(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0041088
(43) 공개일자 2012년04월30일

(51) 국제특허분류(Int. Cl.)
G06F 21/00 (2006.01) *G06F 17/00* (2006.01)
G06K 9/20 (2006.01)
(21) 출원번호 10-2010-0118619
(22) 출원일자 2010년11월26일
심사청구일자 2010년11월26일
(30) 우선권주장
1020100102287 2010년10월20일 대한민국(KR)

(71) 출원인
한국인터넷진흥원
서울특별시 송파구 중대로 135 (가락동)
(72) 발명자
전명근
충청북도 청주시 흥덕구 1순환로 776, 전자전기컴퓨터공학부 (개신동, 충북대학교)
이혜원
서울특별시 송파구 중대로 109, 대동빌딩 12층 (가락동)
(뒷면에 계속)
(74) 대리인
특허법인다인

전체 청구항 수 : 총 21 항

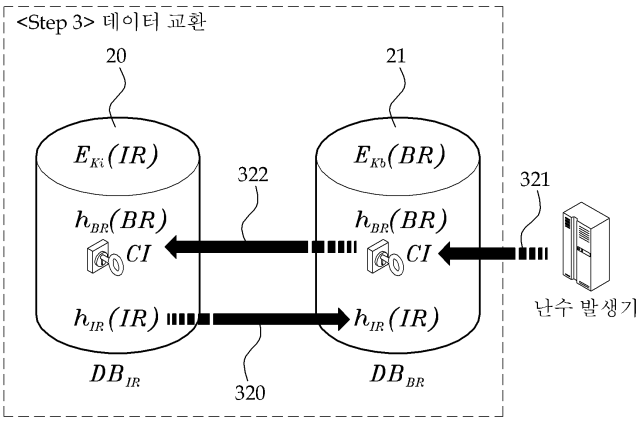
(54) 발명의 명칭 **데이터베이스 분리운영 환경에서의 개인식별정보와 바이오인식정보의 안전한 결합 및 무결성 보장 방법**

(57) 요 약

본 발명은 데이터베이스 분리운영 환경에서의 개인식별정보와 바이오인식정보의 안전한 결합 및 무결성 보장 방법에 관한 것으로서, 바이오인식정보와 개인식별정보를 분리하여 저장/관리하는 데이터베이스 분리운영 환경에서 공통 식별자를 이용하여 바이오인식정보와 개인식별정보를 안전하게 결합하고, 암호화 기법과 해싱 기법을 통하여 데이터베이스의 무결성을 보장함으로써, 바이오인식 시스템의 보안 및 프라이버시를 강화하고자 한다.

이를 위하여, 본 발명은, 데이터베이스 분리운영 환경에서 개인식별정보와 바이오인식정보를 결합하는 방법에 있어서, 개인식별정보 데이터베이스가 개인식별정보에 대한 해쉬값을 생성하는 단계; 바이오인식정보 데이터베이스가 상기 개인식별정보에 대응하는 바이오인식정보에 대한 해쉬값을 생성하는 단계; 상기 데이터베이스 간에 각기 생성한 해쉬값을 상호 교환하는 단계; 및 상기 데이터베이스 각각이, 교환을 통해 획득한 해쉬값, 공통 식별자, 및 해당 식별정보를 저장하는 단계를 포함하는 것을 특징으로 한다.

대 표 도 - 도3c



(72) 발명자

이용준

경기도 김포시 전원로 28, 전원마을 101동 803호 (장기동)

정현철

서울특별시 송파구 중대로 109, 대동빌딩 12층 (가락동)

이재일

서울특별시 송파구 중대로 109, 대동빌딩 12층 (가락동)

이 발명을 지원한 국가연구개발사업

과제고유번호	2010-P1-30
부처명	지식경제부
연구사업명	정보통신표준기술력향상사업
연구과제명	차세대 바이오인식 응용기술 표준개발
주관기관	한국인터넷진흥원
연구기간	2010.01.01 ~ 2010.12.31

특허청구의 범위

청구항 1

데이터베이스 분리운영 환경에서 개인식별정보와 바이오인식정보를 결합하는 방법에 있어서,

개인식별정보 데이터베이스가 개인식별정보에 대한 해쉬값을 생성하는 단계;

바이오인식정보 데이터베이스가 상기 개인식별정보에 대응하는 바이오인식정보에 대한 해쉬값을 생성하는 단계;

상기 데이터베이스 간에 각기 생성한 해쉬값을 상호 교환하는 단계; 및

상기 데이터베이스 각각이, 교환을 통해 획득한 해쉬값, 공통 식별자, 및 해당 식별정보를 저장하는 단계

를 포함하는 개인식별정보 및 바이오인식정보의 안전한 결합 방법.

청구항 2

제 1 항에 있어서,

상기 공통 식별자는,

난수를 이용하여 설정되는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 안전한 결합 방법.

청구항 3

제 2 항에 있어서,

상기 공통 식별자는,

상기 바이오인식정보 데이터베이스가 난수 발생기로부터 획득한 난수를 이용해 설정하여 상기 개인식별정보 데이터베이스에 전송하는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 안전한 결합 방법.

청구항 4

제 2 항에 있어서,

상기 공통 식별자는,

상기 개인식별정보 데이터베이스 및 상기 바이오인식정보 데이터베이스 각각에서 해당 비밀키로 암호화되어 저장되는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 안전한 결합 방법.

청구항 5

제 1 항 내지 제 4 항 중 어느 한 항에 있어서,

상기 해쉬값 교환 단계는,

상기 데이터베이스 간의 통신채널이 불안정한 경우, 상기 데이터베이스 각각은 각기 생성한 해쉬값을 공유비밀키를 이용해 암호화하여 상호 교환하는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 안전한 결합 방법.

청구항 6

제 5 항에 있어서,

상기 데이터베이스 각각이 해쉬값을 상호 교환하는 경우, 해당 데이터베이스 식별자 및 임시 비표를 상기 공유 비밀키를 이용해 암호화하여 상대방 데이터베이스에 추가 전송하는 단계

더 포함하는 개인식별정보 및 바이오인식정보의 안전한 결합 방법.

청구항 7

제 6 항에 있어서,

상기 데이터베이스 각각이 상대방 데이터베이스로부터 수신한 데이터베이스 식별자 및 임시 비표를 검증하여 성공하면 수신한 해쉬값을 복호화하여 저장하는 단계

를 더 포함하는 개인식별정보 및 바이오인식정보의 안전한 결합 방법.

청구항 8

데이터베이스 분리운영 환경에서 개인식별정보 및 바이오인식정보의 무결성을 보장하는 방법에 있어서,

개인인증 요청에 따라 개인식별정보 데이터베이스가 해당 개인식별정보를 검색해 해쉬값을 생성하여, 해당 공통 식별자 및 바이오인식정보 해쉬값과 함께 바이오인식정보 데이터베이스에 전송하는 전송 단계;

상기 바이오인식정보 데이터베이스가 수신된 공통 식별자를 이용해 해당 바이오인식정보와 개인식별정보 해쉬값을 검색한 후, 상기 검색된 바이오인식정보에 대한 해쉬값을 생성하는 검증준비 단계; 및

상기 바이오인식정보 데이터베이스가 상기 검증준비 단계에서 검색/생성된 해쉬값과 상기 개인식별정보 데이터베이스로부터 수신한 해쉬값을 비교하여 무결성 검증을 수행하는 검증 단계

를 포함하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 9

제 8 항에 있어서,

상기 검증 단계는,

상기 검증준비 단계에서 생성된 바이오인식정보 해쉬값과 상기 개인식별정보 데이터베이스로부터 수신된 바이오인식정보 해쉬값을 비교하는 단계; 및

상기 검증준비 단계에서 검색된 개인식별정보 해쉬값과 상기 개인식별정보 데이터베이스로부터 수신된 개인식별정보 해쉬값을 비교하는 단계

를 포함하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 10

제 9 항에 있어서,

상기 무결성 검증이 성공하면, 상기 바이오인식정보 데이터베이스가 상기 검색된 해당 바이오인식정보를 외부에 전송하는 단계

를 더 포함하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 11

제 10 항에 있어서,

상기 개인식별정보 데이터베이스가 개인식별정보 소유자로부터 상기 개인인증 요청을 수신함에 따라, 상기 바이오인식정보 데이터베이스가 무결성이 검증된 해당 바이오인식정보를 바이오인식 시스템의 비교부에 전송하는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 12

제 8 항 내지 제 11 항 중 어느 한 항에 있어서,

상기 전송 단계는,

상기 데이터베이스 간의 통신채널이 불안정한 경우, 전송 대상이 되는 해쉬값과 공통 식별자를 공유비밀키를 이용해 암호화하여 전송하는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 13

제 12 항에 있어서,

상기 전송 단계는,

해당 데이터베이스 식별자 및 임시 비표를 상기 공유비밀키를 이용해 암호화하여 추가 전송하는 과정을 더 수행하는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 14

제 13 항에 있어서,

상기 검증준비 단계를 수행하기 전에, 상기 바이오인식정보 데이터베이스가 상기 개인식별정보 데이터베이스로부터 수신한 데이터베이스 식별자 및 임시 비표를 복호화하여 검증하는 단계

를 더 포함하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 15

데이터베이스 분리운영 환경에서 개인식별정보 및 바이오인식정보의 무결성을 보장하는 방법에 있어서,

개인식별정보 요청에 따라 바이오인식정보 데이터베이스가 해당 바이오인식정보를 검색해 해쉬값을 생성하여, 해당 공통 식별자 및 개인식별정보 해쉬값과 함께 개인식별정보 데이터베이스에 전송하는 전송 단계;

상기 개인식별정보 데이터베이스가 수신된 공통 식별자를 이용해 해당 개인식별정보 및 바이오인식정보 해쉬값을 검색한 후, 상기 검색된 개인식별정보에 대한 해쉬값을 생성하는 검증준비 단계; 및

상기 개인식별정보 데이터베이스가 상기 검증준비 단계에서 검색/생성된 해쉬값과 상기 바이오인식정보 데이터베이스로부터 수신한 해쉬값을 비교하여 무결성 검증을 수행하는 검증 단계

를 포함하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 16

제 15 항에 있어서,

상기 검증 단계는,

상기 검증준비 단계에서 생성된 개인식별정보 해쉬값과 상기 바이오인식정보 데이터베이스로부터 수신된 개인식

별정보 해쉬값을 비교하는 단계; 및

상기 검증준비 단계에서 검색된 바이오인식정보 해쉬값과 상기 바이오인식정보 데이터베이스로부터 수신된 바이오인식정보 해쉬값을 비교하는 단계

를 포함하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 17

제 16 항에 있어서,

상기 무결성 검증이 성공하면, 상기 개인식별정보 데이터베이스가 상기 검색된 해당 개인식별정보를 외부에 전송하는 단계

를 더 포함하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 18

제 17 항에 있어서

상기 바이오인식정보 데이터베이스가 바이오인식 시스템의 결정부로부터 상기 개인식별정보 요청을 수신함에 따라, 상기 개인식별정보 데이터베이스가 무결성이 검증된 해당 개인식별정보를 상기 결정부에 전송하는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 19

제 15 항 내지 제 18 항 중 어느 한 항에 있어서,

상기 전송 단계는,

상기 데이터베이스 간의 통신채널이 불안정한 경우, 전송 대상이 되는 해쉬값과 공통 식별자를 공유비밀키를 이용해 암호화하여 전송하는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 20

제 19 항에 있어서,

상기 전송 단계는,

해당 데이터베이스 식별자 및 임시 비표를 상기 공유비밀키를 이용해 암호화하여 추가 전송하는 과정을 더 수행하는 것을 특징으로 하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

청구항 21

제 20 항에 있어서,

상기 검증준비 단계를 수행하기 전에, 상기 개인식별정보 데이터베이스가 상기 바이오인식정보 데이터베이스로부터 수신한 데이터베이스 식별자 및 임시 비표를 복호화하여 검증하는 단계

를 더 포함하는 개인식별정보 및 바이오인식정보의 무결성 보장 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 데이터베이스 분리운영 환경에서의 개인식별정보 및 바이오인식정보의 저장/관리에 관한 것으로, 더욱 상세하게는 바이오인식정보와 개인식별정보를 분리하여 저장/관리하는 데이터베이스 분리운영 환경에서 공통식별자를 이용하여 바이오인식정보와 개인식별정보를 안전하게 결합하고, 암호화 및 해싱(Hashing) 기법을 통하여 데이터베이스의 무결성을 보장함으로써, 바이오인식 시스템의 보안 및 프라이버시를 강화할 수 있는, 데이터베이스 분리운영 환경에서의 개인식별정보와 바이오인식정보의 안전한 결합 및 무결성 보장 방법에 관한 것이다.

[0002] 본 발명은 지식경제부의 정보통신표준기술력향상사업의 일환으로 수행한 연구로부터 도출된 것이다[과제관리번호: 2010-P1-30, 과제명: 차세데 바이오 인식 응용기술 표준개발].

배 경 기 술

[0003] 바이오인식 기술은 인터넷 뱅킹, 금융서비스, 인터넷을 통한 비대면 거래 등에 있어서 중요한 정보보호 기법의 하나로 이용되고 있으며, 테러 용의자, 범죄자 등의 접근을 차단하는 최첨단 감시시스템에서도 이용되고 있다.

[0004] 개인마다 타고난 신체적(생태학적)/행동적 특징을 이용한 바이오인식정보의 불변성은 인증시스템의 성능을 극대화하는 긍정적 측면을 가지고 있는 반면에, 이러한 바이오인식정보가 분실되거나 다른 사람에 의해서 도용되었을 경우에는 비밀번호나 식별번호와 달리, 사용자의 의사에 따라 변경하는 것이 어렵다는 문제점을 지니고 있다.

[0005] 이러한 이유로 인하여, 바이오인식정보의 유출에 따른 프라이버시(Privacy) 논의와 더불어 바이오인식정보를 데이터베이스화하거나 온라인상에서의 바이오인식정보의 사용을 기피하는 경향이 있다.

[0006] 종래의 바이오인식정보 기술 및 그 연구 동향을 살펴보면, 바이오인식정보를 은닉함으로써 불법 사용자로 하여금 그 은닉된 바이오인식정보에 접근하지 못하게 하는 "워터마킹(Watermarking)"에 대한 다양한 연구들이 진행되고 있다.

[0007] 첫째, 지문 영상에 얼굴정보를 삽입할 수 있는 지문 영상 워터마킹기법이 있는데, 이는 얼굴의 특징인 고유 얼굴을 지문 영상에 워터마크로써 삽입하고, 그 복원된 얼굴 영상을 해당 사용자의 얼굴 확인에 이용하는 기법이다.

[0008] 둘째, 웨이블렛(Wavelet)을 이용한 워터마킹 기법이 있는데, 이는 웨이블렛을 이용하여 워터마크 삽입 위치를 결정하고 배경 영상의 특성을 고려한 적응적 가중치 설정방법에 의해 워터마크를 효과적으로 은닉한 후, 필요에 따라 효과적으로 바이오인식특징을 추출하여 디지털 워터마킹 기법으로서, 커버 이미지(Cover Image)에 대해서도 높은 인식률을 갖는다.

[0009] 셋째, 변환 가능한 바이오 템플릿(Changeable Biometric Template) 또는 취소 가능한 바이오 템플릿(Cancellable Biometric Template) 기법이 있는데, 이는 원래의 바이오 영상에 임의의 변형을 가하여 바이오인식 템플릿을 추출(생성)함으로써 설령 이렇게 추출(생성)된 템플릿이 유출되더라도 원래의 영상에 새로운 변형을 가함으로써 기존의 템플릿을 폐기하고 새로운 템플릿을 발행할 수 있는 장점이 있다.

[0010] 다음은, 바이오인식 시스템의 운영에 있어서 개인식별정보와 바이오인식 템플릿이 공격당할 수 있는 위협 요소와 공격의 예를 살펴보고, 프라이버시 보호를 위한 바이오인식 템플릿의 운영에 대한 종래 기법을 설명하기로 한다.

[0011] 바이오정보(바이오인식정보) 보호의 사회적 필요성에 부응하여 한국인터넷진흥원에서는 '바이오정보보호 가이드라인'을 제정하여 시행하고 있는데, 이에 따르면 제13조(보호조치)의 제1항에서 “*운영자는 바이오정보 및 바이오인식시스템을 보호하기 위하여 필요한 기술적.관리적 보호조치를 취하여야 하며, 보호 조치의 구체적인 사항은 <별표>와 같다*” 라고 기술하고 있다. 그리고, 정보 저장에 관해서는, "바이오정보 보관시 바이오정보와 제공자를 알 수 있는 정보를 분리"하여 저장하도록 권고하고 있다.

[0012] 또한, 이와 관련하여, 두 개의 데이터베이스의 분리 운영을 위하여 안전한 채널과 불안전한 채널의 경우로 나누어서 각각의 프로토콜을 제시하고 있는데, 이는 공통식별자를 생성하기 위해서 메시지 인증 코드(MAC: Message Authentication Code) 기법이 요구되고, MAC 구현을 위해서는 두 개의 데이터베이스 간에 공동암호키를 사용하

여야 한다는 요구 사항이 있다.

[0013] 요컨대, 패스워드(Password)를 이용한 개인인증과 같은 단순한 개인인증 방법의 단점으로 지적되어온 타인에 의한 도용 등의 문제점을 극복하고자, 개인마다 타고난 신체적/행동적 특성을 이용하는 바이오인식 시스템이 등장하였으며, 이에 사용되는 바이오인식정보 또한 개인정보의 일종으로, 개인의 프라이버시와 관련된 민감한 개인정보에 해당하는 바, 이에 대한 보호가 절실히 요구되고 있다. 특히, 바이오인식정보가 개인을 식별할 수 있는 다른 정보(예를 들어, 주민등록 번호, 여권번호, 전화번호 등)와 결합하여 저장/전송/사용될 경우, 특정 개인을 식별할 수 있는 유일 식별자로 사용될 수 있기 때문에 이들의 안전을 위하여 강도 높은 보안기법이 요구된다.

발명의 내용

해결하려는 과제

[0014] 따라서 본 발명은 바이오인식정보와 개인식별정보를 서로 분리된 데이터베이스를 통하여 저장/관리함에 있어서 두 정보를 안전하게 결합하고 각 데이터베이스의 무결성을 보장할 수 있는, 데이터베이스 분리운영 환경에서의 개인식별정보와 바이오인식정보의 안전한 결합 및 무결성 보장 방법을 제공하는데 그 목적이 있다.

[0015] 본 발명의 목적들은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있으며, 본 발명의 실시예에 의해 보다 분명하게 알게 될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

과제의 해결 수단

[0016] 본 발명은 상기와 같은 목적을 달성하기 위하여, 바이오인식정보와 개인식별정보를 분리하여 저장/관리하는 데이터베이스 분리운영 환경에서, 공통 식별자를 이용하여 바이오인식정보와 개인식별정보를 안전하게 결합하고, 암호화 및 해싱 기법을 이용하여 데이터베이스의 무결성을 보장하는 것을 특징으로 한다.

[0017] 더욱 구체적으로, 본 발명은, 데이터베이스 분리운영 환경에서 개인식별정보와 바이오인식정보를 결합하는 방법에 있어서, 개인식별정보 데이터베이스가 개인식별정보에 대한 해쉬값을 생성하는 단계; 바이오인식정보 데이터베이스가 상기 개인식별정보에 대응하는 바이오인식정보에 대한 해쉬값을 생성하는 단계; 상기 데이터베이스 간에 각기 생성한 해쉬값을 상호 교환하는 단계; 및 상기 데이터베이스 각각이, 교환을 통해 획득한 해쉬값, 공통 식별자, 및 해당 식별정보를 저장하는 단계를 포함한다.

[0018] 또한, 본 발명은, 데이터베이스 분리운영 환경에서 개인식별정보 및 바이오인식정보의 무결성을 보장하는 방법에 있어서, 개인인증 요청에 따라 개인식별정보 데이터베이스가 해당 개인식별정보를 검색해 해쉬값을 생성하여, 해당 공통 식별자 및 바이오인식정보 해쉬값과 함께 바이오인식정보 데이터베이스에 전송하는 전송 단계; 상기 바이오인식정보 데이터베이스가 수신된 공통 식별자를 이용해 해당 바이오인식정보와 개인식별정보 해쉬값을 검색한 후, 상기 검색된 바이오인식정보에 대한 해쉬값을 생성하는 검증준비 단계; 및 상기 바이오인식정보 데이터베이스가 상기 검증준비 단계에서 검색/생성된 해쉬값과 상기 개인식별정보 데이터베이스로부터 수신한 해쉬값을 비교하여 무결성 검증을 수행하는 검증 단계를 포함한다.

[0019] 또한, 본 발명은, 데이터베이스 분리운영 환경에서 개인식별정보 및 바이오인식정보의 무결성을 보장하는 방법에 있어서, 개인식별정보 요청에 따라 바이오인식정보 데이터베이스가 해당 바이오인식정보를 검색해 해쉬값을 생성하여, 해당 공통 식별자 및 개인식별정보 해쉬값과 함께 개인식별정보 데이터베이스에 전송하는 전송 단계; 상기 개인식별정보 데이터베이스가 수신된 공통 식별자를 이용해 해당 개인식별정보 및 바이오인식정보 해쉬값을 검색한 후, 상기 검색된 개인식별정보에 대한 해쉬값을 생성하는 검증준비 단계; 및 상기 개인식별정보 데이터베이스가 상기 검증준비 단계에서 검색/생성된 해쉬값과 상기 바이오인식정보 데이터베이스로부터 수신한 해쉬값을 비교하여 무결성 검증을 수행하는 검증 단계를 포함한다.

발명의 효과

[0020] 상기와 같은 발명은, 데이터베이스 분리운영 환경에서 공통 식별자(CI : Common Identifier)를 이용하여 바이오인식정보와 개인식별정보를 안전하게 결합하고, 암호화 기법과 해싱 기법을 통하여 데이터베이스의 무결성을 보장함으로써, 바이오인식 시스템의 보안과 개인의 프라이버시 보호를 증대시킬 수 있는 효과가 있다.

[0021] 또한, 본 발명은 개인식별정보 및 바이오인식정보를 데이터베이스에 등록하거나 인증을 위하여 데이터베이스 간에 정보를 전송함에 있어서 통신채널의 안전성 여부에 따라 서로 다른 절차를 수행하되, 특히 데이터베이스 간의 통신채널이 불안정한 경우 공유비밀키를 이용한 암호화 과정과 별도의 검증 과정을 추가로 수행함으로써, 개인의 프라이버시와 관련된 중요 정보에 대한 보안을 강화하는 효과가 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명이 적용되는 바이오인식 시스템의 구성예시도,

도 2는 본 발명에 적용되는 개인식별정보 및 바이오인식정보에 대한 개념 설명도,

도 3a 내지 도 3d 및 도 4a 내지 도 4d는 본 발명에 따른 데이터베이스 분리운영 환경에서의 개인식별정보 및 바이오인식정보의 안전한 결합 방법에 대한 일실시예 흐름도,

도 5a, 도 5b, 도 6a, 및 도 6b는 본 발명에 따른 데이터베이스 분리운영 환경에서의 개인 인증(Verification)을 위한 데이터베이스 무결성 보장 방법에 대한 일실시예 흐름도,

도 7a, 도 7b, 도 8a 및 도 8b는 본 발명에 따른 데이터베이스 분리운영 환경에서의 개인 식별(Identification)을 위한 데이터베이스 무결성 보장 방법에 대한 일실시예 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 상술한 목적, 특징 및 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 또한, 본 발명을 설명함에 있어서 본 발명과 관련된 공지 기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에 그 상세한 설명을 생략하기로 한다. 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명하기로 한다.

[0024] 도 1은 본 발명이 적용되는 바이오인식 시스템의 구성도이다.

[0025] 바이오인식 시스템(Biometric System)(11)은 개인(10)의 신체적 또는 행위적 특징에 기반하여 해당 개인을 식별하는 기법에 대한 것이다. 즉, 바이오인식 시스템(11)은 인터넷 환경과 같이 비대면의 개인인증 환경에서 인증대상자가 개인의 신체정보나 서명과 같은 동적 특성 등의 특징정보를 제시하면, 등록단계에서 미리 저장해 놓은 특징 정보와의 비교를 통하여 확인대상이 되는 개인의 신분을 확인하는 역할을 수행한다.

[0026] 도 1은 국제표준기구(ISO)의 표준화 문서를 기반으로 한 생체인식 시스템(바이오인식 시스템)(11)에 대한 예시도로서, 본 발명에 따른 데이터베이스 분리운영 환경과 개인식별정보(Identity Reference) 흐름을 명확하게 나타낸 것이다.

[0027] 이러한 바이오인식 시스템(11)은 일반적으로 등록(Enrollment) 과정, 개별인식(Identification) 과정, 및 개인인증(Verification) 과정을 수행한다.

[0028] 첫째, 등록 과정은 제시되는 대상자(10)의 바이오인식정보로부터 개인식별 과정이나 개인인증 과정에서 필요로 하는 바이오인식정보(Biometric Reference)를 생성하고 저장하는 과정을 나타내는 것으로, 본 발명에서는 공통식별자를 이용하여 두 정보를 결합하는 바, 이하 더 넓은 의미를 갖는 "결합 과정" 또는 "결합 방법"을 사용하기로 한다.

[0029] 둘째, 개인식별 과정은 주어진 바이오인식정보에 대해서 "이것이 누구의 것인지" 신원을 밝히기 위한 과정이다. 이때, 바이오인식 시스템(11)은 데이터 저장부(113) 내의 모든 바이오인식정보와의 비교를 통하여 가장 유사도가 높은 대상자의 식별정보를 제공한다.

[0030] 셋째, 개인인증 과정은 대상자(10)가 본인의 바이오인식정보와 함께 개인식별정보(Identity Reference)를 제시

하는 경우, 그 제시된 바이오인식정보에 대해서 "이것이 주장하고 있는 본인이 맞는지 여부"를 판별하는 과정이다. 이때 바이오인식 시스템(11)은 데이터 저장부(113) 내의 해당 개인식별정보의 바이오인식정보와의 비교를 통하여 대상자(10)의 인증 여부를 결정한다.

[0031] 도 1에 도시된 바와 같은 바이오인식 시스템(11)은 데이터 취득부(111), 신호처리부(112), 데이터 저장부(113), 비교부(114), 및 결정부(115)를 포함하여 이루어진다. 각각의 구성요소의 기본적인 동작은 공지 기술에 해당하는 바, 이하 간단히 설명하기로 한다.

[0032] 데이터 취득부(Data Capture Subsystem)(111)는 대상자(10)의 바이오인식 특징을 수집할 수 있는 입력 장치를 포함한다. 여기서, 입력 장치의 예로는 카메라, 지문 스캐너, 좌표를 입력받기 위한 입력 판, 마이크로폰 등이 있다. 바이오인식 시스템(11)이 대상자(10)를 올바르게 인식하기 위해서는 추출되는 바이오인식정보가 저장되어 있는 대상자의 바이오인식 템플릿과 일치해야 한다.

[0033] 신호처리부(Signal Processing Subsystem)(112)는 데이터 취득부(111)로부터 획득된 바이오인식 데이터를 받아서 비교부(114)가 요구하는 형태의 데이터로 변환하여 준다.

[0034] 데이터 저장부(Data Storage Subsystem)(113)는 등록된 사용자의 바이오인식 템플릿을 저장하며 등록된 템플릿의 추가, 삭제, 및 복구 기능을 제공할 수도 있다. 또한, 데이터 저장부(113)는 단일 대상자를 위한 단일 바이오인식정보만을 저장할 수도 있고, 다수의 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 디바이스 내의 저장소 등이 있다. 기본적으로, 저장소에 저장된 데이터는 사용자의 템플릿과 사용자의 개인식별정보(Identity Reference)를 포함하고 있는데, 이러한 개인식별정보는 개인 식별(개인확인)(Identification)이나 개인 인증(Verification)시에 주어지는 바이오인식 템플릿과의 비교 결과에 따라 함께 주어지게 된다.

[0035] 본 발명과 관련하여 데이터 저장부(113)는 데이터베이스 시스템의 일종으로, 논리적 또는 물리적으로 구분된 개인식별정보(IR) 데이터베이스와 바이오인식정보 데이터베이스를 포함하여 이루어지며, 특히 본 발명에 따라 데이터베이스 분리운영 환경에서 개인식별정보와 바이오인식정보를 안전하게 결합하고 데이터베이스의 무결성을 보장한다. 이에 대해서는 도 2 내지 도 8d에서 상세히 설명하기로 한다.

[0036] 비교부(Matching Subsystem)(114)는 신호처리부(113)에서 처리된 대상자의 바이오인식 특징값과 데이터 저장부(113)에 저장되어 있는 바이오인식정보를 비교하는 역할을 수행한다. 여기서, 주로 사용되는 비교 방식은 신호처리부(112)에서 처리된 특징값과 데이터 저장부(113)에 저장된 바이오인식정보 간의 거리척도 등을 이용하여 두 개의 값이 얼마나 정확하게 일치하는가를 나타내는 수치 값(Score)을 계산하는 과정을 포함한다.

[0037] 결정부(Decision Subsystem)(115)는 비교부(114)로부터 스코어(Score)를 받고, 시스템 결정 정책에 기초하여 대상자를 식별 또는 인증한다. 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.

[0038] 도 2는 본 발명에 적용되는 개인식별정보 및 바이오인식정보에 대한 개념 설명도로서, 개인식별정보 데이터베이스(DB)(20)와 바이오인식정보 데이터베이스(BD) (21)로 분리 운용되는 환경에서 각각의 데이터베이스에 저장되는 정보를 나타낸다.

[0039] 바이오인식 시스템(11)에서의 바이오인식정보(BR: Biometric Reference)를 국제 표준(ISO)에 따라 정의하면, 이는 비교를 위해 개인식별 대상자에 대해서 추출한 속성으로서, 하나 또는 다수의 저장된 바이오인식 샘플, 바이오인식 템플릿, 바이오인식 모델 등을 의미한다.

[0040] 위의 정의에 따르면, 얼굴이나 지문 영상과 같은 바이오인식 샘플뿐만 아니라, 이들로부터 추출된 고유얼굴(Eigenface)에 대한 계수값이나 지문인식에 있어서의 특징점(Minutiae)의 위치/각도값과 같은 특징값이 저장된 형태의 바이오인식 템플릿을 포함한다. 또한, 음성인식 시스템에 있어서 화자의 발음으로부터 추출된 가우시언 혼합모델(Gaussian Mixture Model)도 바이오인식정보에 포함된다.

[0041] 한편, "개인식별정보"의 개념에 대하여 살펴보면, 한 개인의 신원을 나타내는 식별자(Identity)는 그 사람이 신원 확인하기를 바라는 상황에서 대상자와 관련된 모든 속성이라고 할 수 있으며, 따라서 한 사람에 대해서 다수

의 식별자가 제시될 수도 있다.

[0042] 이런 관점에서 보면, 위에서 설명한 바이오인식정보(BR)도 개인식별정보(Identity Reference)의 일종으로 볼 수 있다. 그러나, 통상적으로 바이오인식 시스템(11)에서는 개인식별정보(IR)를 바이오인식정보(BR)와 분리하여 생각하는 바, 본 발명과 관련해서는 바이오인식정보(BR)와 개인식별정보(IR)를 분리하여 취급하기로 한다. 하지만, 경우에 따라 단순히 "식별정보"라 하면, 이 둘을 지칭하는 것으로 한다.

[0043] 도 2는 위에서 설명된 바이오인식정보(BR)와 개인식별정보(IR)의 구체적인 예를 나타낸다. 즉, 개인식별정보(IR)에는 성명(Name), 사회보장번호(Social Security Number), 여권번호(Passport Number), 신분증 번호(Identity Card Number) 등에 포함되며, 필요에 따라 간략히 "IR"로 표기하기로 한다. 그리고, 바이오인식정보(BR)에는 지문 이미지(Fingerprint Image), 얼굴 이미지(Face Image), 지문 특징점(Fingerprint Minutiae) 등이 포함되며, 필요에 따라 간략히 "BR"로 표기하기로 한다.

[0044] 개인식별정보(IR)는 어떠한 형태가 되었든 그 정보를 소유하고 있는 사람(정보 소유주)을 식별할 수 있는 정보라고 볼 수 있다. 바이오인식정보(BR)가 단독으로 존재하는 경우, 특정 개인을 판별하는 정보로 사용하는 것은 용이하지 않다. 그러나, 이러한 바이오인식정보(BR)가 개인식별정보(IR)와 "결합"할 경우에는 매우 민감한 개인정보로 간주할 수 있다. 예를 들어, 지문의 특징점 정보만이 유출된 경우에는 그것이 누구인지 판별하기가 불가능하나, 그와 관련된 이름, 전화 번호, 주민번호, 계좌번호가 결합된 채로 유출된 경우에는 바이오인식정보(BR)에 대한 소유주가 누구인지 쉽게 알 수 있고, 이는 다른 바이오인식 시스템을 이용하는 시스템에 오용되어 질 수 있기 때문이다.

[0045] 본 발명과 관련하여 명세서 전체에서 언급하는 "개인식별정보 데이터베이스", "바이오인식정보 데이터베이스"는 단순한 저장소를 의미하는 협의의 데이터베이스를 말하는 것이 아니라, 데이터 저장뿐만 아니라 결합 과정/무결성 보장 과정과 관련된 일련의 절차를 처리할 수 있는 광의의 데이터베이스를 말한다.

[0046] 도 3a 내지 도 3d 및 도 4a 내지 도 4d는 본 발명에 따른 데이터베이스 분리운영 환경에서의 개인식별정보와 바이오인식정보의 안전한 결합 방법에 대한 일실시예 흐름도로서, 도 3a 내지 도 3d는 개인식별정보 데이터베이스(20)와 바이오인식정보 데이터베이스(21) 간에 "안전한 통신채널"이 있는 경우의 결합 과정을 나타내고, 도 4a 내지 도 4d는 위의 두 데이터베이스(20, 21) 간에 "불안전한 통신채널"이 있는 경우의 결합 과정을 나타낸다. 여기서 안전한 통신 채널은 전송되는 자료들이 외부 공격자에게 노출되거나 혹은 외부 공격자에 의해 위·변조 등의 개입이 불가능한 통신 채널을 의미한다. 그리고, 결합 과정은 개인식별정보/바이오인식정보 등록 과정을 포함하는 넓은 개념으로 사용하기로 한다.

[0047] 먼저, 개인식별정보 데이터베이스(DB)(20)와 바이오인식정보 데이터베이스(DB)(21)의 분리 운영에 대하여 설명하면, 다음과 같다.

[0048] 본 발명은 개인식별정보 데이터베이스(DB)(20)와 바이오인식정보 데이터베이스(DB)(21)를 논리적이나 물리적으로 분리하여 운영하되, 두 개의 정보(개인식별정보, 바이오인식정보)를 결합할 수 있도록, 두 개의 정보를 공통으로 지칭할 수 있는 공통 식별자(CI: Common Identifier)를 이용하는 것을 특징으로 한다. 특히, 이러한 상황에서는 다음과 같은 보안 요구사항을 만족하는 것이 요구된다.

[0049] 첫째, 공통 식별자(CI) 자체만으로는 바이오인식정보나 개인식별정보를 추출할 수 없어야 한다.

[0050] 둘째, 만약 두 개 중 어느 하나의 데이터베이스(DB)가 침해되고 내용들이 불법적으로 수정되어 무결성에 문제가 생겼다면, 데이터베이스(DB) 운영자들은 이러한 사실을 감지할 수 있어야 한다.

[0051] 셋째, 데이터베이스(DB)의 운영 중에 적절한 비밀키를 가지고 있는 운영자에 의해 데이터베이스(DB) 내용이 수정되더라도 다른 쪽 데이터베이스(DB)의 운영자가 이 사실을 감지할 수 있어야 한다.

[0052] 이하, 도 1에 도시된 바와 같은 바이오인식 시스템(11)에서, 개인식별정보(IR) 데이터베이스(20)와 바이오인식정보(BR) 데이터베이스(21)가 분리운용 환경에서, 개인식별정보(IR)와 바이오인식정보(BR)를 안전하게 결합하는 방안을 상세히 설명하고자 한다. 이때, 개인식별정보(IR)를 위한 데이터베이스는 "DB_{IR}"로, 바이오인식정보(BR)에 대한 데이터베이스는 "DB_{BR}"로 간단히 표기하기로 한다.

[0053] 또한, 본 발명은 전술한 보안 요구사항을 만족하기 위하여 보안 기술의 일종인 비밀키 방식을 사용한다. 즉, 개인식별정보 데이터베이스(DB_{IR})(20)는 비밀키 K_i를 사용하고 바이오인식정보 데이터베이스(DB_{BR})(21)는 비밀키 K_b

를 사용한다. 또한 두 개의 데이터베이스(DB_{IR}, DB_{BR})(20, 21)는 불안전한 채널에서의 전송 메시지 보호를 위해서 공유 비밀키 K_e를 공유한다.

[0054] 먼저, 도 3a 내지 도 3d를 참조하여, 분리 운영되는 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 "안전한 통신채널"이 있는 경우의 개인식별정보/바이오인식정보 결합 과정을 설명하면, 다음과 같다.

[0055] 특히, 본 발명에 따른 결합 과정은 개인식별정보(IR) 등록, 바이오인식정보(BR) 등록, 데이터 교환, 및 데이터 저장 등과 같은 4개 단계를 포함하여 이루어지는데, 이하 각각의 단계별로 분리하여 설명하기로 한다. 설명의 편의상, 데이터베이스에서의 동작을 해당 데이터베이스 표시 부분(예를 들어, 원통 모양) 밖에 표현하기로 한다.

[0056] < Step 1: 개인식별정보(IR) 등록 >

[0057] 도 3a에 도시된 바와 같이, 개인식별정보 데이터베이스(DB_{IR})(20)는 개인식별정보(IR) 소유자로부터 해당 개인식별정보(IR)를 받으면, 비밀키 K_i를 이용해 개인식별정보(IR)를 암호화하여 E_{Ki}(IR)을 얻고(300), 개인식별정보(IR)를 해싱하여 해쉬값(해싱값, 해쉬함수값) h_{IR}(IR)을 얻는다(301).

[0058] < Step 2: 바이오인식정보(BR) 등록 >

[0059] 도 3b에 도시된 바와 같이, 바이오인식정보 데이터베이스(DB_{BR})(21)는 신호 처리부로부터 대응하는 바이오인식정보(BR)를 받으면, 비밀키 K_b를 이용하여 바이오인식정보(BR)를 암호화하여 E_{Kb}(BR)을 얻고(310), 바이오인식정보(BR)를 해싱하여 해쉬값 h_{BR}(BR)을 얻는다(311).

[0060] < Step 3: 데이터 교환 >

[0061] 도 3c에 도시된 바와 같이, 개인식별정보 데이터베이스(DB_{IR})(20)는 도 3a("301")에서 획득한 h_{IR}(IR)을 바이오인식정보 데이터베이스(DB_{BR})(21)로 전송하는데(320), 이때 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 안전한 통신 채널이 설정되어 있기 때문에 별도의 암호화 과정없이 전송한다. 그에 따라, 바이오인식정보 데이터베이스(DB_{BR})(21)는 전송받은 h_{IR}(IR)를 저장한다.

[0062] 다음으로, 바이오인식정보 데이터베이스(DB_{BR})(21)는 기존에 사용하고 있는 공통 식별자(CI)와 충돌하지 않는 새로운 공통 식별자(CI)를 설정하여(321) 데이터베이스 해당 레코드의 외부키(Foreign Key)로 사용한다. 이때 기밀성을 위해서 공통 식별자(CI)는 비밀키 K_b를 이용하여 암호화된다. 실시예에 따라 다양한 공통 식별자(CI) 설정 과정이 있을 수 있는데, 그 일예로는, 난수 발생기로부터 미리 정해진 길이만큼의 "난수(Random Number)"를 획득하여 기존에 사용하고 있는 공통 식별자(CI)와의 충돌 여부를 확인하고, 그 확인 결과에 따라 충돌하면 재발행하고(즉, 새로운 난수를 획득하여 충돌 여부를 확인하고) 충돌되지 않으면 이를 공통 식별자(CI)로 설정하는 경우가 있다.

[0063] 다음으로, 바이오인식정보 데이터베이스(DB_{BR})(21)는 공통 식별자(CI)와 도 3b("311")에서 구한 h_{BR}(BR)를 개인식별정보 데이터베이스(DB_{IR})(20)로 전송한다(322). 이때, 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 안전한 통신 채널이 설정되어 있기 때문에 별도의 암호화 과정없이 전송한다.

[0064] < Step 4: 데이터 저장 >

[0065] 도 3d에 도시된 바와 같이, 바이오인식정보 데이터베이스(DB_{BR})(21)는 개인식별정보 데이터베이스(DB_{IR})(20)로부

터 받은 $h_{IR}(IR)$을 포함하여 {$E_{Kb}(CI)$, $E_{Kb}(BR)$,$h_{IR}(IR)$}을 저장한다. 이때, 공통 식별자(CI)는 비밀키 K_b로 암호화되어 저장된다.

[0066] 한편, 개인식별정보 데이터베이스(DB_{IR})(20)는 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 수신한 공통 식별자(CI) 및 $h_{BR}(BR)$을 포함하여 {$E_{Ki}(CI)$, $E_{Ki}(IR)$, $h_{BR}(BR)$}을 저장한다. 이때, 공통 식별자(CI)는 비밀키 K_i로 암호화되어 저장된다.

[0067] 다음은, 도 4a 내지 도 4d를 참조하여, 분리 운영되는 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 "불안전한 통신채널"이 있고 공유비밀키(공통 암호화키) Ke를 갖는 경우에서의 개인식별정보/바이오인식정보 결합 과정을 설명하기로 한다. 특히, 본 발명에 따른 결합 과정은 개인식별정보(IR) 등록, 바이오인식정보(BR) 등록, 데이터 교환, 및 데이터 저장 등과 같은 4개 단계를 포함하여 이루어지는데, 이하 각각의 단계별로 분리하여 설명하기로 한다.

[0068] < Step 1: 개인식별정보(IR) 등록 >

[0069] 도 4a에 도시된 바와 같이, 개인식별정보 데이터베이스(DB_{IR})(20)는 개인식별정보(IR) 소유자로부터 해당 개인식별정보(IR)를 받으면, 비밀키 K_i를 이용해 개인식별정보(IR)를 암호화하여 $E_{Ki}(IR)$을 얻고(400), 개인식별정보(IR)를 해싱하여 해쉬값 $h_{IR}(IR)$을 얻는다(401). 또한, 개인식별정보 데이터베이스(DB_{IR})(20)는 공유비밀키 Ke를 이용해 $h_{IR}(IR)$, $IDDB_{IR}$, 및 N_i를 암호화하여 $E_{Ke}(h(IR), IDDB_{IR}, N_i)$를 얻는다. 여기서 $IDDB_{IR}$는 개인식별정보 데이터베이스(DB_{IR})(20)를 위한 유일한 식별자이며, N_i는 개인식별정보 데이터베이스(DB_{IR})(20)에 의해 생성된 임시적인 비표(임시 비표)(Time Stamp 또는 Sequence Number)이다.

[0070] < Step 2: 바이오인식정보(BR) 등록 >

[0071] 도 4b에 도시된 바와 같이, 바이오인식정보 데이터베이스(DB_{BR})(21)는 신호 처리부로부터 대응하는 바이오인식정보(BR)를 받으면, 비밀키 K_b를 이용하여 바이오인식정보(BR)를 암호화하여 $E_{Kb}(BR)$을 얻고(410), 바이오인식정보(BR)를 해싱하여 해쉬값 $h_{BR}(BR)$을 얻는다(411).

[0072] < Step 3: 데이터 교환 >

[0073] 도 4c에 도시된 바와 같이, 개인식별정보 데이터베이스(DB_{IR})(20)는 $E_{Ke}(h_{IR}(IR), IDDB_{IR}, N_i)$를 바이오인식정보 데이터베이스($DB_{BR}$)(21)로 보내고, 바이오인식정보 데이터베이스(DB_{BR})(21)는 개인식별정보 데이터베이스(DB_{IR})(20)로부터 $E_{Ke}(h_{IR}(IR), IDDB_{IR}, N_i)$을 받아 공유비밀키 Ke를 이용하여 {$(h_{IR}(IR), IDDB_{IR}, N_i$}을 복호화하고, $IDDB_{IR}$과 N_i를 검증한다. 만약 검증이 실패하면 에러 메시지를 제공하고 종료하고, 검증이 성공한 경우에는 상기 복호화한 $h_{IR}(IR)$를 저장한다.

[0074] 다음으로, 바이오인식정보 데이터베이스(DB_{BR})(21)는 기존에 사용하고 있는 공통 식별자(CI)와 충돌하지 않는 새로운 공통 식별자(CI)를 설정하여(421) 데이터베이스 해당 레코드의 외부키(Foreign Key)로 사용한다. 이때 기밀성을 위해서 공통 식별자(CI)는 비밀키 K_b를 이용하여 암호화된다. 여기서, 공통 식별자(CI) 설정은 도 3c에서 설명한 바와 같다.

[0075] 이후, 바이오인식정보 데이터베이스(DB_{BR})(21)는 공유비밀키 K_e를 이용하여 $E_{Ke}(CI, h_{BR}(BR), IDDB_{BR}, N_b)$로 암호화하여 개인식별정보 데이터베이스($DB_{IR}$)(20)로 전송한다(422). 그러면, 개인식별정보 데이터베이스(DB_{IR})(20)는 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 수신한 $E_{Ke}(CI, h_{BR}(BR), IDDB_{BR}, N_b)$를 CI, $h_{BR}(BR)$, $IDDB_{BR}$, N_b로

복호화한 후 $IDDB_{BR}$과 N_b를 검증한다. 이때, 검증이 실패하면 에러 메시지를 제공하고 종료한다. 여기서 $IDDB_{BR}$은 바이오인식정보 데이터베이스(DB_{BR})(21)를 위한 유일한 식별자이고, N_b는 바이오인식정보 데이터베이스(DB_{BR})(21)에 의해 생성된 임시적인 비표(Time Stamp 또는 Sequence Number)이다.

[0076] < Step 4: 데이터 저장 >

[0077] 도 4d에 도시된 바와 같이, 바이오인식정보 데이터베이스(DB_{BR})(21)는 개인식별정보 데이터베이스(DB_{IR})(20)로부터 받은 $h_{IR}(IR)$을 포함하여 {$E_{Kb}(CI)$, $E_{Kb}(BR)$,$h_{IR}(IR)$}을 저장한다. 이때, 공통 식별자(CI)는 비밀키 K_b로 암호화되어 저장된다.

[0078] 한편, 개인식별정보 데이터베이스(DB_{IR})(20)는 검증($IDDB_{BR}$과 N_b 검증)이 성공하면 {$E_{Ki}(CI)$, $E_{Ki}(IR)$, $h_{BR}(BR)$}을 저장한다(도 4d). 이때, 공통 식별자(CI)는 비밀키 K_i로 암호화되어 저장된다.

[0079] 도 5a, 도 5b, 도 6a, 및 도 6b는 본 발명에 따른 데이터베이스 분리운영 환경에서의 개인 인증(Verification)을 위한 데이터베이스 무결성 보장 방법에 대한 일실시예 흐름도로서, 개인 바이오 인증(개인 인증: Verification)을 위하여 바이오인식정보 데이터베이스(DB_{BR})(21)가 해당 바이오인식정보(BR)를 바이오인식 시스템(11)의 비교부(114)에 전송하는 과정을 나타낸다. 특히, 도 5a 및 도 5b는 개인식별정보 데이터베이스(20)와 바이오인식정보 데이터베이스(21) 간에 "안전한 통신채널"이 있는 경우, 도 6a 및 도 6b는 위의 두 데이터베이스 간에 "불안전한 통신채널"이 있는 경우를 나타낸다.

[0080] 먼저, 도 5a 및 도 5b를 참조하여, 분리 운영되는 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 "안전한 통신채널"이 있는 경우, 개인 인증(Verification)에 필요한 바이오인식정보(BR)를 검증하여 비교부(114)에 전송하는 과정을 설명하기로 한다. 특히, 본 발명에 따른 무결성 보장 방법은 개인인증 요구에 의한 개인식별정보(IR) 레코드 검색, 무결성 검증, 및 바이오인식정보 전송 등과 같은 3개 단계를 포함하여 이루어지는데, 이하 각각의 단계별로 분리하여 설명하기로 한다.

[0081] < Step 1: 개인식별정보(IR) 레코드 검색>

[0082] 도 5a에 도시된 바와 같이, 개인식별정보 데이터베이스(DB_{IR})(20)는 개인식별정보(IR) 소유자로부터 적법한 개인인증 요구를 받으면, 개인식별정보(IR)의 암호화값 $E_{Ki}(IR)$(500)에 해당되는 데이터 레코드를 검색하고, 또한 개인식별정보(IR)을 해싱하여 $h_{IR}(IR)$을 생성한다(501). 그리고 나서, 개인식별정보 데이터베이스(DB_{IR})(20)는 생성된 개인식별정보(IR) 해쉬값[$h_{IR}(IR)$]과, 상기 검색된 데이터 레코드로부터 획득한 공통 식별자(CI) 및 바이오인식정보 해쉬값[$h_{BR}(BR)$](이는 "$h_{IR}(BR)$"로도 표시할 수 있는데, 이러한 표기 변경에 대해서는 후술하기로 한다)을 바이오인식정보 데이터베이스(DB_{BR})(21)로 전송한다(502). 여기서, $h_{IR}(BR)$은 도 3a 내지 도 3d의 결합 과정에서 개인식별정보 데이터베이스(DB_{IR})(20)가 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 수신하여 저장하고 있던 $h_{BR}(BR)$로서, 무결성 검증시 비교 대상을 명확히 파악할 수 있도록 아래 첨자를 "IR"로 변경한 것에 불과하다.

[0083] 즉, 개인식별정보 데이터베이스(DB_{IR})(20)는 {CI, $h_{IR}(IR)$, $h_{IR}(BR)$}를 바이오인식정보 데이터베이스(DB_{BR})(21)에 전송한다(502). 이때, 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 안전한 통신 채널이 설정되어 있기 때문에 별도의 암호화 과정 없이 전송한다.

[0084] < Step 2: 무결성 검증 >

[0085] 도 5b에 도시된 바와 같이, 바이오인식정보 데이터베이스(DB_{BR})(21)는 개인식별정보 데이터베이스(DB_{IR})(20)로부

터 {CI, h_{IR}(IR),h_{IR}(BR)}을 수신하면, 그 수신된 공통 식별자(CI)(외부키에 해당함)를 추출한 후(510), 그 추출된 공통 식별자(CI)를 이용하여 E_{Kb}(BR)을 검색하여(511) 복호화함으로써 바이오인식정보(BR)를 복원한다(512). 여기서, h_{IR}(BR)은 <Step 1>에서 설명한 바와 같다.

[0086] 그리고 나서, 바이오인식정보 데이터베이스(DB_{BR})(21)는 복원된 바이오인식정보(BR)의 해쉬 값[h_{BR}(BR)]을 구한 후(513), 개인식별정보 데이터베이스(DB_{IR})(20)로부터 수신한 바이오인식정보(BR)의 해쉬 값[h_{IR}(BR)](514)과 비교한다(515). 또한, 도 5b에는 도시되어 있지 않으나, 바이오인식정보 데이터베이스(DB_{BR})(21)는 "502"를 통하여 수신된 h_{IR}(IR)과, 이미 저장되어 있는 h_{BR}(IR)을 비교한다. 여기서, h_{BR}(IR)은 도 3a 내지 도 3d의 결합 과정에서 바이오인식정보 데이터베이스(DB_{BR})(21)가 개인식별정보 데이터베이스(DB_{IR})(20)로부터 수신하여 저장하고 있는 h_{IR}(IR)로서, 무결성 검증시 비교 대상을 명확히 파악할 수 있도록 아래 첨자를 "BR"로 변경한 것에 불과하다.

[0087] < Step 3: 바이오인식정보(BR) 전송 >

[0088] 도 5b에 도시된 바와 같은 무결성 검증 결과, 비교대상 해쉬값이 정합하면(검증이 성공하면)(515), 바이오인식정보 데이터베이스(DB_{BR})(21)는 바이오 인증을 할 수 있도록, 비교부(114)로 해당 바이오인식정보(BR)를 안전하게 전송한다(516). 그렇지 않으면(정합하지 않으면), 에러메시지를 제공하고 종료한다.

[0089] 다음은, 도 6a 및 도 6b를 참조하여, 분리 운영되는 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 "불안전한 통신채널"이 있고 공유비밀키(공통 암호화키) Ke를 갖는 경우, 개인 인증(Verification)에 필요한 바이오인식정보(BR)를 검증하여 비교부(114)에 전송하는 과정을 설명하기로 한다.

[0090] 특히, 본 발명에 따른 무결성 보장 방법은 개인인증 요구에 의한 개인식별정보(IR) 레코드 검색, 무결성 검증, 및 바이오인식정보 전송 등과 같은 3개 단계를 포함하여 이루어지는데, 이하 각각의 단계별로 분리하여 설명하기로 한다.

[0091] < Step 1: 개인식별정보(IR) 레코드 검색>

[0092] 도 6a에 도시된 바와 같이, 개인식별정보 데이터베이스(DB_{IR})(20)는 개인식별정보(IR) 소유자로부터 적법한 개인인증 요구를 받으면, 개인식별정보(IR)의 암호화값(600)에 해당되는 데이터 레코드를 검색하고 개인식별정보(IR)를 해싱하여 해쉬값 h_{IR}(IR)을 생성한다(601). 그리고 나서, 개인식별정보 데이터베이스(DB_{IR})(20)는 개인식별정보(IR) 해쉬값[h_{IR}(IR)]과, 상기 검색된 데이터 레코드에 있는 공통 식별자(CI) 및 바이오인식정보 해쉬값[h_{BR}(BR)](이는 "h_{IR}(BR)"로 표시할 수 있는데, 이러한 표기 변경에 대해서는 후술하기로 한다)과, 개인식별정보 데이터베이스(DB_{IR})(20)를 위한 식별자($IDDB_{IR}$)와, 개인식별정보 데이터베이스(DB_{IR})(20)에 의해 생성된 임시적인 비표(N_i)를 암호화하여 바이오인식정보 데이터베이스(DB_{BR})(21)에 전송한다(602). 여기서, h_{IR}(BR)은 도 4a 내지 도 4d의 결합 과정에서 개인식별정보 데이터베이스(DB_{IR})(20)가 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 수신하여 저장하고 있던 h_{BR}(BR)로서, 검증시 비교 대상을 명확히 파악할 수 있도록 아래 첨자를 "IR"로 변경한 것에 불과하다.

[0093] 즉, 개인식별정보 데이터베이스(DB_{IR})(20)는 {CI, h_{IR}(IR), h_{IR}(BR), $IDDB_{IR}$, N_i}를 공유 비밀키 Ke로 암호화하고 그 결과인 E_{Ke}(CI, h_{IR}(IR), h_{IR}(BR), $IDDB_{IR}$, N_i)를 바이오인식정보 데이터베이스(DB_{BR})(21)에 전송한다(602). 이때, 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간의 통신채널이 불안전하기 때문에 암호화하여 전송하는 것이다.

[0094] < Step 2: 무결성 검증 >

[0095] 도 6b에 도시된 바와 같이, 바이오인식정보 데이터베이스(DB_{BR})(21)는 개인식별정보 데이터베이스(DB_{IR})(20)로부터 E_{Ke}(CI, h_{IR}(IR), h_{IR}(BR), $IDDB_{IR}$, N_i)을 수신하면(610), 공유 비밀키 Ke로 복호화를 통하여 {CI, h_{IR}(IR), h_{IR}(BR), $IDDB_{IR}$, N_i}를 복원하고(611) $IDDB_{IR}$과 N_i를 검증한다(612). 만약 $IDDB_{IR}$과 N_i의 검증이 실패하면 에러메시지를 제공하고 종료한다. 여기서, h_{IR}(BR)은 <Step 1>에서 설명한 바와 같다.

[0096] $IDDB_{IR}$과 N_i의 검증이 성공하면, 바이오인식정보 데이터베이스(DB_{BR})(21)는 복원된 {CI, h_{IR}(IR), h_{IR}(BR), $IDDB_{IR}$, N_i}에서 공통 식별자(CI)(외부키에 해당함)를 추출한 후(613), 그 추출된 공통 식별자(CI)를 이용해 E_{Kb}(BR)을 검색하여(614) 복호화함으로써 바이오인식정보(BR)를 복원한다(615).

[0097] 그리고 나서, 바이오인식정보 데이터베이스(DB_{BR})(21)는 복원된 바이오인식정보(BR)의 해쉬 값[h_{BR}(BR)]을 구한 후(616), 개인식별정보 데이터베이스(DB_{IR})(20)로부터 수신한 바이오인식정보(BR)의 해쉬 값[h_{IR}(BR)]과 비교한다(617). 또한, 도 6b에는 도시되지 않았으나, 바이오인식정보 데이터베이스(DB_{BR})(21)는 개인식별정보 데이터베이스(DB_{IR})(20)로부터 수신된 h_{IR}(IR)과 이미 저장되어 있는 h_{BR}(IR)을 비교한다. 여기서, h_{BR}(IR)은 도 4a 내지 도 4d의 결합 과정에서 바이오인식정보 데이터베이스(DB_{BR})(21)가 개인식별정보 데이터베이스(DB_{IR})(20)로부터 수신하여 저장하고 있는 h_{IR}(IR)로서, 검증시의 비교 대상을 명확히 파악할 수 있도록 아래 첨자를 "BR"로 변경한 것에 불과하다.

[0098] < Step 3: 바이오인식정보(BR) 전송 >

[0099] 도 6b에 도시된 바와 같은 검증 결과(617), 비교대상 해쉬값이 정합하면(검증이 성공하면), 바이오인식정보 데이터베이스(DB_{BR})(21)는 바이오 인증을 할 수 있도록, 비교부(114)로 해당 바이오인식정보(BR)를 안전하게 전송한다(618). 이때, 바이오인식정보 데이터베이스(DB_{BR})(21)는 전송 대상이 되는 바이오인식정보(BR)를 단순 전송하거나, 암호화하여 전송한다. 만약, 비교 결과(617), 정합하지 않으면 에러메시지를 제공하고 종료한다.

[0100] 도 7a, 도 7b, 도 8a 및 도 8b는 본 발명에 따른 데이터베이스 분리운영 환경에서의 개인 식별(Identification)을 위한 데이터베이스 무결성 보장 방법에 대한 일실시예 흐름도로서, 개인 식별(Identification)에 필요한 개인식별정보(IR)의 요청에 따라, 바이오인식정보 데이터베이스(DB_{BR})(21)가 개인식별정보 데이터베이스(DB_{IR})(20)에 개인식별정보(IR)를 요구하고, 그에 따라 개인식별정보 데이터베이스(DB_{IR})(20)가 해당 개인식별정보(IR)를 바이오인식 시스템(11)의 결정부(115)에 전송하는 과정을 나타낸다. 특히, 도 7a 및 도 7b는 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 "안전한 통신채널"이 있는 경우, 도 8a 및 도 8b는 위의 두 데이터베이스 간에 "불안전한 통신채널"이 있는 경우를 나타낸다.

[0101] 먼저, 도 7a 및 도 7b를 참조하여, 분리 운영되는 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 "안전한 통신채널"이 있는 경우, 개인 식별(Identification)에 필요한 개인식별정보(IR)를 검증하여 결정부(115)에 전송하는 과정을 설명하기로 한다. 특히, 본 발명에 따른 무결성 보장 방법은 개인식별정보(IR) 요청, 무결성 검증, 및 개인식별정보 전송 등과 같은 3개 단계를 포함하여 이루어지는데, 이하 각각의 단계별로 분리하여 설명하기로 한다.

[0102] < Step 1: 개인식별정보(IR) 요청 >

[0103] 도 7a에 도시된 바와 같이, 바이오인식정보 데이터베이스(DB_{BR})(21)는 바이오 인식 시스템의 결정부(115)로부터 특정 바이오인식정보에 해당되는 개인식별정보(IR)의 요청(IR Request)을 받으면(700), 그 입력된 바이오인식정보와 가장 근사값을 갖는 바이오인식정보(BR) 값("근접 BR")을 바이오인식정보 데이터베이스(DB_{BR})(21)로부터

추출(검색)하고(701), 그에 대한 해쉬값 $h_{BR}(BR)$을 획득하여(702) 공통 식별자(CI) 및 개인식별정보 해쉬값 [$h_{BR}(IR)$]과 함께 개인식별정보 데이터베이스(DB_{IR})(20)에 전송한다(703).

[0104] 즉, 바이오인식정보 데이터베이스(DB_{BR})(21)는 {CI, $h_{BR}(IR)$, $h_{BR}(BR)$}을 개인식별정보 데이터베이스(DB_{IR})(20)에 전송한다(703). 여기서, $h_{BR}(IR)$은 도 3a 내지 도 3d의 결합 과정에서 바이오인식정보 데이터베이스(DB_{BR})(21)가 개인식별정보 데이터베이스(DB_{IR})(20)로부터 수신하여 저장하고 있는 $h_{IR}(IR)$로서, 검증시 비교 대상을 명확히 파악할 수 있도록 아래 첨자를 "BR"로 변경한 것에 불과하다.

[0105] < Step 2: 무결성 검증 >

[0106] 도 7b에 도시된 바와 같이, 개인식별정보 데이터베이스(DB_{IR})(20)는 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 {CI, $h_{BR}(IR)$, $h_{BR}(BR)$}을 수신하면(710), 그 수신된 {CI, $h_{BR}(IR)$, $h_{BR}(BR)$}로부터 공통 식별자(CI)를 추출한다(711). 개인식별정보 데이터베이스(DB_{IR})(20)는 그 추출된 공통 식별자(CI)를 이용해 $E_{Ki}(IR)$을 검색한 후(712), 복호화 및 해싱함으로써 해쉬값 $h_{IR}(IR)$을 구하여(713) 상기 수신된 $h_{BR}(IR)$과 비교한다(714).

[0107] 또한, 개인식별정보 데이터베이스(DB_{IR})(20)는 수신된 $h_{BR}(BR)$(710)과 이미 저장되어 있는 $h_{IR}(BR)$을 비교한다(716). 여기서, $h_{IR}(BR)$은 그 수신된 공통 식별자(CI)(711)를 이용하여 추출한 것이다(715). 그리고, $h_{IR}(BR)$은 도 3a 내지 도 3d의 결합 과정에서 개인식별정보 데이터베이스(DB_{IR})(20)가 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 수신하여 저장하고 있는 $h_{BR}(BR)$로서, 검증시의 비교 대상을 명확히 파악할 수 있도록 아래 첨자를 "IR"로 변경한 것에 불과하다.

[0108] < Step 3: 개인식별정보 전송 >

[0109] 도 7b에 도시된 바와 같은 검증 결과(714, 716), 비교대상 해쉬값이 정합하면(무결성 검증이 성공하면), 개인식별정보 데이터베이스(DB_{IR})(20)는 결정부(115)로 해당 개인식별정보(IR)를 안전하게 전송한다(718). 이때, 개인식별정보 데이터베이스(DB_{IR})(20)는 전송 대상이 되는 개인식별정보(IR)를 단순 전송하거나, 암호화하여 전송한다. 그리고, 만약, 정합하지 않으면(무결성 검증이 실패하면), 에러메시지를 제공하고 종료한다.

[0110] 다음은, 도 8a 및 도 8b를 참조하여, 분리 운영되는 개인식별정보 데이터베이스(DB_{IR})(20)와 바이오인식정보 데이터베이스(DB_{BR})(21) 간에 "불안전한 통신채널"이 있고 공유비밀키(공통 암호화키) Ke를 갖는 경우, 개인 식별(Identification)을 위한 개인식별정보(IR)의 요청에 따라, 바이오인식정보 데이터베이스(DB_{BR})(21)가 개인식별정보 데이터베이스(DB_{IR})(20)에 개인식별정보(IR)를 요구하고, 그에 따라 개인식별정보 데이터베이스(DB_{IR})(20)가 해당 개인식별정보(IR)를 바이오인식 시스템(11)의 결정부(115)에 전송하는 과정을 설명하기로 한다. 특히, 본 발명에 따른 무결성 보장 과정은 개인식별정보(IR) 요청, 무결성 검증, 개인식별정보 전송 등과 같은 3개 단계를 포함하여 이루어지는데, 이하 각각의 단계별로 분리하여 설명하기로 한다.

[0111] < Step 1: 개인식별정보(IR) 요청 >

[0112] 도 8a에 도시된 바와 같이, 바이오인식정보 데이터베이스(DB_{BR})(21)는 바이오 인식 시스템의 결정부(115)로부터 특정 바이오인식정보에 해당되는 개인식별정보(IR)의 요청(IR Request)을 받으면(800), 그 입력된 바이오인식정보와 가장 근사값을 갖는 바이오인식정보(BR) 값("근접 BR")을 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 추출(검색)하고(801), 그에 대한 해쉬값 $h_{BR}(BR)$을 획득한 후(802), {CI, $h_{BR}(IR)$, $h_{BR}(BR)$, $IDDB_{BR}$, N_b}를 공유비밀키 Ke로 암호화하여 E_{Ke}(CI, $h_{BR}(IR)$, $h_{BR}(BR)$, $IDDB_{BR}$, N_b)를 개인식별정보 데이터베이스(DB_{IR})(20)에 전송한다(803). 여기서, CI는 공통 식별자, $IDDB_{BR}$은 바이오인식정보 데이터베이스(DB_{BR})(21)를 위한 식별자, N_b는 바이오

인식정보 데이터베이스(DB_{BR})(21)에 의해 생성된 임시적인 비표를 나타낸다. 그리고, $h_{BR}(IR)$은 도 7a에서 이미 설명한 바와 같다.

[0113] < Step 2: 무결성 검증 >

[0114] 도 8b에 도시된 바와 같이, 개인식별정보 데이터베이스(DB_{IR})(20)는 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 $E_{Ke}(CI, h_{BR}(IR), h_{BR}(BR), IDDB_{BR}, N_b)$을 수신하면(810), 공유비밀키 Ke로 복호화하여 $\{CI, h_{BR}(IR), h_{BR}(BR), IDDB_{BR}, N_b\}$를 복원하고(811), $IDDB_{BR}$과 N_b를 검증한다(812). 만약 $IDDB_{BR}$과 N_b의 검증이 실패하면 에러 메시지를 제공하고 종료한다.

[0115] 만약, $IDDB_{BR}$과 N_b의 검증이 성공하면, 개인식별정보 데이터베이스(DB_{IR})(20)는 복원된 데이터 $\{CI, h_{BR}(IR), h_{BR}(BR), IDDB_{BR}, N_b\}$에서 공통 식별자(CI)(외부키에 해당함)를 추출한 후(813), 그 추출된 공통 식별자(CI)를 이용해 $E_{Ki}(IR)$을 검색하여(814) 복호화함으로써 해당 개인식별정보(IR)를 획득한다(815). 그리고 나서, 개인식별정보 데이터베이스(DB_{IR})(20)는 그 획득한 개인식별정보(IR)에 대한 해쉬값 $h_{IR}(IR)$을 구하여(816) 상기 수신된 $h_{BR}(IR)$과 비교한다(817). 또한, 개인식별정보 데이터베이스(DB_{IR})(20)는 바이오인식정보 데이터베이스(DB_{BR})(21)로부터 수신된 $h_{BR}(BR)$(810)과 이미 저장(등록)하고 있던 $h_{IR}(BR)$을 비교한다(819). 여기서, $h_{IR}(BR)$은 그 수신된 공통 식별자(CI)를 이용하여 추출한 것으로서(818), 도 7b에서 이미 설명한 바와 같다.

[0116] < Step 3: 개인식별정보 전송 >

[0117] 도 8b에 도시된 바와 같은 검증 결과(817, 819), 비교대상 해쉬값이 정합하면(무결성 검증이 성공하면), 개인식별정보 데이터베이스(DB_{IR})(20)는 결정부(115)로 해당 개인식별정보(IR)를 안전하게 전송한다(820). 이때, 개인식별정보 데이터베이스(DB_{IR})(20)는 전송 대상이 되는 개인식별정보(IR)를 단순 전송하거나, 암호화하여 전송한다. 그리고, 만약 정합하지 않으면(무결성 검증이 실패하면), 에러메시지를 제공하고 종료한다.

[0118] 한편, 전술한 바와 같은 본 발명의 방법은 컴퓨터 프로그램으로 작성이 가능하다. 그리고 상기 프로그램을 구성하는 코드 및 코드 세그먼트는 당해 분야의 컴퓨터 프로그래머에 의하여 용이하게 추론될 수 있다. 또한, 상기 작성된 프로그램은 컴퓨터가 읽을 수 있는 기록매체(정보저장매체)에 저장되고, 컴퓨터에 의하여 판독되고 실행됨으로써 본 발명의 방법을 구현한다. 그리고 상기 기록매체는 컴퓨터가 판독할 수 있는 모든 형태의 기록매체를 포함한다.

[0119] 이상에서 설명한 본 발명은, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 의해 한정되는 것이 아니다.

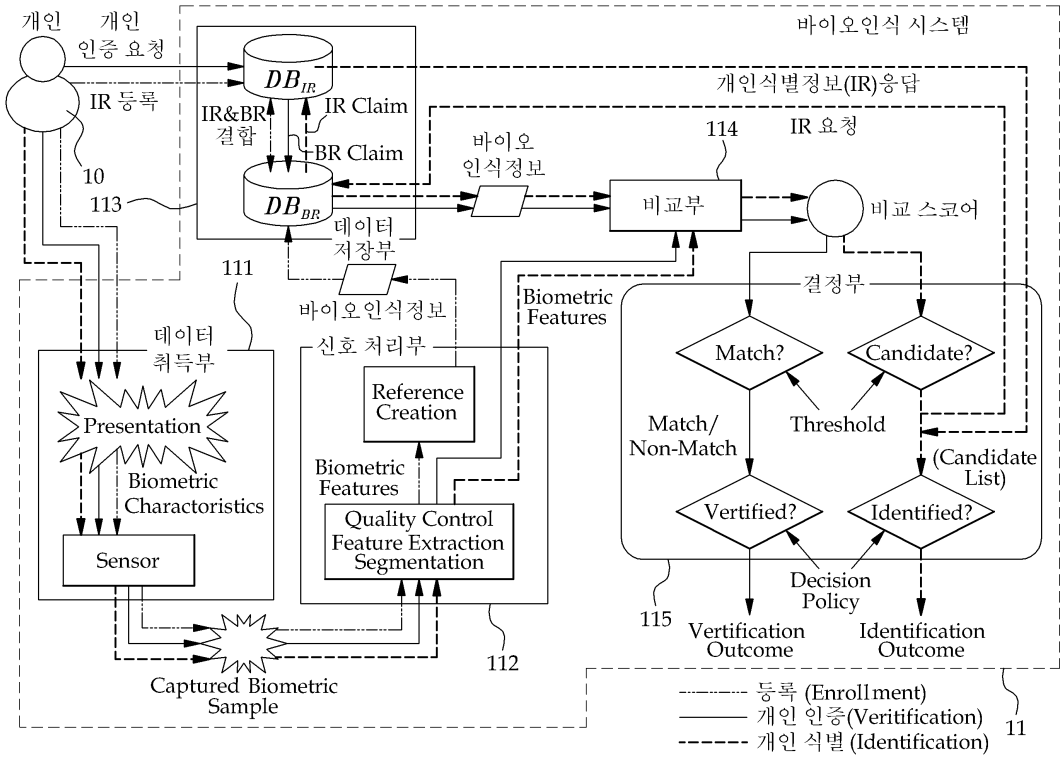
부호의 설명

[0120]

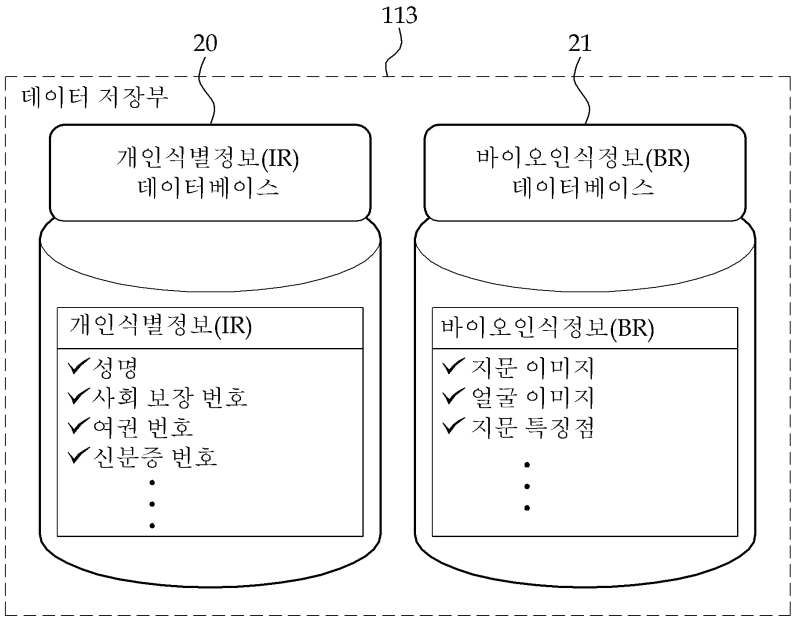
11: 바이오인식 시스템	111: 데이터 취득부
112: 신호처리부	113: 데이터 저장부
114: 비교부	115: 결정부
20: 개인식별정보 데이터베이스	21: 바이오인식정보 데이터베이스

도면

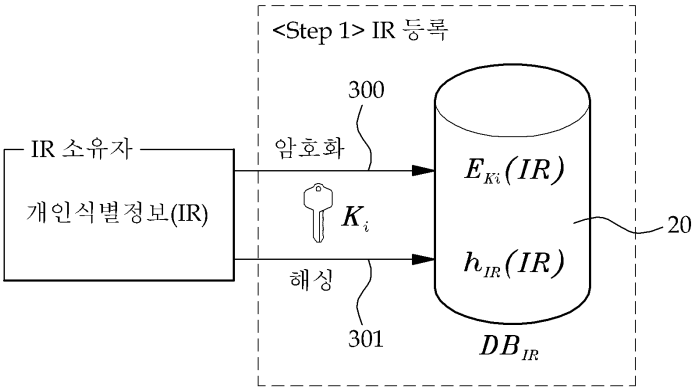
도면1


개인
개인
인증 요청
IR 등록
10
113
DB_{IR}
IR Claim
IR&BR
결합
BR Claim
DB_{BR}
데이터
저장부
111
바이오
인식정보
바이오인식 시스템
개인식별정보(IR)응답
114
IR 요청
비교부
비교 스코어
결정부
Biometric
Features
Match?
Candidate?
Match/
Non-Match
Threshold
(Candidate
List)
Vertified?
Identified?
Decision
Policy
115
Vertification
Outcome
Identification
Outcome
바이오인식정보
데이터
취득부
Presentation
Biometric
Charactoristics
Sensor
신호 처리부
Reference
Creation
Biometric
Features
Quality Control
Feature Extraction
Segmentation
112
Captured Biometric
Sample
등록 (Enrollment)
개인 인증(Veritification)
개인 식별 (Identification)
11

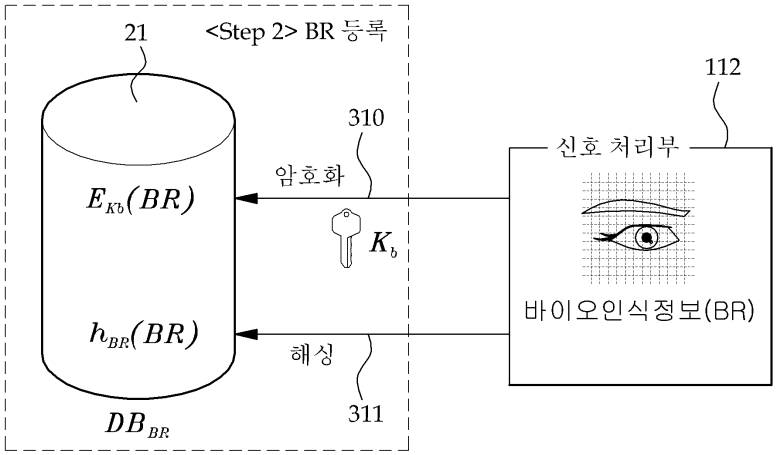
도면2


113
20
21
데이터 저장부
개인식별정보(IR)
데이터베이스
바이오인식정보(BR)
데이터베이스
개인식별정보(IR)
✓성명
✓사회 보장 번호
✓여권 번호
✓신분증 번호
바이오인식정보(BR)
✓지문 이미지
✓얼굴 이미지
✓지문 특징점

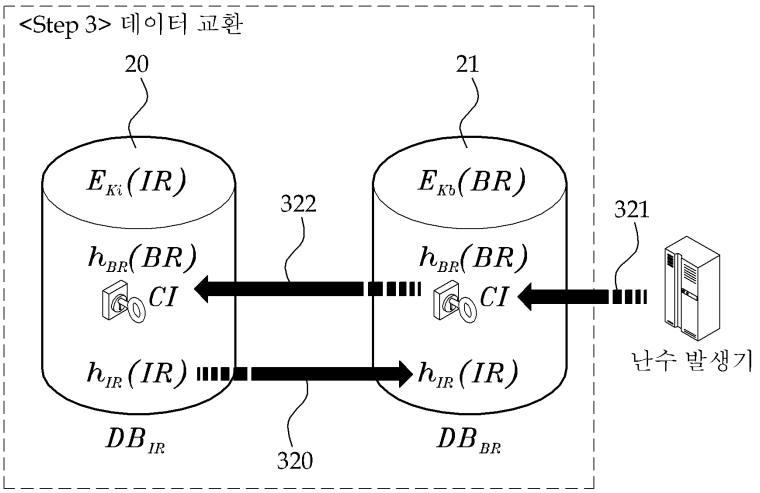
도면3a



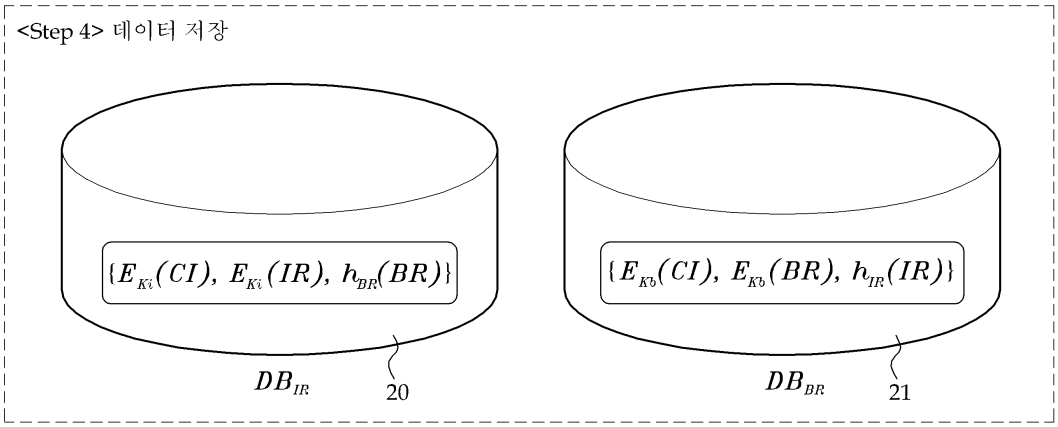
도면3b



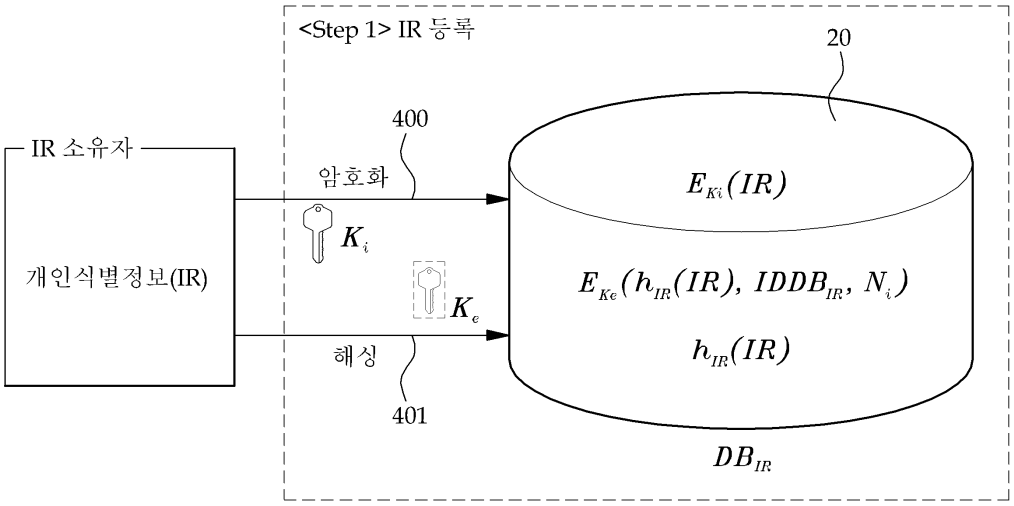
도면3c



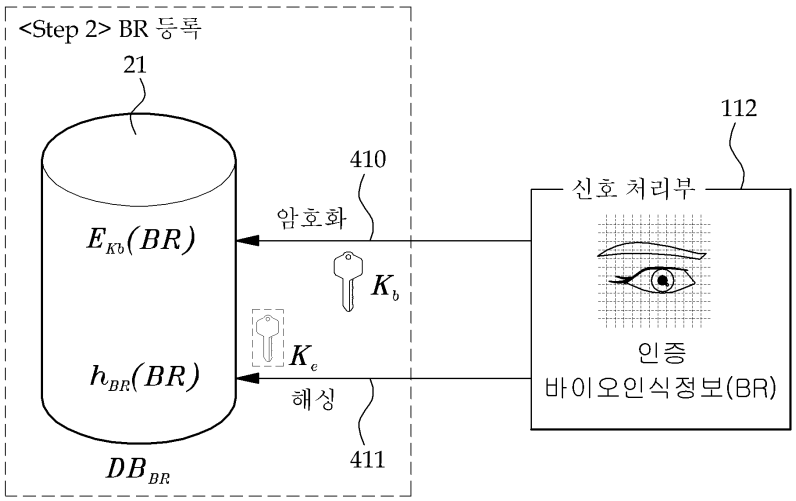
도면3d



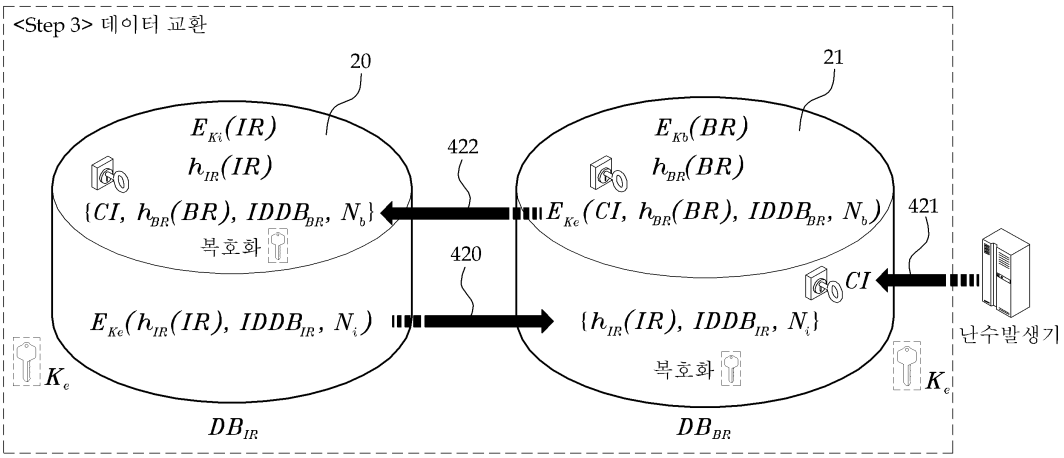
도면4a



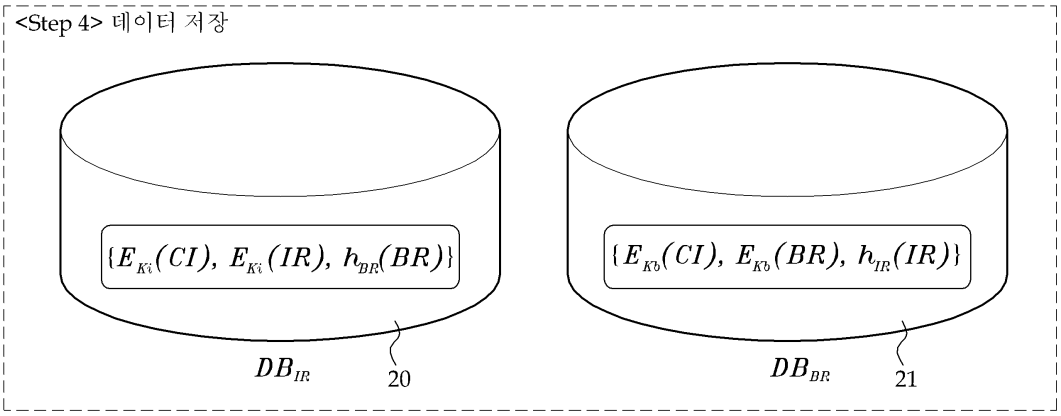
도면4b



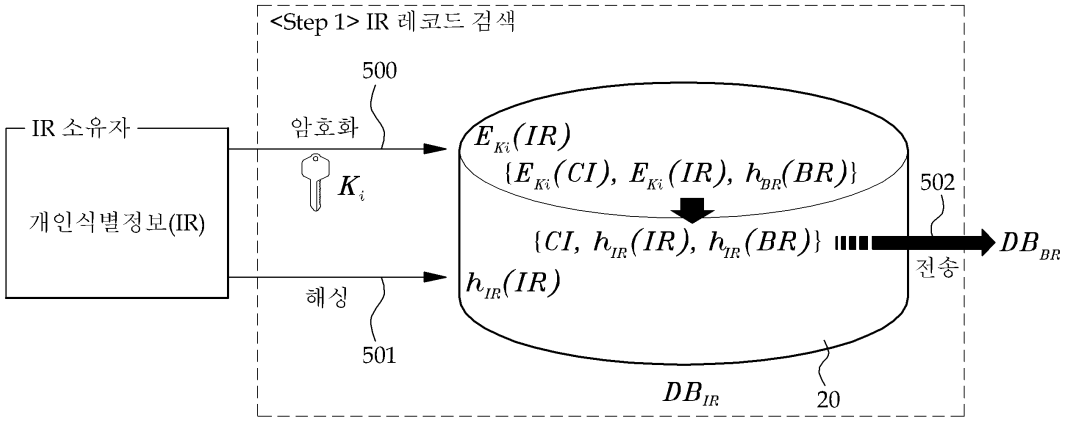
도면4c



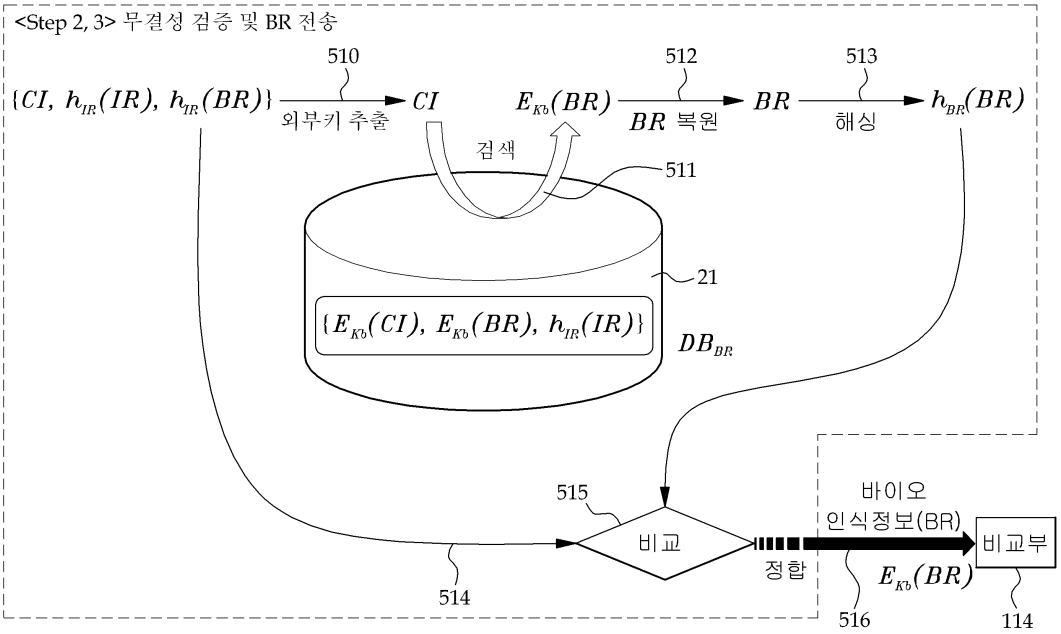
도면4d



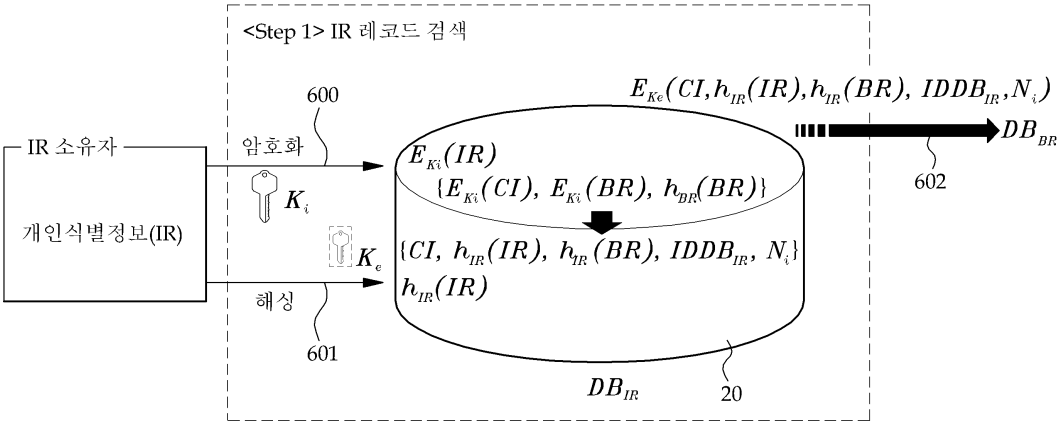
도면5a



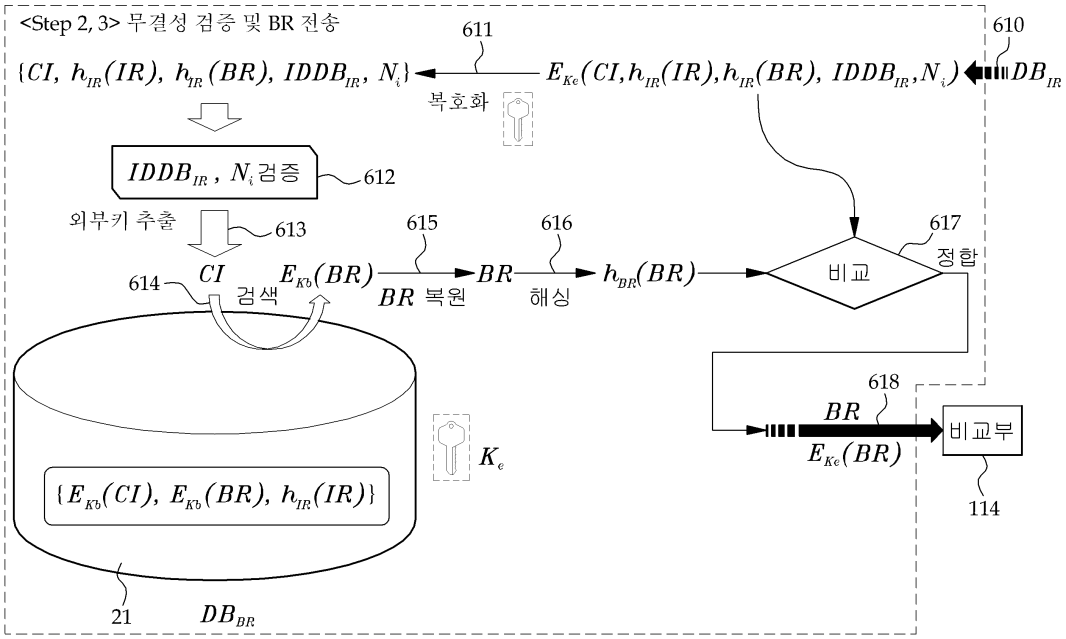
도면5b


<Step 2, 3> 무결성 검증 및 BR 전송
510
512
513
$\{CI,\ h_{IR}(IR),\ h_{IR}(BR)\}$
외부키 추출
CI
$E_{Kb}(BR)$
BR 복원
BR
해싱
$h_{BR}(BR)$
검색
511
21
$\{E_{Kb}(CI),\ E_{Kb}(BR),\ h_{IR}(IR)\}$
DB_{BR}
515
비교
바이오
인식정보(BR)
비교부
정합
$E_{Kb}(BR)$
514
516
114

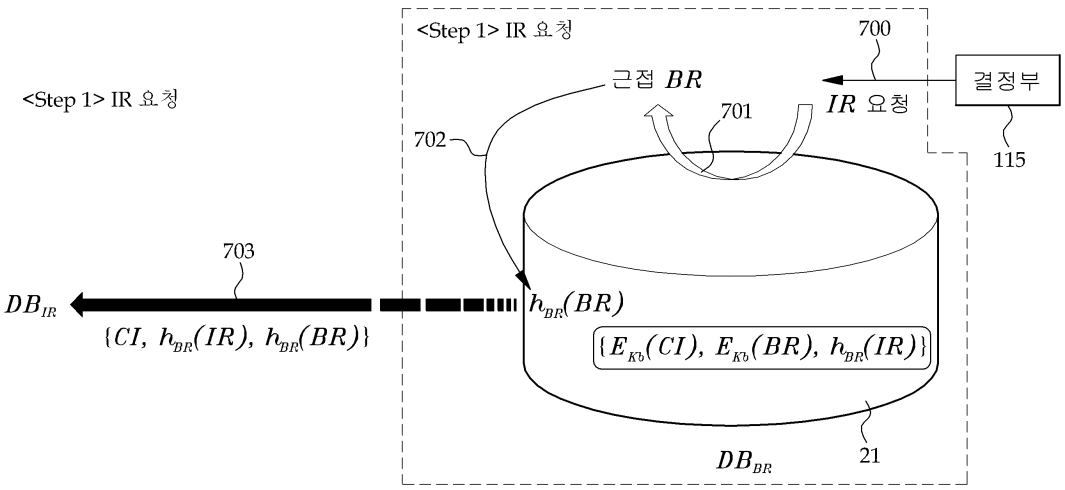
도면6a


<Step 1> IR 레코드 검색
600
$E_{Ke}(CI, h_{IR}(IR), h_{IR}(BR),\ IDDB_{IR}, N_i)$
DB_{BR}
IR 소유자
암호화
$E_{Ki}(IR)$
$\{E_{Ki}(CI),\ E_{Ki}(BR),\ h_{BR}(BR)\}$
602
K_i
개인식별정보(IR)
K_e
$\{CI,\ h_{IR}(IR),\ h_{IR}(BR),\ IDDB_{IR},\ N_i\}$
$h_{IR}(IR)$
해싱
601
DB_{IR}
20

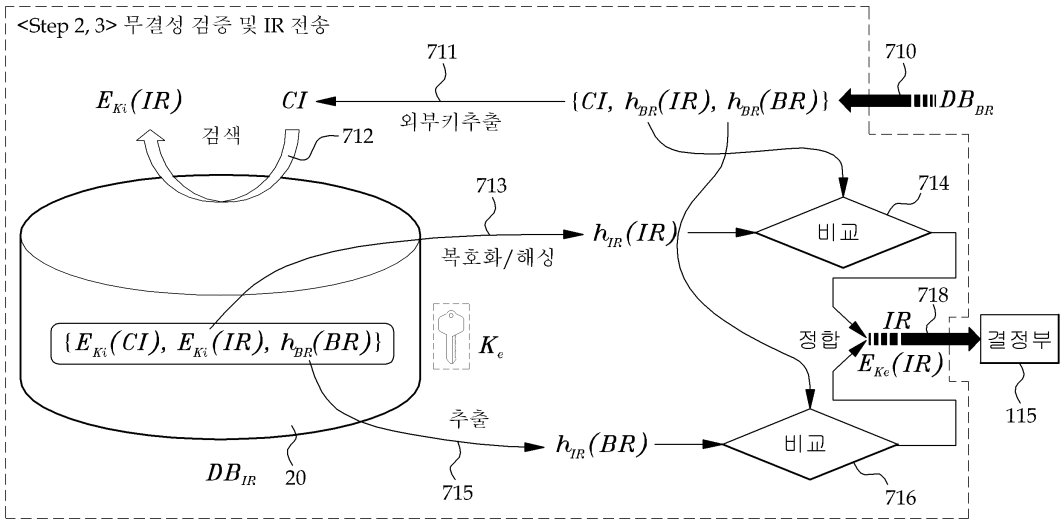
도면6b


<Step 2, 3> 무결성 검증 및 BR 전송
611
610
$\{CI, h_{IR}(IR), h_{IR}(BR), IDDB_{IR}, N_i\}$
$E_{Ke}(CI, h_{IR}(IR), h_{IR}(BR), IDDB_{IR}, N_i)$
DB_{IR}
복호화
$IDDB_{IR}$, N_i 검증
612
외부키 추출
613
615
616
617
정합
614
CI
$E_{Kb}(BR)$
BR
$h_{BR}(BR)$
비교
검색
BR 복원
해싱
618
BR
$E_{Ke}(BR)$
비교부
114
K_e
$\{E_{Kb}(CI), E_{Kb}(BR), h_{IR}(IR)\}$
21
DB_{BR}

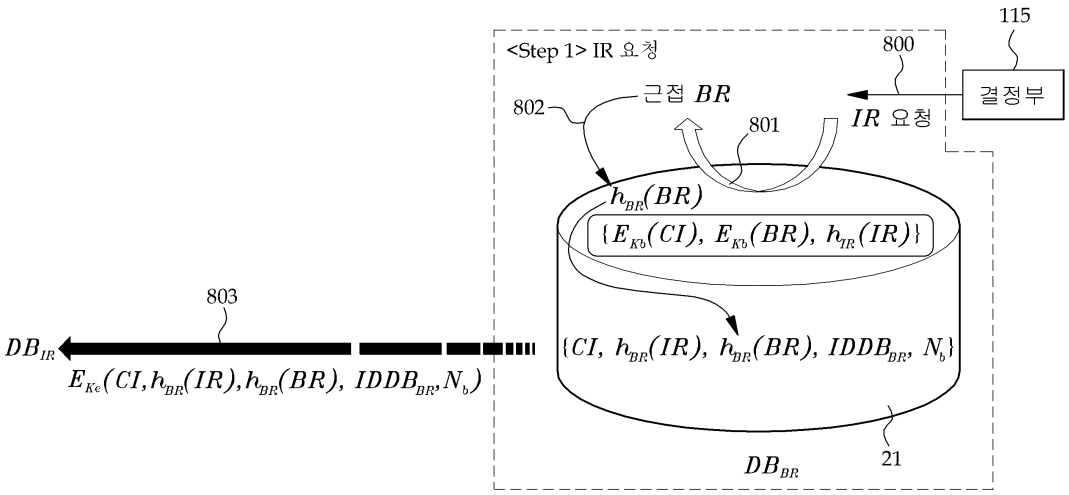
도면7a


<Step 1> IR 요청
<Step 1> IR 요청
700
결정부
근접 BR
701
IR 요청
115
702
703
DB_{IR}
$h_{BR}(BR)$
$\{CI, h_{BR}(IR), h_{BR}(BR)\}$
$\{E_{Kb}(CI), E_{Kb}(BR), h_{BR}(IR)\}$
DB_{BR}
21

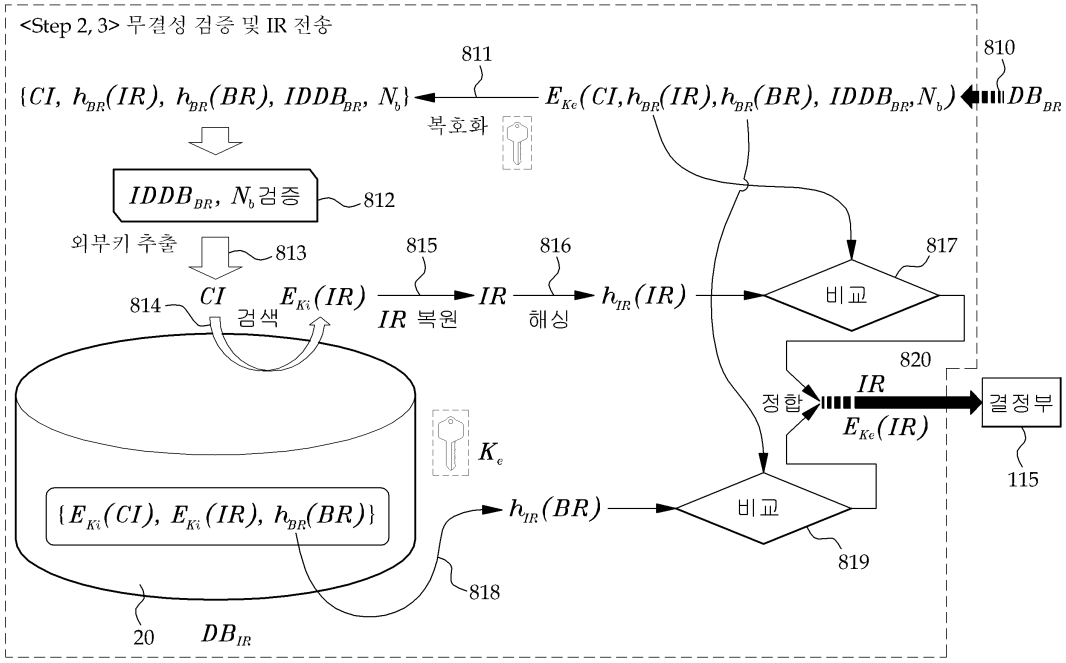
도면7b


<Step 2, 3> 무결성 검증 및 IR 전송
711
710
$E_{Ki}(IR)$
CI
$\{CI,\ h_{BR}(IR),\ h_{BR}(BR)\}$
DB_{BR}
외부키추출
검색
712
713
714
$h_{IR}(IR)$
비교
복호화/해싱
718
IR
정합
결정부
$\{E_{Ki}(CI),\ E_{Ki}(IR),\ h_{BR}(BR)\}$
K_e
$E_{Ke}(IR)$
115
추출
$h_{IR}(BR)$
비교
DB_{IR}
20
715
716

도면8a


115
<Step 1> IR 요청
800
결정부
802
근접 BR
IR 요청
801
$h_{BR}(BR)$
$\{E_{Kb}(CI),\ E_{Kb}(BR),\ h_{IR}(IR)\}$
803
DB_{IR}
$\{CI,\ h_{BR}(IR),\ h_{BR}(BR),\ IDDB_{BR},\ N_b\}$
$E_{Ke}(CI, h_{BR}(IR), h_{BR}(BR),\ IDDB_{BR}, N_b)$
DB_{BR}
21

도면8b


<Step 2, 3> 무결성 검증 및 IR 전송
811
810
{CI, h_BR(IR), h_BR(BR), IDDB_BR, N_b}
E_Ke(CI, h_BR(IR), h_BR(BR), IDDB_BR, N_b)
DB_BR
복호화
IDDB_BR, N_b 검증
812
외부키 추출
813
815
816
817
814
CI
E_Ki(IR)
IR
h_IR(IR)
비교
검색
IR 복원
해싱
820
정합
IR
E_Ke(IR)
결정부
115
K_e
{E_Ki(CI), E_Ki(IR), h_BR(BR)}
h_IR(BR)
비교
819
818
20
DB_IR