바이오인식 모델에 따른 프라이버시 침해위협 분석

윤성현 (백석대학교), 이형우 (한신대학교)

차 례

1. 바이오인식 모델

1.1 인증 및 식별

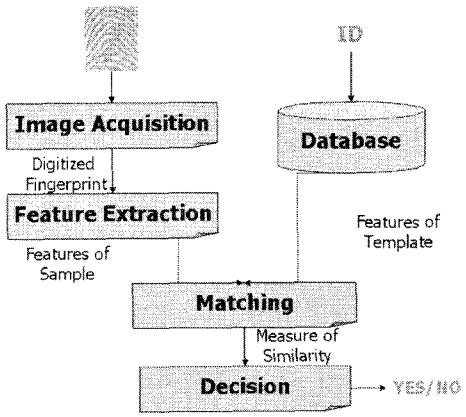
사람들은 이미 오래전부터 얼굴, 목소리 등의 신체적 특징을 이용하여 상대방을 구분해 왔다. 19세기 후반에 이미 사람의 지문을 이용하여 사용자 식별을 할 수 있는 방법이 만들어졌고, 이에 따라서 범인들의 지문을 데이터베이스(카드 파일)에 등록시키는 법안이 만들어졌다. 이렇게 만들어진 데이터베이스는 사건 현장의 지문을 이용하여 사용자를 식별하는 용도로 사용되었다. 이와 같이 바이오 정보를 이용한 사용자 인식은 주로 범인을 식별하는 용도로 사용되었는데, 최근에는 각종 사회적 영역에서 개인 식별 및 인증을 위한 수단으로 급속히 그 사용범위가 확장되고 있다.

바이오인식은 기술적으로 지문, 정맥, 홍채, 망막, 얼굴, 서명 및 음성 등 다양한 개인 고유의 정보를 추출하여 미리 등록되어있는 특징정보와 비교하기 위한 기술을 의미한다. 따라서 개인의 식별 혹은 인증을 위한 목적으로 주로 사용되고 있으며, 더 나아가서 접근제어를 위한 기술로 활용되고 있다.

바이오인식 시스템은 사용자의 원본정보를 추출하여 특징정보를 생성하고 이를 이용하여 데이터베이스에 저장된 특징정보들과 비교하는 패턴 인식 시스템이다. 이용목적에 따라서 바이오인식은 식별과 인증 모델로 구분된다.

(1) 인증 모델

[그림 1]은 지문을 이용한 인증 모델을 보여준다. 인증은 사용자 신분 확인을 위한 절차로 구성되는데 입력한 사용자 특징정보와 등록된 사용자 특징정보를 일대일로 비교하여 사용자를 인식하는 방법이다. 사용자는 바이오 정보와 더불어 주민등록번호, 사용자 이름, 스마트카드 또는 PIN 번호를 제출하고 시스템은 이를 이용하여 사용자 ID에 해당하는 특징정보를 데이터베이스에서 찾아 일대일로 특징정보들을 비교한다. 인증은 일반적으로 근태관리, 여권 심사 등과 같은 긍정적 인식에 사용된다. [그림 1]의 인증 모델의 구성요소 및 인증 절차는 다음과 같다.



▶▶ 그림 1. 인증 모델

• 원본정보 획득(Image Acquisition)

바이오 센서를 이용하여 사용자 지문을 캡춰하고 원본정보를 디지털 파일로 저장한다.

• 특징점 추출(Feature Extraction)

특징점 추출 단계는 센서로부터 입력된 원본정보를 가공하고 이를 이용하여 특징점을 추출하는 절차로 구성된다. 원본정보는 노이즈 제거, 지문 융선 복원, 세선화 등

이 논문은 2006년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2006-521-D00464)
교신저자: 윤성현(shyoon@bu.ac.kr)

의 작업을 거치며 가공된 이미지로부터 좌표 및 각도 정보를 갖는 특징점을 추출한다. 지문의 특징점은 지문 융선이 끝나는 단점과 갈라지는 분기점으로 구성된다. 특징점 정보들로 구성된 사용자 특징정보 파일을 생성한다.

• 매칭(Matching)

인식과정에서 취득한 특징정보와 데이터베이스에 저장된 특징정보를 비교하여 매칭 스코어를 산출한다. 매칭 스코어를 토대로 사용자에 대한 인증을 한다. 특징정보는 같은 사용자라도 매 번 인식과정에서 똑 같은 값을 얻을 수 없기 때문에 등록된 특징정보와의 유사도를 측정하는 방법으로 사용자를 인식하게 된다. 따라서 임계치(threshold value)에 따라 동일한 사용자인데도 인식이 안 될 수 있고 또는 다른 사용자가 오인식될 수 있는 경우가 발생한다. 이용 환경 및 목적에 따라서 임계치를 조정하여 보안성과 인식률 사이의 상반 관계를 조절해야 한다.

• 판단(Decision)

매칭 스코어를 토대로 사용자 인식이 성공했는지 실패했는지 결정한다.

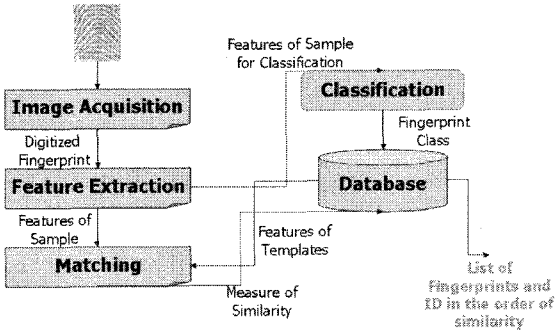
• 데이터베이스

등록된 사용자들의 특징정보를 저장하기 위한 용도로 사용된다.

(2) 식별(Identification)

[그림 2]는 식별 모델을 보여준다. 식별 모델은 사용자 식별을 위하여 데이터베이스에 저장된 모든 사용자들의 특징정보를 비교한다. 긍정적 인식에도 사용되지만 일반적으로 범죄 수사와 같이 부정적 인식에 주로 사용된다. 부정적 인식에서 시스템은 부인하고 있는 사용자가 누구인지 입증한다. 사용자가 여러 아이디를 사용하는 것을 방지한다. 인증 모델과 달리 일대다 비교를 통해서 사용자 신분을 알아내며 사용자 특징정보가 저장되어 있지 않으면 사용자를 식별할 수 없다.

식별은 사용 편의를 위해서 긍정적 인식에도 사용될 수 있다. 이 경우에 사용자는 신분 정보를 제출하지 않아도 된다. 긍정적 인식은 바이오정보 외에 주민등록번호, 키, 토큰 값들을 이용해야 하지만 부정적 인식은 바이오정보 만을 이용하여 수행될 수 있다. [그림 2]의 식별 모델의 구성요소 및 인증 절차는 다음과 같다.



▶▶ 그림 2. 식별 모델

• 원본정보획득

바이오 센서를 이용하여 사용자 지문 이미지를 캡춰하고 파일로 원본정보를 저장한다.

• 특징점 추출

특징점 추출 모듈은 센서로부터 입력된 원시 이미지를 가공하고 이를 이용하여 특징점을 추출한다. 특징점들의 좌표 및 각도 정보로 구성된 사용자 특징정보는 매칭 모듈과 분류 모듈로 전송된다.

• 분류(Classification)

데이터베이스에 저장된 특징정보들은 지문 유형에 따라서 색인되어 보관된다. 입력된 사용자 특징정보의 유형을 찾아내고 이와 비교할 데이터베이스의 특징정보들을 분류한다.

• 매칭

인식 과정에서 취득한 특징정보와 데이터베이스에 저장된 특징정보들을 비교하여 매칭 스코어를 산출한다. 매칭 스코어를 데이터베이스에 보낸다.

• 데이터베이스

등록된 사용자들의 특징정보를 저장하기 위한 용도로 사용된다. 매칭 모듈에서 보내온 매칭 스코어에 따라서 유사도 순으로 사용자 ID와 특징정보를 출력한다.

1.2 인증 및 식별 시스템 분류

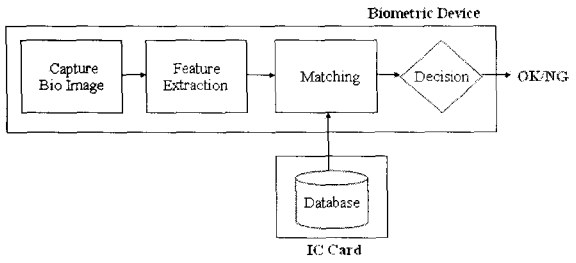
[표 1]은 특징정보를 어디에 보관하는가에 따라서 인증과 식별 시스템을 다섯 가지로 구분한다.

표 1. 인증 및 식별 시스템 분류

이용 목적	인식 모델	주요 특징	프라이버시 침해위협성	기타
인증	카드기반 인증 시스템	카드에 특징정보 저장	낮다	카드를 소지해야함
	Stand-Alone 인증 시스템	Stand-Alone 시스템에 특징정보 저장	보통	PIN번호를 기억해야함
	네트워크 기반 인증 시스템	인증서버에 특징정보 저장	높다	PIN번호를 기억해야함
식별	Stand-Alone 식별 시스템	Stand-Alone 시스템에 특징정보 저장	보통	
	네트워크 기반 식별 시스템	식별서버에 특징정보 저장	높다	

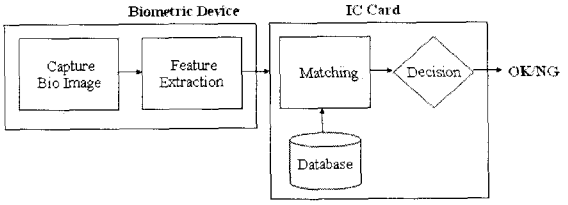
(1) 카드기반 인증 시스템

카드기반 인증 시스템은 [그림 3], [그림 4]와 같이 STOC(STore On Card) 모델과 MOC(Match On Card) 모델로 구분된다. 각각의 기능 및 특징에 대해서 살펴보면 다음과 같다.



▶▶ 그림 3. 카드기반 인증 시스템(STOC)

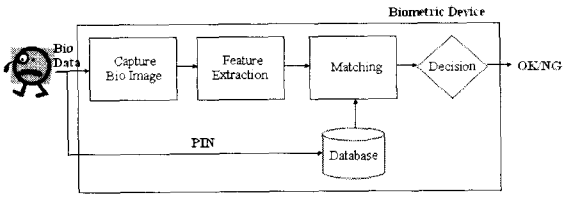
[그림 3]의 STOC 카드기반 인증 시스템은 IC 카드 또는 스마트카드에 사용자 특징정보를 저장하고 사용자 인식 시에 해당 카드를 바이오인식 장비에 접속시킨 다음에 사용자 인식을 수행하는 방식으로 진행된다. 바이오인식 장비는 사용자 원본정보를 캡춰하고 특징점을 추출하여 특징정보를 생성한다. 생성된 특징정보와 사용자 카드에 저장된 특징정보를 비교하여 맞는 사용자인지 확인한다. 특징정보는 한 번 도용되면 다시 재사용할 수 없는 치명적인 단점을 갖는다. 카드 기반 모델은 특징정보를 카드에 저장하여 사용자가 휴대할 수 있도록 한 것으로 특징정보에 대한 사용 책임을 사용자 자신에게 부여하는 특성을 갖는다. [그림 3]의 STOC 모델의 단점은 IC 카드로부터 바이오인식 장비에 사용자 특징정보가 전송된다는 것이다. 따라서 특징정보에 대한 보안을 IC 카드 뿐만 아니라 이를 받아서 처리하는 바이오인식 장비에 대해서도 고려해야 한다.



▶▶ 그림 4. 카드기반 인증 시스템(MOC)

[그림 4]는 MOC 카드기반 인증 시스템을 보여준다. 바이오인식 장비는 사용자의 바이오정보 캡춰와 특징점 추출 모듈로 구성된다. IC 카드는 사용자 특징정보 보관과 더불어 매칭 기능을 함께 수행한다. 바이오인식 장비는 센서로서의 역할만 수행하고 나머지는 IC 카드에서 처리하는 모델로 데이터베이스에 저장된 사용자 특징정보를 외부에 노출시키지 않는다는 측면에서 STOC 모델보다 특징정보에 대한 안전성이 높다. 하지만 이 경우도 바이오인식 장비에서 캡춰한 이미지로부터 생성된 특징정보를 IC 카드로 보내야 하기 때문에 이 구간에 대한 보안에 대해서 고려해야 한다.

(2) Stand-Alone 인증 시스템



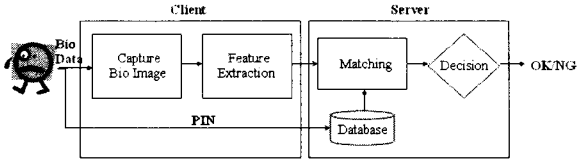
▶▶ 그림 5. Stand-Alone 인증 시스템

[그림 5]는 Stand-Alone 인증 시스템을 보여준다. 사용자는 먼저 자신의 특징정보를 등록 과정을 거쳐서 인증 시스템의 데이터베이스에 저장해야 한다. 연구소나 사무실의 출퇴근 근태관리 시스템에 적용될 수 있다. 사용자는 PIN(Personal Identification Number) 번호를 키 패드로 입력하고 바이오정보를 센서에 입력한다. 인증 시스템은 사용자의 바이오정보를 캡춰하고 이로부터

특징점을 추출하여 특징정보를 생성한다. 생성된 특징정보와 PIN 번호에 해당하는 등록된 사용자 특징정보를 데이터베이스에서 찾아 두 특징정보를 비교하여 정당한 사용자인지 인증한다.

Stand-Alone 인증 시스템은 데이터베이스에 여러 사용자들의 특징정보를 PIN 별로 저장해야 하고 바이오인식과 관련된 모든 프로세스를 한 곳에서 처리한다. 인증 시스템의 입력과 출력은 사용자 바이오정보와 사용자 인식 결과로 구성된다. 인식 과정에서 생성되는 특징정보 또는 데이터베이스에 저장된 특징정보가 외부로 노출되지 않는다. 따라서 인증 시스템에 대한 보안이 안전하다면 특징정보 노출에 대해서 카드 기반 인증 시스템보다 안전하다고 할 수 있다.

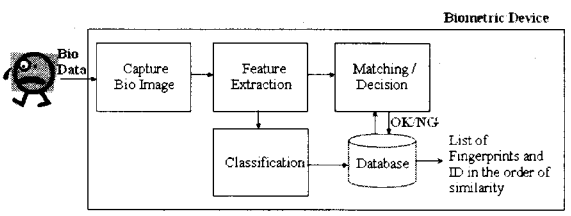
(3) 네트워크 기반 인증 시스템



▶▶ 그림 6. 네트워크 기반 인증 시스템

[그림 6]은 네트워크 기반 인증 시스템을 보여준다. 그림에서 보는 바와 같이 사용자 특징정보와 PIN 정보가 네트워크를 통해서 클라이언트에서 서버로 전송되며 서버에서 이를 가지고 데이터베이스에 등록된 사용자 특징정보를 비교하여 사용자 인식을 수행한다. 인터넷과 같은 공중망을 이용한다고 가정할 때에 특징정보 노출 위험이 가장 크다. 따라서 공중망으로 전송되는 사용자의 민감한 정보들은 노출의 위험에 대처하기 위해서 암호화 및 서명 등 정보보호 기법의 적용이 필수적이다.

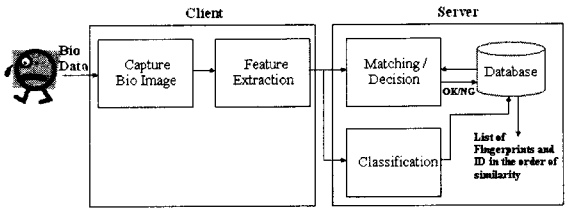
(4) Stand-Alone 식별 시스템



▶▶ 그림 7. Stand-Alone 식별 시스템

[그림 7]은 Stand-Alone 식별 시스템을 보여준다. 범죄 수사에서 사건 현장의 지문을 채취하여 범죄인 데이터베이스에 기록된 특징정보들과 비교하여 범인이 누구인지 식별하는 용도로 활용될 수 있다. Stand-Alone 식별 시스템은 사용자 바이오정보를 입력받아 이로부터 특징정보를 생성하고 데이터베이스에 저장된 특징정보들과 일대다로 비교하여 유사도가 높은 순으로 후보 특징정보들과 해당 사용자 ID를 출력한다.

(5) 네트워크 기반 식별 시스템



▶▶ 그림 8. 네트워크 기반 식별 시스템

[그림 8]은 네트워크 기반 식별 시스템을 보여준다. 등록된 사용자 특징정보들을 보관하고 있는 데이터베이스와 식별 시스템이 원거리에 있을 경우에 활용될 수 있는 시스템이다. 클라이언트 모듈은 사용자 바이오정보를 입력받아 이로부터 사용자 특징정보를 생성한다. 생성된 특징정보는 네트워크를 통하여 서버로 전송되며 서버에서 나머지 식별 과정을 수행하게 된다. 인터넷과 같은 공중망을 이용하여 사용자 바이오정보 또는 특징정보가 전송되어야 하기 때문에 클라이언트와 서버간의 안전한 통신 채널 설정이 필수적인 요구사항이다.

2. 프라이버시 침해위협 분석

2.1 바이오 인식 시스템에 따른 침해위협

(1) 카드기반 인증 시스템

카드기반의 인증 시스템은 특징정보를 카드에 저장하고 이를 사용자가 휴대하고 다니기 때문에 프라이버시 침해위협요소가 가장 낮다고 할 수 있다. 연구소나 회사에서 직원들의 근태관리 용도로 활용될 수 있으며 다음과 같은 시나리오를 가정해 보고 이에 대해서 분석한다.

1) 가정

- OO 연구소에서는 연구원 근태 관리를 위하여 출입문에 카드기반 바이오인식 시스템을 구축한다.
- 마루자는 OO 연구소 연구원으로 연구소 출입시에 IC 카드를 바이오인식장비에 접속하고 자신의 바이오정보를 센서에 입력한다.
- 사용자 인식이 성공하면 출입문이 열리며 누가 언제 연구소에 들어오고 나왔는지 중앙의 데이터베이스에 기록된다.

2) 분석

- 마루자의 특징정보는 IC 카드에 저장되어 있기 때문에 IC 카드를 잃어버리지 않는 한 특징정보 유출에 대해서 안전하다.
- IC 카드를 타인에게 양도하여 대리로 출퇴근할 수 없다. IC 카드를 바이오인식 장비에 접속하고 사용자의 바이오정보를 센서에 입력해야만 사용자 인증을 수행할 수 있다.
- 마루자의 출퇴근 기록 및 연구소에 있었던 시간 등이 데이터베이스에 저장된다. 따라서 데이터베이스 관리자 또는 마루자의 근태 기록을 참조할 수 있는 상사에 의해서 마루자의 행동 양식에 대한 분석이 가능해 프라이버시 침해가 예상된다.
- IC 카드를 분실하여 특징정보가 도용될 경우에 바이오정보의 특성상 다시 카드를 재발급 받을 수 없다. 본 시스템은 특징정보를 카드에 저장함으로써 특징정보에 대한 책임을 사용자에게 부여하고 있다. 마루자는 항상 카드 보관 및 관리에 대한 부담을 갖게 된다.
- IC 카드와 바이오인식 장비 간의 접속은 접촉식(유선) 또는 비접촉식(무선)으로 구분된다. STOC와 MOC 모델 모두 IC 카드의 사용자 특징정보를 전송하게 되는데 비접촉식인 경우에 사용 환경에 따라서 특징정보 노출로 인한 프라이버시 침해의 위험성이 접촉식인 경우에 비해서 높다.

(2) Stand-Alone 인증 시스템

Stand-Alone 인증 시스템에서 특징정보는 바이오인식 시스템에 저장되고 사용자는 PIN 값과 자신의 바이오정보를 이용하여 사용자 인증을 수행한다. 인증 시스템의 데이터베이스에 미리 사용자들의 바이오 특징정보가 등록되어 있고 사용자는 항상 자신의 ID, 즉 PIN 값을 기억하고 있어야 한다. 연구소 내의 특정 실험실에 대한 접근제어 등의 목적으로 활용될 수 있다. 다음과 같은 시나리오를 가정해 보고 이에 대해서 분석한다.

1) 가정

- OO 연구소내의 A 실험실은 인가받은 연구원만 출입할 수 있도록 Stand-Alone 바이오 인증 시스템을 구축한다.
- 마루자는 OO 연구소 연구원으로 A 실험실 출입 자격을 얻기 위하여 바이오정보를 인증 시스템에 PIN 값과 함께 등록한다.
- 마루자는 A 실험실에 들어가기 위해서 바이오인식 장비의 키 패드를 이용하여 PIN 값을 입력하고 자신의 바이오정보를 센서에 입력한다. 사용자 인식이 성공하면 출입문이 열리며 누가 언제 A 실험실에 들어오고 나왔는지 데이터베이스에 기록된다.

2) 분석

- 마루자의 특징정보는 바이오인식 장비에 저장되어 있기 때문에 IC 카드를 항상 휴대하고 다녀야 하는 부담이 없다.
- 마루자의 실험실 출입 기록은 데이터베이스에 저장된다. 따라서 데이터베이스 관리자 또는 실험실 관리자에 의해서 마루자의 출입 기록이 노출된다. 마루자는 실험실에 들어갈 때 마다 항상 감시당하는 느낌을 갖게 된다.
- Stand-Alone 시스템은 사용자 특징정보를 시스템 내부에 보관하기 때문에 시스템에 대한 보안이 안전하다면 특징정보 노출로 인한 프라이버시 침해에 대해서 안전하다고 할 수 있다. 하지만 시스템의 데이터베이스를 관리하는 관리자 또는 상급자에 의해서 특징정보 및 행위 기록이 노출될 위험이 있다.

(3) 네트워크 기반 인증 시스템

네트워크 기반 인증 시스템에서 특징정보는 서버에 저장되고 사용자는 PIN 값과 자신의 바이오정보를 클라이언트에 입력한다. 클라이언트는 서버에 사용자 데이터를

전송하고 서버에서 사용자 인증을 수행한다. 인증 시스템의 세 가지 모델 중 정보 노출에 대해서 가장 취약한 시스템이다. 클라이언트와 서버 간에 인터넷과 같은 공중망을 이용하여 데이터를 전송하기 때문에 암호 및 서명과 같은 정보보호 기술의 접목이 반드시 필요하다. 네트워크 기반의 인증 시스템은 인터넷 쇼핑몰 사업 등에 응용될 수 있다. 다음과 같은 시나리오를 가정해 보고 이에 대해서 분석한다.

1) 가정

- A 쇼핑몰은 디지털 콘텐츠 및 소프트웨어를 판매하는 업체로 라이센스 도용을 방지하기 위해서 콘텐츠 구매 및 실행 시 바이오정보로 사용자 인증을 수행하는 네트워크 기반의 인식 시스템을 구축한다.
- 마루자는 A 쇼핑몰의 데이터베이스에 사용자 바이오정보를 ID 정보인 PIN 값과 함께 등록한다.
- 마루자는 A 쇼핑몰에서 쇼팽의 야상곡을 다운로드 받는다. 전용 플레이어로 음악을 듣기 위해서 라이센스를 구매한다. 마루자는 먼저 노트북의 지문인식 센서로 지문 정보를 입력하고 PIN 값을 입력하여 A 쇼핑몰에 전송한다. A 쇼핑몰은 마루자의 신분을 인증하고 음악을 5 회 들을 수 있는 라이센스 키를 전송한다.
- 마루자의 구매 정보 및 라이센스 정보는 A 쇼핑몰 서버의 데이터베이스에 저장된다.

2) 분석

- 마루자의 특징정보는 A 쇼핑몰 서버의 바이오인식 시스템에 저장 된다. 온라인으로 바이오정보를 등록할 경우에 전송 중에 마루자의 바이오정보가 노출될 위험이 크다. 네트워크 기반 인증 시스템은 특징정보 보안 측면에서 상기한 모델과 비교하여 매우 취약하다.
- 마루자의 구매 정보, 개인 신상 정보 및 바이오정보 등은 A 쇼핑몰 서버에서 관리한다. 데이터 마이닝 기법 등 지능형 알고리즘을 이용하여 사용자의 구매 정보를 기반으로 사용자에 대한 구매 경향을 분석하며, 이 과정에서 다수의 개인정보에 대한 노출이 필연적으로 발생할 수 있다. 또한 쇼핑몰 회원들의 개인 정보 등을 제 3자에게 판매할 수 있는 위험이 있다. 마루자의 바이오정보와 연계되어 있는 기록들도 본인 동의 없이 이용할 가능성이 크다.
- 온라인에서 바이오정보를 이용한 사용자 인식은 카드기반, Stand-Alone 형태의 인증 시스템과 비교하여 프라이버시 침해 가능성이 매우 크다.

(4) Stand-Alone 식별 시스템

Stand-Alone 식별 시스템에서 특징정보는 바이오 식별 시스템의 데이터베이스에 저장된다. 식별은 입력된 사용자 바이오정보가 누구의 것인지 알아내는 것으로 데이터베이스에 저장되어 있는 특징정보들과 일대다로 비교하여 그 결과를 출력하는 시스템이다. 과학수사 연구소 등에서 사용될 수 있는 지문 식별 시스템이 한 예이다. 다음과 같은 시나리오를 가정해 보고 이에 대해서 분석한다.

1) 가정

- A 과학수사 연구소는 전과 기록이 있는 전과자들의 지문 특징정보를 전과 유형별로 분류하여 보관할 수 있는 지문 식별 시스템을 구축한다.
- 마루자는 사건 현장에서 채취한 지문을 A 과학수사 연구소에 보내고 범인 식별을 요청한다.
- A 연구소는 마루자가 보낸 지문과 사건 유형에 따라서 검색할 특징정보들을 분류한 후에 데이터베이스에 저장되어 있는 특징정보들과 비교를 수행한다. 유사한 지문 소지자들의 리스트를 마루자에게 보낸다.
- 마루자는 A 연구소로부터 온 용의자 리스트를 보고 수사의 범위를 좁혀 나간다.

2) 분석

- 식별은 시나리오에서와 같이 주로 부정적 인식에 사용된다. 전과자들의 바이오 특징정보는 항상 범죄 수사에 이용될 수 있도록 데이터베이스에 저장된다. 이러한 용도의 지문 식별 시스템은 데이터베이스에 저장된 특징정보 사용자들의 동의 없이 조회 및 비교가 수행될 가능성이 크다.
- 전과가 남게 되면 사용자 바이오정보가 데이터베이스에 등록되고 모든 범죄 수사에 데이터베이스가 이용된다. 이 경우에 사용자는 자신의 바이오정보

가 부정적 인식에 항상 사용되고 있다는 부담과 거부감을 지니고 평생을 살아야 한다. 또한 식별 시스템의 특성상 유사한 바이오정보를 갖는 사용자들은 용의자로 분류되어 자신과 무관한 사건에 마루자의 감시와 취조를 받게 될 수 있다.

- 지문 식별 시스템은 과학 수사 등 다양한 용도로 활용될 수 있지만 상기한 바와 같이 범법 행위를 한 사용자들의 인권 및 프라이버시를 침해할 수 있다.

(5) 네트워크 기반 식별 시스템

네트워크 기반 식별 시스템에서 특징정보는 바이오 식별 시스템 서버의 데이터베이스에 저장된다. 식별은 입력된 사용자 바이오정보가 누구의 것인지 알아내는 것으로 서버 데이터베이스에 저장되어 있는 특징정보들과 일대다로 비교하여 그 결과를 출력한다. 클라이언트는 사용자 바이오정보를 캡춰하고 특징정보를 생성하여 서버로 전송하는 역할을 한다. 클라이언트와 서버 간에 네트워크를 이용하여 민감한 정보를 주고받기 때문에 정보보호 기술의 접목이 필수적이다. 네트워크 기반 식별 시스템은 국가 간 과학 수사가 필요할 때 등과 같이 원거리에서 중앙의 식별 시스템을 사용하고자 하는 응용에 적합하다.

2.2 침해위협 비교 분석

바이오인식은 이용목적에 따라서 인증과 식별 시스템으로 구분되며 우리 생활의 여러 분야에 다양하게 응용되어 편리함을 가져다 줄 수 있는 기술이다. 하지만 본 절에서 살펴본 것과 같이 프라이버시 보호와 관련된 중대한 도전 과제들이 있으며 이에 대한 대응방안을 수립하는 것이 필요하다. 정보사회의 진보가 정보통신 기술의 발전에 따른 혜택인 반면, 앞서 살펴본 것처럼 의도적으로 악용된 개인정보 등 프라이버시와 관련된 문제는 신용사회와 정보사회의 전반적인 후퇴를 가져올 수도 있다.

프라이버시 보호는 어떤 이론적인 문제가 아닌, 실제 생활에서 이루어지는 개인의 정보 침해로 인해 제기되는 삶의 질에 관한 문제이다. 정보사회의 특징 가운데 하나는 기술 진보와 그 기술을 통한 생활환경의 개선이라고 할 수 있다. 그렇지만 기술에 의존하다 보면 기술 중심의 생활, 더 나아가 기술 우위의 사회문화가 형성될 것이다. 지문, 음성, 홍채, DNA 등 개인의 신체적인 특징에 의해 본인 여부를 확인하는 기술도 현재 다수 개발되어 있다. 그러나 무엇보다도 신체적 특징은 프라이버시 정보이기도 하기 때문에 이런 정보의 관리 방법에는 각별한 배려가 필요하다.

이용목적에 따라서 카드기반 인증 시스템, Stand-Alone 인증 및 식별 시스템, 네트워크 기반 인증 및 식별 시스템에서의 프라이버시 침해위협 요소들을 살펴보았다. 본 절에서는 특징정보 노출, 개인정보 이용, 감시, 사용 편의성 항목에 대하여 다섯 가지 시스템을 비교 분석한다. [표 2]는 다섯 가지 시스템에 대한 프라이버시 침해위협 요소를 비교한 결과이다.

표 2. 이용목적에 따른 프라이버시 침해위협 요소 비교

이용 목적	인식 모델	특징정보 노출	개인정보 이용	감시
인증	카드기반 인증 시스템	낮음 (사용자)	낮음	보통
	Stand-Alone 인증 시스템	보통 (사용자/관리자)	보통	보통
	네트워크 기반 인증 시스템	높음 (사용자/관리자/제3자)	높음	높음
식별	Stand-Alone 식별 시스템	보통 (사용자/관리자)	보통	보통
	네트워크 기반 식별 시스템	높음 (사용자/관리자/제3자)	높음	높음

1) 특징정보 노출

사용자 특징정보가 노출되면 바이오정보의 특성상 재사용할 수 없게 된다. 따라서 특징정보에 대한 안전성 확보는 매우 중요하다. 카드 기반 시스템은 특징정보를 사용자가 휴대 및 관리하기 때문에 사용자 자신이 특징정보에 대한 안전을 책임진다. Stand-Alone 시스템은 사용자와 시스템 관리자가 특징정보에 접근할 수 있고 네트워크 기반 시스템은 사용자, 시스템 관리자뿐만 아니라 해커와 같은 제3자의 위협도 고려해야 한다.

2) 개인정보 이용

바이오인식 시스템의 용도에 따라서 사용자 개인 정보를 본인의 동의 없이 상업적으로 이용할 수 있는데 이에 대한 위험 정도를 비교한다. 카드 기반 시스템은 주로 출퇴근 관리 등 소규모 응용에 사용되기 때문에 개인정보의 상업적 이용에 대한 위험은 상대적으로 낮다. 네트워

크 기반의 시스템은 대량의 사용자 특징정보 데이터베이스를 요구하는 응용이 많기 때문에 개인정보의 상업적 이용 위험이 매우 높다.

3) 관리자에 의한 감시

바이오인식 및 식별 시스템 관리자가 사용자들의 모든 기록을 이용하여 원하는 용도에 맞게 가공하여 해당 사용자들을 감시하는 경우의 위험에 대해서 분석한다. 카드 기반 시스템과 같이 응용이 제한적인 경우에는 침해 위협이 상대적으로 낮다고 할 수 있으며 Stand-Alone 시스템, 네트워크 기반 시스템과 같이 응용 분야가 많은 경우에 직원들에 대한 감시 목적으로 활용될 가능성이 높다. 특히 네트워크 기반 시스템의 경우에 전자상거래와 같이 대용량 데이터베이스를 이용하는 응용에서는 데이터 마이닝 알고리즘 등을 이용하여 사용자 정보를 보다 세밀하게 분석하여 상업적 또는 정치적으로 이용할 수 있는 위험성이 매우 높다.

4) 사용 편의성

사용자가 인식 및 식별 시스템을 얼마나 쉽게 사용할 수 있는가에 대해서 분석한다. 카드 기반 시스템은 항상 카드를 휴대하고 있어야 하고 없을 경우에 바이오인식 시스템을 사용할 수 없기 때문에 사용 편의성이 가장 낮다고 할 수 있다. Stand-Alone 및 네트워크 기반 인증 시스템은 바이오정보 외에 ID 정보를 기억하고 입력해야 한다. 식별 시스템은 바이오정보만 제공하기 때문에 상대적으로 사용 편의성이 가장 높다고 할 수 있다.

3. 결론 및 대응방안

인증 및 식별 시스템 모두 특징정보 보호가 가장 중요한 프라이버시 이슈가 된다. 바이오정보는 고유하기 때문에 한 번 도용되면 재사용할 수 없는 특성이 있기 때문이다. 앞서 살펴본 바이오 인식 시스템에서의 특징정보 보호 방법과 기타 위험 요소에 대한 대응 방안을 살펴본다.

(1) 인증 시스템

카드기반 인증 시스템은 STOC(STore On Card) 모델과 MOC(Match On Card) 모델로 구분된다. [그림 3]의 STOC 모델은 특징정보가 IC 카드에 저장되며 나머지 바이오인식 프로세스는 장비에서 수행된다. [그림 4]의 MOC 모델은 특징정보와 매칭 프로세스가 IC 카드에 저장된다. 특징정보 유출은 카드를 분실한 경우와 바이오인식 장비를 통해서 가능하다. 카드기반 시스템은 본인의 특징정보에 대한 보호를 본인이 책임지도록 함으로써 Stand-Alone 시스템 또는 네트워크 기반의 시스템에서처럼 특징정보를 보관하는 서버 또는 관리자를 신뢰해야 하는 부담을 덜어준다. 카드분실시의 특징정보 보호를 위해서는 취소가능한 특징정보를 생성하고 보관하는 방법이 필요하며 카드내의 저장소에 대한 불법적인 읽기 및 쓰기 동작이 수행되면 저장 장치를 지우거나 또는 카드 자체를 사용할 수 없도록 하는 등의 기술적인 방법이 필요하다(tamper-proof device). 카드는 접촉식 또는 비접촉식으로 바이오인식 장비와 접속되는데 비접촉식인 경우에 특징정보 전송 중에 가로채기의 위험이 높다. 따라서 카드에 저장되어 있는 특징정보 전송시에 암호화 등 정보보호 기법의 적용이 필요하다. 바이오인식 장비는 원본정보를 캡춰하여 특징정보를 만들고 사용자 카드의 특징정보를 읽어들여 두 값을 비교한다. 사용자 원본정보 및 특징정보를 처리하기 때문에 장비 설계 및 구현시 사용자 바이오정보에 대한 노출을 최소화할 수 있도록 고려해야 한다.

[그림 5]의 Stand-Alone 인증 시스템과 [그림 6]의 네트워크 기반 인증 시스템은 먼저 사용자 자신의 특징정보를 등록하는 과정을 거쳐서 인증 시스템의 데이터베이스에 특징정보를 저장해야 한다. 등록 과정에서 사용자 신분 확인을 위한 절차가 필요하며 로컬 또는 네트워크에 위치한 데이터베이스에 특징정보를 안전하게 저장 및 관리할 수 있는 방법이 필요하다. 카드기반 시스템과 마찬가지로 특징정보는 취소가능한 특징정보로 만들어서 보관해야 한다. 특징정보를 관리하는 데이터베이스에 대한 보안이 필수적이며 관리자에 의한 정보 유출 등을 방지하기 위해서 공개키 암호 기법 등을 적용한 특징정보 암호화 및 서명 등의 기술이 필요하다. 인증 시스템은 일대일로 특징정보를 매칭하여 사용자 인식을 하는 과정이기 때문에 데이터베이스의 사용자 정보를 가져오기 위해서 PIN 번호가 필요하다. PIN 번호 및 취소가능한 특징정보 생성 및 추출시 필요한 패스워드 정보는 노출되지 않도록 정기적으로 변경하고 키패드로 입력시 트로이목마 등의 악성코드에 의한 유출을 방지하기 위한 키보

드 보안 프로그램의 적용이 필요하다.

(2) 식별 시스템

[그림 7]의 Stand-Alone 식별 시스템과 [그림 8]의 네트워크 기반 식별 시스템은 인증 시스템과 마찬가지로 먼저 사용자 자신의 특징정보를 등록하는 과정이 필요하며 식별 시스템의 데이터베이스에 특징정보가 저장된다. 특징정보는 취소가능한 형태로 변환하여 보관해야 하며 이를 관리하는 데이터베이스에 대한 보안이 필수적이다. 특히 식별 시스템은 부정적 인식에 주로 사용되기 때문에 식별 데이터베이스는 상급 기관에 의한 감시 및 조회 용도로 사용자 동의 없이 이용될 가능성이 높다. 관리자에 의한 데이터베이스 내용 공개 및 배포 등을 방지할 수 있는 기술적 대응 방안이 필요하다.

(3) 기타 대응 방안

프라이버시 침해위협에도 불구하고 바이오인식은 사용자 인증 및 식별을 위한 응용에 많은 장점을 제공하기 때문에 막연히 바이오정보의 이용을 반대할 것이 아니라 적극적으로 위험요소를 진단하고 이에 대한 대응 방안을 마련하여 폭 넓게 활용할 수 있도록 해야 한다. OECD에서 권고하고 있는 프라이버시 보호를 위한 바이오인식 시스템 설계 및 구현 지침을 살펴보면 다음과 같다.

- 시스템 설계 및 구현은 공개적으로 이루어져야 하며 각계 각층으로부터 의견을 수렴해야 한다.
- 바이오인식 장비를 사용하는 사용자에 대한 적합한 수준의 감독 기능을 제공해야 한다.
- 사용자 실수 또는 오류로 인한 사고 발생시에 다시 원래대로 복원할 수 있는 절차를 보장해야 한다.
- 바이오인식 시스템 모듈은 보안과 프라이버시를 지원할 수 있어야 하며 원본정보 또는 특징정보를 이용하여 사용자 개인정보를 노출해서는 안 된다.
- 대규모 시스템을 설계 및 구현하기에 앞서서 소규모 시스템을 먼저 만들어서 충분히 시험하여 성능 및 보안에 대해서 보장할 수 있어야 한다.
- 바이오인식 성능을 최대화하고 프라이버시 문제를 최소화하기 위해서는 일대다 비교 방식인 식별 시스템보다 일대일 비교를 하는 인증 시스템에 집중해야 한다.
- 원본정보는 반드시 사용자의 동의를 구해서 공개적으로 추출되어야 한다.
- 가능하다면 특징정보는 중앙의 데이터베이스에 보관하지 말고 스마트카드 또는 토큰에 저장해서 사용자가 소지할 수 있도록 한다.

OECD 설계 및 구현 지침에 따르면 프라이버시 측면에서 인증보다는 식별이 매우 취약한 것으로 나타난다. 식별은 데이터베이스에 저장된 사용자들의 특징정보를 검색하여 유사한 정보를 갖는 사용자들의 ID 정보를 제공한다. 검색 과정에서 관련없는 사용자들의 특징정보가 읽혀지고 비교되는데 이러한 경우 대부분 해당 사용자들의 동의 없이 이루어지게 된다. 또한 유사한 정보를 갖는 사용자들의 ID와 특징정보가 결과물로 제공되는데 이 경우에도 식별 대상자가 아닌 사용자들의 개인정보가 노출되게 된다. 상기한 바와 같이 식별 시스템은 그 특성상 프라이버시 침해위협을 내재하고 있다. 범죄 수사, 테러리스트 식별 등 부정적인 응용에 주로 사용되며 전과자들과 같은 사회적 소외 계층에 대한 프라이버시가 보장되지 않는다.

따라서 OECD 지침에도 언급된 바와 같이 바이오인식 시스템의 사회적 적용은 사용자 인증에 초점을 두고 개발되어야 할 것이며, 프라이버시 보호를 위해서 카드 기반의 인증 시스템이 가장 적합할 것으로 판단된다. Stand-Alone 시스템 또는 네트워크 기반 시스템은 중앙의 데이터베이스를 필요로 하기 때문에 특징정보의 보관 및 관리가 매우 중요하다. 특히 네트워크 기반 시스템은 바이오인식 프로세스가 분산되어 있기 때문에 프로세스 상의 모든 구간에 대해서 침해위협 요소를 정의하고 이에 대한 대응 방안을 마련해야 한다.

사용자 인증은 인터넷 기반의 전자상거래, 선거, 전자정부 구축을 위해서 필수적인 요구사항 중 하나이다. 대면할 수 없는 상황에서 본인임을 입증할 수 있는 가장 적합한 방법이 바이오인식이다. 지금까지는 카드 기반, Stand-Alone 형태의 인증 시스템이 주로 개발되고 있지만 상기한 바와 같이 폭 넓은 활용을 위해서는 앞으로 네트워크 기반의 바이오인식 시스템에 대한 연구가 필수적이다.

참고문헌

[1] Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition,," IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image and Video Based Biometrics, Vol. 14, No. 1, January 2004.

[2] N. K. Ratha et al., "Enhancing security and privacy in biometric-based authentication systems," IBM System Journal, Vol.40, No.3, 2001.

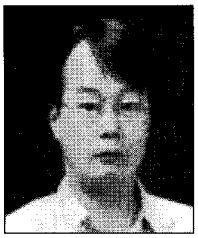
[3] Kresimir Delac, Mislav Grgic, "A SURVEY OF BIOMETRIC RECOGNITION METHODS," 46th International Symposium Electronics in Marine, ELMAR-2004, 16-18 June 2004.

[4] "Report on International Data Privacy Laws and Application to the Use of Biometrics in the United States," www.nationalbiometric.org, National Biometric Security Project Publication 0205, 2006.3.

[5] "Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities," Safeguards in a World of Ambient Intelligence (SWAMI), http://swami.jrc.es, Information Society Technologies, 2006.1.

저자소개

● 윤 성 현(Sung-Hyun Yun) 정회원



- 1994년 2월 : 고려대학교 컴퓨터학과 일반대학원(이학석사)
- 1997년 2월 : 고려대학교 컴퓨터학과 일반대학원(이학박사)
- 1998년 3월 ~ 2002년 2월 : LG 전자/정보통신 중앙 연구소 선임연구원
- 2002년 3월 ~ 현재 : 백석대학교 정보통신학부 조교수

<관심분야> : 콘텐츠 보호, 바이오인식, 정보보호

● 이 형 우(Hyung-Woo Lee) 정회원

- 1996년 2월 : 고려대학교 컴퓨터학과 일반대학원(이학석사)
- 1999년 2월 : 고려대학교 컴퓨터학과 일반대학원(이학박사)
- 1999년 3월 ~ 2003년 2월 : 천안대학교 정보통신학부 조교수
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터정보학부 부교수

<관심분야> : 네트워크 보호, 정보보호, 바이오 정보보호