Feature and Rank Level Fusion for Privacy Preserved Multi-Biometric System

Padma Polash Paul, Department of Computer Science, University of Calgary, Calgary, AB, Canada

Marina Gavrilova, Department of Computer Science, University of Calgary, Calgary, AB, Canada

ABSTRACT

Privacy protection in biometric system is a newly emerging biometric technology that can provide the protection against various attacks by intruders. In this paper, the authors have presented a multi-level of random projection method based on face and ear biometric traits. Privacy preserved templates are used in the proposed system. The main idea behind the privacy preserve computation is the random projection algorithm. Multiple random projection matrixes are used to generate multiple templates for biometric authentication. Newly introduced random fusion method is used in the proposed system; therefore, proposed method can provide better template security, privacy and feature quality. Multiple randomly fused templates are used for recognition purpose and finally decision fusion is applied to generate the final classification result. The proposed method works in a similar way human cognition for face recognition works, furthermore it preserve privacy and multimodality of the system.

Keywords: Biosignal Processing, Cancelability, Cognitive Signal Processing, Machine Learning, Multimodal Cancelable Biometrics, Random Projection, Rank Level Fusion, Template Security

1. INTRODUCTION

In the recent years, the link between the cognitive informatics community and biometric security has grown stronger. It is evident from the number of publications that span both domains that deal with issues of applying intelligent techniques to biometric processing, and with developing new cognition methods for biometric and security applications and research (P. Paul & Gavrilova, 2012; Wang & Berwick, 2012; Patel et al., 2013; P. P. Paul & Gavrilova, 2012). Computational intelligence and algorithm finds its many uses in biometric domain (P. P. Paul, Gavrilova, & Alhajj, 2014; P. P. Paul, Gavrilova, & Klimenko, 2014; Perlovsky & Kuvich, 2013; Wang, 2007; Gavrilova & Monwar, 2013; P. Paul & Gavrilova, 2014). In addition, virtual reality also benefits
from novel biometric methods (Gavrilova & Yampolskiy, 2010). The concept of cancelable biometric or cancelability has become popular very recently (P. P. Paul & Gavrilova, 2013; Feng, Yuen, & Jain, 2010). This new trend focuses on how to transform a biometric data or feature into a new one so that users can change their single biometric template in a biometric security system. Up until now, multimodal system cancelability has not been considered. However, this can be argued that template protection is even more crucial in such systems. Multimodal biometric system uses a numbers of biometric credentials, so it is cooperative to the attackers to get more evidence if they manage to break the system. Once templates from the multimodal system are compromised, individual loses all the sensitive data stored in the current security system, and all other systems related to that individual. This is why it is crucial for a multi-biometric system to provide the template security and cancelability. It can be claimed that using cancelability for each biometric trait separately in multimodal biometric system can solve the problem. However, this is not as easy as it looks; the solution may be costly in term of computation efforts and performance. If one trait is compromised, similar method can be used to break other traits. Another concern can be key protection and storage; system needs to issue key for each biometric trait. In this paper, we tackle the above problems and present a novel solution for cancelable biometrics in a multimodal system. We develop a new cancelable biometric template generation algorithm using random cross folding of multiple biometric traits, random projection and transformation-based feature extraction and selection. Performance of the proposed algorithm is validated on a virtual multi-modal face and ear database. Specifically, algorithm security is validated by issuing different original and fake keys for different subjects of the database. Algorithm discriminability remains high because of the similar cross fold indices and random projection matrix (vectors) for a class. Similarly, revocability and diversity are ensured by issuing different sets of keys for training and testing process.

Multimodal Biometric System is a relatively new alternative to Unimodal Biometric System. Multimodality can be achieved in various ways: such as combining multiple biometric traits, selecting distinct feature sets from the same source of biometric, using separate sensors, fusing the decision of individual biometric system, etc. (A. Ross et al., 2006). In our system, we have used diverse feature sets from different biometric traits. From the literature, it is found that multimodal biometric system often outperforms a unimodal biometric system in terms of accuracy and reliability (A. Ross et al., 2006). It can solve some common problems of unimodal biometric system such as intra-class variability, interclass similarity, non-universality, sensitivity to noise and other issues. Multimodal biometric system can improve the performance of a biometric system in a number of aspects, including accuracy, circumvention, resistance to errors and spoof attacks (A. Ross et al., 2006). Multimodal biometric systems are more secure compared with unimodal systems (P. P. Paul, Monwar, & Gavrilova, 2011) in terms of authentication accuracy. Individual’s biometric traits are stored in a template database during both the training and the matching. The most important part of the biometric system from the point of view of security and privacy is the template database. Previous studies (A. Ross, Shah, & Jain, 2007; Adler, 2003) have shown that the raw image or text can be recovered from the template stored within the database. A first approach to deal with biometric security and privacy was to store the transformed version of original template (A. Ross, Shah, & Jain, 2007; Adler, 2003). Ross et al., 2007 reconstructed fingerprint image from stored minutiae points. In previous research on biometric template protection, authors suggested the dependency of cancelable biometric algorithm on security, discriminability, recoverability, performance and diversity of the system (P. Paul & Gavrilova, 2012; Maltoni, Maio, Jain, & Prabhakar, 2009; Feng et al., 2010). They noted that it is computationally hard to reconstruct the original template from the transformed template. The discriminability of the original biometric template should not be lost after the cancelable
Related Content

Artificial Neural Network and Metaheuristic Strategies: Emerging Tools for Metal Cutting Process Optimization
Indrajit Mukherjee and Pradip Kumar Ray (2008). Handbook of Computational Intelligence in Manufacturing and Production Management (pp. 366-397).
www.igi-global.com/chapter/artificial-neural-network-metaheuristic-strategies/19368?camid=4v1a

Secure Key Generation for Static Visual Watermarking by Machine Learning in Intelligent Systems and Services
www.igi-global.com/chapter/secure-key-generation-static-visual/56166?camid=4v1a
Symbiotic Aspects in e-Government Application Development
[www.igi-global.com/article/symbiotic-aspects-government-application-development/39104?camid=4v1a](www.igi-global.com/article/symbiotic-aspects-government-application-development/39104?camid=4v1a)

Commonsense Reasoning in Intelligent Computer Systems
[www.igi-global.com/chapter/commonsense-reasoning-intelligent-computer-systems/38490?camid=4v1a](www.igi-global.com/chapter/commonsense-reasoning-intelligent-computer-systems/38490?camid=4v1a)