Journal of KIIT. Vol. 16, No. 4, pp. 109-122, Apr. 30, 2018. pISSN 1598-8619, eISSN 2093-7571 109
http://dx.doi.org/10.14801/jkiit.2018.16.4.109

생체 인증에서의 프라이버시 보호 기술

박희진*, 이윤호**

Survey on Privacy-preserving Techniques for Biometric Authentication

Heejin Park*, Younho Lee**

이 연구는 서울과학기술대학교 교내연구비 지원으로 수행되었습니다.

요 약

사용자 인증 수단으로 생체 정보의 이용이 늘고 있으며 이에 따라 생체 정보 누출에 따른 개인 정보 프라이버시 침해가 우려되고 있다. 이를 해결하기 위해 법제화를 통한 해결책과 더불어 개인정보 침해가 되지 않는 프라이버시 보존 기능을 포함하는 안전한 생체 인증 기술이 연구되고 있다. 본 논문에서는 생체 인증에서의 개인 정보 침해 유형을 기술하고, 이러한 침해를 막기 위해 제안된 다양한 프라이버시 보존 기반 생체 인증 방법들에 대해 논의한다. 구체적으로, 최근까지 제안된 방법들을 생체 정보와 키 정보의 연결을 기반으로 하는 방법과 생체 정보 자체를 변형하여 보호하는 방법으로 분류하고, 각 분류에 속한 기술들에 대해 알아보고 장단점을 분석한다.

Abstract

The use of biometric information is increasingly used as a user authentication means, and accordingly, there is a concern that privacy of personal information may be infringed due to leakage of biometric information. In order to solve this problem, a secure biometric authentication technology including privacy preservation function that does not infringe personal information is being studied in addition to solution through legislation. In this paper, we describe the types of personal information infringement in biometric authentication and discuss various privacy-preservation based biometric authentication methods proposed to prevent such infringement. Specifically, the methods proposed to recent have been classified into two types: one based on linking of biometric information and key information and another one of transforming and protecting biometric information itself. Then, the techniques belonging to each category are analyzed including finding out the pros and cons of them compared with each other.

Keywords

biometric authentication, privacy protection, authentication, cryptography, security

* 서울과학기술대학교 IT정책전문대학원 산업정보시스템전공
- ORCID: http://orcid.org/0000-0003-2173-0320
** 서울과학기술대학교 글로벌융합산업공학과 ITM 전공(교신저자)
- ORCID: http://orcid.org/0000-0003-1767-6165

· Received: Mar. 12, 2018, Revised: Mar. 29, 2018, Accepted: Apr. 01, 2018·
· Corresponding Author: Younho Lee
ITM Division, Dept. Industrial and Systems Engineering, SeoulTech, Korea.
Tel.: +82-2-970-7283, Email: younholee@seoultech.ac.kr

Ⅰ. 서 론

IT 기술의 지속적인 발달, 개인용 휴대기기의 급속한 보급, IoT기기 및 기술의 보편화가 진행되면서 각 개인과 휴대기기 그리고 시스템간의 연결, 그리고 그 연결에 있어서의 사용자 인증이 중요해지고 있다. 이에 따라 다양한 방식의 사용자 인증 방법이 제안되었으며, 그 중 생체 인증(Biometric Authentication)이 사용자를 인증하는 중요한 수단으로 주목 받고 있다. 생체 정보는 사용자가 인증을 위해 사용되는 다른 정보와는 달리 사용자의 관리 비용이 적은 장점이 존재한다. 그러나 생체정보가 가지는 불변성, 고유성으로 인하여 생체정보의 누출은 그 사람의 개인정보 누출과 똑같기에, 생체 인증에 있어 생체 정보가 누출되지 않아야 하는 것은 생체정보 인증의 안전성을 위해 중요한 요구 조건 중의 하나이다.

본 연구에서는 생체 정보에 대한 프라이버시 보호가 가능하면서도 본래의 인증 목적을 이룰 수 있는 다양한 접근 방법에 대해 논의한다. 구체적으로 생체 정보를 인증을 위한 키 정보와 연관시키는 방법과 생체 정보 자체를 다양한 암호학적 도구로 보호하여 인증을 수행하는 방법이 있다. 각 유형별로 다양한 방법들을 소개하고 그것들 간의 장단점을 비교한다.

본 논문의 2장에서는 생체 인증을 소개하고 3장에서는 생체 정보의 개인 프라이버시 보호 문제를 소개한다. 4장에서는 프라이버시 보존 생체 인증 방법들에 대해 소개한다. 5장에서는 그들의 장단점을 비교한다. 마지막으로 6장에서는 결론 및 향후 연구 과제에 대해 논의한다.

Ⅱ. 생체 인증 소개

본 절에서는 생체 인증 방법에 대해 소개한다. 1 세부 절에서는 생체 인증 기술 일반에 대해 기술하고, 2 세부 절에서는 생체정보기반 인증 기술의 절차에 대해 소개한다.

2.1 생체정보기반 인증 기술 소개

생체 인식 기술(Biometric Technology)은 인간의 고유한 생물학적 특성의 분석을 통해 얻은 생체 특성 정보를 계산적 방법으로 처리하는 기술이다[1]. 생체 인증은 이러한 생체인식 기술을 이용하여 특정 개인을 인증하는 것으로, 어떤 개인의 신원을 그 개인의 고유한 생체적 특성을 이용해서 자동화된 방법으로 측정하여 인증하는 것이라 할 수 있다[2].

이러한 생체 인증은 미국의 FBI(Federal Bureau of Investigation)에 의한 지문 데이터베이스 구축과 운영[3], 한국의 주민등록증 시스템의 지문 데이터베이스[4] 등과 같이 국가 기관에 의해 공공의 목적으로 활용되는 경우가 많았으나, 최근 몇 년 사이에 Apple사의 iPhone에서의 지문 인증에 의한 디바이스 사용제한 해제, 한국 삼성페이의 지문 인증을 이용한 지불 결제 등 민간 영역에서의 생체 인증 활용이 급격하게 증가하고 있다[5].

상기한 바와 같이 민간에서의 생체 인증 이용이 급격히 증가한 데에는, 모바일 폰의 사용이 일상화되고 이를 이용한 전자상거래가 늘어나면서 모바일 폰 사용자에 대한 인증이 보안성 있으면서도 편리하게 제공되어야 했기 때문이다[6][7]. 일반적으로 사용자 인증에 가장 많이 사용되는 비밀번호 입력 방식에 비해, 지문 혹은 얼굴 등 생체 정보를 이용한 생체 인증이 입력 시간이 짧아 편리하고, 본인 외에는 인증이 되지 않을 확률이 더 높아 보안성이 우수한 것으로 알려져 있다[7].

2.2 생체 인증 절차

생체 인증은 크게 등록과 인증의 두 개의 단계를 거쳐 수행된다[8]. 첫 번째 단계는 등록 단계로, 사용자의 생체 정보를 센서 장치를 통해서 입력받아 특정한 형태의 데이터 구조로 저장하는 단계이다. 두 번째 단계는 인증 단계로, 사용자의 생체 정보를 입력받고, 앞의 등록 단계에서 저장해 둔 생체 데이터와 비교하는 단계이다. 이러한 인증 단계에서, 해당 사용자가 등록 단계에서 생체 정보를 입력한 사용자와 같은지 판가름하게 된다.

III. 생체 인증에서의 프라이버시 보호 문제

이전 절에서 살펴본 바와 같이, 생체 인증 기술은 편리함과 보안성으로 그 활용이 증가하고 있으나, 몇 가지 문제를 가지고 있다. 그중에서 사용자 관점에서 가장 문제가 되는 것의 하나는 사용자의 개인 프라이버시 정보 보호의 문제이다[6]. 이는 주로 생체 인증의 등록 단계를 통해 저장된 사용자의 생체 정보가 누출되거나 오용될 가능성 때문에 생긴다[9].

생체 정보의 누출로 인해 야기되는 피해는 패스워드의 누출로 인해 생기는 피해보다 더 크다고 할 수 있는데, 이는 사용자의 생체 정보가 그 사람의 일생 동안 변경되지 않기에, 누출된 생체 정보를 삭제하고 다시 재발급하기 어렵다는데 기인한다[10]. 이에 따라 유럽연합에서는 2016년 GDPR(General Data Protection Regulation)을 개정하면서 사용자의 동의 없이 생체 정보를 이용하여 그 사람임을 파악하려는 시도를 엄격히 제한하게 하였고[11], 미국에서는 2017년 7월에 워싱턴 주가 일리노이 주와 텍사스 주에 이어 3번째로 생체 정보에 대한 프라이버시 관련 법률을 제정하는 등[12], 점점 더 생체 정보에 대한 프라이버시 보호의 중요성이 높아지고 있는 추세이다.

3.1 생체 정보 시스템에서의 개인 정보 프라이버시 침해 유형

생체 인증을 포함한 생체 정보 관련 시스템의 사용 과정에서 개인 정보가 침해되는 유형은 '다른 서비스에 사용', '부가정보 취출', '오용' 의 3가지 유형으로 볼 수 있다[13].

1) 다른 서비스에서의 사용: 어떤 서비스에서 사용되고 있는 생체정보를 그 개인의 인지와 동의 없이, 다른 서비스나 응용에서 사용됨으로써 발생되는 침해를 말한다. 이는 생체정보가 어떤 개인에 있어 고유하고 불변인 성질 때문에 가능한 침해이다. 즉, 한 개인이 가지고 있는 생체 정보를 한 응용이 독자적인 방법으로 취득하였더라도, 이 생체 정보가 누출되었을 때에는, 그 생체 정보가 그 개인이 갖고 있는 고유한 정보에서 기인하였기에, 다른 서비스나 응용에서도 사용될 수 있는 개연성이 있다는 것이다.

2) 부가 정보 취출: 생체 정보로부터 그 사람의 인종 정보 혹은 질병 정보 등 다른 부가 정보가 노출되어 침해되는 경우이다. 지문 정보로부터 그 사람의 혈액형을 유추할 수 있다는 연구 결과가 있고[14], 얼굴 인증을 위해 취득된 얼굴 이미지로부터는 피부 색깔로부터 그 사람의 인종을 유추할 수 있고, 질병도 유추할 수 있다[15]. 이 경우 생체 정보는 원래 목적하였던 기능 이상의 정보를 알려주고 있는 것으로, 사용자가 인지하지 못하고 있는 상태에서 사용자의 정보가 누출된 것이라 할 수 있고, 피부색으로부터 얻어낸 인종 정보로 개인을 차별화하는 등의 수단으로 악용될 수 있다.

3) 오용: 생체 정보의 오용은, 생체 정보가 원래의 사용 목적의 범위를 벗어나서 그 사람의 동의 없이 사용되는 것을 말한다. 생체정보가 오용될 수 있는 가장 큰 가능성 및 문제는 중앙에 보관된 생체정보가 누출되는 경우이다[16]. 이 경우 누출된 생체정보가 본래의 목적과 다르게 사용되어 생체정보의 원주인이 인지하지 못하는 사이에 다른 주체가 해당 정보의 원 주인인 척 가장되어 사용하는 오용이 존재할 수 있다.

중앙 데이터베이스에 보관되어 있는 데이터가 탈취되는 것은 계속해서 발생하고 있는 문제이며[17], 최근 인도에서는 범국가적으로 인도 국민 모두에 대해서 지문, 얼굴, 홍채를 수집해서 국가 차원의 정보로 이용하려는 UIDAI(Aadhaar) 시스템으로 부터[18] 데이터 누출이 있었고, 이로 인하여 약간의 비용과 시간으로도 생체데이터를 취득할 수 있다는 기사가 있었다[19]. 이러한 사례에서 보듯이 데이터 누출에 의한 오용은 국가에 의해 유지되는 시스템에서도 벌어질 수 있는 일이다.

이렇게 데이터베이스의 정보가 누출되지 않더라도 생체정보의 사용에 대한 세밀한 설계가 이루어지지 않았을 경우 오용이 발생할 수 있다. 예를 들어, 지문의 경우 범죄 사건이 벌어졌을 때 범인을 찾기 위한 법의학적인 식별 방법으로 사용될 수 있고 이는 경찰의 범인 수색을 쉽게 할 수 있다. 그러나 이러한 정보가 범죄기록 데이터베이스로 사용될

수 있고, 이는 범법 행위의 증거 없이 일반 시민에 대한 감시로 오용될 수도 있는 것이다[20].

Ⅳ. 생체 인증에서의 프라이버시 보호 방법

본 절에서는 이전 절에서 제시한 다양한 생체 정보 노출로 인한 프라이버시 침해를 방지하기 위한 생체 인증에서의 프라이버시 보호 기법들을 소개한다.

ISO/IEC 24745에서는 이전 절에서 상기한 바와 같은 생체정보에 의한 개인정보 침해가 이루어지지 않기 위해, 등록과정을 통해 저장되는 생체정보가 1) 원래의 생체 정보로의 변환이 불가해야 하는 비가역성(Irreversibility), 2) 저장된 생체 정보가 다른 응용이나 데이터베이스 간에 연계가 가능하지 않아야하는 불연계성(Unlinkability), 3) 외부로부터 비인가 된 주체로부터의 생체정보에 대한 접근이 불가하도록 생체 정보가 드러나지 않아야 하는 참조 기밀성(Confidentiality), 4) 생체 정보가 노출되었을 경우 이를 폐기하고 새로운 생체 정보로 재발급할 수 있는 폐기성과 재발급성(Revocability and Renewability)과 같은 특성을 가져야 한다고 권고하고 있다[21]. 또한, 생체정보를 다루는 시스템은 1) 비 인가된 사람으로부터의 접근이 불가해야 하는 접근 기밀성, 2) 저장된 생체 정보 데이터의 일부가 변경되거나 위조되지 않음이 보장되어야 하는 무결성(Integrity), 3) 생체 정보의 누출 등 문제가 발생했을 때 혹은 미래의 침해 위협에 대응하기 위해 생체 정보를 폐기하고 새롭게 등록될 수 있어야 하는 폐기 및 재발급성등 보안성과 같은 성질 및 기능을 제공해야 한다고 기술하고 있다[21].

시스템에서 요구되는 폐기 및 재발급성은 위의 개인정보 보호에서 요구되는 재발급성과는 다른 요구 사항으로, 시스템 상에서 해당 생체 정보를 폐기하고 새롭게 재발급할 수 있는 것을 의미하고, 개인정보 보호에서 요구되는 재발급성은 같은 동일인에 대해서 서로 다른 생체데이터를 재발급해야 함을 의미한다.

위와 같은 조건에 맞는 생체 정보 시스템의 구축을 위해 직관적으로 암호학적 방법의 도입을 고려할 수 있다. 즉, 현재 사용되는 표준 암호 알고리즘인 AES, RSA 등을 사용하여 생체정보를 암호화 하는 것이다. 그러나 이러한 방법은 생체 정보에 대한 개인 정보 침해를 막는 방법으로 부적절하다[9]. 이것은 생체 정보를 암호화해서 보관하면 확실한 기밀성이 보장되어 개인 정보 보호가 된다고 할 수 있으나 암호화된 생체 정보를 가지고는 생체 정보 간 유사도를 측정할 수 없는데 기인한다. 생체 정보는 취득할 때마다 미세하게나마 다른 정보로 취득이 되고, 생체 정보를 비교한다는 것은 그 생체 정보의 디지털 값을 일대일로 비교하는 것이 아니고 벡터 값을 이용해서 유사도를 비교하는 것이기에[22], 암호화되어 저장된 값과 인증을 위해 새롭게 입력받은 생체정보와 비교할 수 없는 것이다. 따라서 비교를 위해서는 암호화된 것을 복호화해서 서로 비교해야 하는데, 이것은 인증 시점마다 생체정보가 평문으로 인증 모듈에 전달되는 것이기에 안전하지 못하다.

위와 같이 일반적인 암호화 기법으로는 생체정보에 대한 개인정보 침해를 막을 수 없기에, 기존의 전형적인 암호화 기법과는 다른 방법들이 제시되었다. 본 방법들의 핵심은 생체정보를 데이터로 표현하는 방식인 템플릿을 암호학적 기법을 이용하여 보호하는 것이다. [9]에서는 이러한 템플릿을 보호하는 방법을 크게 1) 생체정보의 특성 변환과 2) 생체 암호화의 두 가지로 분류하였다. 생체정보의 특성 변환을 하는 방법은 바이오해싱에 의한 솔팅(Salting) 방법과 비가역 변환 방법이 있고, 생체 암호화에는 키를 결합하는 방법과 키를 생성하는 방법으로 그림 1과 같이 구분하였다.

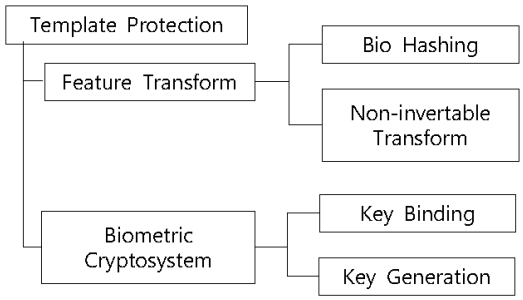

그림 1. 템플릿 보호 방법 [9]
Fig. 1. Template protection method [9]

이 외에도 [23]에서는 개인 정보 보호를 위한 템플릿 보호방법을 1) 보안 스케치(Secure Sketch) 2) 퍼지 확약(Fuzzy Commitment) 3) 취소 가능한 생체 인증(Cancelable Biometrics) 4) 등록 시점에서의 생체 암호화로 구분을 했다.

이와 같은 분류 방법들을 종합해보면 결국 생체 정보에서 개인 정보를 보호하는 방법은 1) 그림 2와 같이 키 데이터는 생체 정보와 연결되며 이것은 올바른 생체 데이터 입력으로 추출될 수 있으며 생체정보를 이용해서 암호화 키를 결합 혹은 생성하거나 2) 그림 3과 같이 암호화 키를 이용해서 생체 정보를 변환 혹은 암호화하는 방법으로 생각할 수 있다.

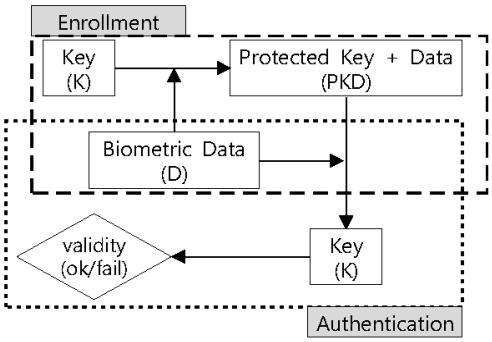

그림 2. 키 생성 기반 생체 암호 시스템을 이용하여 생체 정보가 보호되는 경우의 등록 및 인증 방법

Fig. 2. Enrollment and authentication mechanism when biometric data is protected using a key generation biometric cryptosystem

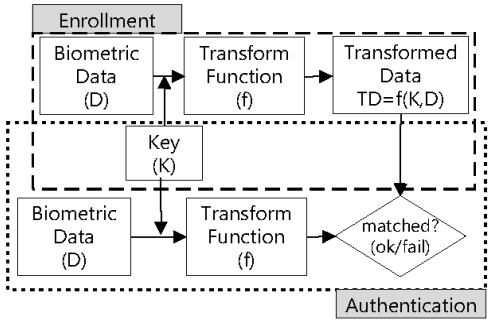

그림 3. 생체 정보가 외부 키 데이터를 이용하여 보호될 경우의 등록 및 인증 방법

Fig. 3. Enrollment and authentication mechanism when biometric data is protected by added external key data

1)번 방법은 생체정보가 암호화키를 뽑아내기 위한 수단이 되는 것이고 2)번 방법은 반대로 암호화키가 수단이 되어서 생체정보를 변환 혹은 암호화해서 비교하는 것이다. 이후 각 세부 절에서는 이러한 1) 과 2)의 접근 방식을 구현하는 다양한 방법들에 대해 구체적으로 논의한다.

4.1 생체 정보 이용 키 결합/생성

생체 정보와 결합하여 암호화 키를 숨기거나 생체 정보를 이용해서 암호화 키를 생성하는 방법에 대해서 논의한다. 이러한 유형의 방법에서 인증을 위해 최종적으로 사용되는 것은 등록 시점과 인증 시점에 사용되는 암호화 키의 동일성이지만, 그 과정에 존재하는 생체정보 템플릿도 암호화 키와 결합 혹은 변형된 형태로 존재하며, 사용되는 암호알고리즘은 연산 결과물로부터 사용된 키의 기밀성을 보장하므로 키 생성 또는 변형에 사용된 생체 정보의 누출을 방지한다. 따라서 본 방법은 개인 생체정보의 프라이버시를 보호할 수 있는 기법이라 할 수 있다[9].

생체 정보와 키를 결합하는 방법으로는 퍼지 확약[24], 퍼지 볼트(Fuzzy Vault)[25]가 있고, 생체 정보로부터 암호화 키를 생성하는 방법으로는 퍼지 추출(Fuzzy Extractor)[26]이 있다.

1) 퍼지 확약 방식: 본 방식은 [24]에 의해 처음 소개되었으며, 에러 보정코드(ECC, Error Correction Code)와 해시(Hash)함수를 이용해서 생체정보를 숨기는 방식이다. 그림 4는 퍼지 확약 방식에 의한 등록과정을 보여준다. 입력으로 생체정보 x와 에러 보정코드 c가 들어가고, 이 두 정보를 이용해서 결합함수가 두 정보의 차이 벡터 d를 생성하고, 해시함수를 이용해서 ECC c에 대한 해시값 h(c)를 생성한다. 생성된 두 값 d와 h(c)는 데이터베이스에 보관된다. 여기서 에러 보정코드 c는 에러 보정코드 집합 C에서 선택된 값이고, 추측될 수 없고 오직 생체정보 x와 충분히 유사한 x'이 입력되었을 때만 알아낼 수 있는 값이다. 즉, c는 숨기고자 하는 비밀 키에 해당한다.

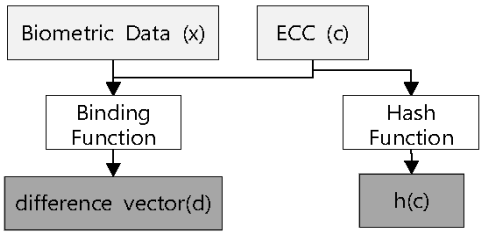

그림 4. Fuzzy commitment 방식에서의 등록 과정
Fig. 4. Enrollement process in fuzzy commitment

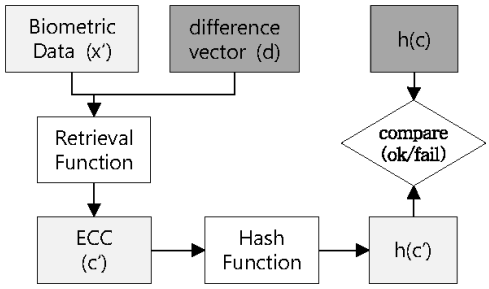

그림 5. Fuzzy commitment 에서의 인증 과정
Fig. 5. Authentication process in fuzzy commitment

퍼지 확약 방식의 인증과정은 그림 5와 같다. 인증용으로 입력된 사용자의 생체정보 x'과, 이미 저장되어 있던 차이 벡터 d가 복원함수의 입력으로 들어가서 에러 보정코드 c'이 생성된다. 이 값은 해시함수를 통해 해시값 h(c')이 계산된 후, 이미 저장되어 있던 해시값 h(c)와의 비교를 통해 인증이 완료된다. 이때, 인증용으로 제시된 사용자의 생체정보 x'이 원래 등록과정에서 제시되었던 생체정보 x와 충분히 유사해야만 등록과정에서와 같은 에러 보정코드 c가 복원되어 인증 성공한다.

퍼지 확약에서의 동작 과정은 다음의 예를 통해 좀 더 쉽게 이해될 수 있다.

ECC를 이루는 집합을 이차원 좌표계에서 u, v가 정수일 때의 {100u, 100v}라 하고, 복원함수 f를 입력된 좌표값에서 가장 가까운 ECC 좌표 쌍이라고 정의하자. 즉, f(78, 90)=(100,100). 이제 ECC로 u=1, v=1일 때의 c=(100,100)으로 지정하고, 사용자의 생체정보에 해당하는 x의 값을 이차원 좌표계의 값 (372, 90)라 할 때, 차이 값 d=x-c로부터 d=(272,-10)이 계산된다. 이제 이 d값과 c의 해시값 h(c)가 저장되는데, h(c)로부터 c로의 유추는 해시함수의 일방향성에 의해 불가하고, c를 모르는 상태에서 d값만을 이용해서 x를 유추해낼 수는 없다.

인증과정에서 x의 값과 유사한 x'=(36, 80)이 들어왔다고 가정하자. 그렇다면 c'=x'-d=(88, 90)이 되고, 복원함수 f를 이용해서 f(c')을 계산해보면 f(c') = f(88, 90) = (100, 100)이 되어서, 등록과정에서의 c값과 같게 되므로, 두 해시값 h(c)와 h(c')은 일치하게 된다.

연구자들은 퍼지 확약 방식을 다양한 유형의 생체 정보에 적용할 수 있도록 기능성을 확장하였다. [24]은 실제 홍채 데이터를 이용해서 퍼지 확약 적용을 처음으로 시도하여, 2048비트의 홍채 데이터로부터 140비트의 키를 추출하는 방안을 제시하였다. 또한 [27]은 홍채 데이터를 이용함에 있어서 효과적인 에러 보정 디코딩 방법을 제시하였다.

[28]은 생체 정보가 균일하게 랜덤하지 않아도 퍼지 확약 방식이 적용될 수 있는 방식을 지문데이터를 이용해서 제시했으며, [29]은 지문 이미지가 아닌 특징점 기반의 지문인증에도 사용될 수 있는 방안을 제시하였다. 또한 [30]은 얼굴에 대한, [31]은 수기 서명에 대해 퍼지 확약 적용을 제시했다.

[24]에 의해 제시된 퍼지 확약 방식은 개념이 간단하면서도 여러 ECC 방식을 사용할 수 있고, 입력되는 생체 정보값이 균일한 랜덤성만 보장된다면 에러 보정 코드값의 보안 강도에 따라 보안성이 결정되는 장점이 있다[32]. 그러나 이 방식은 등록된 생체정보 값 x와 인증 시 입력되는 생체 정보값 x' 값이 어느 정도 달라도 동작 되는 '값에 대한 에러 보정'에는 강하나, 생체 정보 값의 순서가 달라지는 것에 대한 '순서변동오류'에는 약하다. 즉, 생체정보 값이 회전 혹은 이동되었을 경우 다르게 인식될 수 있다. 또한, 생체 정보가 균일한 분포 값을 가지지 않을 때의 보안성 보장이 쉽지 않은 단점이 있다[32]. 이러한 단점을 보완하면서 생체정보와 암호화키 결합을 통한 개인정보 보호를 가능하게 제안된 것이 퍼지 볼트방식이다.

2) 퍼지 볼트 방식: 퍼지 볼트는 [32]에서 제시된 방법으로, 위에서 살펴본 퍼지 확약과 마찬가지로 생체 정보와 암호화 키의 결합을 통해 생체정보에 대한 개인 정보 보호가 가능하게 하면서, 퍼지 확약의 단점이 보완된 방법이다. 그림 6은 퍼지 볼트의 등록 과정이다.

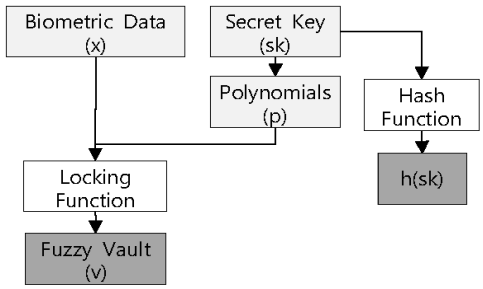

그림 6. 퍼지 볼트 방법의 생체정보 등록 과정
Fig. 6. Enrollment process in fuzzy vault scheme

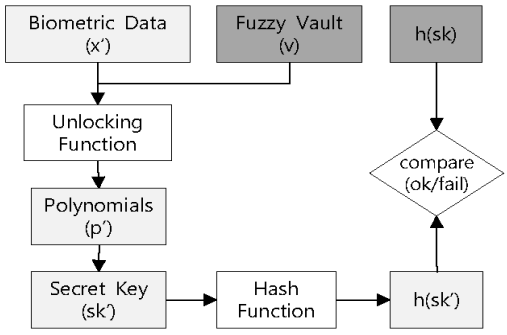

그림 7. 퍼지 볼트 방법의 인증 과정
Fig. 7. Authentication process in fuzzy vault scheme

임의의 비밀키 sk를 이용해서 다항식 p를 만든다. 예를 들어 다항식 sk를 계수로 해서 한 개의 변수를 가지는 다항식 p를 만든다. 그리고, 생체 데이터 값 x를 이 다항식에 입력한 값을 구하고, 다항식 p에 위치하지 않는 임의의 값들을 합쳐서 퍼지 볼트 값 v를 생성한다. 이차원 좌표에서의 그래프로 생각하면, 어떤 다항식 그래프에서, 생체정보 x에 의해 투영되는 다항식 그래프 p위의 값들과 이 그래프 p 위에 위치하지 않는 혼돈값들이 퍼지 볼트 v가 된다. 이 혼돈값들로 인해 퍼지 볼트 v로부터 다항식 p를 유추하는 것이 어렵게 되고, 이는 sk를 알 수 없다는 것이 된다.

비밀키 sk는 일방향 해시함수에 의해 해시값 h(sk)로 변환되어 저장되고, 이는 일방향 함수 특성에 의해 h(sk)를 가지고 원래의 sk를 알아낼 수 없다.

퍼지 볼트의 인증과정은 그림 7과 같다. 저장되어 있었던 퍼지 볼트값 v에서, 인증용으로 입력된 생체정보 값 x'에 대응하는 값을 추출하고, 이 값을 이용해서 다항식 p'을 생성한다. 만약 x'이 등록할 때 사용되었던 원래의 생체정보 x와 충분히 유사하다면, x'에 의해 생성되는 다항식 p'은 원래의 다항식 p와 같을 것이다. 생성된 다항식 p'으로부터 비밀키 sk'을 추출하고, 해시함수를 이용해서 해시값 h(sk')을 계산 후 보관하고 있던 해시값 h(sk)와 비교해서 인증이 완료되게 된다.

처음으로 퍼지 볼트를 실제로 사용한 것은 [25]에서였다. 스마트카드에 보관된 비밀키를 올바른 지문정보가 들어와야 사용할 수 있게 하는 데 사용하였다. 지문의 특징점 정보가 추출되어 그 좌표와 값으로 이루어지 mi가 생성되고, 비밀키 sk에 의해 다항식 f가 생성된 후, 지문 특징점 정보에 매칭되는 f(mi)를 구해서 (mi, f(mi))쌍을 구한 후 혼돈점을 더해서 퍼지 볼트를 만들었다. 이 퍼지 볼트값은 스마트카드 내에 저장되어 있다가, 올바른 지문이 입력된 경우 비밀키를 사용할 수 있는 메커니즘이다. [25]의 경우 지문의 특징점 정보가 미리 정렬되어야 하는 전제조건이 있어야 했고 이는 실제 적용성을 저하 시키는 요인이다. 이러한 미리 정렬돼야 하는 문제는 조을 없앤 방안이 [33]에 의해 제시되었다. 퍼지 볼트에 있어서 생체 인증에 대한 정확도도 중요한 주제인데, 생체 이미지에 있어서 시작점 정보를 도입해서 정확도를 높이는 방법[34], 혼돈점을 빠르고 효율적으로 계산할 수 있는 방법으로 혼돈점을 많이 사용해서 정확도를 높이는 방법들이 연구되었다[35]. 또한, 지문이 아닌 다른 유형의 생체 수단인 홍채[36], 장문[37], 얼굴[38]에 대한 퍼지 볼트의 적용도 연구되었다.

3) 퍼지 추출 방식: 퍼지 추출 방식은 [38]에서 제시되었으며, 생체 정보 자체로부터 암호화 키를 뽑아내는 방식이다. [38]에서는 두 가지 기본 모듈인 보안 스케치와 퍼지 추출을 정의한다. 보안 스케치는 생체정보 x를 입력받아 공개되는 정보 P를 만들어 내는데, 향후 x와 충분히 유사한 생체정보 x'이 제시되었을 때 원래의 x를 복원해내는 모듈이다. 즉, 생체 정보가 입력될 때마다 조금씩 다른 오류가 있음에도 동일한 생체 정보로 복원할 수 있는 기능이다.

퍼지 추출은 입력된 생체 정보가 충분히 비슷하면 같은 랜덤 문자열 R을 출력하는 모듈이고, 이 R은 일반적인 암호화 키로 사용될 수 있다. 그림 8은 퍼지 추출 방식에서의 등록과정이다.

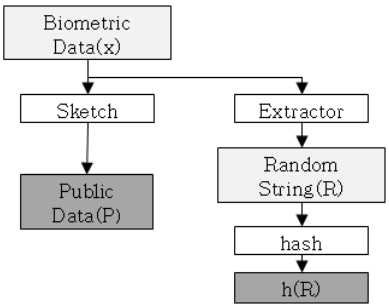

그림 8. Fuzzy Extractor 방법에서의 등록 과정
Fig. 8. Enrollment process in fuzzy extractor scheme

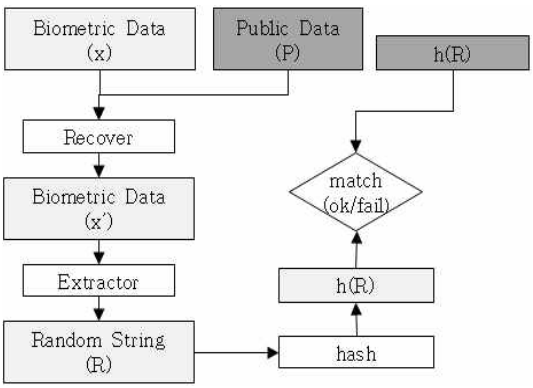

그림 9. Fuzzy Extractor 방법에서의 인증 과정
Fig. 9. Authentication process in fuzzy extractor scheme

생체정보는 스케치 모듈을 통해, 공개되는 데이터인 P로 변환이 되고, 이 P만을 가지고 x로 변환될 순 없다. 또한, 생체정보는 퍼지 추출기를 통해서 난수 문자열 R이 추출된다. 퍼지 추출기는 x와 충분히 비슷한 정보 x'이 입력되면 동일한 R을 만들어 낸다. 이 R은 해시함수를 통해 해시값이 생성돼서 저장된다.

퍼지 추출방식에서의 인증과정은 그림 9와 같다.

인증을 위해 입력된 생체정보 x'과 저장되어 있던 공개 데이터 P가 복원 모듈을 통해 생체정보 x로 복원되고, 이 값은 퍼지 추출기를 통해 난수 문자열 R이 추출되고, 이 R에 대한 해시값 h(R)과 저장되어 있던 h(R)을 비교함으로써 인증이 완료된다.

퍼지 추출방식이 앞서 살펴본 퍼지 확약과 퍼지 볼트와 다른 점은, 퍼지 확약과 퍼지 볼트가 주어진 암호화키를 생체정보와 함께 '결합'했다가, 생체정보에 의해 그 암호화 키를 사용하는 데 반해, 퍼지 추출 방식은 각 생체정보마다 가지고 있는 고유한 불규칙성인 엔트로피를 이용해서 암호화키로 사용될 수 있는 난수 문자열을 생성하는 데 있다. 따라서, 생체정보가 가지고 있는 엔트로피에 따라 추출될 수 있는 암호화키의 길이가 결정되고, 또한 이 엔트로피(k) 보다 큰 에러(t)가 들어오는 경우(t>k), 즉 처음 등록한 생체 정보와 많이 다른 생체 정보가 들어와서 그 에러 크기가 생체 정보가 함유할 수 있는 엔트로피보다 큰 경우는 암호화 키를 제대로 생성할 수 없다[26]. [39]에서는 에러가 엔트로피보다 큰 경우(t>k)에도 동작될 수 있는 방법이 제시되었다.

이 방법을 이용해서 지문 정보로부터 약 40비트의 암호화 키를 생성하는 방법[40], 홍채 정보로부터 140비트의 암호화 키를 생성하는 방법[40], 186비트를 생성하는 방법[41], 240비트를 생성하는 방법[42], 얼굴 정보로부터 암호화 키를 생성하는 방법[43], 목소리 정보로부터 암호화 키를 생성하는 방법[44] 등이 제시되었다.

퍼지 추출 방식은 생체 정보 자체만을 이용해서 키를 생성할 수 있기에 편리하고 저장해야 할 데이터가 작아 메모리가 적게 들지만, 같은 생체정보를 가지고 다르게 등록할 수 있어야 하는 재발급성이 약하고[45], 입력되는 생체 정보가 정렬되어 있지 않거나 특이한 에러가 발생하는 경우에 취약하고[46], 생체 정보로부터 생성되는 공개 데이터가 원래의 생체 정보로 변환되지 않는 보안성은 좋으나 개인을 식별할 수 정보로 쓰일 수 있는 취약성이 있다[47]. 최근에는 재발급성이 확보된 퍼지추출방식도 제안되었다[39].

4.2 생체 정보 변환/암호화 방식

생체 정보를 변환하거나 암호화해서 개인정보 보호를 하는 방식은, 변형함수가 주요 수단이 되어서 생체 정보를 변형시키는 방식이다. 이 방법으로는 변형 함수에 따라 원래의 생체 정보가 여러 형태로 변형될 수 있는 폐기형 생체 인증 방식[48], 암호화 키로 생체 정보 자체를 암호화한 후 암호화된 상태에서 생체 인증이 가능하게 하는 동형암호(Homomorphic Encryption)[49]-[54] 방식이 있다.

1) 폐기형 생체 인증: 폐기형 생체 인증은 [48]에

서 처음으로 개념이 소개되었다. 어떤 비가역적인 변형 함수를 이용해서 생체 정보를 변형하는 것으로, 등록할 때마다 다른 변형 함수를 사용함으로써, 같은 사람의 생체 정보라도 등록할 때마다 다른 형태의 생체 정보로 변형되어 저장되고 매칭될 수 있는 방법이다. 따라서 어떤 시스템에 등록한 생체 정보가 도용되었다 하더라도, 비가역함수에 의해 변형되었기에 원래의 생체 정보로 복원되어 그 개인의 생체 정보 자체가 누출되지 않는 것이고, 다른 변형 함수를 사용하여 재등록하게 함으로써 문제를 해결할 수 있다.

폐기형 생체 인증 방식에서의 등록과정은 다음과 같다. 생체 정보 x가 변형 함수에 의해 변형되어 저장되고, 인증 과정에서 새롭게 입력된 생체 정보 x' 이 동일한 변형 함수로 변형된 후, 두 정보가 비교된다.

[55]에서는 실제 지문 인증에서의 폐기형 생체 인증 적용방안이 제시되었다. 지문 인증에 있어서 변형함수를 적용하기 전에 먼저 위치에 대한 상대 좌표계를 일치시키는 작업을 해야 한다. 예를 들어 [56]에서 정의한 지문 중심점(Core)와 삼각주(Delta)를 지문 이미지에서 찾고, 이 특이점(Core and Delta)을 기준으로 각 특징점 벡터의 상대 좌표를 계산한다. 즉, 등록할 때마다 조금씩 달라지게 되는 지문 이미지의 위치와 방향성을 통일시키기 위함이다. 이후 상대좌표로 표시되는 특징점 벡터 $m_i(x_i,y_i,v_i)$에 대해서 변형 함수를 통해 그 위치값이 변형되어 저장되게 된다. [55]에서는 직교좌표 변환, 극좌표 변환, 표면 접기 변환의 3가지 변환에 대한 방안이 제시되었다. 여기서 직교좌표 변환을 살펴보면 다음과 같다.

먼저 지문의 각 특징점 좌표가 중심점과 삼각주를 기준으로 해서 계산된다. 그리고 좌표계는 가로 h개와 세로 v개의 셀로 구성되도록 정의되고, 각 셀은 순차적으로 번호가 부여된다. 이 셀들이 변형함수에 의해서 그 위치가 변경될 것이고, 이에 따라 그 셀안에 위치했던 특징점들의 좌표도 그에 따라 변경된다. 셀의 위치 변경은 매핑배열 M에 의해 변경되게 되는데, 원래의 셀을 C라하고 변경된 셀을 C'이라할 때, C' = CM이 되게 된다.

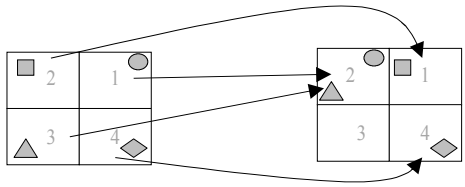

그림 10. 매핑 배열에 따른 각 셀의 변환
Fig. 10. Each cell is transformed according to the mapping array

예를 들어 C가 2 x 2의 셀이고 각각의 번호가 {1,2,3,4}, 그리고 매핑배열이 아래 식과 같이 주어질 때, 그 변형은 식 (1)과 같이 진행된다.

$$(1\,2\,3\,4)\begin{pmatrix}0&1&0&0\\1&0&1&0\\0&0&0&0\\0&0&0&1\end{pmatrix}=(2\,1\,2\,4) \tag{1}$$

이와 같은 변형을 셀 관점에서 보면 그림 10과 같다. (1 2 3 4) → (2 1 2 4) 이기에 최종 변형된 셀의 모양은, 1번셀에는 예전 2번셀이, 2번셀에는 1번과 3번셀이, 3번셀에는 대응되는 것이 없고, 4번셀에는 4번셀이 대응되게 된다. 여기서 주목할 것은 2번셀에 예전 1번과 3번셀이 대응되었기에, 변형된 셀 정보 및 매핑 배열을 알고 있다 하더라도, 셀2에 있는 정보가 1번에서 왔는지 3번에서 왔는지 결정할 수 없게 된다. 즉, 이러한 방식으로 변형된 생체 템플릿 정보는 원래의 생체정보 템플릿으로 복구 불가하고, 매핑 배열을 다르게 하면 다시 생체정보를 다른 형태로 변형해서 재등록 할 수 있게 되는 것이다.

지문에 대해서 [55]에서와 같이 비가역 변환을 사용하여 폐기형 생체 인증을 한 것 외에, 바이오해싱(BioHashing)[57], 바이오토큰(Biotokens)[58], 동적 랜덤 투영[59], 최소거리 그래프[60], 단축된 순환 회신[61] 방식 등이 제시되었다.

또한, 홍채에 대해서[62], 얼굴에 대해서[63], 장문에 대해서[64] 방법들이 제시되었다.

폐기형 생체 인증은 상기한 하나의 생체정보 소스로부터 여러 개의 생체 정보를 생성할 수 있다는 장점 외에, 변형된 생체 정보의 일부를 사용자가 보관하고 또 일부는 서버 단에 보관해서 두 데이터가 합쳐져야 인증이 완료되게 하는 분산 저장 방법이

가능하고, 생체 정보가 변형되고 난 후에는 변형된 생체 정보만 남기고 원본은 파기할 수 있는 장점이 있다[65]. 그러나 여러 변형 데이터로부터 원래의 생체 정보로 복원할 수 있는 가능성이 논의되고 있고[65], 변형 과정을 거치기 전에 같은 좌표계로 일치시키는 등록 과정이 필요하고, 아직 대규모의 생체 데이터를 가지고 검증된 방법이 존재하지 않다[65]는 문제를 가지고 있다.

2) 동형암호 기반 생체 인증: 동형암호는 1978년에 RSA 암호의 개발 주역이었던 Rivest와 Adelman에 의해 처음 제시되었고[49], 그 후 덧셈, 곱셈 등 일부 연산에 대한 동형성을 지원하는 암호기법들이 여러 학자에 의해 제시되다가, 2009년 Gentry에 의해 모든 연산이 지원되는 '완전 동형암호(FHE, Fully Homomorphic Encryption)가 제안되어[50], 암호화된 상태에서 모든 연산(비트 별 AND와 XOR)이 가능하게 되었다.

동형암호에 의한 생체 인증의 등록 및 인증과정은 그림 11, 12와 같다.

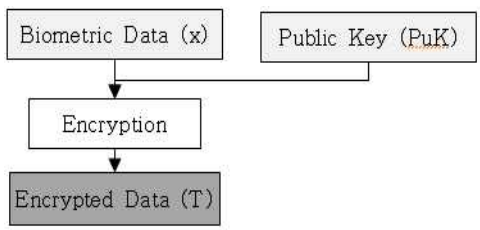

그림 11. 동형암호 기반 방법에서의 등록 과정
Fig. 11. Enrollment process in homomorphic encryption scheme

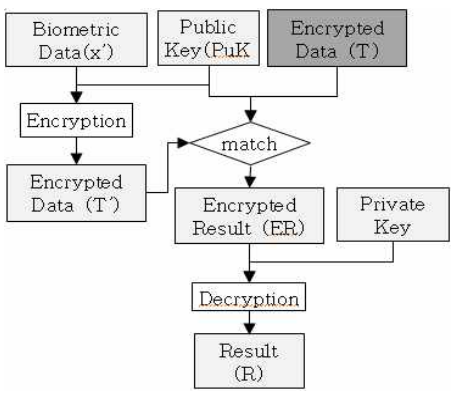

그림 12. 동형암호 기반 방법에서의 인증 과정
Fig. 12. Authentication process in homomorphic encryption

등록과정에서 생체정보 x가 동형암호의 공개키 PuK에 의해 암호화되어 저장된다. 암호화된 데이터는 원래의 생체정보를 노출하지 않으며, 개인키 PrK가 제공되지 않는 한 정보노출이 되지 않음이 보장된다.

인증과정에서 입력된 생체정보가 등록과정에서 사용되었던 공개키 PuK로 동일하게 암호화 되고, 이 암호화된 데이터 T'과 저장되어 있던 암호화 데이터 T와 비교가 수행된다. 이때 특이한 점은 암호화된 상태에서 비교가 진행되고, 이를 위해 공개키가 입력되야 한다는 점이다. 비교된 결과는 암호화된 상태로 개인키가 있어야만 그 결과를 알 수 있다.

동형암호의 경우 암호화된 상태에서 생체 정보의 특성의 변형 없이 실제 생체 인증 비교가 수행될 수 있기에, 생체 정보와 키의 결합, 생체 정보의 변형, 생체 정보에 의한 키의 생성 등에서 필연적으로 생길 수밖에 없는 생체 인증 정확도 감소가 발생하지 않는 장점이 있다. 그러나 완전 동형암호의 경우 모든 연산이 가능하여 적용 가능성은 크나 소요되는 메모리와 수행 시간이 현재 컴퓨팅 기술로는 생체 인증에 요구되는 시간을 맞추기 힘들고[51][52], 덧셈 혹은 곱셈 연산에 대한 동형성을 가지는 부분 동형암호를 이용한 생체 인증 기법이 주로 연구되고 있다[52].

V. 프라이버시 보호 방법 간의 장단점 비교

앞 절에서 살펴본 생체정보 인증에서의 개인 프라이버시 정보 침해 방어 기술들의 장단점 및 보안 위협을 비교해보면 표 1과 같다. 본 표의 내용은 향후 프라이버시 보존 생체 인증 방법의 선택 시 고려할 수 있는 사항이라 할 수 있다.

VI. 결 론

본 연구에서는 생체정보 기반 인증을 위한 시스템에서의 개인 프라이버시 정보 침해를 막는 데 필요한 기술들에 대하여 조사하였다. 구체적으로 퍼지 확약, 퍼지 볼트, 퍼지 추출, 폐기형, 동형암호에 의한 방식들의 동작 방식을 살펴보고 그것들 간의 장단점을 비교하였다.

표 1. 프라이버시 보존 생체 인증 기술의 비교
Table 1. Comparison for each privacy preserving technology

Fuzzy Commitment (S) possible to adopt various error correcting code (W) Weak in alignment volatility of biometric information (T) Security is poor when biometric information is not evenly distributed
Fuzzy Vault (S) Strong in alignment volatility of biometric information (T) Possibility of stealing secret key by brute force attack
Fuzzy Extraction (S) Simple system, required storage is small for biometric data (W) Weak renewability (T) Modified biometric information may be used as a personal identification code
Cancelable (S) Strong for revocability and renewability (W) Registration process required to match coordinate system (T) Original biometric information restoration possibility exists from the transformed biometric information
Homomorphic encryption based approach (S) No accuracy loss in biometric matching (W) Require large memory, Low performance

* (S): Strong point, (W): Weak point, (T):Security Threat

기존의 방법들과는 달리, 동형암호 방식은 생체정보 인식 성능 및 생체정보 폐기 및 재발급 가능성에서 우수한 성능을 보이나, 동형암호 자체의 성능적인 문제를 해결해야하는 중요한 문제점을 안고 있다.

생체 인증에 있어 개인정보 보호문제가 해결된다면, 다중 요소 인증등의 다양한 응용 분야에 생체 인증이 활용될 것으로 예상된다[66].

References

[1] R. Hopkins, "An introduction to biometrics and large scale civilian identification", International Review of Law, Computers & Technology, Vol. 13, No. 3, pp. 337-363, Dec. 1999.

[2] D. E. Standard, "Federal information processing standards publication 46", National Bureau of Standards, US Department of Commerce, pp. 31, Sep. 1994.

[3] J. Lynch, "FBI combines civil and criminal fingerprints into one fully searchable database", ELECTRONIC FRONTIER FOUNDATION, Sep. 2015.

[4] Ji Woong Yoon, Ho Kyu Lee, and Chan Mi Choo, "The evolution of the resident registration system in korea", Knowledge Sharing Program, Dec. 2015.

[5] Srinivasa Rajaram, "Biometrics: Technologies and Global Markets", BCC Research, Jan. 2016.

[6] N. Memon, "How biometric authentication poses new challenges to our security and privacy [in the spotlight]", IEEE Signal Process. Mag., Vol. 34, No. 4, pp. 196-194, Jul. 2017.

[7] D. Brown and K. Bradshaw, "Enhanced biometric access control for mobile devices", Sep. 2017.

[8] C. Soutar et al, "Biometric encryption: Enrollment and verification procedures", Optical Pattern Recognition IX, pp. 24-36, Mar. 1998.

[9] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security", EURASIP Journal on Advances in Signal Processing, Vol. 2008, pp. 113, Jan. 2008.

[10] L. Lai, S. Ho, and H. V. Poor, "Privacy–security trade-offs in biometric security systems—Part II: Multiple use case", IEEE Transactions on Information Forensics and Security, Vol. 6, No. 1, pp. 140-151, Mar. 2011.

[11] European Parliament and Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC", European Parliament and Council, Apr. 2016.

[12] Paul Shukovsky, "Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin", Bloomberg Law: Privacy & Data Security, Jul. 2017.

[13] J. Breebaart, B. Yang, I. Buhan-Dulman, and C.

Busch, "Biometric template protection", Datenschutz Und Datensicherheit-DuD, Vol. 33, No. 5, pp. 299-304, Jul. 2009.

[14] I. N. E. Fayrouz, N. Farida, and A. Irshad, "Relation between fingerprints and different blood groups", Journal of Forensic and Legal Medicine, Vol. 19, No. 1, pp. 18-21, Jan. 2012.

[15] K. Wang and J. Luo, "Detecting visually observable disease symptoms from faces", EURASIP Journal on Bioinformatics and Systems Biology, Vol. 2016, No. 1, pp. 13, Aug. 2016.

[16] A. Alruban et al, "Insider misuse attribution using biometrics", Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 42, Aug. 2017.

[17] Taylor Armerding, "The 17 biggest data breaches of the 21st century", Jan. 2018.

[18] Unique Identification Authority of India. Jan. 2018.

[19] The Tribunne, "Rs 500, 10 minutes, and you have access to billion Aadhaar details", The Tribunne, Jan. 2018.

[20] R. Subramanian, "Computer security, privacy, and politics: Current issues, challenges, and solutions", IGI Global, pp. 110, Mar. 2008.

[21] ISO/IEC 24745/2011, "Information Technology - Security Techniques - Biometric Information Protection", ISO/IEC, Aug. 2011.

[22] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 4-20, Jan. 2004.

[23] S. Rane, "Standardization of biometric template protection", IEEE Multimedia, Vol. 21, No. 4, pp. 94-99, Nov. 2014.

[24] A. Juels and M. Wattenberg, "A fuzzy commitment scheme", Proceedings of the 6th ACM Conference on Computer and Communications Security, pp. 28-36, Nov. 1999.

[25] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication", Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, pp. 45-52, Jan. 2003.

[26] B. Fuller, X. Meng, and L. Reyzin, "Computational fuzzy extractors", International Conference on the Theory and Application of Cryptology and Information Security, pp. 174-193, Jun. 2013.

[27] C. Rathgeb and A. Uhl, "Adaptive fuzzy commitment scheme based on iris-code error analysis", Visual Information Processing (EUVIP), 2010 2nd European Workshop on, pp. 41-44, Jul. 2010.

[28] A. B. J. Teoh and J. Kim, "Secure biometric template protection in fuzzy commitment scheme", IEICE Electronics Express, Vol. 4, No. 23, pp. 724-730, Dec. 2007.

[29] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum", Information Forensics and Security (WIFS), 2010 IEEE International Workshop on, pp. 1-6, Dec. 2010.

[30] M. Ao and S. Z. Li, "Near infrared face based biometric key binding", International Conference on Biometrics, pp. 376-385, Jun. 2009.

[31] E. Maiorana, P. Campisi, and A. Neri, "User adaptive fuzzy commitment for signature template protection and renewability", Journal of Electronic Imaging, Vol. 17, No. 1, pp. 011011, Mar. 2008.

[32] A. Juels and M. Sudan, "A fuzzy vault scheme", Des. Codes Cryptogr., Vol. 38, No. 2, pp. 237-257, Feb. 2006.

[33] P. Li et al, "An alignment-free fingerprint cryptosystem based on fuzzy vault scheme", Journal of Network and Computer Applications, Vol. 33, No. 3, pp. 207-220, May 2010.

[34] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors", Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, pp. 1-4, Dec. 2008.

[35] X. Wu et al, "A novel cryptosystem based on

iris key generation", Natural Computation, 2008. ICNC'08. Fourth International Conference on, pp. 53-56, Oct. 2008.

[36] X. Wu, K. Wang, and D. Zhang, "A cryptosystem based on palmprint feature", Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, pp. 1-4, Dec. 2008.

[37] Y. Wu and B. Qiu, "Transforming a pattern identifier into biometric key generators", Multimedia and Expo (ICME), 2010 IEEE International Conference on, pp. 78-82, Jul. 2010.

[38] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data", International conference on the theory and applications of cryptographic techniques, pp. 523-540, May 2004.

[39] R. Canetti et al, "Key derivation from noisy sources with more errors than entropy", IACR Cryptology ePrint Archive, 2014/243, Apr. 2014.

[40] P. Tuyls, A. H. Akkermans, T. A. Kevenaar, G. Schrijen, A. M. Bazen, and R. N. Veldhuis, "Practical biometric authentication with template protection", International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 436-446, Jul. 2005.

[41] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively", IEEE Trans. Comput., Vol. 55, No. 9, pp. 1081-1088, Jul. 2006.

[42] S. Kanad et al, "Three factor scheme for biometric-based cryptographic key regeneration using iris", Biometrics Symposium, 2008. BSYM'08, pp. 59-64, Sep. 2008.

[43] H. Garcia-Baleo et al, "Bimodal biometric system for cryptographic key generation using wavelet transforms", Computer Science (ENC), 2009 Mexican International Conference on, pp. 185-196, Sep. 2009.

[44] M. Van Der Veen et al, "Face biometrics with renewable templates", Security, Steganography, and Watermarking of Multimedia Contents VIII, pp. 60720J, Feb. 2006.

[45] K. Simoens, P. Tuyls, and B. Preneel, "Privacy weaknesses in biometric sketches", Security and Privacy, 2009 30th IEEE Symposium on, pp. 188-203, May 2009.

[46] W. Yang, J. Hu, and S. Wang, "A delaunay triangle-based fuzzy extractor for fingerprint authentication", Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference On, pp. 66-70, Jun. 2012.

[47] Q. Li, M. Guo, and E. Chang, "Fuzzy extractors for asymmetric biometric representations", Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on, pp. 1-6, Jun. 2008.

[48] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Syst J, Vol. 40, no. 3, pp. 614-634, Mar. 2001.

[49] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms", Foundations of Secure Computation, Vol. 4, No. 11, pp. 169-180, 1978.

[50] C. Gentry, "A fully homomorphic encryption scheme", Stanford University, Sep. 2009.

[51] C. Aguilar-Melchor et al, "Recent advances in homomorphic encryption: A possible future for signal processing in the encrypted domain", IEEE Signal Process. Mag., Vol. 30, No. 2, pp. 108-117, Feb. 2013.

[52] M. Gomez-Barrero et al, "Multi-biometric template protection based on homomorphic encryption", Pattern Recognit, Vol. 67, pp. 149-163, Jul. 2017.

[53] Dai-Hwan Lim, "Personal Authentication System Using Multimodal Biometric Algorithm", Journal of KIIT, Vol. 15, No. 12, pp. 147-156, Dec. 2017.

[54] J. H. Cheon, et al, "Ghostshell: Secure biometric authentication using integrity-based homomorphic evaluations", IACR Cryptology ePrint Archive,

2016/484, May 2016.

[55] N. K. Ratha et al, "Generating cancelable fingerprint templates", IEEE Trans. Pattern Anal. Mach. Intell., Vol. 29, No. 4, pp. 561-572, Jan. 2007.

[56] E. R. Henry, "Classification and uses of finger prints", HM Stationery Office, 1905.

[57] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: Two factor authentication featuring fingerprint data and tokenised random number", Pattern Recognit, Vol. 37, No. 11, pp. 2245-2255, Nov. 2004.

[58] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis", Computer Vision and Pattern Recognition, CVPR'07. IEEE Conference on, pp. 1-8, Jun. 2007.

[59] B. Yang et al, "Dynamic random projection for biometric template protection", Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on, pp. 1-7, Sep. 2010.

[60] P. Das, K. Karthik, and B. C. Garai, "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs", Pattern Recognit, Vol. 45, No. 9, pp. 3373-3388, Sep. 2012.

[61] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution", Pattern Recognit, Vol. 47, No. 3, pp. 1321-1329, Mar. 2014.

[62] J. K. Pillai et al, "Secure and robust iris recognition using random projections and sparse representations", IEEE Trans. Pattern Anal. Mach. Intell., Vol. 33, No. 9, pp. 1877-1893, Sep. 2011.

[63] A. B. Teoh, A. Goh, and D. C. Ngo, "Random multispace quantization as an analytic mechanism for biohashing of biometric and random identity inputs", IEEE Trans. Pattern Anal. Mach. Intell., Vol. 28, No. 12, pp. 1892-1901, Dec. 2006.

[64] L. Leng and J. Zhang, "Palmhash code vs. palmphasor code", Neurocomputing, Vol. 108, pp. 1-12, May 2013.

[65] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review", IEEE Signal Process. Mag., Vol. 32, No. 5, pp. 54-65, Sep. 2015.

[66] Dai-Hwan Lim, "Personal Authentication System Using Multimodal Biometric Algorithm", Journal of KIIT, Vol. 15, No. 12, pp. 147-156, Dec. 2017.

저자소개

박 희 진 (Heejin Park)

2002년 2월 : 연세대학교 컴퓨터공학과 (석사)
2013년 2월: KAIST EMBA (석사)
2014년 3월 ~ 현재 : 서울과학기술대학교 IT 정책전문대학원 산업정보시스템 전공 박사과정
관심분야 : 데이터마이닝, 보안

이 윤 호 (Younho Lee)

2006년 8월 : KAIST 전산학과 박사
2007년 10월 ~ 2009년 2월 : GeorgiaTech GTISC 박사후과정
2013년 9월 ~ 현재 : 서울과학기술대학교 ITM전공 부교수
관심분야 : 응용암호, 데이터보안