생체정보보호를 위한 연구

신용녀*,이동근*,최진영**
*한국정보보호진흥원
**고려대학교 컴퓨터공학과
e-mail:ynshin@kisa.or.kr

A Study on Biometric Template Protection Procedures

Yong-Nyuo Shin*, Dong-Gun Lee*, Jin-Young Choi**
*Korea Information Security Agency
**Dept of Computer Science and Engineering, Korea University

요 약

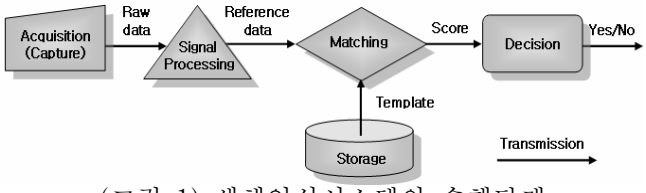
정부의 민원서비스등 다양한 용도로 개방 환경에 생체인식시스템이 구축될 수 있는 가능성이 많아졌다. 본 고에서는 생체인식시스템이 구축될 때 발생할 수 있는 취약점을 정의 해 보고 이를 해결하기 위한 기술적 가이드라인을 제시한다. 한번 유출된 생체정보에 대한 피해의 심각성이 크기 때문에, 가능한 모든 공격에 대해서 강인성(Robust)을 가져야 하는 반면에 생체정보 변형에 따른 복잡성은 성능에 현격한 저하가 없어야 한다.

1. 서론

최근 학교 급식시설이나 회사의 직원 근태 관리의 일환으로 생체인식시스템의 이용이 확산되고 있으나 인권침해의 논란과 더불어 생체정보 보호에 대한 관심과 요구가 증대되고 있다. 물론 이러한 논란을 제거하기 위해서는 합의에 의한 제도적 장치의 마련이 시급하지만 이를 위해 개인정보보호의 사회적 요청에 대응할 수 있는 정보보호 기술 개발이 필수적이라 하겠다. 본 고에서는 생체인식시스템이 구축될 때 발생할 수 있는 취약점을 정의하고 이를 대비하기 위한 기술적 가이드라인을 제시하고, 이를 해결하기 위해 필요한 기술적 연구를 논하고자 한다.

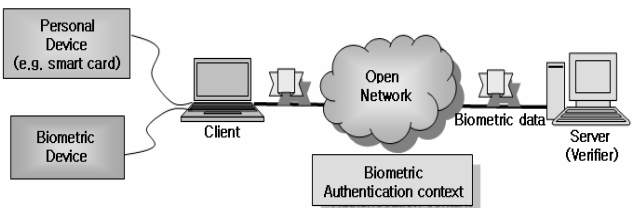
2. 생체인식시스템 구성요소와 취약점

개인의 생체정보는 영원히 변하지 않는다는 것이 프라이버시 문제의 시작이다. 즉, 한번 유출된 생체정보에 대한 피해의 심각성이 크기 때문에, 가능한 모든 공격에 대해서 강인성(Robust) (다양한 입력 장치를 고려한 환경 변화 및 주위 잡음 그리고 연령 및 세월의 변화에 강인함)을 가져야 하는 반면에 생체정보 변형에 따른 복잡성은 성능에 현격한 저하가 없어야 한다. 일반적인 생체인식 시스템의 처리 단계는 다음의 (그림 1)과 같다. 센서 등의 생체 디바이스에서 생체정보를 획득한 후 신호처리를 통하여 특징을 추출하는 단계가 공통적으로 포함된다. 이를 기반으로 사전에 동일한 단계를 통하여 변환되어 저장된 데이터베이스 내의 생체정보와 비교하여 결과를 결정하는 단계로 구성된다.



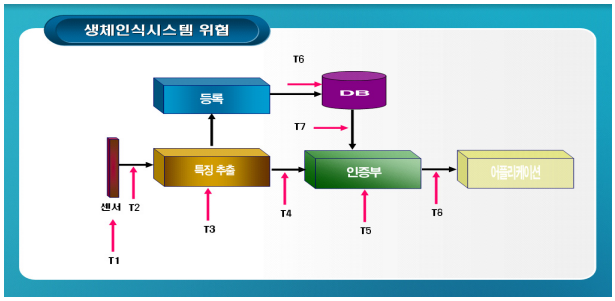
(그림 1) 생체인식시스템의 수행단계

네트워크망을 통한 생체인식 시스템은 (그림 2)와 같으며 클라이언트에서는 개인의 정보와 생체정보를 획득하여 위에서 설명된 생체인식 단계가 탑재된 서버로 전송하는 구성도를 나타낸 것이다.



(그림 2) 생체인식시스템의 수행단계

상기에 설명된 생체인식 시스템의 처리 단계에서 해킹 등의 원인으로 인하여 정보보호에 취약성이 노출되는 부분을 도식화하면 (그림 3)과 같다.



(그림 3) 생체인식시스템의 취약점

각 부분별 취약성(Treat)을 나타내면 다음과 같다.

T1 : 센서 등을 통하여 위·변조된 생체 데이터가 입력되는 경우

T2 : 입력된 생체 데이터를 처리하기 이전에 가로채는 경우

T3 : 공격자에 의해 생성된 특징 값이 선택되는 경우

T4 : 공격자에 의해 진짜의 특징 값이 다른 값으로 대체되는 경우

T5 : 유사도에 대한 결과 값을 변경하는 경우

T6 : 데이터베이스에 저장된 템플릿에 대하여 가감, 변경하는 경우

T7 : 저장된 템플릿을 변경하는 경우

T8 : 인증 결과를 변경하는 경우

3. 생체정보 획득과정 보호

생체데이터를 취급하는 시스템에 있어서 사용자로 하여금 처음 생체데이터를 입력받는 작업은 매우 중요하다고 할 수 있다. 가장 최초로 입력되는 사용자의 생체데이터의 품질이 어떠한가에 의해 생체데이터를 취급하는 전체 시스템의 성능이 결정되기도 하기 때문에 생체데이터를 획득하는 디바이스에 대한 보호는 매우 중요하다고 할 수 있다. 또한 이렇게 취득된 생체데이터는 사용자의 개인정보로 취급 될 수 있는 얼굴이나 지문, 홍채, 음성 등과 같은 중요한 생체 원본 데이터이기 때문에 외부로의 유출되어 인가되지 않은 곳에 무단으로 사용되거나 또는 부정적인 방법으로 원래 획득되어야 할 데이터가 아닌 다른 데이터가 사용되거나 할 수 있는 요소들이 있어 이러한 디바이스에 대한 보호는 반드시 이루어 져야 한다.

3.1 취약점 포인트

(1) 비 인가된 불법 디바이스에 의해 사용자의 원본 생체데이터가 아닌 조작된 생체데이터가 입력되어 질 수 있다.

(2) 획득되어지는 생체 데이터가 라이브 데이터가 아닌 모조지문이나 얼굴 사진, 녹음기 등을 통한 가짜 정보가 입력되어 질 수 있다.

(3) 디바이스로부터 획득된 데이터가 안전한 전송이 되어지기 전에 외부로부터 침입을 당해 유출되어 질 수 있다.

(4) 디바이스 오작동에 의해 잘못된 데이터가 획득되어 질 수 있다.

(5) 취약점 포인트 T1에 해당한다고 볼 수 있다.

3.2 보호를 위한 가이드라인

(1) 생체인증 시스템은 현재 사용되고 있는 디바이스에 고유한 값을 저장해 두거나 하는 방법을 이용해 사용하기 전에 그 값을 검사해 디바이스가 다른 외부의 누군가에 의해 교체된 것이 아닌지를 확인 할 수 있는 기능이 제공되어져 비 인가된 불법 디바이스가 사용되는 것을 막을 수 있어야 한다.

(2) 디바이스 또는 생체인증 시스템은 현재 입력된 데이터가 실제 사용자에 의해 입력된 라이브 데이터인지를 알 수 있는 방법을 제공하여야 하며 라이브 데이터가 아닌 경우에는 데이터 입력을 받지 않거나 획득된 데이터를 무시 할 수 있어야 한다. 지문인식 디바이스의 경우 입력되는 지문에 미세한 전류를 흘려 실제 사람 손가락인지를 확인하거나 적외선을 통한 라이브 지문 확인 등의 방법을 사용 할 수 있으며 얼굴인식의 경우 획득되어진 얼굴 이미지의 변형되는 모양을 분석하여 실제 사람에 의한 데이터인지 또는 사진과 같은 모조 데이터인지를 구분할 수 있는 방법 등을 제공하고 있다. 디바이스 차원에서 실제 라이브 생체 데이터인지를 판별하는 기능을 가지도록 하는 것이 바람직하며, 보안성을 높이기 위해서는 라이브 데이터가 아닐 경우에는 획득조차 하지 않도록 해야 한다.

(3) 생체 데이터를 획득하는 디바이스는 외부로부터 안전하게 보호받을 수 있는 형태로 구성되어야 하며 외부의 분해나 조작 등으로부터 쉽게 노출되지 않는 형태로 만들어 져야 한다. 또한 외부의 침입으로부터 안전한 곳에 디바이스가 설치되도록 하여야 한다.

(4) 생체인증 시스템은 현재 사용되고 있는 디바이스가 정상적으로 동작중인지를 항상 검사할 수 있도록 하는 기능을 제공해 디바이스의 오작동 여부를 탐지 할 수 있도록 하는 것이 좋다.

4. 생체정보 전송 과정 보호

디바이스로부터 입력된 생체데이터는 그 생체데이터를 처리할 생체인증 시스템으로 안전하게 전송되어

져야할 필요가 있다. 생체획득 디바이스로부터 정확한 데이터가 입력되었다 하더라도 디바이스가 획득된 생체데이터를 인증시스템에 전송하는 중에 오류가 발생하거나 다른 외부적인 침입에 의해 다른 데이터로 바뀌어 진다면 생체데이터 보호에 심각한 문제를 일으킬 수 있다. 특히 생체데이터 입력 디바이스가 인증 시스템과 멀리 떨어져 있어 네트웍 등과 같은 통신망을 이용해 전달되거나 블루투스와 같은 무선 통신을 통해 전달될 경우 전송에 있어 보호조치가 마련되어야 한다. 또한 생체데이터는 개인의 프라이버시를 침해 할 수 있는 개인정보에 해당하기 때문에 디바이스로부터 얻어진 생체데이터가 다른 곳으로 불법 유출되는 문제에 대한 보호도 반드시 필요하다고 할 수 있다.

4.1 취약점 포인트

(1) 디바이스로부터 입력되어진 데이터가 정상적으로 인증시스템에 전송되지 않고 외부로부터 가공되어 만들어진 가짜 생체데이터를 전송해 인증 할 수 있다.
(2) 디바이스로부터 입력되어진 데이터가 인증시스템에 전송 중 외부 침입자에 의해 가로채어져 다른 부정적인 용도로 사용되어 질 수 있다.
(3) 데이터 전송상의 오류로 인해 전송되어진 데이터가 손상되어 인증을 방해 할 수 있다.
(4) 취약점 포인트 T1에 해당한다고 볼 수 있다.

4.2 보호를 위한 가이드라인

(1) 디바이스로부터 넘어오는 데이터에 대해 무결성 검사를 통해 안전한 데이터가 전송되어져 왔다는 것을 알 수 있는 방법을 제공하여야 한다. 이를 위해 디바이스에 특정 암호화 키를 제공하고 디바이스는 획득된 생체정보를 전달받은 암호화 키를 이용해 암호화 해 전송하는 방법 등을 사용 할 수 있다. 이렇게 할 경우 외부에 의해 다른 데이터가 들어오더라도 암호화 방식이 다름으로 인해 인증시스템에 영향을 주지 않게 된다. 무선 통신을 통한 전송일 경우 반드시 무선 통신에 적합한 암호화 방식을 사용해 전송되는 데이터를 보호하는 것이 필요하다. 또한 디바이스와 생체인증 시스템간의 전송되는 라인이나 방식이 외부의 물리적 침해로부터 안전하게 보호되어져야 하며, 다른 곳으로 유출되더라도 사용할 수 없도록 해야 한다.
(3) 전송되어지는 데이터의 유효성을 판별 할 수 있는 기능이 필요 할 수 있다. 전송상의 데이터 오류를 검출하기 위한 작업이 수반되어질 수 있고 해쉬 함수와 같은 암호화 기법을 이용해 전송된 생체 데이터가 손상되지 않았음을 확인 할 수 있는 방법이 제공되어야 한다.

5. 생체 데이터베이스 보호

생체정보는 개인의 프라이버시 유출과 직결될 수 있기 때문에 수집, 보관, 탐색, 접근 제한 등이 기존 DB와는 다른 방식으로 관리 정책이 수립되어야 한다. 생체인식을 위한 이미지부터 추출된 템플릿, 매칭 결과 등 어느 하나의 데이터 보호에도 소홀해서는 안된다. 생체정보가 전혀 포함되지 않은 매칭 결과조차도 개인 프라이버시 보호 차원에서 보호되어야 한다. 생체데이터가 저장되는 데이터베이스는 개인정보를 저장하는 데이터베이스와 물리적으로도 분리되어 있어야 하며 인가된 사용자에 의해 해당 인터페이스로만 생체데이터 DB에 접근할 수 있도록 하는 DB 보안기능이 필요하므로 다음과 같은 보호조치가 요구된다.

5.1 생체 정보의 수집

프라이버시보호를 위해서는 생체데이터 수집 단계부터 기술적·관리적 조치를 취해야 한다. 생체데이터 데이터베이스를 개인정보 데이터베이스와 물리적으로도 분리하고, 생체데이터를 유일한 식별자로 사용해서는 안되며, 생체정보를 포함한 개인의 모든 정보 수집을 최소화 하여야 한다. 생체 데이터가 유일한 식별자로 사용되어 다양한 데이터베이스로부터 개인 정보가 수집될 수 있는 취약점이 있다.

5.1.1 보호를 위한 가이드라인

(1) 생체정보는 일반적으로 유일한 식별자로서 사용되어서는 안된다. 생체정보는 적절한 장소에서 높은 보안 강도로 보호되어야 하며, 생체정보가 유일한 식별자로 사용되어서는 안된다. 일반적으로 유일한 식별자는 다양한 데이터베이스로부터 개인 정보 수집을 용이하게 한다. 오용 되었을 경우 프라이버시 보호에 심각한 위협이 될 수 있다.
(2) 생체정보를 포함한 개인의 모든 정보 수집은 제한되어야 한다. 생체인식 시스템에서 식별과 검증을 위해 필요한 최소한의 정보를 제외하고는 생체정보가 아닌 정보에 대해서도 최소한의 정보만이 수집되고 저장되어야 한다. 대부분의 시스템에서 개인 정보는 생체정보와는 독립적으로 이미 존재하고 있다. 이러할 경우는 생체정보를 수집할 때 중복적으로 개인정보를 수집하지 않는 것이 바람직하다.

(3) 조작 가능성에 따라 생체인식시스템은 생체정보 제공자가 얼마간은 익명으로 등록할 수 있도록 디자인되어야 한다. 웹 환경에서 개개인은 이메일이나 사용자이름으로 식별할 수 있도록 되어 있다. 사용자가 자신임을 주장 하는것을 검증할 수 있는 한 생체인식 시스템이 누구와 상호작용하고 있는지를 알 필요는 없다.

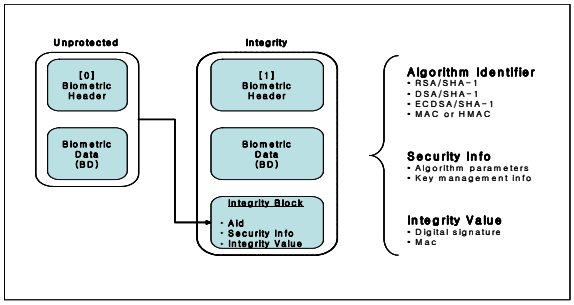
(4) 생체 정보는 이름, 주소, 의료 정보, 금융 정보와 같은 개인 정보와 분리되어 저장되어야 한다. 생체 데이터의 저장 방식에 따라 이 분리는 논리적일 수도 있고 물리적일 수도 있다.

5.2 데이터베이스 조작 및 변조에 대한 대처 방안

인가된 사용자가 인위적인 목적이나 무의식적인 실수 등으로 DB에 저장된 생체 데이터를 조작, 변경하는 경우나 인가되지 않은 사용자가 DB에 접근하여 악의적인 목적으로 생체 데이터를 조작 및 변조할 경우 시스템 인증 결과에 대한 문제뿐만 아니라 변경된 생체 데이터를 악용할 소지가 있으므로 등록된 생체 데이터는 조작이나 변경이 불가능하도록 하는 방안이 필요하다. 취약점 포인트 T6, T7에 해당한다고 볼 수 있다. 생체데이터는 센서 등을 통한 입력 후에 각 단계를 수행하면서 특징 데이터 등으로 변환된다. 이렇게 각 단계별로 진행될 때 공격자 등에게 노출되어 데이터의 내용이 변조될 수 있다. 이에 각 단에서는 변조되지 않은 원본 데이터가 도착했는지를 검사하는 방법이 필요하다.

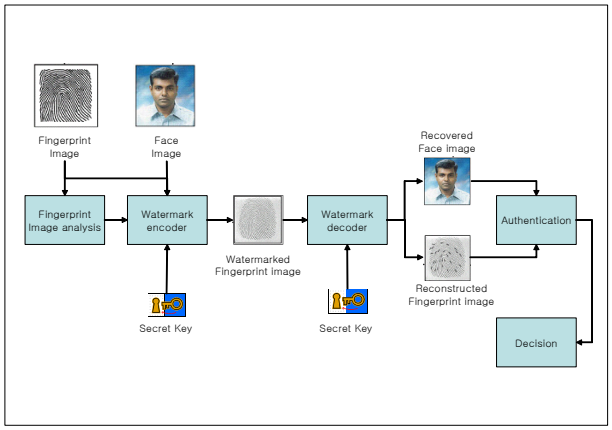
5.2.1 보호를 위한 가이드라인

DB에 저장된 생체 데이터의 인위적인 조작, 변경을 막기 위해서는 CBEFF(Common Biometric Exchange Format) 등에서 권고한 (그림 4)와 같은 방법을 사용할 수 있다. 권고한 내용은 다음 그림과 같이 생체 데이터 구성 부분에 일반적인 보안 알고리즘 등이 포함된 보안 블록을 추가하여 구성함으로써 해당 부분에 판독 없이는 생체 데이터의 내용을 해독뿐만 아니라 변경할 수 없게 하는 방법이다.



(그림 4) CBEFF에서 권고한 생체데이터 구성

일반적인 무결성 보장을 위한 기본적인 메커니즘인 해수함수등을 사용하거나, 생체 데이터 전송 전에 워터마크를 삽입하고 수신단에서 워터마크를 확인함으로써 영상데이터 자체를 안전하게 전송할 수 있으며 유출 후에도 워터마크를 확인함으로써 유출된 시스템의 추적이 가능하게 구성할 수도 있다.



(그림 5) 생체정보의 워터마킹

6. 결론

인터넷으로 주민등록증을 발급 받고, 지문을 이용하여 돈을 출금하는 일은 주위에서 흔히 볼 수 있는 일이 되어버렸다. 그러나 많은 시민단체나 개인은 자신의 영구적 생체정보가 누군가에게 도용되거나 사생활 침해의 한 일환으로 사용되지 않을까 불안 해하고 있다. 이를 해결하기 위해서는 무엇보다 이를 극복할 수 있는 기술적 연구가 시급하다. 이기종의 생체인식시스템간의 상호운영성을 보장하기 위해서 ISO/IEC JTC1 SC37에서 생체정보 표준화가 발 빠르게 진행되고 있다. 그러나 생체정보의 표준화는 프라이버시 보호를 위해 생체정보를 Changeable하게 만드는 기술들과 충돌관계에 있다고 할 수 있다. 향후 이에 대한 좀 더 심도 있는 연구를 진행해 나가고자 한다.

참고문헌

[1] Enhancing Security and Privacy in biometrics-based authentication systems," Ratha, Connell and Bolle, IBM System Journal, Vol. 40, No 3, 2001

[2] S.Liu and M.Silverman, "A Practical Guide to Biometric Security Technology", IEEE Computer Society, IT Prosecurity, Jan-Feb, 2001.

[3] ANSI, X9.84:Bioemtric Information Management and Security, American National Standards Institute.