Design and Implementation of Identity Authentication System Based on Fingerprint Recognition and Cryptography

Feng Fujun, Li Xinshe, Wang Litao
Elementary Command College
Rocket Force University of Engineering
Xi'an, China
e-mail: f_fjun@163.com

***Abstract*—A new scheme based on fingerprint recognition and cryptography technology is proposed. The scheme verifies the user's identity using the unique, reliable and stable fingerprint information, and realizes identity authentication to "person". It provides the design and implementation of user register and authentication, encrypts some important information using MD5, and realizes the double authentication, which includes username/password and fingerprint recognition. The testing results show it is more available, reliable and secure.**

Keywords-fingerprint recognition; cryptography; identity authentication; MD5

I. INTRODUCTION

Identity authentication is the first door of information security, and as the important defense line for network security [1], which means the procession of establishing trust through identifying specific users or systems. The realization of traditional authentication based on password is simple, but it may be divulged or decrypted easily; the method of authentication based on smart card or USBKey is relatively secure, but the devices may be lost or carried inconveniently. The method of biological authentication uses the unique， reliable and stable physiologic features, and realizes identity authentication to "person" [2].

As one kind technology of biometric recognition, with the characteristics of commonality, uniqueness and persistence, fingerprint recognition is extensively applied in identity authentication systems, and greatly improves security of information procession. Most researches focus on the fingerprint recognition algorithms [3-5] and systems [6-8], but the fingerprint recognition systems can be intruded by illegal users through forging fingerprint films. So the key point is how to resolve shortages of fingerprint authentication. In this paper, a secure double identity authentication scheme based on fingerprint recognition and cryptography is proposed.

II. FINGERPRINT RECOGNITION

Finger ridge is formed by concavo-convex front skin of finger end, and fingerprint is formed by ridge arranging regularly. Fingerprint minutiae include starting point, ending point, joining point and bifurcation point. In fingerprint recognition, classification is realized by global features such as ridge and triangle point, identity authentication is realized by local features such as location and orientation.

The principle of fingerprint recognition is in Fig.1. Fingerprint images are obtained and preprocessed, then fingerprint features are extracted, and recognition results are got by the matching algorithms. A whole fingerprint recognition system includes fingerprint collecting, image preprocessing, feature extraction and image matching. Fingerprint image processing includes image enhancement, binarization and thinning.

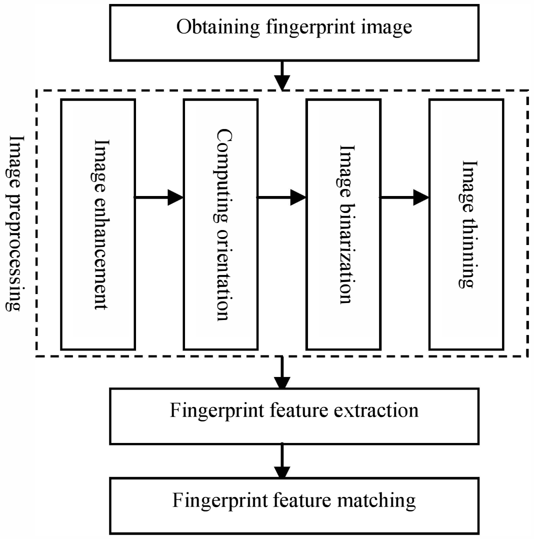

Figure 1. Principle of fingerprint recognition

III. DESIGN AND IMPLEMENTATION

The targets of this scheme proposed are high security, good reliability and simple operation, and it includes two functions: double identity authentication and sensitive data protection. Double identity authentication means username/password is as the first line of secure defense and fingerprint recognition as the second, users can legally login the system if they pass the two defenses. The passwords are encrypted and stored in the system database, which realizes the data protection.

978-1-4673-9026-2/16/$31.00 ©2016 IEEE

A. Design Target

The design target of the identity authentication scheme based on fingerprint recognition includes three sides as blow:

(1) High security

Security is the first target of the identity authentication system proposed, and it can realize the identity authentication to a "person" and protect the system from masquerade attack. There exist many leaks for the traditional username/password, so it must enhance the security of the identity authentication system.

(2) Good reliability

The reliability denotes the low fault rate and the stable system performance. There are many factors influencing the reliability, such as the precision of the device and the advanced degree of fingerprint recognition algorithms. In biological system, the reliability is measured by FRR (False Rejection Rate), FAR (False Acceptation Rate) and ERR (ERR Registration Rate) and the work velocity.

(3) Simple operation

The system proposed must satisfy the simple operation, and good interface. The login time can be controlled in an acceptable range.

B. Environment

Software: operation system is Win7; database is Microsoft SQL Server 2008; programming is Visual Studio 2010; secondary development is biokey+SDK5.0; program language is C++.

Hardware: fingerprint device URU4000B, which is used extensively in fingerprint encryption and the embedded systems.

C. User Register

It demands friendly interface of human-computer interaction and complete functions, register information of users is stored securely in the database, which is convenient to information matching when a user login. The system functions are listed below:

(1) Collecting and storage of basic information of users. The basic information of users includes username/password, telephone and email address.

(2) Collecting and storage of fingerprint information. The collecting of fingerprint information is after inputting the basic information of users. Firstly the fingerprint device initializes, and then fingerprint templates are extracted and stored in database.

(3) Encryption with MD5

MD5 is a secure hash algorithm, it input a text in a group with 512bit, and then the group is divided to 16 blocks with 32bit, after hash it outputs 4 blocks with 32bit, that is the hash value with 128bit. In the scheme proposed, the register information of users are encrypted with MD5 and hash values are stored in the database, which is used to confirm the identities of users by matching those of information inputted when users login. The procession of user register is in Fig. 2, and the database is designed as Table I.

TABLE I. DATABASE DESIGN OF BASIC INFORMATION OF USERS

Field	Type	Length	Remark
NAME#	Char	20	Name(key)
ID	Char	20	password
PHONENUM	Char	11	Telephone number
Email	Char	40	Email address
Fingerprint	text	20	Fingerprint template

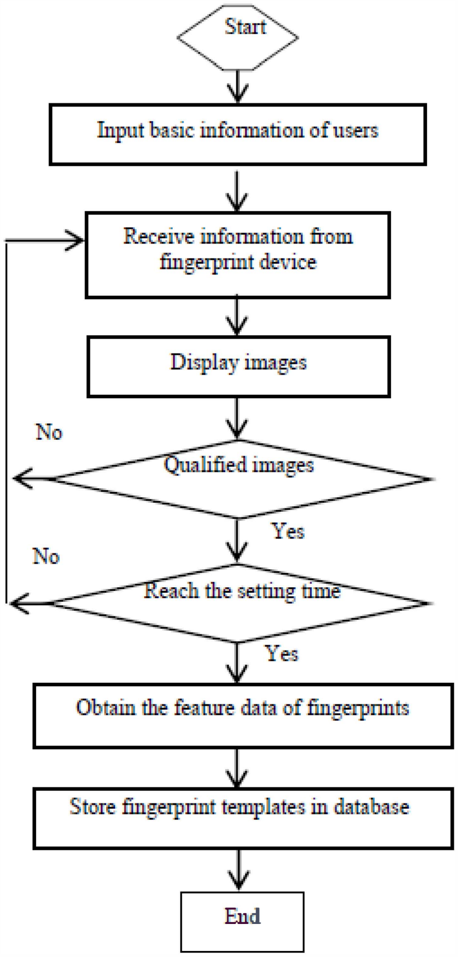
Start
Input basic information of users
Receive information from fingerprint device
Display images
No
Qualified images
Yes
No
Reach the setting time
Yes
Obtain the feature data of fingerprints
Store fingerprint templates in database
End

Figure 2. Procession of user register.

The architecture of the system proposed is based on C/S, which is login is in the client and register is in the server. When a user logins the system, the password the user inputted is computed with MD5, it is compared to the MD5 value stored in the system, and then it can confirm whether the password is correct. Through MD5 the legality of the user identity can be confirmed under the circumstance that the text of the password is not known by the system.

D. Double Identity Authentication

The procession of double identity authentication is in Fig.3. Login includes two parts: username/password and fingerprint recognition.

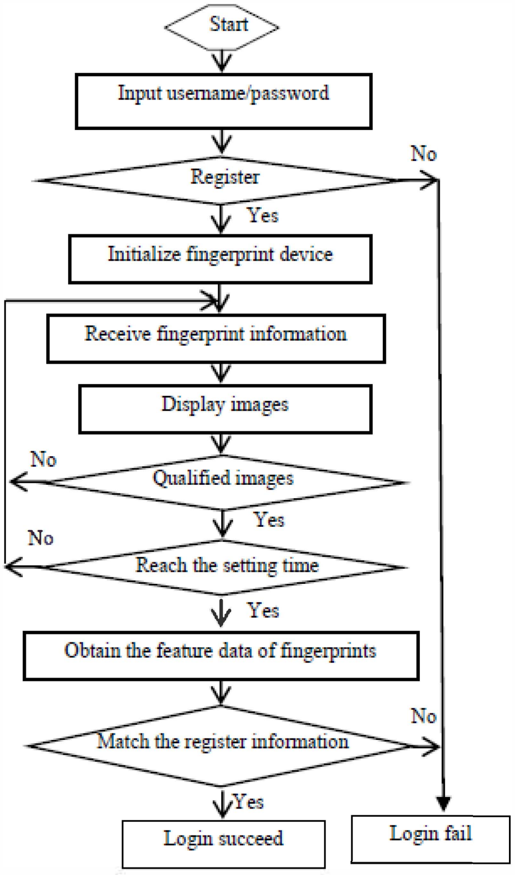

Figure 3. Procession of user login.

(1) Login with username/password

The username/password is encrypted with MD5, and we get a hash value. The identity of a user can be ensured whether legal through matching the hash value we got with that registered in database.

(2) Fingerprint matching

Users will be authenticated with fingerprints after they pass the authentication with username/password. The fingerprint device initializes, and fingerprint information will be inputted after the device works normally. Then extraction of fingerprint templates and display of fingerprint images are completed by the computer, and judge the fingerprint images are whether qualified, qualified fingerprints will be matched with templates registered in database, unqualified ones will be abandoned, and users should login again.

IV. Performance Analysis and Verification

A. Usability Analysis

Usability is an important index for evaluating authentication scheme. A user must use the registered finger to input information, and legality of the user is verified by fingerprint matching. A user can access the system if he input the correct username/password and fingerprint information, this procession need about 20 seconds, which is very convenient.

The fingerprint database is established for performance verification. It chooses 25 users randomly, each user registers ten fingers, and each finger registers three times, so it has 750 fingerprint templates. For verifying the performance of the system, another two indexes for evaluating usability are given, that are register time and login time. The register time means the time from collecting fingerprint to writing fingerprint templates into the database. The login time means the total time for completing username/password and fingerprint authentication.

We choose a test user randomly, and the register time of the left hand is in TABLE II, and that of the right hand in Table III. Then we choose 5 registered users, the register time is in Table IV. From testing results, the register time needs about 10 seconds, and the login time needs about 15 seconds, so it can satisfy the requirements of users.

TABLE II. Register Time of the Left Hand of Tester

Finger	1	2	3	4	5
Register Time(sec.)	10.3	9.5	8.3	7.4	16.4

TABLE III. Register Time of the Right Hand of Tester

Finger	1	2	3	4	5
Register Time(sec.)	9.2	8.7	9.0	11.8	9.3

TABLE IV. Login Time of the Registered Users

User	1	2	3	4	5
Login Time(sec.)	15.5	13.2	23.3	15.4	14.4

B. Reliability Analysis

The evaluation indexes of the fingerprint recognition include FRR, FAR and ERR. FRR denotes the false rejection rate which considers the same fingerprints to the different. Because the different outside conditions, the fingerprints becomes incomplete and fuzzy, which make the detecting fingerprints not match to the registered ones. FRR is expressed as

$$FRR = \frac{N(\textit{the mumber of the rejection fingerprints})}{M(\textit{the total mumber of sampling})} \times 100\%$$

FAR denotes the false accept rate which considers the illegal fingerprints to the legal ones. In some environments with high security, FAR is demanded to low as far as possible, which ensures the illegal users cannot be accepted. FAR is expressed as

$$FAR = \frac{S(\textit{the mumber of the false acception fingerprints})}{M(\textit{the total mumber of sampling})} \times 100\%$$

ERR denotes the ERR registration rate which means the probability of the fingerprint device not login or operation because the fault of images capture or feature extraction. ERR is expressed as

$$FAR = \frac{R(the\ number\ of\ the\ error\ registration\ fingerprints)}{M(the\ total\ number\ of\ sampling)} \times 100\%$$

We choose 10 registered users and 5 unregistered users to test different fingers, so there are 100 registered and 50 unregistered fingerprints, and we can get FRR, FAR and ERR through matching with 750 templates in the database. The testing results show that in 750 sampling there are 3 false rejections and 19 false registrations in 100 registered fingerprint templates, 0 false acceptation and 11 false registrations in 50 unregistered fingerprint templates. The results of the reliability testing are in Table V.

TABLE V. THE RESULTS OF RELIABILITY TESTING

Index	FRR	FAR	ERR
Result	0.4%	0	3%

The results above can't represent all conditions, because the number of testing fingerprints is limited, but the number in specific applications is larger than that in the experiment, so the results of FRR, FAR and ERR maybe change, and the limitations of the fingerprint device are presented.

C. *Security Analysis*

(1) Identity verification

It is difficult to copy or steal the fingerprint information, and the fingerprint device has the ability against fake. Even the fingerprint information is acquired by the illegal users, it is difficulty to utilize the information, because the algorithms of fingerprint feature extraction are different for different fingerprint devices that means it will not influence the private information of users if the fingerprint information is leaked.

The fingerprint recognition can realize identity authentication to "person". If the recognition algorithm is rigorous and the threshold value sets too high, the fingerprint from the same finger is considered from the different one, which results in high FRR. Similarly, if the threshold value sets too low, the fingerprint from the different finger is considered from the same one, which results in high FAR. FRR is relative with FAR, and the reduction of FRR can result in increasing of FAR. So it can't accurately judge the identities of users by fingerprint recognition, but the properties of easy carrying and uniqueness make fingerprint recognition as the most reliable method for identity authentication.

(2) Protection of sensitive information

The password information of the registered users is encrypted with MD5 and stored in the database, which ensure the security of transmitting the registered information and legal accessing information stored in database. The username/password encrypted with MD5 is the supplement of fingerprint recognition, which enhances the security of authentication scheme proposed in some degree.

V. CONCLUSIONS

There exists some vulnerability for network identity authentication system, which is difficult to conquer. Fingerprints as one of the biological properties can uniquely authenticate the identity of a "person". For balancing the restrictions of FRR and FAR, the username/password is encrypted with MD5, and a double identity authentication system based on fingerprint recognition and cryptography is proposed in this paper. The testing results show that it is high secure and strong reliable.

REFERENCES

[1] Chen Hongsong, "Network Security and Management," Press of TsingHua University, 2010.

[2] Li Zhenshan, "Fingerprint Recognition Technology in Status Authentication Application and Research," Netinfo Security, no. 3, pp. 12–14, 2011.

[3] M.A.Wahby Shalaby, and M. Omair Ahmad, "A Multilevel Structural Technique for Fingerprint Representation and Matches," Signal Processing, vol. 93, no. 1, pp. 56–69, 2013.

[4] M. Ayyue, Kizrak, and Figen Ozen, "A New Median Filter Based Fingerprint Recognition Algorithm," Procedia Computer Science, no. 3, pp. 859–865, 2011.

[5] F.g. Hashad, and T. M. Halim, "Figerprint Recognition Using Mel-Frequency Cepstral Coefficients," Pattern Recognition and Image Analysis, vol. 20, no. 3, pp. 360–369, 2010.

[6] Chen Liding, and Ren Zhigang, "Design and Implementation of Fingerprint Identification System Based on VC++," Automation & Instrumentation, no. 7, pp. 60–63, 2011.

[7] Huang Hailong, and Chen Saiping, "USBKey Based on Fingerprint Identification of E-commerce Authentication System," Proc. Applied Social Science, 2011, pp. 15-20.

[8] Yan Weiwei, and Huang Wei, "Embedded Authentication Systems Fusing Shared-key Authentication and Fingerprint Verification," Chinese Computer Systems, vol. 31, no. 12, pp. 2453–2456, 2010.