국내 생체인식 표준화 작업의 필요성과 고려사항*

김경원 · 박연규 · 김종희** · 이필중

포항공과대학교, 정보통신대학원 **전자전기공학과

Consideration of Korean Biometric Standardization

Kyoung-Weon Kim · Yeon-Kyu Park · Jong-Hee Kim** · Pil-Joong Lee

Graduate School for Information Technology, **Department of Electronic & Electrical Engineering POSTECH

요 약

생체인식은 인간의 측정 가능한 생물학적인 또는 행동상의 특징을 이용하여 신원을 확인, 검증하는 방법이다. 현재 국외의 경우, 생체인식 관련 표준화 부분에 있어서 상당한 진척을 보이고 있다. 그러나 국내의 경우 아직 표준화 관련 작업이 미흡한 실정이다. 따라서 본 논문에서는 국제 표준화 동향에 대해 살펴보고 국내 생체인식 표준화의 필요성과 고려사항을 제시한다.

I. 서론

생체인식이란 개인의 독특한 신체적 특성이나 행동양식을 이용하여 개개인의 신원을 확인하는 방법이다. 기존의 사용자 계정(Identification)과 비밀번호(Password)를 이용한 인증(Authentication)에 비해 생체인식은 개인 특유의 신체적인 특징("Something an individual is")을 이용하므로 사용상의 장점을 가지고 있다. 이러한 이유로 예전부터 생체인식이 사용자 인증에 사용되고 있었다. 그러나 생체측정 기술들간의 호환성이 제공되지 않았다. 이러한 문제점을 인식하여 국외의 경우 표준화 부분에 있어서 상당한 진척을 보이고 있으며, 표준화 단계의 결과물로 BAPI(Biometric Application Programming Interface)[1], HA-API(Human Authentication-API)[2], BioAPI[3], CBEFF(Common Biometric Exchange File Format)[4], EFTS(Electronic Fingerprint Transmission Specification)[5] 등이 공개되었고, ANSI X9.84[6]가 ISO/IEC에 DIS(Draft International Standard)로 상정한 상태이다.

국내 생체인식 업계들은 좁은 국내 시장보다는 국제 시장으로 진출하는 특징을 보이고 있다. 그러나 국내 생체인식 표준화 작업은 국제표준화 움직임에 대해 대응하지 못하고 있는 실정이며, 국내표준이 마련되지 않아 업체간 연동이 불가능한 상태이다. 이는 국내 생체인식 업계들의 국제 시장진출에 걸림돌이 되고, 시장 진출 비용의 증가 원인이 된다.

따라서 국제표준과 호환성을 유지하면서 국내 실정에 적합한 국내 생체인증 시스템 보안기술 표준을 마련하는 것이 시급한 실정이다.

본 논문은 다음과 같이 구성되어 있다. 2.1에서는 국외 생체인식 표준화 동향을 살펴보고 2.2에서는 국내 표준의 필요성과 고려사항 및 결론을 제시한다.

II. 본문

* 이 논문은 한국정보보호진흥원에 의해서 진행중인 정보통신부 국책과제인 Biometric 인증 시스템 보안성 평가 기술 개발의 일환으로 추진된 국내 생체인증시스템 보안기술 표준(안) 개발 소과제에 의해 지원 받은 것임.

1. 국외 생체인식 기술들

본 장에서는 서론에서 언급한 표준화 단계의 결과물들을 통해 국외 생체인식 표준화 동향에 대해서 살펴본다.

1) BAPI

민간 업체 주도로 1998년 9월 30일에 version 1.2를 발표하였다. 이 표준화의 주요 응용 목표는 스마트 카드 소유자 확인, 물리적 접근 통제, 안정적 전자상거래, 금융거래, 워크스테이션 보안의 사용자 인증, 파일이나 데이터베이스 암호화 등이다.

BAPI의 최상위 계층인 Application 계층은 하드웨어에 독립적이며, BAPI를 세 가지 Level 중 하나로 호출할 수 있다. 세 가지 Level은 응용 프로그램 개발자가 BAPI 사용 시 복잡성에 따라 분류한 것으로 그 내용을 간단히 살펴보면 다음과 같다. Level 3은 가장 사용이 쉬운 것으로 기본적인 함수만의 사용을 통해 BAPI에 접근할 수 있다. Level 2는 보다 복잡한 BAPI 사용 절차를 통한 생체 인식 기기의 기능을 발휘할 수 있도록 한다. 마지막으로 Level 1은 저수준 입출력 함수 사용을 통한 개별 기기 성능을 최적화 할 수 있다. 응용 프로그램 개발 시 Level 1은 사용 방법이 매우 어렵기 때문에 일반 응용 프로그램 개발자들은 Level 2와 Level 3을 통해서 BAPI를 접근한다. BAPI.DLL은 장치 관리 기능과 모든 응용 프로그램에 표준 인터페이스를 제공한다.

현재 BAPI는 Windows 계열 OS, Serial, Parallel, PCMCIA, USB 등과 C/C++, VB을 지원하고 있다.

2) HA-API

HA-API는 1997년 12월 30일에 version 1.03이 발표되었고 이어서 1998년 4월에 version 2.0이 발표되었다. 미 국방부는 컴퓨터 보안 영역에서 생체인식을 적용하는 분야에 관심이 있었다. 그 중에서 사용될 수 있는 생체인식기술로 사용자 인식과 인증 분야를 결정하였고, 1997년 12월 제 10회 US Biometric Consortium 회의에서 국방성의 지원을 받은 National Registry Inc에 의해 소개되었다. HA-API는 생체인식에 관련된 기술 구현을 좀 더 빠르게 하였고 최초로 HA-API compliant application을 변형시키지 않고 다른 생체인식기술을 기존 application에 쉽게 추가 가능하도록 하였다. 그리고 생체인식 API의 주요 기능과 같이 생체인식 기술의 용이한 대체, 동일한 인터페이스를 이용한 다중 생체인식기술의 간단한 통합, 다중 application에 생체인식기술의 빠른 확산을 가능하도록 하였다.

3) BioAPI

2001년 3월 16일에 version 1.1을 발표하였고 민관 주도로 활동이 이루어지고 있다.

1998년 12월에 I/O Software는 BioAPI Consortium과 협력하면서 BAPI specification을 BioAPI specification의 하위 Level로 통합 결정하였고, 1999년 3월에 NIST의 ITL(Information Technology Laboratory)과 US Biometric Consortium이 주최한 단일화(Unification) 회의에서 BioAPI Consortium과 HA-API working group의 활동을 통합하기로 동의하였다. 동의 내용 중에 BioAPI Consortium의 조직을 다시 재구성할 계획도 포함되어 있었다. 현재 BioAPI Consortium에는 생체인식기술, 통합회사 및 이용자 집단 등 약 45개 회사들이 포함되어 있다. 그리고 4개의 Working Group이 활동하고 있다.

- Application Level Working Group
- External Liaisons Working Group
- Reference Implementation Working Group
- Conformance Test Suite Working Group

이 문서는 이용자에 대한 생체인식 등록 데이터에 대해 템플릿(template)이라는 용어를 이용하여 사용자의 생체측정 정보를 저장한다. 사용자가 인증을 받기 위해서는 제공한 샘플이 저장된 템플릿과 일치해야 한다. 여기서 BIR(Biometric Identification Record)이라는 용어를 사용하는데 이는 처리 전 데이터(raw sample data), 중간 데이터(intermediate data), 처리된 데이터(completely processed data), 등록 데이터(enrollment data)를 포함하여 응용 프로그램으로 돌려보내는 어떤 생체측정 데이터를 포괄적으로 지칭한다.

4) EFTS

1999년 1월 29일 version7.0이 발표되었고, 관주도 및 독자 영역 내 활동을 하고 있다.

다른 API와 달리 전적으로 범죄 수사 업무 지원을 목적으로 하고 있다. 거의 전 분야의 생체정보와 멀티미디어 정보를 포함하는 자료 수록을 범위로 삼고 있으며, FBI 작업과 납품 규격에서 ANSI로 적용 중이고, 향후 세계 표준인 ISO를 목표로 하고 있다. 또한 하드웨어에 관련된 부분도 정의되어 있으며, 현재 생체 정보 및 문자 정보에

대한 보안 및 암호화 기능 지원까지 확장 계획 중이다.

주요 내용은 개인 신상 정보, 사건 의뢰와 접수 등 일반 관리 기록, 범죄 경력, 잉크를 사용한 지문(지별 회전 압착 날인, 네 손가락 전체의 평면 압착 날인, 장문), 사건 현장의 유류 지문, 지문 특징점, 얼굴 사진, 신체 흉터, 문신 등의 기록, 범죄 현장 사진, 총기류 사용 후 탄흔 및 탄도 사진, 흉채, 음성 기록 등에 관련된 기록들이 수록되어 있다.

5) CBEFF

1999년 2월 21일에 NIST와 Biometric Consortium은 지문 템플릿의 형식에 대한 워크숍을 개최했다. 주된 내용은 지문 템플릿 형식을 공통된 포맷으로 사용하자는 것이었다. 1999년 5월 10일, 9월 17일, 12월 1일에 NIST와 Biometric Consortium이 함께 개최한 연이은 3번의 워크숍을 통해 CBEFF의 최초 개념적 정의가 이루어졌다. 그리고 워크숍 결과로 기술 개발팀이 형성되었고, CBEFF를 개발하게 되었다. 2001년 1월 3일에 발표하였다.

CBEFF의 목적을 다음과 같이 정리해 볼 수 있다.

- 다양한 생체인식 기술을 지원하기 위해 필요로 하는 공통된 데이터 요소들을 정의
- 생체데이터교환이 가능함에 따라 생체인식기술을 기초로 한 응용프로그램과 시스템의 상호운용(interoperability)을 촉진
- 처리기술에 호환성 제공
- 하드웨어/소프트웨어 통합 처리의 단순화
- 새로운 포맷이 어떻게 만들어질 수 있는지에 대한 설명

CBEFF 데이터 요소들은 CBEFF 파일 내에 필드로 존재한다. 이 필드는 3개의 주요 부분으로, 즉 SBH(Standard Biometric Header), BSMB(Biometirc Specific Memory Block), SB(Signature Block)로 구성되어 있다.

6) ISO/DIS 21352 (ANSI X9.84)

최근 선진국에서는 국제 표준화를 주도하여 생체인식시장을 선점하기 위한 노력을 기울이고 있다. ANSI의 X9소위원회 working group F4에서는 생체인증 데이터를 안전하게 주고받기 위하여 생체인증 데이터 구조와 생체인증 데이터에 대한 최소보안요구사항을 표준으로 정하였다(X9.84 Biometric Information Management and Security). 이 문서는 ISO/IEC에 DIS(Draft International Standard)로 상정한 상태이다.

X9.84의 생체인증 데이터에 대한 최소 보안요구사항은 다음과 같다.

- 캡쳐 디바이스로부터 생체인증 데이터를 안전하게 캡쳐하도록 한다.
- 캡쳐된 데이터는 정해진 절차를 이용하여 인가된 인터페이스를 통해서 수용하도록 한다.
- 생체인증 데이터의 조작을 막기 위한 안전한 메커니즘의 구현과 생체인증 데이터의 손실 혹은 노출 방지를 위한 메커니즘을 구현한다.

X9.84에서는 생체인증 데이터 DB의 조작을 금지하고 생체인증 데이터 DB내의 데이터에 대한 검증단계를 통해 외부 위협으로부터 데이터를 보호하도록 하는 접근제한 메커니즘이 있다. 생체인증 데이터는 공개키(public key)를 통해서 무결성을 유지하도록 되어 있으며, 또한 조작된 생체인증 데이터로부터 시스템 또는 개인정보를 보호하고 생체인증 데이터의 수집(collection), 분산(distribution), 처리(processing), 인증 등을 위한 보안요구사항과 생체인증 데이터의 암호화, 전송 및 저장, life cycle, 프라이버시(privacy), 무결성(integrity)기술 등의 보안요구사항이 있다. 일반적으로 정의되는 무결성 알고리즘은 RSA/SHA-1, DSA/SHA-1, ECDSA/SHA-1, MAC, HMAC가 있고, 비밀키 알고리즘은 DES, Triple DES, AES가 있다. 또한 생체인증 데이터의 프라이버시 보호를 위하여 MAC이나 전자서명과 같은 암호 메커니즘을 제공한다.

X9.84의 내용 중 '관리 및 보안 요구조건'과 '생체측정 객체'에 대해 간략히 살펴볼 것이다. 먼저 관리 및 보안 요구조건에서는 생체측정 시스템의 기본적인 구성요소가 되는 데이터 수집, 신호 처리, 정합, 저장, 결정, 전송 등에 대해 필요한 보안 요구 조건을 제시하고 있다. 각 구성요소가 반드시 따라야 할 핵심 보안 요구조건은 다음과 같다.

- 두 구성요소간에 주고받는 생체측정 데이터와 검증 결과는 적절한 메커니즘을 통해 무결성이 유지되어야 한다.
- 송신자와 수신자는 적절한 메커니즘을 통해 상호 인증을 해야한다.
- 필요하다면 적절한 메커니즘을 통해 두 구성요소간이나 한 구성요소 내에서의 생체측정 데이터는 기밀성을 보장해야 한다.

보안 요구조건과 각각의 구성요소별로 필요한 보안 요구조건에 따라 생체측정 객체는 크게 기본 생체측정 객체, 무결성이 제공되는 생체측정 객체, 프라이버시가 제공되는 생체측정 객체, 그리고 무결성과 프라이버시가 함께 제공되는 생체측정 객체로 나눌 수 있다. 기본 생체측정 객체는 생체측정 헤더 블록과 생체측정 데이터 블록으로 구성된다. 무결성을 제공하는 생체측정 객체는 기본 생체측정 객체의 블록과 무결성 블록으로 구성된다. 프라이버시를 제공하는 생체측정 객체는 기본 생체측정 객체의 블록과 프라이버시 블록으로 구성된다. 마지막으로 무결성과 프라이버시를 제공하는 생체측정 객체는 기본 생체측정 객체와 프라이버시 블록 그리고 무결성 블록으로 구성된다.

2. 국내 표준안 마련 시 고려사항 및 결론

지금까지 국외 생체인식 관련 기술에 대해 간단히 살펴보았다. 궁극적으로 생체인식 관련 기술의 표준화 활동은 공통된 생체측정 포맷을 사용하여 생체측정 기술간의 상호운용이 가능하도록 하자는 것이다.

국내 생체인식 관련 표준안 마련 시 다음과 같은 사항은 고려되어야 할 것이다. 먼저 암호학적인 보안 기법에 있어 국내 암호 알고리즘을 사용할 것인가 아니면 국제 표준 암호 알고리즘을 사용할 것인가 하는 문제이다. 국내 표준안인 경우, 국내 암호 알고리즘을 사용해야 하지만 국외 표준화 동향을 고려한다면 서로 호환이 가능한 암호 알고리즘이 반드시 명시되어야 할 것이다.

현재 생체인식에 관련한 OID(Object Identifier) 등록은 IBIA(International Biometric Industry Association)[7]에서 이루어지고 있다. 따라서 생체측정 데이터를 소유하고 있는 국내의 개인, 회사, 기관의 OID 등록을 위한 등록원에 관한 문제도 고려하여야 한다.

생체측정 시스템을 사용하기 위해 생체측정 데이터를 소유하고 있는 기업이나 기관들의 의견을 수렴하는 것 또한 중요한 일이라 생각된다. 생체인식 기술을 보유한 산업체의 의견 수렴을 하지 않는다면 국내 생체인식 기술의 실정을 반영하지 못하게 될 것이다. 또한 기업체의 의견을 수렴하여 국외의 표준화 동향을 따르면서 독자적인 국내 표준 기술을 확립할 수 있을 것이다.

위에서 제시한 것 이외에도 국내 생체인식 표준화 작업에 있어서 고려되어야 할 사항은 더욱 많을 것으로 생각된다.

본 논문은 국내 생체인식 관련 표준 마련의 필요성을 인식시키고 표준안 마련 시 고려해야 할 사항에 대해 간략하게 언급하였다. 국내 생체인식 관련 표준안이 마련된다면 국내 기업체의 국제 경쟁력 향상을 기대할 수 있을 것이다.

참고문헌

[1] http://www.bapi.org
[2] Interface Specification Human Authentication - Application Program Interface(HA-API) Ver 2.0 http://www.biometrics.org
[3] The BioAPI Consortium, BioAPI Specification, Version 1.1, March 16, 2001, http://www.ibia.org/
[4] Common Biometric Exchange File Format (CBEFF), NISTIR 6529, January 3, 2001 http://wwww.nist.gov/cbeff
[5] http://www.interpol.int
[6] ISO/DIS 21352, "Biometric information management and security"
[7] http://www.ibia.org