Journal of Network and Computer Applications 34 (2011) 1979–1989

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Dual-key-binding cancelable palmprint cryptosystem for palmprint protection and information security

Lu Leng, Jiashu Zhang*

Sichuan Province Key Lab of Signal and Information Processing, Southwest Jiaotong University, Chengdu, Sichuan 610031, PR China

ARTICLE INFO

Article history:
Received 11 December 2010
Received in revised form
14 June 2011
Accepted 2 July 2011
Available online 8 July 2011

Keywords:
Dual-key-binding cancelable palmprint
Biometric cryptosystem
Cancelable biometrics
Palmprint Phasor
Biometric protection
Information security

ABSTRACT

Biometric cryptosystems and cancelable biometrics are both practical and promising schemes to enhance the security and privacy of biometric systems. Though a number of bio-crypto algorithms have been proposed, they have limited practical applicability because they lack of cancelability. Since biometrics are immutable, the users whose biometrics are stolen cannot use bio-crypto systems anymore. Cancelable biometric schemes are of cancelability; however, they are difficult to compromise the conflicts between the security and performance. By embedded a novel cancelable palmprint template, namely "two dimensional (2D) Palmprint Phasor", the proposed palmprint cryptosystem overcomes the lack of cancelability in existing biometric cryptosystems. Besides, the authentication performance is enhanced when users have different tokens/keys. Furthermore, we develop a novel dual-key-binding cancelable palmprint cryptosystem to enhance the security and privacy of palmprint biometric. 2D Palmprint Phasor template is scrambled by the scrambling transformation based on the chaotic sequence that is generated by both the user's token/key and strong key extracted from palmprint. Dual-key-binding scrambling not only has more robustness to resist against chosen plain text attack, but also enhances the secure requirement of non-invertibility. 2D Palmprint Phasor algorithm and dual-key-binding scrambling both increase the difficulty of adversary's statistical analysis. The experimental results and security analysis confirm the efficiency of the proposed scheme.

1. Introduction

Biometric characteristics are immutable. When biometrics are compromised, user cannot revoke and reissue their biometric templates. Besides, the biometric templates of one user may be stored and shared in various databases with more and more biometric systems appearing in our daily life, which imperils biometric security and users' privacy (Jain et al., 2008). Ratha et al. (2001) summarized eight potential and vulnerable security holes, which can be attacked easily, in a normal biometric system. Furthermore, they first proposed the concept of "cancelable biometrics". Cancelable biometrics, distorted version of original biometrics, can be revoked and reissued like a password. It is universally acknowledged that a cancelable biometric scheme should meet four objectives:

(1) *Diversity*: multiple templates are able to be generated from the same biometric to ensure that cancelable biometric is unique in every application. The diversity of multiple templates is enough to resist against brute force attack.

(2) *Revocability/reusability*: templates are easily revoked and reissued when compromised. The new template and the old template must not be similar, in other words, cancelable template should be sensitive to token/key updating. Otherwise, the system cannot resist against replay attack. Furthermore, cancelable template should be sensitive to inter-class variance. It is better that the similarity degree between the templates generated from different classes is low. An ideal cancelable biometric algorithm is sensitive to both token/key updating and inter-class variance.

(3) *Non-invertibility*: cancelable biometric template is commonly generated by the combination of user's token/key and biometric features. Non-invertibility ensures that an adversary cannot restore original biometric features even when he has successfully stolen both the user's token/key and the protected template, that is, the system is attacked successfully only when an adversary has both the user's token/key and original biometric features. The transform algorithm for cancelable biometric is public, so the security of the system should depend on the secret key rather than the privacy of transform algorithm.

(4) *Performance*: cancelable biometric scheme should not weaken recognition performance remarkably. Many tests need to be implemented to confirm the verification ability of cancelable

* Corresponding author.
E-mail address: jszhang@home.swjtu.edu.cn (J.S. Zhang).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.07.003