. The module will accept the following command only if the verification is passed.

The differences of the two working modes are shown in Table 1.

Table 1. Differences between two working mode

Project	Separate module	Command module
Working method	Separate	Receive and execute upper computer commands
Fingerprint database capacity	64 pieces	512 pieces
Fingerprint section	Not segmented	High and low two sections (256 pieces each)
OUT2	Pulse width	1800 ms
Automatic power saving management	Yes (contrasting state)	No

3 Communication Protocols

Communication protocols define the exchanging rules between the fingerprint identification module and the upper computer. The communication protocols of the fingerprint identification module include four levels, which are in Table 2.

Table 2. Communication protocol in fingerprint identification module

Level	Content and Role of?protocol
Application layer	Top level. Specifying rules for specific applications. Application oriented. Mainly providing standard interface for application system
Representation layer	Expression of module working status and execution results of instructions
Transport layer	Specifying convention of data structure rules, response and instruction process
Physical layer	Communication medium and connection of module and upper computer. Mechanical, electrical functions and regulation

3.1 Physical Layer

Module provides two kinds of electrical level Serial communication interfaces: 0 communication interface meeting RS-232C electrical level standard and 1 communication interface adopting standard 5 V logical electrical level (TXD, RXD pin).

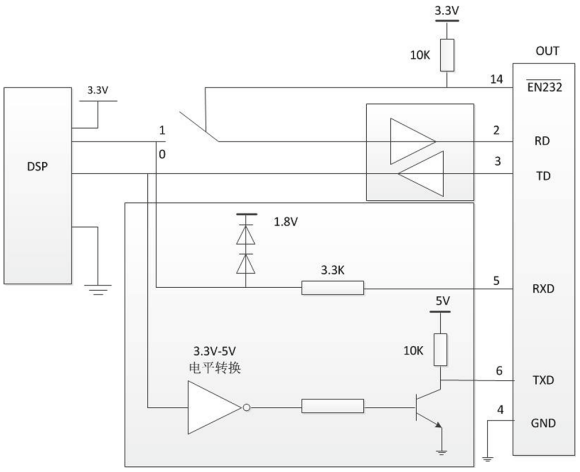

Fig. 2. Serial communication section hardware equivalent diagram.

Auxiliary pin has communication port choosing pin (EN232) and ground (GND). Equivalent Diagram of module inner Serial communication hardware is shown in Fig. 2.

Operating Principle

DSP communicates data with external through serial interfaces. One of them is converted to electrical level fitting for RS232C through 3.3V-RS232C logical level, then linked to the 0 communication port of user interface (that is TD, RD pin). The other is converted to logical electrical level of 3.3 V–5 V, and linked to 1 communication port of user interface (that is TXD, RXD pin).

To prevent interference to the 0 communication port and the 1 communication port, a control pin EN232 is added. When the pin hangs in the air, high level is available, by which the data import of the 0 communication interface is shielded, with only the 1 communication interface available.

When the pin short connects with ground (GND), 0 communication interface is available.

The external links of using serial port are shown in Fig. 3.

Interface Communication Protocols

When the data communicates, the protocol is in semi-duplex asynchronous communication. Porter rate is 57600 bit/s by default.

The porter rate can be set to 115200 bit/s through command. The transferred frame format is 10 bits. One bit 0 is level start bit. 8 bits consist of data and one stop bit and there is no check bit. Frame format is shown in Fig. 4.

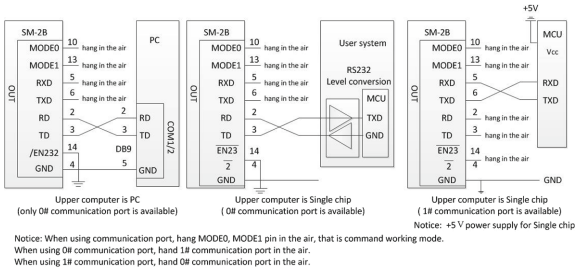

Fig. 3. External connection of serial port diagram.

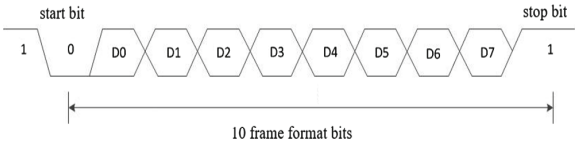

Fig. 4. Frame format.

3.2 Transport Layer

This layer protocol stipulates data structure, sending mechanism and process and convention of directions corresponding to ensure the correctness and reliability of data communication.

Data Flow
The process of data transferring from the module to the upper computer is called upload. The opposite process is called download.

Package Format and Definition
Data transferring adopts the data package of unified structure, whether it is uploaded or downloaded. Data package format is shown in Table 3.

Table 3. Packet format

Packet ID	Address code	Packet length	Packet content	Checksum
	Reserved word		(Instruction/data/parameter)	

The detailed definition of data package is as shown in Table 4.

Table 4. Definition of data packet

Name	Symbol	Length	Instructions
Package ID	PID	1Byte	01H represents command packet 02 H represents data packet and Follow-up packets are available 03 H represents EndData packet
Address code	ADDER	2Bytes	Keep words now, functional extensions later. (0000H)
Packet length	LENGTH	1Byte	Length of packet contents (byte) decided by maximum received buffer size of module, maximum 128 bytes
Packet content			Instructions, data or instruction parameters. Fingerprint feature value and fingerprint template are all data
Checksum	SUJM	2Bytes	Arithmetic cumulative sum from packet ID to the last byte of Packet content. High byte is in front and low byte is in the back, carry more than 2 bytes is ignored

Answer Word

In the course of data communication, module and upper computer check the data transmitted from the other side respectively. In order to confirm the correctness of data transmitted or enable the other side to take remedial measure, verification results to the other side have to be responded. The definition of the answer words are as follows:

(a) The module responds the upper computer

The answer word content package of module responding to upper computer data is 2 bytes, including the answer word and its check. Answer word checking is the original code of answer word. The detailed rules are shown in Table 5.

Table 5. The meaning of module response words

Sequence number	Meaning	Code	Featuring
1	Package received correctly	81H	ACK
2	Package received error, upper computer reissuing packet is required	82H	REIN
3	Package received error, terminate the current packet	83H	EOT
4	Module is busy	84H	BUSY

(b) Upper computer responding module

The answer word content package of upper computer data responding to module is 2 bytes, including answer word and answer word checking. Answer word checking is original code of answer word. The detailed rules are shown in Table 6.

Table 6. The meaning of upper computer response word

Sequence number	Meaning	Code	Featuring
1	Package received correctly	81H	ACK
2	Package received error, upper computer reissuing packet is required	82H	REIN
3	Package received error, terminate the current packet	83H	EOT

Rules of Direction Process

Typical direction process is as shown in Fig. 5.

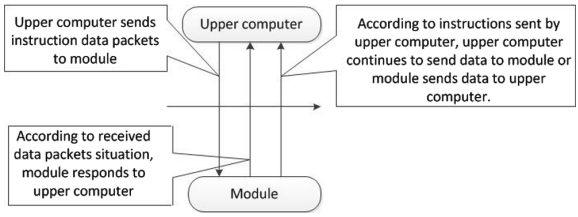

Fig. 5. Typical instruction flow.

3.3 Representation Layer

Representation Layer protocol is the formulation about module working states and direction implementation results. Layers below representation layer only care about transmitting bit stream, while the representation layer cares about grammar and semantics of transmitted information.

Representation Layer protocol divides feedback information into four parts:

(1) States of command completion (success, failure, in progress, await orders etc);
(2) directions types (fingerprint entry, operation, contrasting, searching etc);
(3) results obtained (authentication approved, authentication denied, security level etc);

(4) ID number searched.

This layer protocol stipulates that the application layer obtains module states of implementation and processing results through the states direction.

Module feedback information is through states words (2 bytes).

The first byte was recorded as Ack States (state indication words). The feedback information is mentioned in (1) and (2) above.

The last byte is recorded as Rst States (result indication words). Feedback information is mentioned in (3) above.

4 Module Instruction System

Fingerprint identification module integrates 28 basic instructions, therefore it fits all the fingerprint management functions in practical applications, and can be combined with these basic instructions:

Fingerprint local login (store inside module);
Fingerprint remote login (upload to upper computer through module);
Fingerprint deleting;
Templates download (upper computer download fingerprint templates to module);
Fingerprint searching on site (fingerprint on site for searching and contrasting is recorded through sensor);
Remote fingerprint contrasting (contrasting between fingerprints of recorded on site and specified by upper computer);
Access fingerprint image on site (access fingerprint image on site through upper computer);
Provide storage accessing space to remote users;
Different security level;
Set equipment address code (used for mobile communication) etc.

According to the approach of implementation, instructions are divided into One-way execution and Interactive execution. One-way execution means that the module executes immediately after upper computer commanding and the feedback on implementation results is not necessary.

Fingerprint login, generating feature value, fingerprint contrasting, feature value searching, generating fingerprint image, setting password and verifying password are interactive execution instruction. Interactive execution instruction means that the module must feedback the states and results of this instructions execution after the command from the upper computer is received. Upper computer decides the next operation according to the feedback results.

Data flow control instructions are shown in Fig. 6.

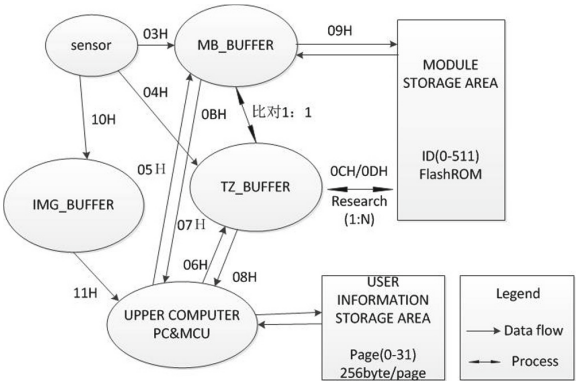

Fig. 6. Data flow control instruction.

5 Conclusion

The principle mentioned in this paper can make up a separate fingerprint identification system or an integrated outer equipment with the help of corresponding fingerprint sensor.

References

1. Jomaa, D., Dougherty, M., Fleyeh, H.: Segmentation of low quality fingerprint images. In: International Conference on Multimedia Computing and Information Technology (MCIT), Sharjah, 2–4 March 2010
2. Iwai, R., Yoshimura, H.: Matching accuracy analysis of fingerprint templates generated by data processing method using the fractional fourier transform. Int. J. Commun. Netw. Syst. Sci. **4**, 24–32 (2011)
3. Perichappan, K.A.P., Sasubilli, S.: Accurate fingerprint enhancement and identification using minutiae extraction. J. Comput. Commun. **5**, 28–38 (2017)
4. Dakhil, I.G., Ibrahim, A.A.: Design and implementation of fingerprint identification system based on KNN neural network. J. Comput. Commun. **6**, 1–18 (2018)
5. Kouamo, S., Tangha, C.: Fingerprint recognition with artificial neural networks: application to e-learning. J. Intell. Learn. Syst. Appl. **08**, 39–49 (2016)
6. Althobaiti, O.S., Aboalsamh, H.A.: An enhanced elliptic curve cryptography for biometric. In: Proceedings of the 7th International Conference on Computing and Convergence Technology, Seoul, 3–5 December, pp. 1048–1055 (2012)
7. Scheirer, W., Bishop, B., Boult, T.: The biocryptographic key infrastructure. In: Proceedings of the IEEE International Workshop on Information Forensics and Security, Seattle, 12–15 December, pp. 1–6 (2010)
8. Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition, 2nd edn. Springer, London (2009). https://doi.org/10.1007/978-1-84882-254-2
9. Maio, D., Maltoni, D., Cappelli, R., Wayman, J.L.: Second fingerprint verification competition. In: Proceedings of the 16th International Conference on Pattern Recognition, vol. 3, pp. 811–814 (2002)
10. Schaad, J.: Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF). 10.RFC 4211 (Proposed Standard) (2005)