암호 키의 보안을 위한 홍채 기반의 퍼지볼트 시스템

*이연주, **박강령, *김재희
연세대학교 전기전자공학과, 생체인식연구센터
상명대학교 미디어학부, 생체인식연구센터
e-mail : *{younjoo, jhkim}@yonsei.ac.kr, **parkgr@smu.ac.kr

Fuzzy Vault System based on Iris for Protecting Cryptographic Key

*Youn Joo Lee, **Kang Ryoung Park, *Jaihie Kim
*Department of Electrical and Electronic Engineering, Yonsei University,
Biometrics Engineering Research Center
**Division of media Technology, Sangmyung University,
Biometrics Engineering Research Center

Abstract

In this paper, we propose a fuzzy vault system using iris data. The fuzzy vault, proposed by Juels and Sudan, has been used to protect cryptographic key with biometric information. In order to combine the fuzzy vault scheme with iris data, we used iris features extracted by ICA method and clustering technique. From our experimental results, we proved that the propose fuzzy vault system is robust to sensed environmental change.

I. 서론

일반적으로 보안 시스템에서는 암호 키의 안전을 위해 패스워드 기반의 인증방식을 이용하고 있다. 그러나 이러한 인증방식은 패스워드가 갖는 분배 및 공유의 가능성 때문에 암호 키의 안전성을 저하시키는 문제가 있다. 따라서 분배와 복사 및 공유의 가능성이 매우 적은 생체정보를 사용한 인증방식이 이러한 문제해결해 준다[1-4]. 최근 암호 키 보호를 목적으로 퍼지볼트(fuzzy vault)와 생체정보를 결합한 암호화-생체인식 시스템에 관한 연구가 활발히 진행되고 있다.

본 논문에서는 Juels와 Sudan이 제안한 퍼지볼트[5]와 홍채정보를 결합하여 128비트 암호 키를 안전하게 암/복호화하는 방법을 제안한다. 퍼지볼트와 홍채정보를 결합하기 위해 독립성분분석(ICA)을 이용한 홍채특징 추출알고리즘[6]을 이용하여 홍채특징을 추출하였고, 홍채특징의 가변성을 줄이기 위해 클러스터링(clustering) 기법을 적용하였다.

II. 본론

홍채 기반의 퍼지볼트 시스템의 구조는 그림1과 같다. 사용자로부터 획득한 홍채영상이 입력되면 기존 연구에서와 같은 방법으로 ICA를 이용한 방법을 적용하여 홍채특징을 추출하고 홍채특징에 나타날 수 있는 가변성을 줄이기 위해 클러스터링 기법을 적용하여 최종적으로 *Iris Codes* 집합을 생성한다[2-4][6]. 이 집합은 퍼지볼트 구조의 인코딩(encoding) 과정에서 128비트 암호 키를 암호화하기 위해 사용되며 이 과정이 끝나면 볼트(vault)가 생성되어 스마트카드(smart card)와 같은 저장장치에 저장된다[4-5]. 볼트로부터

본 연구는 한국과학재단 지정 생체인식연구센터의 지원을 받아 이루어졌습니다.

사용자의 암호 키를 생성하기 위해서는 사용자의 홍채 영상으로부터 *Iris Codes* 집합을 생성하고 퍼지볼트 디코딩 과정을 수행하면 된다[4-5]. 결국 사용자의 홍채정보 없이는 볼트로부터 사용자의 암호 키를 얻어낼 수 없는 퍼지볼트 구조에 의해 암호 키가 안전하게 보호되는 것이다.

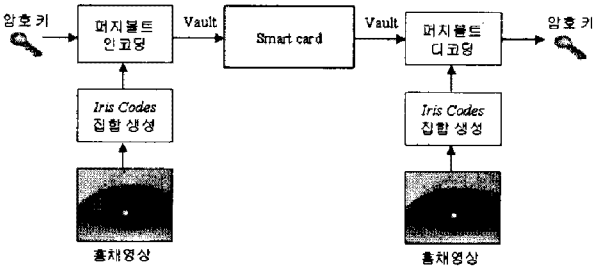

그림 1. 홍채기반의 퍼지볼트 시스템의 전체 흐름도

Ⅲ. 실험 결과 및 분석

홍채영상은 접근식 홍채인식장비에 의해 획득된 BERC_IRIS_DB1[7]로 32명의 홍채에 대해 각 10장씩 총 320장을 사용하였다.

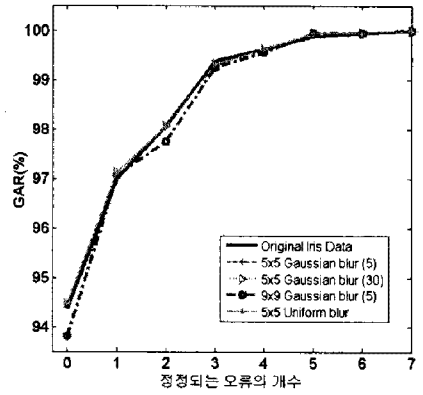

그림 2. 정정되는 오류의 개수에 따른 GAR(%)값 변화를 나타낸 그래프

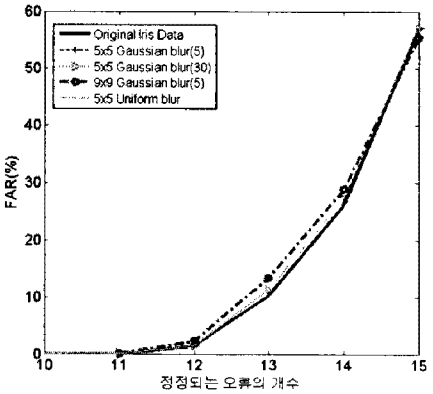

그림 3. 정정되는 오류의 개수에 따른 FAR(%)값 변화를 나타낸 그래프

클러스터링을 위해 사용된 홍채 영상은 10장 중 5장이고, 인증에 사용된 영상은 나머지 5장이다. 또한 제안된 퍼지볼트 시스템이 카메라의 초점변화에서도 동일한 성능을 보이는지 알아보기 위해 인위적으로 blur시킨 영상들에 대해서도 실험해보았다.

실험결과로 정정되는 오류의 개수에 따른 GAR (Genuine Accept Rate)값과 FAR(False Accept Rate) 값의 그래프를 나타내었다. 그림2와 3을 보면 원래의 홍채영상을 인증에 사용할 때나 여러 방법에 의해 blur된 영상을 사용할 때나 모두 비슷한 형태를 갖는다. 또한 EER값도 모두 0%로 동일하다.

이러한 결과는 홍채정보의 가변성을 줄이기 위해 제안된 클러스터링 방법이 제안된 홍채 기반의 퍼지볼트 시스템을 카메라의 초점 변화에 강인하도록 해주었음을 나타낸다.

향후에는 클러스터링 방법이 다른 여러 가지 환경변화에 따른 홍채 특징정보의 가변성에 어떠한 영향을 미치는지에 대한 실험이 필요하다.

참고문헌

[1] Umut Uludag, "Fuzzy Vault for Fingerprints," AVBPA2005, LNCS 3546, pp.310-319, 2005.

[2] 이연주, 이형구, 박강령, 김재희, "홍채 코드 기반 생체고유키 추출에 관한 연구," 대한전자공학회 추계종합학술대회 28권, 2호, pp.1011-1014, 2005.

[3] 이연주, 박강령, 김재희, "퍼지볼트 기반의 암호 키 생성을 위한 불변 홍채코드 추출," 대한전자공학회 하계종합학술대회 29권, 1호, 2006.

[4] Y. J. Lee, K. H. Bae, S. J. Lee, K. R. Park and J. Kim, "Biometric Key Binding: Fuzzy Vault based on Iris Images," Lecture Notes in Computer Science (ICB 2007), *to be appeared*, 2007.

[5] A. Juels and M. Sudan, "A fuzzy vault scheme," Proc. of IEEE International Symposium on Information theory, 2002.

[6] K. H. Bae, S. I. Noh, Park and J. H. Kim, "Iris Feature Extraction Using Independent Component Analysis," LNCS on Audio-and Video-Based Biometric Person Authentication, Vol. 2688, pp. 838-844, 2003

[7] http://berc.yonsei.ac.kr(accessed on 2007. 5. 4)