ID 도난 시나리오에 강인한 불변 홍채 키 생성 방법

이연주, 김재희
연세대학교 전기전자공학과,
생체인식연구센터
e-mail : {younjoo, jhkim}@yonsei.ac.kr

Invariant Iris Key Generation Method Robust To Stolen Token Scenario

Youn Joo Lee and Jaihie Kim
Department of Electrical and Electronic Engineering, Yonsei University,
Biometrics Engineering Research Center

Abstract

Recently, biometric authentication mechanism has been used to provide high level of security in cryptographic systems. In this paper, we propose an efficient method of generating invariant iris key to be applied in cryptographic systems. In order to generate iris key and improve the performance at the stolen token scenario, multiple random projection technique was combined with multiple linear transformation methods. From the experimental results, we proved that invariant iris keys were generated and the proposed method was robust to stolen token scenario.

I. 서론

최근 암호화 기술이 이용되는 보안 시스템에서는 암호 키의 안전을 위해 생체 인식 기술을 도입하고 있다. 기존에는 패스워드 기반의 인증방식을 통해 암호 키의 관리가 이루어지고 있으나 패스워드 자체의 안전성을 보장할 수 없다는 문제가 있다. 그러나 패스워드 대신에 생체정보를 이용하면 보다 안전하고 편리하게 암호 키를 관리할 수 있다.

본 논문에서는 생체 데이터로부터 불변의 생체 키를 생성하기 위한 효과적인 방법을 제안한다. 생체 키의 생성을 위해 multiple random projection (MRP) 방법 [1]과 다양한 linear transformation 방법들을 결합하였다. MRP 방법은 생체 데이터를 보호하면서 불변의 생체 키를 생성할 수 있는 장점이 있지만, 각 사용자마다 다르게 할당된 ID를 도난당할 경우에는 생체 데이터만 사용했을 때의 성능밖에 나타나지 않는다는 단점을 갖는다. 이러한 문제점을 해결하기 위해 MRP 방법에 다양한 linear transform 방법들로, Eigenfeature Regularization and Extraction (ERE) 방법과 Linear Discriminant Analysis (LDA)를 차례로 결합시켰다 [2][3]. 실험결과를 통해 제안한 방법이 불변의 홍채 키를 생성할 수 있으며 ID가 도난당한 경우에도 크게 성능이 저하되지 않는다는 것을 확인할 수 있었다.

II. 본론

본 논문에서 제안한 방법의 전체 흐름도는 그림1과 같다. 사용자로부터 획득한 홍채영상이 입력되면 전처리 과정을 통해 홍채영역을 추출하고 정규화된 홍채 영상을 생성한다. 전처리 과정 이후에 얻어진 홍채 영상에서 눈썹과 눈꺼풀에 의해 가려짐이 매우 적은 region of interest (ROI)를 선택하고 이 영역을 일차원

의 이미지 벡터로 변환한다. MRP 단계에서는 사용자마다 주어지는 ID에 따라 random matrix를 생성하고 이미지 벡터와 matrix를 곱하여 랜덤한 특징 벡터를 얻는다. ERE 단계에서는 특징 벡터들의 훈련(training)과정을 통해 고유 특징 벡터(eigenfeature)를 생성하고 LDA를 적용함으로써 보다 구분력이 있는 특징 벡터를 추출하고자 하였다. 마지막으로 비트열의 홍채 키를 생성하기 위해서 양자화를 수행하였다.

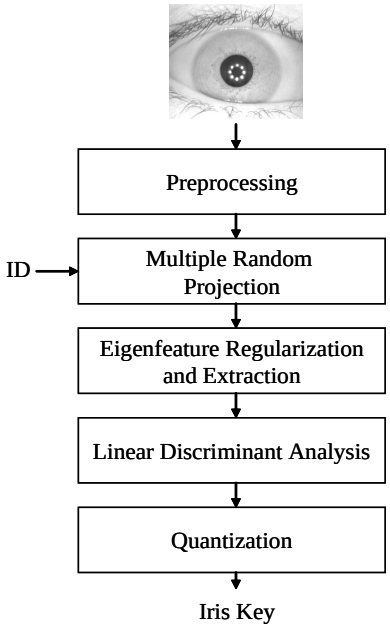

그림 1. 제안한 홍채 키 생성 방법의 전체 흐름도

Ⅲ. 실험 결과 및 분석

본 논문에서 제안한 방법의 성능을 평가하기 위해 접근식 홍채 인식 장비에 의해 획득된 BERC IRIS DB1 [4]를 사용하였다. BERC DB는 99명의 눈 영상으로 각 사람 당 10장씩 총 990장으로 이루어져있다.

표 1은 ID를 도난당한 경우에 MRP만을 적용하였을 때의 성능결과를 나타내며, 표 2는 본 논문에서 제안한 MRP-ERE-LDA 방법의 성능 결과를 나타낸다. 표 1과 2를 비교해보면 ID를 도난당한 경우에도 MRP-ERE-LDA방법은 MRP만을 사용하였을 때보다 성능이 매우 향상되었다는 것을 알 수 있다. 표 1에서와 같이 MRP 방법은 특징벡터가 1000 차원일 때 EER 13.105%를 얻었지만 MRP-ERE-LDA 방법은 128차원에서 4.427% EER로 최적의 성능을 갖는다. 따라서 실험결과를 통해 본 논문에서 제안한 MRP-ERE-LDA 방법이 ID를 도난당한 경우에도 큰 성능 저하 없이 홍채 키를 생성할 수 있다는 것을 확인하였다.

표 1. MRP 방법의 성능 결과 (ID를 도난당한 경우)

차원	100	500	1000	1500	2000
EER(%)	24.579	16.919	13.105	13.733	13.529

표 2. MRP-ERE-LDA 방법의 성능 결과 (ID를 도난당한 경우)

차원	60	80	100	120	128	140
EER(%)	10.427	11.89	13.07	13.452	4.427	14.27

Ⅳ. 결론

본 논문에서는 ID 도난 시나리오에 강인한 불변 홍채 키 생성방법을 제안하였다. ID가 도난당한 경우에 성능 저하를 막기 위해 다양한 선형 변환 방법들을 결합하였다. 실험결과로부터 제안한 방법의 성능이 단일 MRP 방법만을 적용하였을 때보다 향상되었다는 것을 확인하였다.

향후에는 다양한 홍채 DB에 대해서 제안한 방법을 적용해보고, MRP, ERE, LDA 방법을 순차적으로 결합하는 방식 대신에 융합(fusion) 방법을 적용하여 보다 향상된 성능을 갖는 방법에 대한 연구가 필요하다.

Acknowledgment

본 연구는 한국과학재단 지정 생체인식연구센터(BERC)의 지원을 받아 이루어졌습니다.

참고문헌

[1] Y. Kim, and K. -A. Toh, "A method to enhance face biometric security,"proc. IEEE conference on biometrics: Theory, Applications (ICIEA) pp. 815-833, 2006.

[2] Xudong Jiang, Bappaditya Mandal and Alex Kot, "Egenfeature Regularization and Extraction in Face recognition", IEEE trans. on Pattern Analysis and Machine Intelligence, May, 23, 2007.

[3] S. Balakrishnama and A. Ganapathiraju, "Linear Discriminant Analysis - A Brief Tutorial, " Institute for signal and information processing.

[4] http://berc.yonsei.ac.kr(accessed on 2008. 4. 17)