한국지능시스템학회 논문지 2010, Vol. 20, No. 5, pp. 610-616

# 개인식별정보와 바이오인식정보의 안전한 결합방법

# Secure Binding of Identity Reference and Biometric Reference

유미경* · 권만준** · 이상호* · 전명근***+

Mi Kyeong You*, Man-Jun Kwon**, Sang Ho Lee*** and Myung Geun Chun***+

* 충북대학교 전자정보대학 컴퓨터공학부

** 아주자동차대학 자동차계열

*** 충북대학교 전자정보대학 전자공학부

**요 약**

본 논문에서는 바이오인식 시스템에 있어서, 바이오인식 정보와 개인식별 정보가 분리되어 운영되는 상황에서 이들이 결합되어야 할 때, 이들이 보안조건을 만족하도록 안전하게 결합 될 수 있는 방안에 대해서 다룬다. 패스워드를 이용한 개인인증과 같은 단순한 개인인증 방법의 단점으로 지적되어온 타인에 의한 도용 등의 단점을 극복하고자, 개인마다 타고난 신체적·행동적 특성을 이용하는 바이오인식시스템은 바이오인식 정보자체가 또 다른 개인정보의 하나이며, 더욱이 이들 정보가 개인을 식별할 수 있는 다른 정보들과 결합하여 사용될 경우, 특정개인을 식별할 수 있는 유일식별자로 사용될 수 있기 때문에 결합단계에서 안정적인 방법이 요구되고 있다. 이에 본 연구에서는 이와 관련하여 바이오인식 정보와 개인식별 정보를 보관하는 데이터베이스의 분리운영 환경에서 이들을 공통으로 가리킬 수 있는 공통 식별자의 생성과 운영방안 그리고 각각의 데이터베이스의 무결성을 점검하는 방법을 안전한 채널과 불안전한 채널의 경우로 나누어서 각각의 운영 방안을 제시하였다.

**키워드 :** 바이오 인식, 개인식별정보, 정보보호, 프라이버시

**Abstract**

This paper describes how to securely bind the identity reference and biometric reference for satisfying security requirements. To overcome the shortcomings of the simple personal authentication method using a password, such as identify theft, a biometric system that utilizes physical and behavioral characteristics of each person has been adopted. In the biometric system, the biometric information itself is personal information, and it can be used as an unique identifier that can identify a particular it vidual when combining with other identity information. As a result, a son, anb it canmethod is required for manipulat canthese information. Consider canthese issues, this paper proposes a biit canmethod uiter son, anand uisecure channels for generating the common identifier and ensuring security of identity reference and biometric reference that are stored in the separated DBs.

**Key Words** : Biometrics, Personal Identifiable Information, Information Security, Privacy

## 1. 서 론

바이오인식기술은 인터넷 뱅킹, 금융서비스, 인터넷을 통한 비대면 거래에 있어서 중요한 정보보호 기법의 하나로 이용되고 있으며, 테러 용의자, 범죄자 등의 접근을 차단하는 최첨단 감시시스템으로서도 주목받고 있다. 개인마다 타고난 신체적·행동적 특성을 이용한 바이오정보의 불변성은 인증시스템의 성능을 극대화하는 긍정적 측면을 가지고 있는 반면에 이러한 바이오 정보가 분실되거나 다른 사람에 의해서 도용되었을 경우에 비밀번호나 식별번호처럼 사용자가 원하는 경우에 쉽게 변경하기가 어렵다는 단점을 지니고 있다. 이런 이유로 바이오인식정보의 유출에 따른 프라이버시 논의와 더불어 바이오인식 정보를 데이터베이스화하거나 온라인상에서 바이오인식 정보의 사용을 꺼려하고 있는 추세다[1].

바이오인식 정보를 위한 연구 동향을 살펴보면 바이오인식정보를 은닉하여 불법 사용자가 은닉된 정보에 접근하지 못하도록 하는 워터마킹에 대한 연구들이 진행되고 있다. Jain 등[2]은 지문 영상에 얼굴정보를 삽입할 수 있는 지문영상 워터마킹기법을 제시하여 얼굴의 특징인 고유 얼굴을 지문 영상에 워터마크로써 삽입한 후, 복원된 얼굴 영상은 얼굴 확인에 이용될 수 있음을 제안하였다. 국내에서는 웨이블렛을 이용하여 워터마크 삽입위치를 결정하고 배경영상의 특성을 고려한 적응적 가중치 설정방법에 의해 워터마크를 효과적으로 은닉하고. 필요에 따라 효과적으로 바이오인식특징을 추출하여 커버이미지에 대해서도 높은 인식률을 갖는 디지털 워터 마킹 기법이 제시되었다[3].

또다른 기술적 기법으로는 변환 가능한 바이오 템플릿

접수일자 : 2010년 8월 2일
완료일자 : 2010년 10월 4일
본 연구는 지식경제부의 지원을 받는 정보통신표준기술력향상사업의 연구결과로 수행되었음
＋ : 교신저자

(changeable biometric template) 혹은, 취소 가능한 바이오 템플릿(cancellable biometric template) 기법이다[4][5]. 상기의 기법에서는 원래의 바이오 영상에 임의의 변형을 가해서 바이오인식 템플릿을 추출함으로서 설령 이렇게 만들어진 템플릿이 유출되더라도 원래의 영상에 새로운 변형을 가함으로서 기존의 템플릿을 폐기하고 새로운 템플릿을 발행할 수 있다는데 장점이 있다.

한편으로 바이오인식 시스템의 운영에 있어서 개인식별정보와 바이오인식 템플릿이 공격당할 수 있는 위협 요소와 공격의 예를 살펴보고 프라이버시 보호를 위한 바이오인식 템플릿의 운영에 대한 연구가 있었다[6]. 바이오 정보의 보호의 사회적 필요성에 부응하여 한국인터넷진흥원에서는 '바이오정보보호 가이드라인을 제정하여 시행하여 오고 있다. 이에 따르면 제13조(보호조치)의 1항에서 "운영자는 바이오정보 및 바이오인식시스템을 보호하기 위하여 필요한 기술적.관리적 보호조치를 취하여야 하며, 보호 조치의 구체적인 사항은 <별표>와 같다"라고 기술하고 있다[7]. 저장에 관하여 좀 더 구체적으로는 "바이오정보 보관시 바이오정보와 제공자를 알 수 있는 정보를 분리"하여 저장하도록 권고하고 있다. 현재 표준화 추진 중인 [8]의 부록에서는 두 개의 데이터베이스의 분리 운영을 위하여 안전한 채널과 불안전한 채널의 경우로 나누어서 각각의 프로토콜을 제시하였다. 그러나 공통식별자를 생성하기 위해서 MAC(Message Authentication Code) 기법이 요구되며, MAC 구현을 위해서는 두 개의 데이터베이스간에 공동암호키를 추가로 필요로 하는 등의 요구사항이 있다.

이에 본 연구에서는 바이오인식 정보와 개인식별 정보를 보관하는 데이터베이스의 분리운영 환경에서 이들을 공통으로 가리킬 수 있는 공통 식별자의 생성과 운영방안을 데이터베이스 관리시스템에서 널리 쓰이는 외부키의 개념과 해싱함수와 암호기법을 이용하여 각각의 데이터베이스의 무결성을 점검하는 방법을 제시함으로서 기존의 데이터베이스에 추가적으로 쉽게 구현할 수 있도록 하는데 초점을 두었다.

## 2. 바이오인식 시스템과 개인식별정보

바이오인식 시스템은 개인의 신체적 또는 행위적 특징에 기반한 개인식별방법의 일종이라고 할 수 있다. 인터넷 환경과 같이 비대면의 개인인증 환경에서 인증대상자가 제시한 개인의 신체정보나 서명과 같은 동적 특성의 특징정보를 제시함으로서 사전에 등록단계에서 미리 저장시켜 놓은 정보와의 비교를 통하여 확인 받고자 하는 개인의 신분을 확인 하는 역할을 수행한다. 이러한 생체인식시스템의 구성도를 최근에 제출된 국제표준기구(ISO)의 표준화 문서에 따라 나타낸 것이 그림 1이다. 특히, 그림 1은 기존의 [9]에서 제시된 바이오인식 시스템의 구성도를 확대하여 개인식별정보(Identity Reference)의 흐름을 좀 더 명확하게 표기한 것이다.

상기의 그림에서 볼 수 있듯이 바이오인식 시스템은 크게 3가지의 역할로 나누어서 생각해 볼 수 있다. 첫 번째로 등록(enrollment)과정이다. 이 기능은 제시되는 대상자의 바이오정보로부터 개인식별(identification)과정이나 개인인증(verification)과정에서 필요로 하는 바이오인식정보(Biometric reference)를 생성하고 저장하는 과정을 의미한다. 개인식별과정은 주어진 바이오인식정보에 대해서 이것이 누구의 것인지 신원을 밝히는데 목적이 있다. 이때 바이오인식시스템은 저장장치내의 모든 바이오인식정보와의 비교를 통하여 가장 유사도가 높은 대상자의 식별정보를 제공하게 된다. 한편, 개인인증과정은 대상자가 본인의 바이오인식정보와 함께 개인식별정보(Identity Reference)를 제시하게 되는데, 이는 주어진 바이오인식정보에 대해서 이것이 주장하고 있는 본인이 맞는지의 여부를 판별하는데 사용된다. 이때 바이오인식시스템은 저장장치내의 해당 식별정보의 바이오인식정보와의 비교를 통하여 대상자의 인증여부를 결정하게 된다.

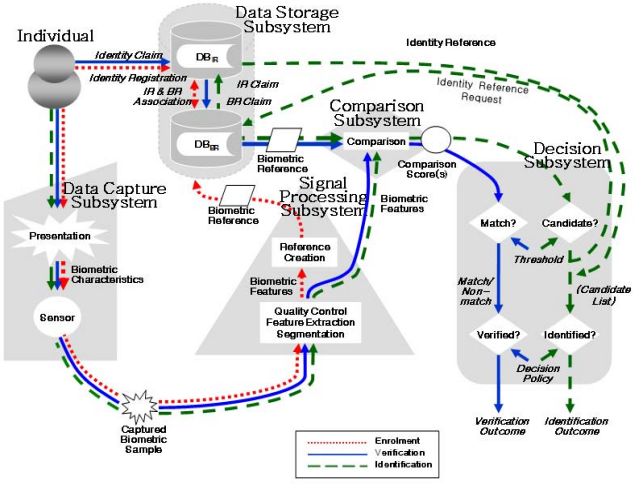



그림 1. 바이오인식 시스템의 구성도
Fig. 1. Biometric System Diagram

### 2.1 바이오인식 시스템의 구성

그림 1에 나타낸 바와 같이 바이오 인식 시스템은 크게 다섯 개의 부분으로 이루어져 있다. 각각의 역할은 다음과 같다.

- **데이터취득부(Data Capture)**: 대상자의 바이오인식 특징을 수집할 수 있는 입력장치를 포함한다. 입력 장치의 예로는 카메라, 지문 스캐너, 좌표를 입력받기 위한 입력 판, 마이크로폰 등이 있다. 바이오인식시스템이 대상자를 올바르게 인식하기 위해서는 추출되는 바이오 인식정보가 저장되어 있는 대상자의 바이오인식템플릿과 일치해야 한다.

- **신호처리부(Signal Processing)**: 데이터취득부로부터 얻어진 바이오인식데이터를 받아서 비교부가 요구하는 형태의 데이터로 변환하여 주는 역할을 한다.

- **데이터저장부(Data Storage)**: 등록된 사용자의 바이오인식 템플릿을 저장하며 등록된 템플릿의 추가, 삭제 그리고 복구 기능을 제공할 수도 있다. 데이터저장부는 단일 대상자를 위한 단일 바이오인식정보만을 저장할 수도 있고, 많은 사용자를 대상으로 수천 개의 바이오인식정보들을 저장할 수도 있다. 예를 들면, 대규모 바이오인식정보 저장을 위한 컴퓨터 시스템 내의 데이터베이스, 스마트 카드와 같은 휴대 가능한 토큰, 바이오인식용 디바이스내의 저장소 등이 있다.

기본적으로 저장소에 저장된 데이터는 사용자의 템플릿과 사용자의 개인식별정보(Identity reference)를 포함하고 있다. 이러한 개인식별정보는 개인확인(Identification)이나 개인인증(verification)시에 주어지는 바이오인식 템플릿과의 비교 결과에 따라 같이 주어지게 된다.

- **비교부(Matching):** 신호처리부에서 처리된 대상자의 바이오인식 특징값과 데이터저장부에 저장 되어 있는 바이오인식정보를 비교하는 역할을 한다. 여기서 주로 사용되는 방법은 거리척도 등을 이용하여 특징값과 바이오인식정보 간의 거리척도 등을 이용하여 두개의 값이 얼마나 정확하게 일치하는가를 나타내는 수치 값을 계산한다.

- **결정부(Decision):** 비교부로부터 스코어를 받고, 시스템 결정 정책에 입각하여 대상자를 식별 또는 인증하게 된다. 검증과정을 위한 시스템이라면 미리 설정된 임계값과 계산된 스코어를 이용하여 대상자의 인증 결과를 "예(match)" 또는 "아니오(nonmatch)"의 이진 값으로 출력한다. 그러나 식별과정에 사용된 시스템이라면 스코어가 높은 순으로 몇 개의 후보군을 그들의 개인식별정보와 함께 출력하게 된다.

### 2.2 바이오인식정보와 개인식별정보

바이오인식 시스템에서의 바이오인식 정보를 설명하기 위하여 먼저 설명되어야할 것이 바이오인식 템플릿이다. 국제 표준(ISO)에 따르면 바이오인식정보는 다음과 같이 정의된다[8].

- **바이오인식 정보(biometric reference):** 비교를 위해 개인식별 대상자에 대해서 추출한 속성으로 하나 또는 다수의 저장된 바이오인식 샘플, 바이오인식 템플릿, 바이오인식 모델 등을 의미한다.

위의 정의에 따르자면, 얼굴이나 지문 영상과 같은 바이오인식 샘플 뿐만 아니라, 이들로부터 추출된 고유얼굴(eigenface)에 대한 계수값이나 지문인식에 있어서 미뉴셔(minutiae)의 위치와 각도값과 같은 특징값이 저장된 형태의 바이오인식 템플릿을 포함한다. 뿐만 아니라 음성인식시스템에 있어서 화자의 발음으로부터 추출된 가우시언 혼합모델(Gaussian Mixture Model) 도 여기에 포함된다.

한편, 한 개인의 신원을 나타내는 식별자(identity)는 그 사람이 신원 en하기를 바라는 상황에서 대상자와 관련된 모든 속성이라 개할 수 있으며, 따라서 한사람에 대해서 다수의 식별자가 제시될 수도 인의

이런 관점에서 넓게 보면 바이오인식 정보(Biometric reference)도 개인 식별정보(Identity Reference)의 일종으로 볼 수 있다. 그러나 통상 바이오 인식 시스템에서는 개인식별정보를 바이오인식 정보와 분리하여 생각하는데[8], 본 논문에서도 이와 같은 관점으로 바이오인식 정보와 개인식별 정보를 분리하여 기술하고자 한다. 그림 2는 앞서 설명된 바이오인식 정보와 개인식별정보의 구체적인 예를 보여 주고 있다.

개인식별 정보는 어떠한 형태가 되었든 그 정보를 소유하고 있는 사람을 식별할 수 있는 정보라고 볼 수 있다. 바이오 인식정보가 홀로 존재하는 경우, 특정 개인을 판별하는 정보로 사용하기가 용이하지 않다. 그러나 이러한 바이오인식 정보가 개인식별 정보와 결합되었을 경우에는 매우 민감한 개인정보로 간주할 수 있다. 예를 들어 지문의 특징점 정보만이 유출된 경우에는 그것이 누구인지 판별하기가 거의 불가능하나, 그와 관련된 이름, 전화 번호, 주민번호, 계좌번호가 결합된 채로 유출된 경우에는 쉽게 바이오인식 정보에 대한 소유주가 누구인지 알 수 있고 이는 다른 바이오인식 시스템을 이용하는 시스템에 오용되어 질 수 있기 때문이다.

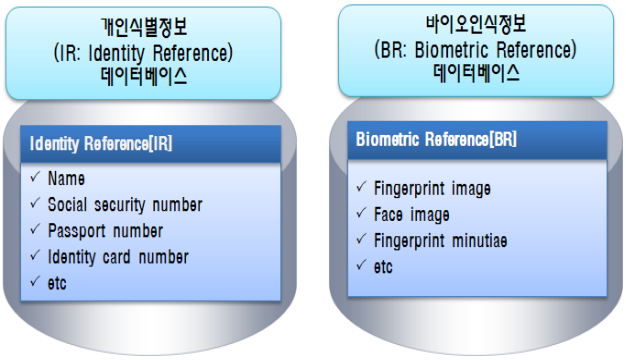



그림 2. 바이오인식 정보와 개인식별정보
Fig. 2. Biometric Reference and Identity Reference

## 3. 개인식별정보와 바이오인식정보의 안전한 결합 방법

개인식별정보와 바이오인식정보 DB를 논리적이나 물리적으로 분리하여 운영하는 것은 바람직하나, 필요에 따라서는 두 개의 식별정보를 공통으로 지칭할 수 있는 공통 식별자(Common Identifier)가 필요하다. 이러한 상황에서 다음과 같은 보안 요구사항을 만족해야 한다[8].

- CI 자체만으로는 바이오인식 정보나 개인식별 정보를 추출할 수 없어야한다.
- 만약 두 개 중 하나의 DB가 침해되고 내용들이 불법적으로 수정되어 무결성에 문제가 생겼다면, DB 운영자들은이러한 사실을 감지 할 수 있어야 한다.
- DB의 운영 중에 적절한 비밀키를 가지고 있는 운영자에 의해 DB 내용이 수정되더라도 다른쪽 DB의 운영자가 이 사실을 감지할 수 있어야 한다.

그림 1에 나타낸 바이오인식 시스템에서 개인식별 정보(IR)와 바이오인식정보(BR)로 분리된 데이터베이스를 가정하여 IR과 BR의 안전한 결합을 위한 방안을 제시하고자 한다. 이때, 개인식별정보를 위한 데이터베이스는 $DB_{IR}$로, 바이오정보에 대한 데이터베이스는 $DB_{BR}$로 표기 한다.

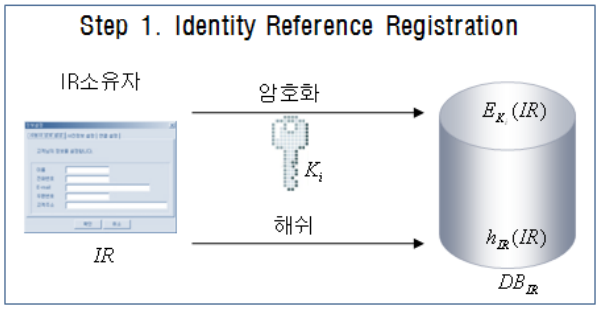
앞서 제시된 보안요구사항을 만족하기 위하여 다음과 같은 보안시스템을 가정한다.

- $DB_{IR}$은 비밀키 $K_i$를 사용하고 $DB_{BR}$은 비밀키 $K_b$를 사용한다. 또한 두 개의 데이터베이스는 불안전한 채널에서의 전송 메시지 보호를 위해서 비밀키 $K_e$를 공유한다.

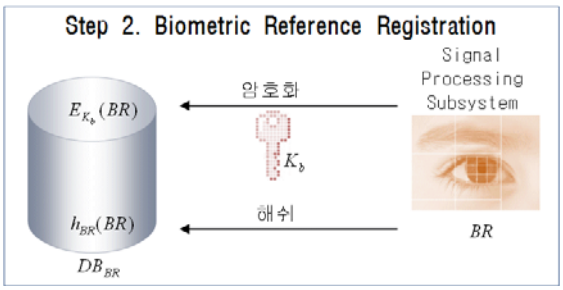
### 3.1 바이오인식정보와 개인식별정보 분리운영-등록 과정

(1) $DB_{IR}$과 $DB_{BR}$ 사이에 안전한 통신 채널이 있는 경우

Step 1) $DB_{IR}$은 IR 소유자로부터 IR을 받고, $E_{Ki}(IR)$을 얻기 위해 $K_i$를 이용하여 IR을 암호화하고, IR을 해싱하여 $h_{IR}(IR)$을 얻는다.



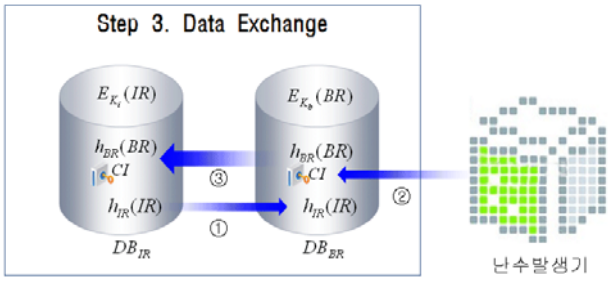

Step 2) $DB_{BR}$은 신호처리부로 부터 대응하는 BR을 받고, $E_{Kb}(BR)$을 얻기 위해 $K_b$를 이용하여 BR을 암호화하고, BR을 해싱하여 $h_{BR}(BR)$을 얻는다.



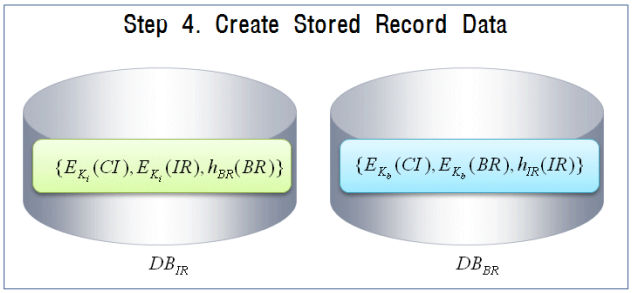

Step 3-1) $DB_{IR}$은 $h_{IR}(IR)$을 $DB_{BR}$로 보내고, $DB_{BR}$은 이를 받아 저장한다.

Step 3-2) $DB_{BR}$은 난수발생기에 의해서 미리 정해진 길이만큼의 난수 CI를 얻어서 기존에 사용하고 있는, CI와의 충돌 여부를 확인 후, 충돌하면 재발행하고, 충돌되지 않으면 이를 데이터베이스 해당 레코드의 외부키(Foreign Key)[10]로 사용하며, 이는 공통 식별자의 역할을 한다. 이때 기밀성을 위해서 CI는 $K_b$를 이용하여 암호화 한다.

Step 3-3) $DB_{BR}$은 h(BR)과 CI를 $DB_{IR}$로 보낸다.

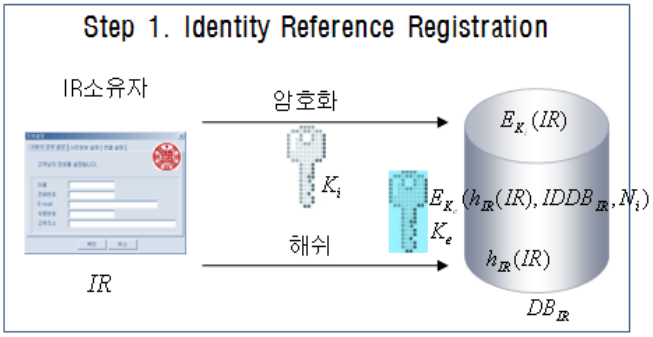



Step 4) $DB_{BR}$은 $\{E_{Kb}(CI), E_{Kb}(BR), h_{IR}(IR)\}$을 저장하고, $DB_{IR}$은 $DB_{BR}$로 부터 CI와 $h_{BR}(BR)$을 받아서 $\{E_{Ki}(CI), E_{Ki}(IR), h_{BR}(BR)\}$을 저장한다.

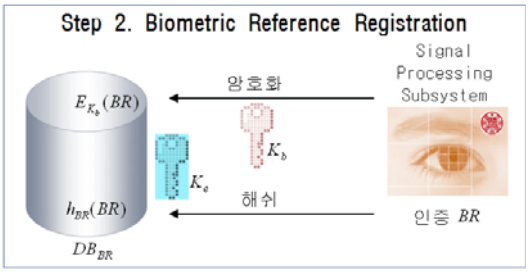



(2) $DB_{IR}$과 $DB_{BR}$ 사이에 불안전한 통신 채널이 있고 공유 비밀키 Ke를 갖는 경우

Step 1) $DB_{IR}$은 IR 소유자로부터 인증 IR을 받고, $E_{Ki}(IR)$을 얻기 위해서 $K_i$를 이용하여 IR을 암호화하고, $h_{IR}(IR)$을 얻기 위해 IR을 해싱하며, 그리고 $E_{Ke}(h(IR), IDDB_{IR}, N_i)$를 얻기 위해서 $K_e$를 이용하여 $\{h_{IR}(IR), IDDB_{IR}, N_i\}$를 암호화한다. 여기서 $IDDB_{IR}$는 $DB_{IR}$을 위한 유일한 식별자이며 $N_i$는 $DB_{IR}$에 의해 생성된 임시적인 비표(time stamp 또는 sequence number)이다[11].



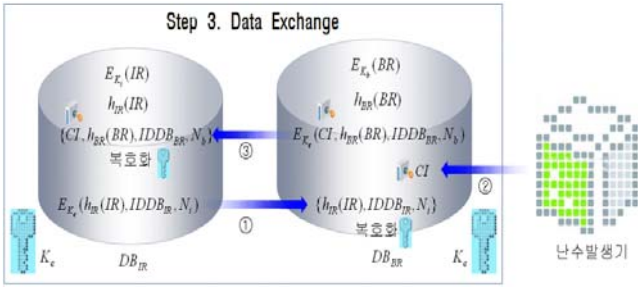

Step 2) $DB_{BR}$은 신호처리부로부터 대응하는 인증 BR을 받고, $K_b$를 이용하며 BR을 암호화하여 $E_{Kb}(BR)$을 얻고, BR을 해싱하여 $h_{BR}(BR)$을 얻는다.



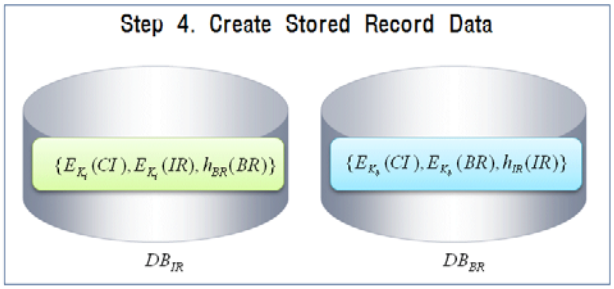

Step 3-1) $DB_{IR}$은 $E_{Ke}(h_{IR}(IR), IDDB_{IR}, N_i)$를 $DB_{BR}$로 보내고, $DB_{BR}$은 $DB_{IR}$로부터 $E_{Ke}(h_{IR}(IR), IDDB_{IR}, N_i)$을 받아 $\{(h_{IR}(IR), IDDB_{IR}, N_i\}$을 복호화하고, $IDDB_{IR}$과 $N_i$를 검증한다(만약 실패하면, 에러 메시지와 함께 멈춘다). 성공시에 $h_{IR}(IR)$를 저장한다.

Step 3-2) $DB_{BR}$은 난수발생기에 의해서 미리 정해진 길이 만큼의 난수 CI를 얻어서 기존에 사용하고 있는, CI와의 충돌 여부를 확인 후, 충돌하면 재발행하고, 충돌되지 않으면 이를 데이터베이스 해당 레코드의 외부키(Foreign Key)[10]로 사용하며, 이는 공통 식별자의 역할을 한다. 이때 기밀성을 위해서 CI는 $K_b$를 이용하여 암호화 한다.

Step 3-3) 공통 암호화키 $K_e$를 이용하여 $E_{Ke}$(CI, $h_{BR}$(BR), $IDDB_{BR}$, Nb)로 암호화하여 $DB_{IR}$로 보낸다. $DB_{IR}$은 $DB_{BR}$로부터 $E_{Ke}$(CI, $h_{BR}$(BR), $IDDB_{BR}$, Nb)를 받아 {CI, $h_{BR}$(BR), $IDDB_{BR}$, Nb}로 복호화하고, $IDDB_{BR}$과 Nb를 검증한다(만약 실패하면, 에러메시지와 함께 멈춘다).




Step 4) $DB_{BR}$은 {$E_{Kb}$(CI), $E_{Kb}$(BR),$h_{IR}$(IR)}을 저장하고, $DB_{IR}$에서는 검증이 성공하면 {$E_{Ki}$(CI), $E_{Ki}$(IR), $h_{BR}$(BR)}을 저장한다.

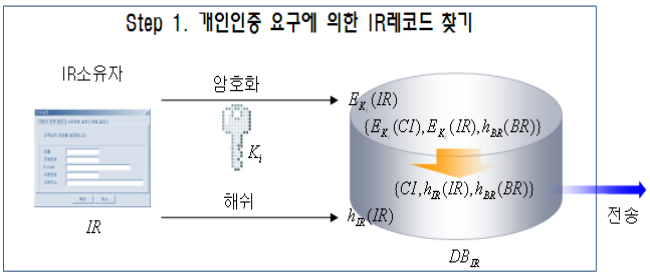



### 3.2 바이오인증을 위한 바이오정보 요구과정

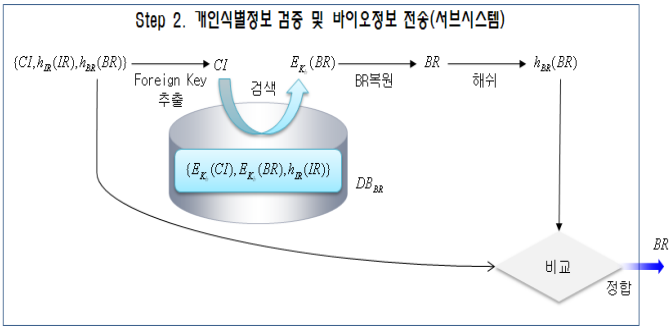
위에서 설명된 방법을 이용하여 바이오인증을 위해서 $DB_{IR}$에서 $DB_{BR}$까지의 BR 요구에 대한 절차는 다음과 같다.

(1) $DB_{IR}$과 $DB_{BR}$ 사이에 안전한 통신 채널이 있는 경우

Step 1) IR 소유자로부터 적법한 개인인증 요구를 받으면, $DB_{IR}$은 IR에 해당되는 데이터레코드를 찾아서 IR을 해싱한 $h_{IR}$(IR)과 함께 {CI, $h_{IR}$(IR),$h_{IR}$(BR)}을 $DB_{BR}$로 보낸다.



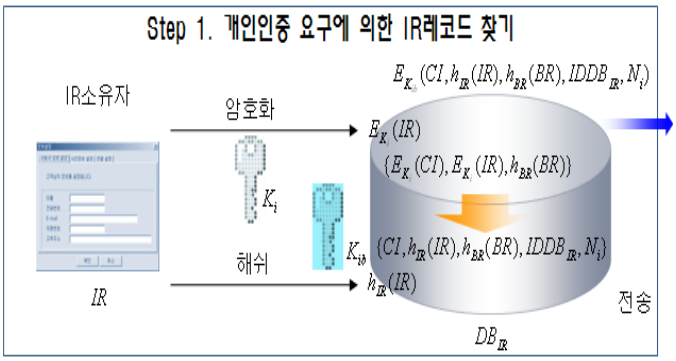

Step 2) $DB_{BR}$은 $DB_{IR}$로부터 {CI, $h_{IR}$(IR),$h_{IR}$(BR)}을 받고, CI를 이용하여 $E_{Kb}$(BR)을 찾아 복호화하여 $h_{BR}$(BR)을 구하여 수신된 $h_{IR}$(BR)과 비교한다. 또한, 수신된 $h_{IR}$(IR)과 저장되어져 있는 $h_{BR}$(IR)을 비교한다.




Step 3) 만약 이것들이 정합하면, $DB_{BR}$은 비교부로 안전하게 BR을 보낸다. 그렇지 않으면, 에러메시지와 함께 멈춘다.

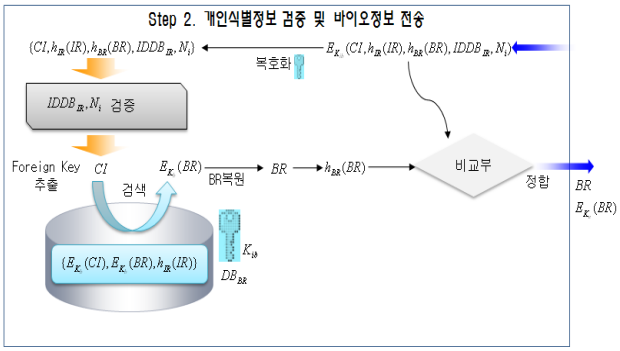
(2) $DB_{IR}$과 $DB_{BR}$ 사이에 불안전한 통신 채널이 있고 공유 비밀키 Ke를 갖는 경우

Step 1) IR 소유자로부터 적법한 개인인증 요구를 받으면, $DB_{IR}$은 IR에 해당되는 데이터레코드를 찾아서 IR을 해싱한 $h_{IR}$(IR)과 함께 {CI, $h_{IR}$(IR), $h_{IR}$(BR), $IDDB_{IR}$, $N_i$}를 암호화하여 $E_{Ke}$(CI, $h_{IR}$(IR), $h_{IR}$(BR), $IDDB_{IR}$, $N_i$)를 $DB_{BR}$로 보낸다.




Step 2) $DB_{BR}$은 $DB_{IR}$로부터 $E_{Ke}$(CI, $h_{IR}$(IR), $h_{IR}$(BR), $IDDB_{IR}$, $N_i$)를 받고, {CI, $h_{IR}$(IR), $h_{IR}$(BR), $IDDB_{IR}$, $N_i$}를 복구하기 위해서 복호화하며, $IDDB_{IR}$과 $N_i$를 검증하고(만약 실패하면 에러메

시지와 함께 멈춘다), CI를 이용하여 $E_{Kb}(BR)$을 찾고, BR을 얻기 위해서 $E_{Kb}(BR)$을 복호화하고, BR을 해싱하여 $h_{BR}(BR)$을 얻은 후 $h_{IR}(BR)$과 비교한다. 또한, 수신된 $h_{IR}(IR)$과 저장되어져 있는 $h_{BR}(IR)$을 비교한다.

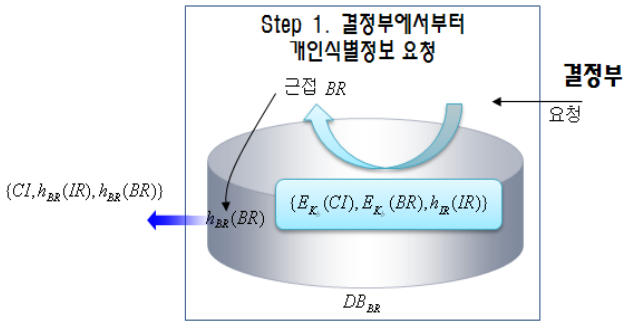



Step 3) 만약 그것들이 정합하면, 비교부로 안전하게 BR을 보낸다. 그렇지 않으면, 에러메시지와 함께 멈춘다.

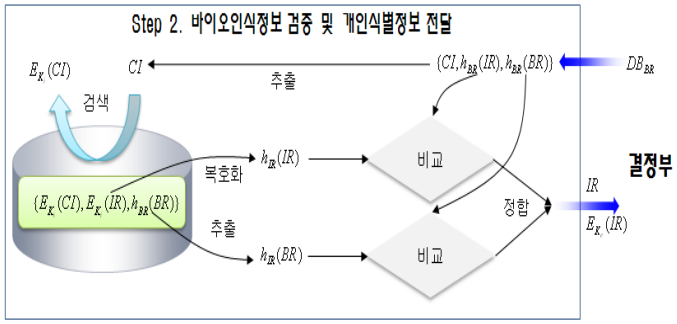
### 3.3 바이오인식에서 개인식별정보 요구과정

(1) $DB_{IR}$과 $DB_{BR}$ 사이에 안전한 통신 채널이 있는 경우 바이오인식 정보를 이용하여 $DB_{BR}$에서 $DB_{IR}$로부터 IR을 요구하는 절차를 설명하면 다음과 같다.

Step 1) $DB_{BR}$은 바이오 인식 시스템의 의사결정 부시스템에서부터, 해당되는 개인식별정보 IR의 요청을 받으면, 입력된 바이오정보와 가장 근사값을 갖는 BR값을 $DB_{BR}$로부터 추출하여, 해싱함으로 $h_{BR}(BR)$을 얻은 후 {CI, $h_{BR}(IR)$, $h_{BR}(BR)$}을 $DB_{IR}$로 보낸다.



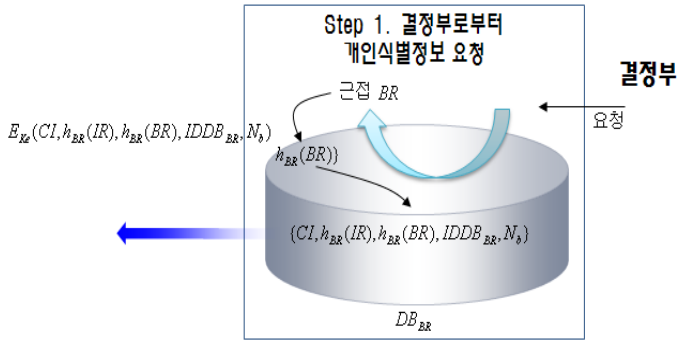

Step 2) $DB_{IR}$은 $DB_{BR}$로부터 {CI, $h_{BR}(IR)$, $h_{BR}(BR)$}을 받고, CI를 이용하여 $E_{Ki}(IR)$을 찾아 복호화하여 $h_{IR}(IR)$을 구하여 수신된 $h_{BR}(IR)$과 비교한다. 또한, 수신된 $h_{BR}(BR)$과 저장되어져 있는 $h_{IR}(BR)$을 비교한다.



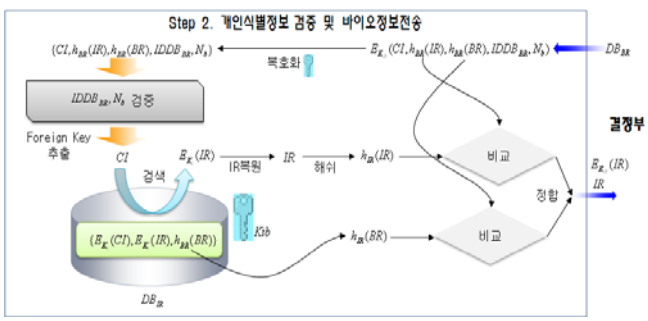

Step 3) 만약 이것들이 정합하면, $DB_{IR}$은 비교부시스템에게 안전하게 IR을 보낸다. 그렇지 않으면, 에러메시지와 함께 멈춘다.

(2) $DB_{IR}$과 $DB_{BR}$ 사이에 불안전한 통신 채널이 있고 공유비밀키 Ke를 갖는 경우

Step 1) $DB_{BR}$은 바이오 인식 시스템의 의사결정 부시스템에서부터, 해당되는 개인식별정보 IR의 요청을 받으면, 입력된 바이오정보와 가장 근사값을 갖는 BR값을 $DB_{BR}$로부터 추출하여, 해싱함으로 $h_{BR}(BR)$을 얻은 후, {CI, $h_{BR}(IR)$, $h_{BR}(BR)$, $IDDB_{BR}$, $N_b$}를 암호화하여 $E_{Kib}$(CI, $h_{BR}(IR)$, $h_{BR}(BR)$, $IDDB_{BR}$, $N_b$)를 $DB_{IR}$로 보낸다.




Step 2) $DB_{IR}$은 $DB_{BR}$로부터 $E_{Kib}$(CI, $h_{BR}(IR)$, $h_{BR}(BR)$, $IDDB_{BR}$, $N_b$)를 받고, (CI, $h_{BR}(IR)$, $h_{BR}(BR)$, $IDDB_{BR}$, $N_b$)를 복구하기 위해서 복호화하며, $IDDB_{BR}$과 $N_b$를 검증하고(만약 실패하면 에러메시지와 함께 멈춘다), CI를 이용하여 $E_{Ki}(IR)$을 찾아 복호화 하여 IR을 얻고 이를 해싱하여 $h_{IR}(IR)$을 얻은 후 수신된 $h_{BR}(IR)$과 비교한다. 또한, 수신된 $h_{BR}(BR)$과 저장되어져 있는 $h_{IR}(BR)$을 비교한다.



Step 3) 만약 그것들이 정합하면, $DB_{IR}$은 비교 부시스템으로 안전하게 IR을 보낸다. 그렇지 않으면, 에러메시지와 함께 멈춘다.

## 4. 결 론

바이오인식 기술은 개인의 생태학적 또는 행위적 특징을 이용하는데, 이들은 개인의 프라이버시를 침해 할 수 있는 민감한 개인정보로 분류 될 수 있기에 이에 대한 보호의 필요성이 어느 때보다도 높게 요구되고 있다. 더욱이 바이오인식사용자는 이러한 민감한 바이오인식 정보가 개인을 식별할 수 있는 주민등록 번호, 여권번호, 전화번호 등과 같이 결합되어 저장되거나 전송 될 때 이들에 대한 안전을 위하여 강도 높은 보안기법을 요구하고 있다.

이에 본 연구에서는 바이오인식 정보와 개인식별 정보의 안전한 결합을 위한 방법을 두 개로 분리된 DB의 운영 상황에서 안전한 채널과 불안전한 채널로 나누어서 제안하였다. 현재 분리 운영되고 있지 않는 데이터베이스에 대해서, 기존의 암호화기법과 해싱기법을 추가하여 구현할 수 있는 구조이므로, 운영 중인 바이오인식 시스템의 보안 및 프라이버시 강화기법으로 적용될 수 있으리라 기대된다.

## 참 고 문 헌


[1] Arun Ross, Jidnya Shah, Anil K. Jain, "From template to image: Reconstucting fingerprints from minutiae points", *IEEE Tr. on Pattern Analysis and Machine Intelligence*, Vol. 29, No.4, 2007

[2] Anil K. Jain, Umut Uludag, "Hiding biometric data," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 25, No. 11, pp. 1494-1498, 2003.

[3] 이욱재, 이대종, 문기영, 전명근, "웨이블렛을 이용한 생체정보의 강인한 워터마킹 알고리즘", *한국퍼지 및 지능시스템학회* Vol. 17, No.5 pp.632-639, 2007.

[4] Jongsun Kim, Chulhan Lee, Jaihie Kim, " A changeable biometric system that uses parts-based localized representation for face recognition" *IEEE Workshop on Automatic identification advanced technologies*, pp.165-168, 2007.

[5] 전명근, 재발급 가능한 바이오인식 정보를 이용한 개인정보 보호 방안, *최종 연구보고서*, 한국인터넷진흥원, 2009.

[6] 신용녀, 이용준, 전명근, "개인정보보호를 위한 바이오인식 템플릿 보안" *한국지능시스템학회 논문지* Vol. 18, No. 4 pp.437-444, 2008.

[7] 한국인터넷진흥원, 바이오정보보호 가이드라인, 2007.

[8] ISO/IEC JTC 1 SC27 - Information technology-Security techniques FCD Biometric information protection.

[9] 신용녀, 권만준, 이용준, 박진일, 전명근, "개인식별정보와 바이오인식정보의 보호기법", *한국지능시스템학회 논문지* Vol. 19 No. 2, pp.160-167, 2009.

[10] J.D.Ullman, J. Widom, *A first course in database systems*, 3rd Edition, Prentice Hall, 2008.

[11] W. Stallings, *Cryptography and network security: Principles and practices*, 5th edition, Prentice Hall, 2010.


## 저 자 소 개


**유미경(Mi Kyeong You)**
충북대학교 대학원 컴퓨터과학과 석박사 통합과정

**권만준(Man-Jun Kwon)**
2009년 제19권 2호 참조

**이상호(Sang Ho Lee)**
충북대학교 전자정보대학 컴퓨터공학부 교수

**전명근(Myung Geun Chun)**
2010년 제20권 3호 참조