Journal of Fiber Bioengineering and Informatics 8:4 (2015) 713–724
doi:10.3993/jfbim00172

Research of Biometric Key Generation Based on Fingerprint Bit-strings ⋆

Chengyang Xie [a,b], Jiayong Liu [a,b,*], Xu Yao [a], Dianhua Tang [b]

[a] *College of Electronics and Information Engineering, Sichuan University, Chengdu 610064, China*
[b] *Science and Technology on Communication Security Laboratory, Chengdu 610041, China*

Abstract

Biometric key technology is the organic combination of biometric encryption technology and traditional cryptography. Biometric key can directly encrypt data or encrypt key, with the character of portable use and not easily being stolen, forgotten and broken. This article provides an algorithm for generating key based on the fingerprint feature bit-strings, extracting fingerprint feature information with bit-strings form as first step, generating key by the combination of this feature information and BCH error correcting code secondly. Experiments show that the algorithm can generate stable key of encryption on the premise of protecting the user's fingerprint information. It can further improve the security strength and reach two-factors protection if the biometric key is stored in the smart card, which has certain practical value.

Keywords: Fingerprint; Fuzzy Schemes; Bit-strings; Error-correcting Code; Biometric Encryption

1 Introduction

1.1 Biometric Encryption

As the core technology of information security, the cryptography technology plays a crucial role in the process of data security protection. Whether it is the symmetric encryption algorithms (single key cryptosystem) or asymmetric encryption algorithms (public key cryptosystem), the security of the system completely depends on the security of the key. If the length of the key is too short, it will be vulnerable to lose key by exhaustive attack and dictionary attack. The traditional key enhances security only by using longer secret keys. But simply relying on people to remember a long key is almost impossible and easily forgotten. Besides, the traditional key is unable to establish a necessary relation with the user, thus causing the illegal sharing of key easily. The key generation technology based on biological characteristics, however, can effectively solve the above problems.

⋆This work was supported by Science and Technology on Communication Security Laboratory (Grant No. 9140C110401140C11053).

*Corresponding author.
Email address: ljy@scu.edu.cn (Jiayong Liu).

Biological characteristics include innate characteristics of human, such as fingerprint, face, iris, palm print [1], DNA, etc, and the behavior characteristics, such as voice, signature, gait etc [2]. The core of the key generation technology which is based on biological characteristics, is how the legitimate users generate a unique and stable key whereas illegal users cannot, which is also the main research in this essay.

At present, scholars home and abroad have carried out many fruitful researches on the generation of biometrics key. Dodis et al. [3] put forward the idea to extract the frame of key from biological characteristics data. In [4], Juels carried out a fuzzy vault scheme, the core idea of which is to hide the biometric information in a large number of interference information while only legitimate users can filter the interference and get the right to use the key. Charles et al. [5] combined the idea of Juels with fingerprint, and made some improvements. However, this scheme still has its own disadvantages. Although the fingerprint feature information is hidden in the disturbance point, the original feature template is not converted and encrypted, and can not fight against cross matching attack, thus causing the fingerprint feature information disclosure easily.

In terms of fingerprint, Zhe Jin et al. [6] proposed a fingerprint template protection method that transforms a set of minutiae points into bit-string via polar gird based on 3-tuple quantization technique. Munaga Prasead et al. [7] proposed an alignment free method to generate the cancelable template by using neighboring relation in every reference minutiae. Wong et al. [8, 9] proposed a cancelable fingerprint template technique based on Multi-line Code (MIC) and an improved method. The above schemes have common in that they achieved the purpose of template protection based on bit-strings.

1.2 Motivation and Scope

Chulhan Lee et al. [10] carried out a template protection scheme based on fingerprint minutiae bit-string. The basic idea is to convert fingerprint minutiae to feature bit string in security domain in order to protect the original minutiae. The advantage of this scheme lies in implementing a cancelable template protection scheme without leaking the original fingerprint information, and achieving fingerprint automatic registration. But this scheme is still insufficient in the following aspects:

(1) In the scheme, it is not safe to directly take feature bit-strings as biological templates. Once an attacker gains parameters of 3D array, he could recover the original fingerprint information from the fingerprint bit-strings, thereby giving away user's privacy information.

(2) The revocation of scheme has limitation for it only realizes the revocation in different application systems. When in the same application system, we cannot use the homologous fingerprint to generate new characteristics of bit string as a biometric template.

(3) Chulhan Lee et al. just put forward one template protection scheme rather than the biometric encryption scheme based on bit-strings, so the advantages of fingerprint feature bit string have not been fully utilized.

On the basis of the above literature, we have put forward a scheme of key generation based on the fingerprint feature bit-strings. First of all, extract the feature bit string of fingerprint, then