The Research and Application of the Fingerprint Key based USB-Key Pin Number Protection System

Yu Lu[1, a], Zhong Liang[2, b], Chen Yue[3, c]

[1]Electronic and Information Engineering, Sichuan University, Chengdu, 610065, China

[2]Electronic and Information Engineering, Sichuan University, Chengdu, 610065, China

[3]Electronic and Information Engineering, Sichuan University, Chengdu, 610065, China

[a]email:microcental_zll@163.com, [b]email: yyl_crstal@sina.com

Keywords: USB-Key; fingerprint key; pin number protection; Fuzzy Vault

Abstract. This paper introduced fingerprint recognition to protect USB Key's pin number. Pin number is easily stolen and sometimes it's too hard to keep in mind. To overcome these problems, a fingerprint key based USB Key pin number protection system has been proposed. Using biometric like fingerprint to protect USB Key pin number improves security and convenience of users. And the fingerprint key is generated by user's fingerprint and several random points. That avoids user's privacy information disclosure because it's hard to restore the template in calculation. With the development of mobile payment and more and more mobile devices are beginning to equip with fingerprint recognition module, the combination of fingerprint and USB Key has a good prospect and portability.

1 Introduction

Along with the rapid development of information technology, e-commerce has an increasingly important position in various fields. As an important indicator of whether e-commerce has healthy development, safety has restricted the development of electronic commerce. For its ease of use, low cost, high security, and other advantages, USB-key is widely used in electronic commerce. It protects the interior certificate by PIN number, however, PIN number is difficult to remember and easily stolen. Besides, it can't resist keyboard record attacks and dictionary attack. All of these threaten the safety of e-commerce transaction system based on USB-key. Against the security problems existing in the current USB-key, this paper combines fingerprint technology and PIN number. And it firstly binds the unique and potable fingerprint feature template of users and the PIN number, to generate a safe fingerprint security lock (vault). Users do not need to memorize complex PIN number, just inputting their fingerprints to complete the authentication.

2 Key Technical Principle

2.1 Fingerprint recognition technology

At present, we gradually introduce biometrics in the authentication technology. It uses "what you have had originally", such as fingerprints, iris and voice to achieve authentication. This paper uses fingerprints as the basis of identity authentication. Firstly, fingerprint is unique for every person. Secondly, the fingerprint is relatively stable and can't be easily changed by external influences. Meanwhile, fingerprint samples are easy to obtain. And because only its characteristic value is extracted, it is stored with small amount and easy to save. Currently, fingerprint recognition technology has been relatively mature with relatively low cost. It has gained considerable development in e-commerce, criminal identification, information security and other fields.

Fingerprint identification process is divided into three parts. Firstly fingerprint collection device captures users' fingerprints, making it clear and available after the original image is treated preliminarily. Then, the fingerprint features are extracted. The holistic features and details (grain pattern, breakpoints, bifurcation or peripheral point) in the fingerprint image are analyzed and extracted through specific calculation and then be saved as a template. Finally, digital template of

to-be-verified fingerprints and registered fingerprints will be matched according to their characteristic values.

2.2 USB-key technology

USB-Key, which is now widely used in e-commerce as a USB interface hardware storage device with a built-in micro smart card processor. This processor uses asymmetric cryptography to encrypt, decrypt and digital signature, having certain security guarantees.

USB-key uses some security measures to ensure the security of transactions. Firstly, it uses the "two-factor authentication mode" including both a USB-key hardware and PIN number. Lack of any one will lead failure of certification. Secondly, USB-key key is stored in its internal locks and not available from the external, so the attacker can't modify the key by malicious programs. At the same time, USB-key has a pair of public and private keys based on PKI system. The public key can authenticate the user while the private key is stored in the key areas. All operations using private key are finished inside the USB-key completely.

2.3 Template Protection Technology

As traditional fingerprint recognition technology doesn't protected users' fingerprint feature adequately, this paper use encryption method of fuzzy vault proposed by Juels. And its purpose is preventing fingerprint information stored leakage through bundling the fingerprint characteristics and key together.

1. Bundle of PIN number and fingerprint:

Firstly, do a series of processing about the entered fingerprints, choose qualifying feature points and get the coordinates of these feature points. Then a 128bit random key is generated by the system and then it will be divided and transformed into a polynomial coefficient to construct a D grade polynomial $p(x)$. Acquired feature points will get the true point set G, $G=\{(a_1, p(a_1)), (a_2, p(a_2)), \ldots, (a_n, p(a_n))\}$ through $p(x)$ reflection. For security, a second set of interference point C is added to protect the template. Points in C are randomly selected, whose coordinates are (b_1, c_1) and c_1 is not equal to $p(b_1)$. Combination of C and G set is indicated by V'. A password file V in the list form will be established through the regulation of points. V is stored in the system as the final vault file as shown in Figure 1.

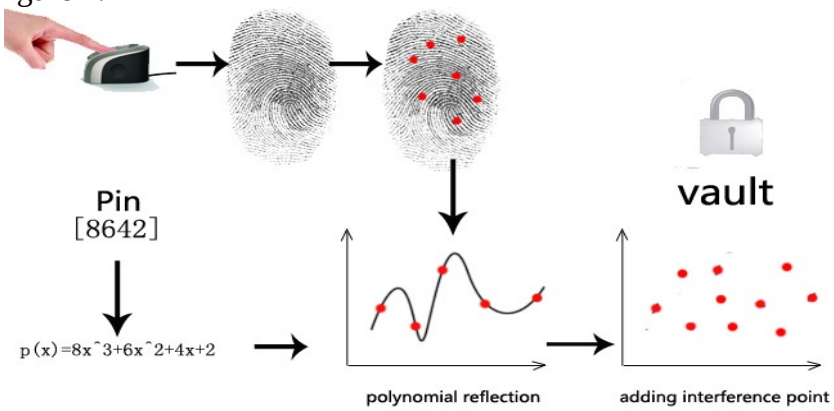

Fig.1. Bundle of PIN number and fingerprint

At this time the stored vault files in the library no longer have users' fingerprint template information, effectively protecting users' fingerprint features.

2. Recovery of PIN number:

In the decryption stage, user's inquiry fingerprint will be made certain process to gain its fingerprint feature points - inquiring feature points set $Q = (u_1, u_2, \ldots, u_n)$. By comparison $(u_1, u_2, \ldots, u_n)$and the horizontal axis value in the library, the corresponding unlock point will be found. If $(D + 1)$ points are found out, then the D grade polynomial coefficients $p(x)$ will be reconstructed. Then combine the polynomial coefficients and convert to a binary code. At last the key can be obtained. It is just as shown in Figure 2.

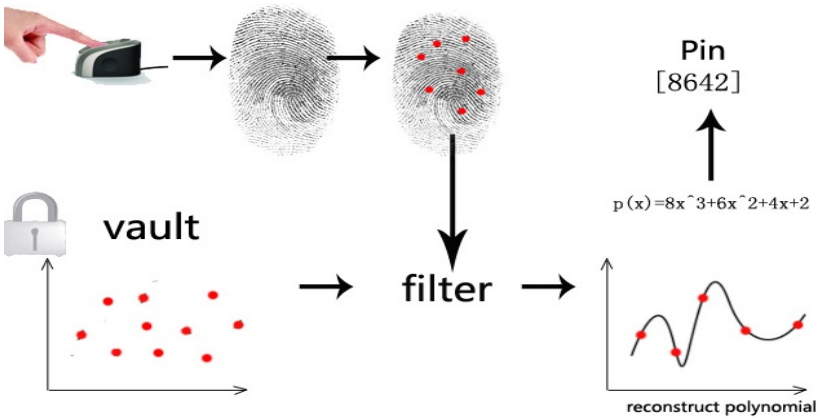

Fig.2. Recovery of PIN number

If the feature points of querying fingerprints cannot be matched to a sufficient number of points in the vault file, there is no way to reconstruct the polynomial, and the key will be protected.

2.4 Security Analysis of USB-key PIN number protection technology based on fingerprint locks

1. Zero storage of fingerprint feature template and PIN number

The scheme proposed doesn't save users' fingerprint template and PIN number at the local area and the server. Today's fingerprint authentication is mostly finished by storing users' fingerprint information at the local area or on Internet. And this scheme does not save users' fingerprint template information. In this scenario, correct users make PIN number recovered from the fingerprint lock (vault) file through fingerprints. Since the fingerprint lock (vault) files are added 100 points, fingerprint templates and binding PIN number will not be extracted in the absence of proper fingerprints. The public fingerprint lock (vault) is safe.

2. Costs of violent decryption

In this scheme, PIN number is a 128bit string which is randomly generated. At least nine real fingerprint details are needed in order to restore the PIN number from the fingerprint lock (vault) file. Fingerprint Lock (vault) file has at least nine minutiae points and 100 interference points. So, if the attacker doesn't have correct fingerprints, he must extract nine real minutiae points from the 109 points. The calculation cost is $C_{109}^{9} \approx 4.26 \times 10^{12}$. However, USB-key will be locked after wrong PIN number has been input for several times, so violent decryption is computationally unfeasible.

3 Realization Program of USB-key PIN number Protection Technology Based on Fingerprint Locks

3.1 Fingerprint binding process

Users input fingerprints through an external fingerprint identification device or built-in fingerprint recognition module in the laptop. After obtaining a clear fingerprint image, users' fingerprint feature point set will be accessible by a series of fingerprint image pre-processing. Then a high-intensity random 128-digit PIN number generated by the program will be bound with fingerprint template. At last the fingerprint lock is uploaded to the server and then the binding process of fingerprint and PIN number will be completed. The process is shown in Figure 3.

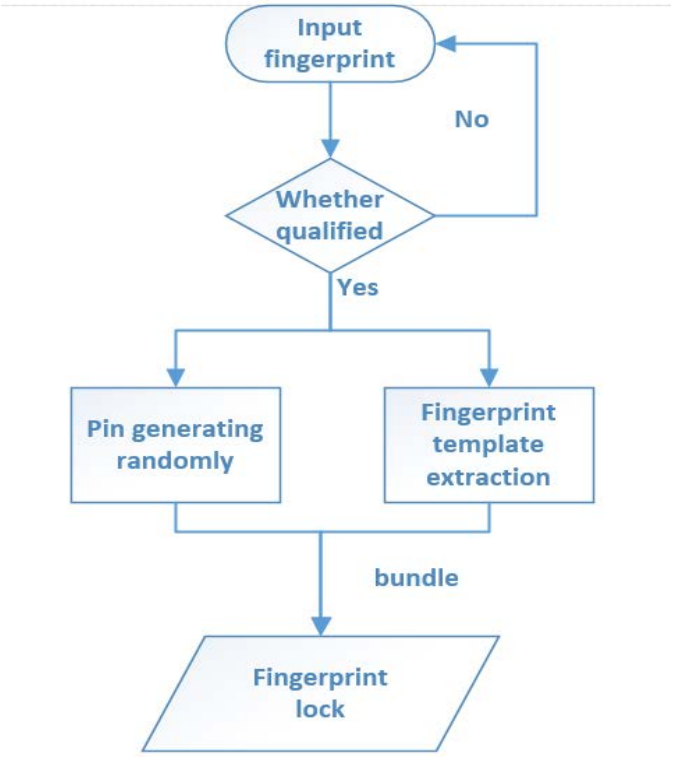

Fig.3. Fingerprint binding process

3.2 Fingerprint Authentication Process

After the user submits a payment request, the server will send the saved corresponding user's fingerprint lock (vault) to the client. The client will extract PIN number from the fingerprint PIN number lock (vault) using the user's input fingerprint. The private key in the certificate of USB-key can be used after verifying the PIN number. The character string sent by the server will be signed and after finishing it will be sent to the server again. The server uses the public key in user's certificate to decrypt the transaction information in the signed information. Then, it will be compared with the real transaction information to complete the whole payment authentication process. The process is shown in Figure 4.

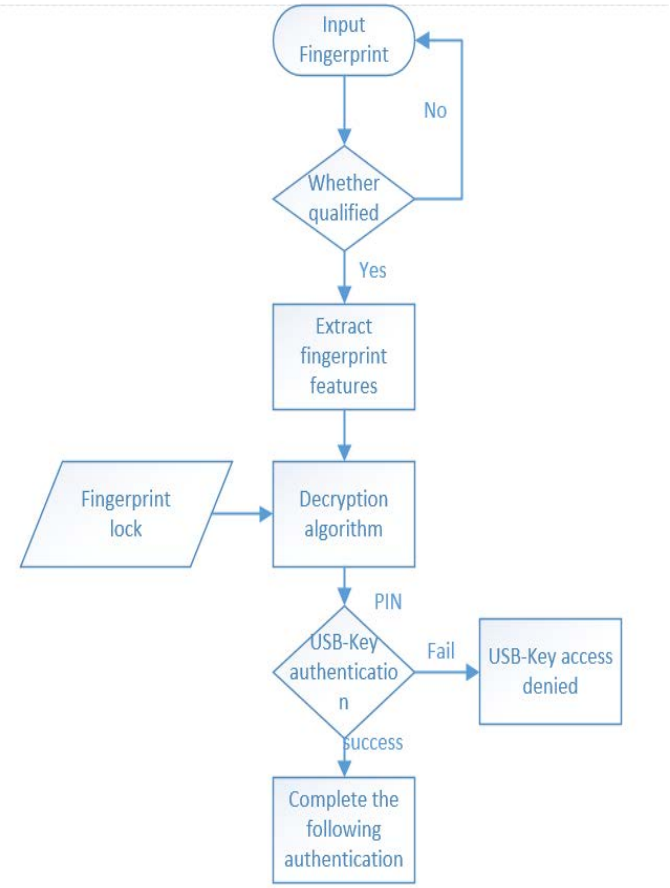

Fig.4. Fingerprint Authentication Process

4 Conclusion

This paper uses Fuzzy Vault fingerprint extraction scheme to achieve binding and storing the fingerprint feature template and PIN number in the case that they two aren't stored, simplifying the use of USB-key and increasing the security of PIN number usage. With the development of mobile Internet, mobile phones, tablet and other mobile devices are gradually replacing PC. More and more people are used to making payments through mobile devices. And the attack targets of hackers have gradually shifted from the traditional PC terminal to the mobile devices. The security threats against mobile devices rapidly grow and mobile payment security has been threatened greatly. Now, mainstream mobile payment applications such as Alipay uses scratchable latex and other methods to protect account security. However, attacks against these security methods increasingly grow and their security becomes an increasingly serious problem. Nowadays more and more mobile phones have joined the fingerprint identification module, such as Iphone 5s, HTC one max, Samsung galaxy5 and other mobile phone models. Fingerprint identification and mobile device binding is the trend. Fingerprint has its own superiority, that is, fingerprint of each person is unique, while its safety, reliability is reliable than the other authentication methods. With good prospects, our scheme can be applied to mobile terminals to achieve the security guarantee of fingerprint-based mobile payment, greatly improving the safety and convenience of mobile payment.

References

[1] DENG Jian-guang, YUAN Hua-qang. Fingerprint minutiae feature encryption based on fuzzy vault scheme [J]. Computer Engineering and Design, 2010, 31(4):720-723

[2] DING Shi-ming, LIU Lian-zhong, LU Zhen. An Authentication Protocol Based on USB- KEY

[J]. Microcomputer Development, 2005 , 15(10):1-3

[3] Chelliah , B.& S. Geetha. Enhancing E-Payment Security through Biometric Based Personal Authentication Using Steganography Scheme – B- PASS [J]. Recent Trends in Computer Networks and Distributed Systems Security Communications in Computer and Information Science, 2014(420), 461-472

[4] Agbontaen, F.O.& Orukpe, P.E. Secured online payment using biometric identification system[J]. Advanced Materials Research, 2013(824), 193-199

[5] Hosseini, Z. Zareh&Barkhordari, E. Barkhordari, E. Enhancement of security with the help of real time authentication and one time password in e-commerce transactions[C]. IKT 2013 - 2013 5th Conference on Information and Knowledge Technology, IEEE, 2013, 268-273