Design of fingerprint identification system based on DES

Cong-Jiu Zhong
Shenyang Aerospace University, Shenyang, China
E-mail: zcj7409@126.com

The fingerprint verification technology is of better feasibility and utility, due to the uniqueness and invariability of fingerprints. So the automated identification based on fingerprints is becoming an attractive alternative to the traditional methods of identification. This system uses DSP chip, the fingerprint acquisition module, serial communication module, SDRAM, EPROM memory element and the CPLD as logic control unit. On the basis of DES encryption function, part fingerprint identification is used to identify the fingerprint characteristics of the 64 results of processing as the key to use the DES algorithm for fingerprint encryption. This system is easy to use, and it has higher security of information transmission.

Keywords: DSP; DES; Encryption; Fingerprints.

1. Introduction

Now many the computer system including much confidential system is the use of "user ID + password" approach to the identity of the user identification and access control. However, this approach implies some problems .For example, the password is easy to be forgot, also easy to be stolen. Although we can require the user to change their password in time to prevent theft behavior, but this method not only increase the burden of the memory of the user, also cannot fundamentally solve the problem [1].

With the progress of technology, the fingerprint identification technology has begun to walk into our daily life. The paper is based on the fingerprint characteristic as the encryption keys. Because the fingerprint of different people is unique, so the security of the whole system is higher, is not easy to be cracked. Because the system need only the user's fingerprint as the secret key, so the use of this system is more convenient. The system use fingerprint using DES algorithm encryption, produce key can be decrypted [2].

2. System Designing

System mainly includes DSP chip, the fingerprint acquisition module, serial communication module, SDRAM, EPROM memory element and the CPLD as logic control unit. Key points of this system is to provide a quick and accurate fingerprint recognition algorithm, on the basis of further implementation file encryption function, improve the security of information transmission. This system mainly uses in fingerprint identification part by fingerprint texture feature of the fingerprint identification. In file encryption section, this system mainly uses the DES encryption algorithm, fingerprint identification part is used to identify the fingerprint characteristics of the 64 results of processing as the key to using the DES algorithm for fingerprint encryption. System block diagram is shown in figure 1.

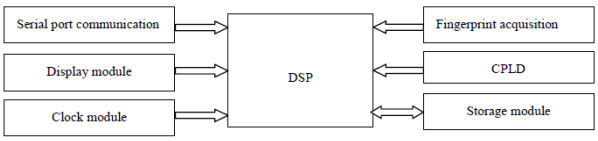

Fig. 1 System block diagram

Fingerprint identification module is central FP200A of the company.FP200A fingerprint identification module is independent, it provides a complete fingerprint acquisition, image processing, the fingerprint feature extraction and fingerprint feature template matching function, and provide no less than 1 m bytes of storage space, used to store user data, user template fingerprint characteristic and verify records (optional).Through the UART serial port communication protocol, outside of the host or the controller system can complete control of FP200A call its various functions, thus FP200A can be used for various application systems.

MCU is TMS320VC5509A, it has two multiplier (MAC), four of the accumulator (ACC), a 40 bits the arithmetic logic unit (ALU), a 16 bits ALU, which greatly enhances the operation ability of DSP. Instruction word length is not only a single 16, highest can be extended to 48, data word 16 bits long; Work under 144 MHZ, instruction cycle can reach 6.94 ns. In the software programming, considering the influence of the speed and accuracy of performance, the fixed-point arithmetic and floating point arithmetic based on fixed-point DSP clever union, not only ensure the processing speed, and improve the computing accuracy and the recognition rate.

SDRAM storage module is used to run the operating system and all kinds of data caching, this design uses 4 MT48LC4M16A2 chip parallel extensible 64 MB of storage space.TMS320VC5509A in phase-locked loop produce storage

control unit of the clock signal, and using this clock MTMS320VC5509A and synchronization of SDRAM, bringing great CPU cores with different memory and speed matching.

A serial port communication module is to use TL16C550 chip, it is a standard serial interface chip, its control register base address 0 x400200, 8 address register occupy TMS320VC5509 unit. A serial port interrupt INT0 connection with TMS320VC5509, users can use TMS320VC5509 interrupt 0 response to a serial port interrupt.

3. Summary of DES

DES is a kind of design for binary coded data, the mathematical operation of the computer data can be password protected. DES through key for 64 - bit binary information is encrypted, the 64 information of plaintext encrypted into a 64 - bit information of the cipher text. As a result of the DES encryption algorithm is public, so the encryption intensity depends on the degree of secrecy keys. The information after being encrypted is available for inverter with corresponding plaintext.DES data encryption system process logic block diagram is shown in figure 2.

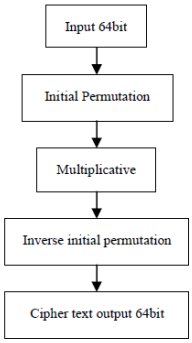

Fig. 2 The main steps of the DES algorithm t

DES algorithm is mainly a nonlinear transformation of the data stream and basic computing through the loop or iterations, with a simple shift to the left, right, 2 addition and so on, such as encryption, decryption transform or change.DES algorithm of the data flow is the basic framework of fixed, through the decomposition of key, will be a 64 - bit key into 16 48 (binary) key, each key control a loop or iteration. The main process is:

1. Will be a 64 - bit key into a set of 16 key 48 seats;
2. 2 addition of module 2;
3. Choose encryption function;

4. Transform the last iteration of the output after block transform the results of a 64 – bit;

5. Initial displacement;

6. Inverse initial permutation [4].

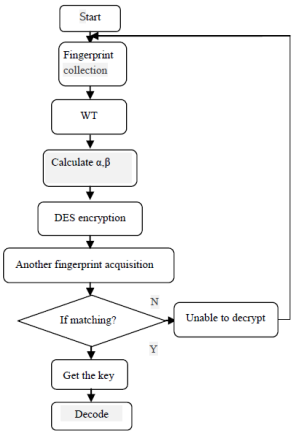

Fig. 3 The fingerprint encryption and decryption process

4. C language Implementation of the DES Algorithm

Based on the fingerprint encryption and decryption process is shown in figure 3. Based on C language implementation of the encryption process flow chart shown in figure 4, the decryption process is the reverse process, is no more [3].

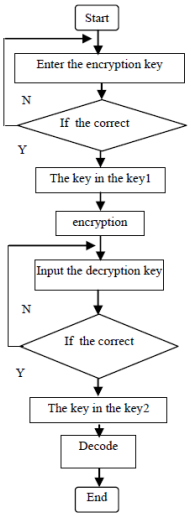

Fig. 4 Encryption process flow chart

5. Conclusion

DES algorithm is a kind of encryption technology the most widely used, although some people think that it's less number of iterations, the key length is short, secrecy intensity is not enough, but until now no one can break it.DES algorithm is also in constant improvement, now has a 128 - bit encryption method. Implementation method of a lot of DES algorithm, using C language to achieve the main because of more popular use of C language, most people are easier to accept. It is simple and easy to understand by C language to implement, more suitable for popularization of data encryption technology [5].

Fingerprint identification technology profit from the development of modern electronic integrated manufacturing technology and the rapid and reliable research of the algorithm. Although fingerprint is only a small part of the human body skin, but the amount of data being used to identify is quite large. The data for comparison is not simple equal and unequal problem. It need for a large number of operations of fuzzy matching algorithm [6].Modern electronic integrated manufacturing technology allows us to make a fairly small fingerprint image reading device, at the same time, the rapid development of the personal computer operation speed is provided on the microcomputer and single chip microcomputer to the possibility of two fingerprints matching operation. In addition, the matching algorithm and constantly improve the reliability, fingerprint identification technology has very practical.

References

1. William stallings. Yang Ming, guang-hui xu, neat Think tank army et al [M]. Password encoding and network security: principles and time. Beijing: electronic industry press, 2001.
2. Wang Yanbo, Xue Tong. Applied cryptography [M]. Beijing: mechanical industry publishing house, 2003.
3. [the] Bruce Schneier. Wu Shizhong. Applied cryptography protocol, algorithm and C source program. Beijing: mechanical industry publishing house, 2001.
4. hai-quan li. Computer network security and encryption technology [M]. Beijing: science press, 2001.
5. Zhou Xueguang Liu Yi. New; Information security [M]. Beijing: mechanical industry press, 2003.
6. A.De Santis, D.lacoviello.An Efficient Adaptive Algorithm for Edge Detection Based on the Likelihood Ratio Test[J],International Journal of Adaptive Control and Signal Processing,2002,Vol.16.