한국지능시스템학회 논문지 2009, Vol. 19, No. 2, pp. 160-167

개인식별정보와 바이오인식정보의 보호기법

Biometric and Identity Reference Protection

신용녀* · 권만준** · 이용준*** · 박진일**** · 전명근*****+

Yong-Nyuo Shin*, Man-Jun Kwon**, Yong Jun Lee***, Jin-Il Park and Myung Geun Chun*****+

* 한국정보보호진흥원 암호응용팀

** 아주자동차대학 자동차계열

*** (주)LG CNS 솔류션사업본부 기술연구부문

*****+ 충북대학교 전기전자컴퓨터공학부 컴퓨터정보통신연구소

요 약

본 논문에서는 바이오인식 시스템에 있어서, 바이오인식 정보와 개인식별 정보가 결합되어 운영되는 상황에서 바이오인식 정보 제공자의 개인정보를 보호 할 수 있는 방안에 대해서 다룬다. 암호를 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 있는 관계로 이들의 생성, 저장, 전송에 있어서 안정적인 보호 수단이 요구 되고 있다. 이에 본 연구에서는 이와 관련된 X9.84 표준을 확장하여 바이오인식 정보와 결합되어 사용되는 개인식별 정보를 포함하여 이들의 저장과 이송에 있어서, 기밀성과 무결성을 보장할 수 있도록 ASN.1으로 표현되는 표준 포맷을 정의하고 이를 구현함으로서 그 유용성을 보였다.

키워드 : 바이오 인식, 개인식별정보, 정보보호, 프라이버시

Abstract

This paper describes how to protect the personal information of a biometric reference provider wherein biometric reference and personally identifiable information are bounded in a biometric system. 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 is usually 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 individual when combining with the other information. As a result, secure protection methods are required for generating, storing, and transmitting biometric information. Considering these issues, this paper proposes a method for ensuring confidentiality and integrity in storing and transferring personally identifiable information that is used in conjunction with biometric information, by extending the related X9.84 standard. This paper also outlines the usefulness of the proposition by defining a standard format represented by ASN.1, and implementing it.

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

1. 서 론

인터넷이 우리 일상 생활의 일부분으로서 이에 기반한 인터넷 뱅킹이나 전자상거래와 같은 다양한 서비스가 제공되고 있다. 한편으로, 이러한 서비스를 제공자와 사용자 사이에 안전한 인증수단의 필요성도 더불어 커지고 있는데 인증 수단으로는 개인식별번호(PIN), 공개키 기반의 전자서명, 바이오인식 기법 등이 제안되어 사용되고 있다[1].

접수일자 : 2008년 10월 30일
완료일자 : 2009년 2월 15일
+ 교신저자
본 논문은 KISA(정보보호진흥원)의 학술연구지원사업의 연구비 지원에 의해 연구되었음

이러한 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[2]. 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 바이오인식시스템의 기술적 발전에도 불구하고 사용자로 하여금 바이오인식정보의 유출에 따른 프라이버시 문제로 바이오인식 정보의 데이터베이스화 하거나 온라인상에서 바이오인식 정보의 사용을 꺼려하고 있는 추세다[3].

바이오인식 정보를 위한 연구 동향을 살펴보면 바이오인식정보를 은닉하여 불법 사용자가 은닉된 정보에 접근하지 못하도록 하는 워터마킹에 대한 연구들이 진행되고 있다. Jain 등[4]은 지문 영상에 얼굴정보를 삽입할 수 있는 지문 영상 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[5].

또다른 기술적 기법으로는 변환 가능한 바이오 템플릿(changeable biometric template) 혹은, 취소 가능한 바이오 템플릿(cancellable biometric template) 기법이다[6][7]. 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[8]. 이와 더불어 바이오 인식 정보를 이용한 개인인증 시스템의 구축에 있어서, 필연적으로 요구되는 개인식별정보와 바이오인식정보의 결합 단계에서 이들 데이터의 저장과 전송중의 기밀성과 무결성을 보장할 수 있는 표준화된 방법이 요구되고 있다.

본 논문의 주요 연구 내용은 다음과 같다.

- 바이오인식 시스템에서 개인식별 정보와 바이오인식정보의 흐름과 결합에 대한 분석
- 바이오인식정보와 개인식별 정보의 결합에 따른 무결성(integrity), 기밀성(confidentiality) 보장을 위한 암호학적 보호기법과 표준 포맷
- ASN.1에 의한 표준 포맷의 구현 방안과 실제 바이오인식 시스템 운영에 따른 실험

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 [8]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.

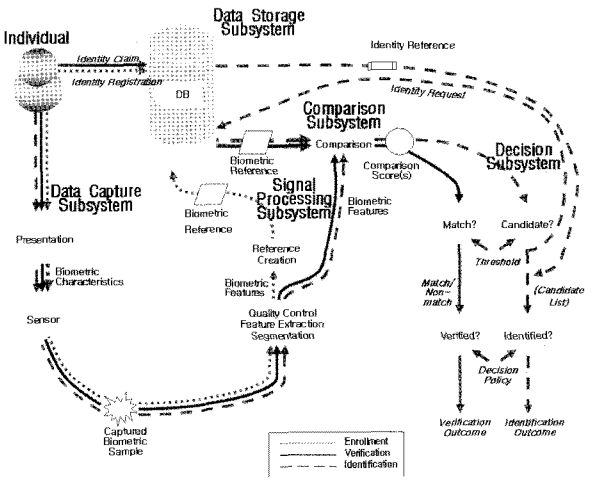

그림 1. 바이오인식 시스템의 구성도
Figure 1. Biometric System Diagram

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. 예를 들어보면, 홍채인식의 경우에는 얼굴영상에서의 동공을 추출하여 눈썹들의 잡음영상을 제거하여 동공의 중심을 추출한 후 이를 기준으로 홍채영역을 추출한 후 Gabor 변환등을 거쳐서 특징값을 추출하게 된다.

- 데이터저장부(Data Storage): 등록된 사용자의 바이오인식 템플릿을 저장하며 등록된 템플릿의 추가, 삭제 그리고 복구 기능을 제공할 수도 있다. 데이터저장부는 단일 대

상자를 위한 단일 바이오인식정보만을 저장할 수도 있고, 많은 사용자를 대상으로 수천 개의 바이오인식정보들을 저장할 수도 있다. 구체적으로 바이오인식 정보들이 저장되는 장소는 대규모 바이오인식정보 저장을 위한 컴퓨터 시스템 내의 데이터베이스, 스마트 카드와 같은 휴대 가능한 토큰, 바이오인식용 디바이스내의 저장소 등이 있을 수 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 계산하여 결정부에서 사용하기에 적절한 형태의 점수를 산출하는 역할을 한다.

- 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 바이오인식 템플릿은 다음과 같이 정의된다[9].

- 바이오인식 템플릿(biometric template): 인식하고자 하는 바이오인식 샘플(sample), 즉 바이오인식 데이터취득부에서 얻어 지는 얼굴영상이나 취득된 지문영상에서 추출된 바이오인식 특징이 저장된 형태라고 볼 수 있다. 예를 들면 얼굴영상에서 고유얼굴(eigenface)에 대한 계수값이나 지문인식에 있어서 미뉴셔(minutiae)의 위치와 각도값 등이 저장부에 저장되어 있는 것을 말한다.

위의 정의에 따르면, 바이오인식 템플릿은 원본영상 등의 정보에서 특징점 값만을 뽑아낸 것으로 개인을 식별할 수 있는 정보가 현저히 떨어진다. 그러나 실제적으로 바이오인식 시스템을 응용하는 경우에 원본 영상을 저장하는 경우가 많으며, 음성인식과 같은 경우에는 개인의 음성특징을 신경회로망과 같은 수학적 모델에 저장하는 경우가 많으므로 위의 바이오인식 템플릿을 포함하면서 더욱 확장된 개념의 바이오인식 정보라는 용어가 널리 쓰이고 있다.

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

한편, 한 개인의 신원을 나타내는 식별자(identity)는 그 사람이 신원 확인하기를 바라는 상황에서 대상자와 관련된 모든 속성이라고 할 수 있으며, 따라서 한사람에 대해서 다수의 식별자가 제시될 수도 있다. 예를 들어 보안의 요구강도가 높은 시스템의 경우에, 그 사람의 주민등록 번호나 여권번호와 더불어 얼굴 사진이나 지문이 등록되어 있는 신분증 등의 요구를 할 수 있다.

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[9], 본 논문에서도 이와 같은 관점으로 바이오인식 정보와 개인식별 정보를 분리하여 기술하고자 한다. 그림 2는 앞서 설명된 바이오인식 정보와 개인식별정보의 구체적인 예를 보여 주고 있다.

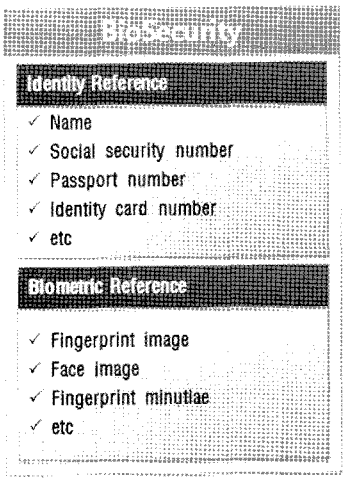

그림 2. 바이오인식 정보와 개인식별정보
Figure 2. Biometric Reference and Identity Reference

개인식별 정보는 어떠한 형태가 되었든 그 정보를 소유하고 있는 사람을 식별할 수 있는 정보라고 볼 수 있다. 바이오 인식정보가 홀로 존재하는 경우, 특히 템플릿의 형태로 존재하는 경우는 직접적으로 특정 개인을 판별하는 정보로 사용하기가 용이하지 않다. 그러나 이러한 바이오인식정보가 개인식별 정보와 결합되었을 경우에는 매우 민감한 개인정보로 간주할 수 있다. 예를 들어 지문의 특징점 정보만이 유출된 경우에는 그것이 누구의 것인지 판별하기가 거의 불가능하나, 그러나 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.

지금까지 바이오 인식시스템에서는 바이오인식 정보 자체만의 저장이나 통신 포맷 등의 표준화가 이루어지고 있었으나, 개인의 식별 정보까지 동시에 고려하는 연구는 이루어지고 있지 않은 실정이다. 따라서 본 연구에서는 바이오인식시스템에서 개인식별 정보와 바이오인식 정보가 결합된 형태로 저장이나 전송될 때의 무결성과 기밀성을 보장할 수 있는 기술적 방안에 대해서 기술하고자 한다.

3. 개인식별정보와 바이오인식정보 보호

앞서 기술된 바이오인식시스템은 실제 운영환경에 있어서 바이오인식정보의 저장과 비교가 이루어지는 장소에 따라 여러 가지 형태로 구분 지을 수 있다[9]. 이들 각각의 운영형태에 따라 개인의 프라이버시에 영향을 미치는 정도와 이에 따른 보안 요구 사항이 다를 수 있는데, 아래 그림 3에서는 바이오인식정보와 개인식별정보가 서버에 저장되어 있고 이들에 대한 비교는 클라이언트에서 이루어지는 형태를 보여 주고 있다.

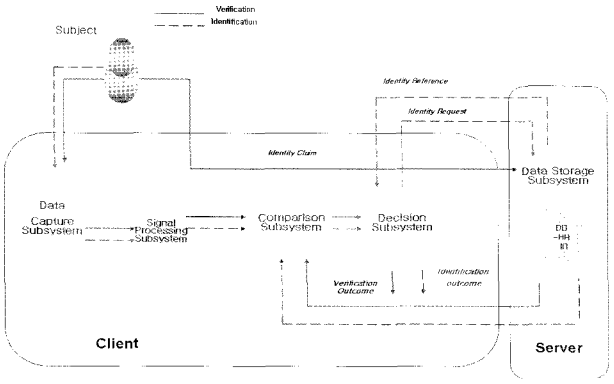

그림 3. 바이오인식 시스템에서의 정보흐름
Figure 3. Information flow in the biometric system

이러한 바이오인식시스템의 운영에 있어서 정보의 흐름을 살펴보면, 사용자는 자신의 ID를 서버로 보내서 여기에 해당되는 바이오인식정보를 가져오게 된다. 이것을 센서로부터 취득된 바이오인식 특징값과 비교하여 개인의 인증여부를 최종적으로 결정짓게 된다. 그림 4는 이를 채용한 전자의료 기록시스템(Electronic Medical Record System)을 나타내고 있다.

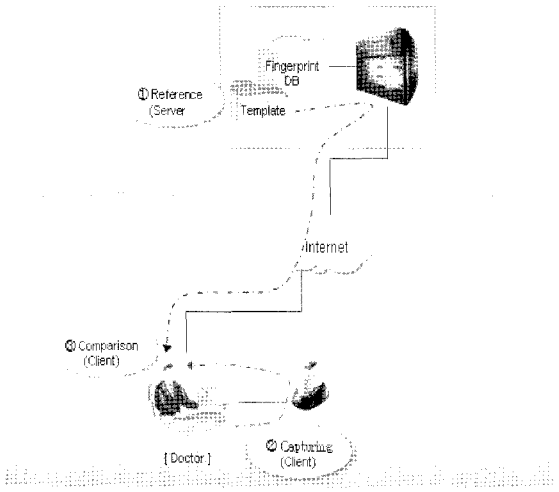

그림 4. EMR 시스템에 사용된 바이오인식시스템[8]
Figure 4. Biometric System used in EMR system[8]

서버와 클라이언트와의 통신을 통해서 개인식별정보와 바이오인식 정보를 주고 받게 되므로, 이들에 대한 기밀성(confidentiality)와 무결성(integrity)을 보장하기 위한 암호화와 전자서명이 필요함을 알 수 있다.

3.1 바이오인식정보와 개인식별정보의 표준화

해외의 생체인식관련 표준화 작업 중 ISO/IEC JTC1산하의 SC37 생체인식 국제 표준화 위원회에서는 BioAPI(Biometric Application Program Interface) 및 CBEFF(Common Biometric Exchange Format Framework)로 대표되는 인터페이스 분야와 지문, 얼굴, 홍채 등의 자료 교환 포맷 분야, 그리고 국경 출입제어(Border control)와 같은 응용기술의 표준화를 주도하고 있다. BioAPI는 생체인식 전 분야에 적용 가능한 응용프로그램 인터페이스를 제공하기 위해 생체데이터 규격을 표준화하는 동시에 클라이언트 서버 응용분야 지원, 일반에게 구현관련 참조사항 및 소스 공개, 플랫폼과 무관한 작동, 등록된 사용자 데이터의 사용자인식을 위한 신분확인 및 인증 등의 기본기능 제공 등의 표준기능을 정의하고 있으며, CBEFF는 같은 종류 또는 다른 종류의 생체 인식 기술들을 지원하는 데 필요한 데이터 요소들을 정의하며, 이러한 데이터는 공통의 파일에 수록되어 서로 다른 시스템 컴포넌트나 시스템 간에 생체 인식 정보를 교환하는데 사용될 수 있도록 하고 있다[10].

한편, 금융 분야에 적용하기 위한 노력의 하나로 데이터의 안전한 전송을 위한 ANSI의 X9 위원회 F4가 생체인증 데이터를 안전하게 주고받을 수 있는 데이터구조와 생체인증 데이터에 대한 최소 보안요구사항과 이를 실현할 수 있는 기술적 방안을 표준으로 정한 것으로 X9.84 -바이오인식 정보 관리 및 보안 규격이 있다[11]. 그러나 X9.84에서도 개인식별정보와 바이오인식 정보가 같이 사용되는 상황에서 이들의 기밀성과 무결성을 보장하기 위한 표준을 반영하지 못하고 있는 실정이다. 이에 본 연구에서는 X9.84 표준안을 토대로 개인 식별정보까지 보안할 수 있는 방안을 제시하고자 한다. 이 둘의 차이점을 명확하게 하기 위하여 아래의 표1에 비교표를 제시하였다.

표준안을 기술하는데 사용되는 언어는 주로 ASN.1(Abstract Syntax Notation)이 사용되는데 ASN.1은 구현에 무관하게 표준을 정의하는 언어이며 표준 작성자가 사용하는 언어이다. 즉, ASN.1은 표준을 설명하는 공용 언어를 제공하여 전문가와 위원회 회원 간의 의사소통을 원활하게 한다. ASN.1은 ITU-T 권고안 X.209 및 X.690에 정의되어 있다. 1988년에 처음 제정되어 1990년, 1994년 그리고 1997에 수정되어 있으며 오늘날에 이르고 있다[12].

표 1. X9.8와 제안된 표준의 비교
Table. 1. Comparison X9.84 with proposed standard

	X9.84	제안된 표준
바이오인식정보의 기밀성 및 무결성	보장	보장
개인식별정보의 기밀성 및 무결성	지원안됨	보장
개인식별정보와 바이오인식정보 결합	지원안됨	지원
결합된 개인식별정보와 바이오인식정보의 기밀성 및 무결성	지원안됨	보장

X9.84의 데이터 포맷에는 개인식별 정보가 없는 것을 감안하여, 다음과 같이 이를 포함 할 수 있는 확장된 개념으로 먼저, BioSecurityObject를 다음과 같이 정의한다.

```
BioSecurityObject ::= SEQUENCE {
  bioSecurityHeader  BioSecurityHeader,
  biometricReference BiometricReference
OPTIONAL,
  identityReference  IdentityReference OPTIONAL,
}
```

여기서 BioSecurityHeader는 다음과 같이 정의된다.

```
BioSecurityHeader ::= SEQUENCE {
 version           BiometricVersion  DEFAULT hv1,
 recordType        RecordType  OPTIONAL,
 dataType          DataType  OPTIONAL,
 purpose           Purpose  OPTIONAL,
 quality           Quality  OPTIONAL,
 validityPeriod ValidityPeriod  OPTIONAL,
 format            Format  OPTIONAL
}
```

그림 5는 위에서 정의된 BioSecurityObject의 구조를 나타내고 있다.

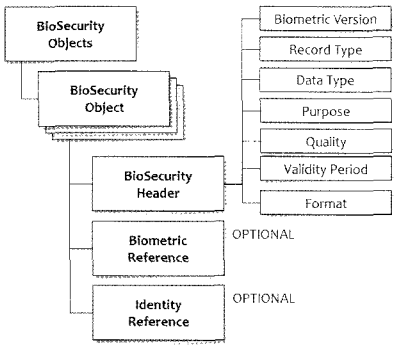

그림 5. BioSecurityObject 구조
Figure 5. BioSecurityObject Structure

BioSecurityObject 내의 BiometricReference는 X9.84 표준안과의 호환을 고려하여, 기존의 BiometricSyntax에 BiometricModel을 추가하는 형태로 정의하였다.

```
BiometricReference ::= SEQUENCE {
  biometricModel  BiometricModel OPTIONAL,
  biometricSyntax BiometricSyntax  -- FROM X9.84
}
```

한편, 개인식별 정보를 정의하기 위한 IdentityReference는 다음과 같이 정의된다.

```
IdentityReference ::= SEQUENCE {
  identityHeader    IdentityHeader,
  identityInfomation          IdentityInformation,
}
```

여기서, 개인식별정보에 대한 헤더는 다음과 같이 정의한다.

```
IdentityHeader ::= SEQUENCE {
 identityVersion       IdentityVersion  DEFAULT hv1,
 purpose           Purpose  OPTIONAL,
 validityPeriod ValidityPeriod  OPTIONAL,
}
```

여기서 identityVersion은 정의된 개인식별정보 헤더의 버전을 나타내며, purpose는 사용되는 개별정보의 용도에 대해서 기술하며, validityPeriod는 사용되는 개인식별정보의 유효기간 또는 보관기간을 나타낸다.

이제 위와 같이 정의된 BioSecurityObject에 대한 무결성 보장블럭을 다음과 같이 정의한다.

```
IntegrityBioSecurityObjects ::= SEQUENCE {
  bioSecurityObjects
EncodedBioSecurityObjects,
  integrityBioSecurityBlock  IntegrityBioSecurityBlock
}

IntegrityBioSecurityBlock ::= CHOICE {
  digitalSignature          DigitalSignature,
  messageAuthenticationCode
MessageAuthenticationCode,
  signedData                SignedData,
  authenticatedData         AuthenticatedData
}
```

위의 무결성 객체는 X9.84과의 호환을 위하여 4가지 무결성 타입 (digitalSignature, messageAuthenticationCode, signedData, authenticatedData)을 선택할 수 있도록 하였다. 그림 6은 앞서 설명된 BioSecurityObject과 무결성 보장블럭이 결합된 형태를 보여주고 있다.

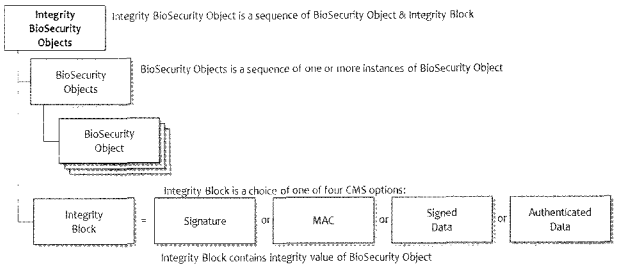

그림 6. 무결성 보장 블럭
Figure 6. Integrity BioSecurity Objects

한편, 앞서 정의된 BioSecurityObject에 대한 기밀성 보장블럭을 다음과 같이 정의한다.

```
PrivacyBioSecurityObjects ::= SEQUENCE {
  bioSecurityHeaders  BioSecurityHeaders  OPTIONAL,
  privacyBioSecurityBlock PrivacyBioSecurityBlock
}
PrivacyBioSecurityBlock ::= CHOICE {
  fixedKey          EncryptedData,
  namedKey          NamedKeyEncryptedData,
  establishedKey  EnvelopedData
}
```

위의 기밀성 객체는 X9.84와의 호환을 위하여 fixedKey, namedKey 그리고 establishedKey의 3가지 중 하나를 선택할 수 있도록 하였다. X9.84의 구현에 관한 자세한 사항은 참고문헌 [13]에 자세히 나와 있다. 그림 7은 앞선 설명된 BioSecurityObject과 기밀성 보장블럭이 결합된 형태를 보여주고 있다.

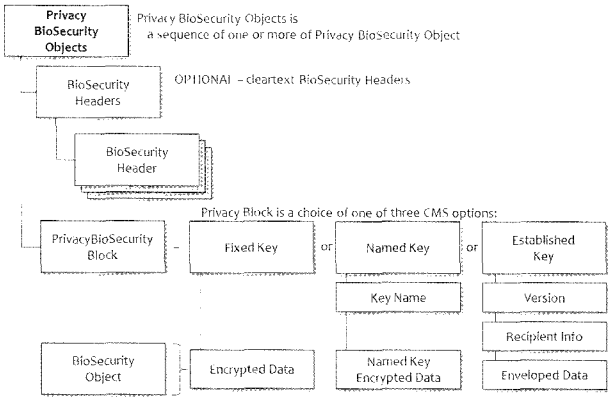

그림 7. 기밀성 보장 블럭
Figure 7. Privacy BioSecurity Objects

한편, 앞서 정의된 BioSecurityObject에 대해 무결성과 기밀성을 동시에 보장하는 오브젝트는 다음과 같이 정의된다.

```
PrivacyAndIntegrityBioSecurityObjects ::= SEQUENCE
{
  bioSecurityHeaders BioSecurityHeaders OPTIONAL,
  privacyBioSecurityBlock PrivacyBioSecurityBlock,
  integrityBioSecurityBlock IntegrityBioSecurityBlock
}
```

그림 8은 앞선 설명된 BioSecurityObject과 무결성 및 기밀성 보장블럭이 결합된 형태를 보여주고 있다.

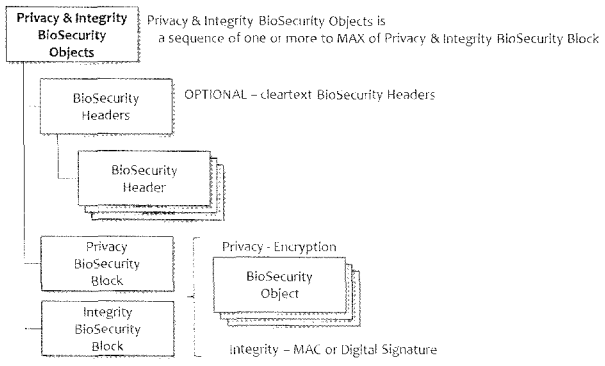

그림 8. 무결성과 기밀성을 보장하는 오브젝트
Figure 8. Integrity and Privacy BioSecurity Objects

지금까지 정의된 오브젝트를 종합하여 보면 다음과 같은 최상위 레벨에서의 데이터 형태로 BioSecuritySyntax를 정의 할 수 있으며, 이를 이용하면 그림 5~그림 8 중의 형태에서 사용자가 원하는 수준의 보안을 만족하는 바이오인식 시스템을 구현 할 수 있다.

```
BioSecuritySyntaxSets ::= SEQUENCE SIZE(1..MAX)
OF BioSecuritySyntax

BioSecuritySyntax ::= CHOICE {
  bioSecurityObjects BioSecurityObjects,
  integrityBioSecurityObjects
IntegrityBioSecurityObjects,
  privacyBioSecurityObjects
PrivacyBioSecurityObjects,
  privacyAndIntegrityBioSecurityObjects
PrivacyAndIntegrityBioSecurityObjects
}
```

그림 9는 앞서 설명된 BioSecuritySyntax의 일반적인 형태를 보여 주고 있다.

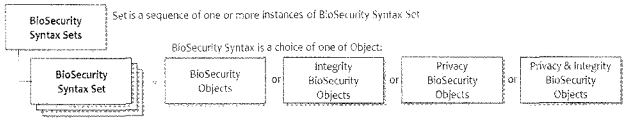

그림 9. BioSecurity 의 일반적인 형태
Figure 9. BioSecurity Syntax Set

4. 개인식별정보와 바이오인식정보보호 구현

앞서 정의된 정보보호 표준 포맷을 구현하고 실험하기 위하여 지문인식을 이용한 서버-클라이언트 구성된 그림 10과 같은 바이오인식 시스템을 구현 하였다.

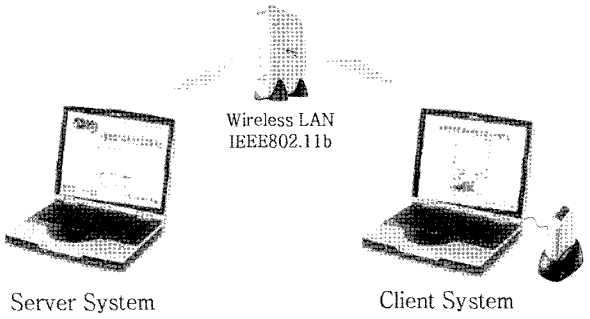

그림 10. 서버 클라이언트 모델의 바이오인식시스템
Figure 10. Server-client biometric system

클라이언트 프로그램은 생체데이터를 수집하기 위해 지문인식기를 인터페이스 하였으며, 서버는 수집된 데이터를 보관하기 위해 데이터베이스 파일을 가질 수 있도록 하였으며 그림 11과 같은 사용자 인터페이스 환경을 구축하였다.

그림 11에 나타낸 바와 같이 바이오인식정보에 전달되는 다양한 항목(버전, 레코더 형식, 데이터 형식, 목적, 품질, 전/후 유효기간, 데이터 포맷의 오너)을 설정할 수 있도록 하였으며, 무결성과 기밀성을 위해 적용되는 암호화 기법을 선택할 수 있도록 하였다.

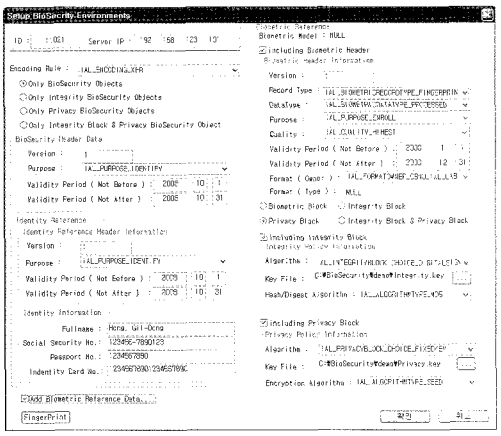

그림 11. 개인식별 정보와 바이오 인식 정보의 보안
Figure 11. Biometric and Identity Reference Protection

앞서 설명된 바와 같이 구현된 시스템을 기반으로 하여 본 논문에서는 바이오인식데이터와 개인식별데이터에 대해서 클라이언트에서 제시된 보호기법으로 저장 및 전송하고 서버에서 이를 복호화 하였을 때의 데이터를 비교하여 전과정이 정상적으로 동작하는지를 검증하였다. 인코딩 규칙은 XER(XML Encoding Rules)을 선택했으며, 무결성을 위해서는 MD5 알고리즘을 적용하였으며, 기밀성을 위해서는 SEED 알고리즘을 적용하여 테스트를 수행하였다.

```
- <BioSecurityObject>
  - <bioSecurityHeader>
      <version>1</version>
    - <recordType>
        <id>5</id>
      </recordType>
    - <dataType>
        <processed />
      </dataType>
    - <purpose>
        <verify />
      </purpose>
      <quality>3</quality>
    - <validityPeriod>
        <notBefore>2008.10.1</notBefore>
        <notAfter>2008.10.31</notAfter>
      </validityPeriod>
    - <format>
      - <formatOwner>
          <oid>2.32.42.9.10.4</oid>
        </formatOwner>
      </format>
    </bioSecurityHeader>
  - <biometricReference>
      <biometricModel>01</biometricModel>
    - <biometricSyntax>
      + <privacyAndIntegrityObjects>
      </biometricSyntax>
    </biometricReference>
  - <identityReference>
    - <identityHeader>
        <version>1</version>
      - <purpose>
          <verify />
        </purpose>
      - <validityPeriod>
          <notBefore>2008.10.1</notBefore>
          <notAfter>2008.10.31</notAfter>
        </validityPeriod>
      </identityHeader>
    - <identityInfomation>
        <fullName>48 6F 6E 67 2C 20 47 69 6C 2D 44 6F 6E 67</fullName>
        <socialSecurityNumber>31 32 33 34 35 36 2D 37 38 39 30 31 32 33</socialSecurityNumber>
        <passportNumber>31 32 33 34 35 36 37 38 39 30</passportNumber>
        <identityCardNumber>31 32 33 34 35 36 37 38 39 30 31 32 33 34 35 36 37 38 39 30</identityCardNumber>
      </identityInfomation>
    </identityReference>
</BioSecurityObject>
```

그림 12. XML로 표현된 바이오인식 및 개인 식별정보 화면
Figure 12. Biometric and identity references in XML

그림 12에서는 privacyAndIntegrityObjects는 공간제약상 축약된 형태로 제시되어 있다. 이러한 서버 클라이언트 환경의 구현을 통하여 바이오인식정보와 개인 식별 정보가 저장 및 전송과정에서 무결성과 기밀성을 유지하고 있음을 확인할 수 있었다. 여기서 언급된 무결성과 기밀성의 보장은, 본 논문에서 제안한 표준 포맷이 이미 국제표준으로 채택되어 널리 사용되고 있는 암호화 및 전자서명의 기법을 사용하기 때문에 가능한 것이다.

5. 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 먼저, 바이오 인식 시스템에서의 개인식별정보와 바이오인식 정보의 결합이나 전송 등의 모델을 제시하고, 현재 바이오인식 정보 자체의 보안에 대해서는 일부 표준화가 진행되고 있으나, 개인식별정보와 연계되었을 때의 상황에 대한 고려가 이루어지지 않았음을 반영하여 ASN.1에 의거하여 표준화 포맷을 정의하고 이들을 실제 구현하여 실행함으로서 제시된 방법의 유용함을 제시하였다. 논문에서 제시된 방법은 개인식별정보 만이 적용되는 개인 정보 처리 시스템이나. 바이오인식 정보만이 적용되는 상황 모두에도 응용될 수 있는 구조를 가지고 있으므로, 개인정보를 취급하는 일반적 인 정보처리시스템에서 이들을 보호 할 수 있는 표준포맷으로 널리 사용될 수 있으리라 생각된다.

참 고 문 헌

[1] S. Y. Kung, M. W. Mak, S. H. Lin, *Biometric Authentication*, Prentice Hall, 2005.

[2] A. A. Ross, K. Nandakumar, A. K. Jain, *Handbook of Multibiometrics*, Springer, 2006.

[3] A. Ross, J. Shah, A. K. Jain, "From template to image: Reconstructing fingerprints from minutiae points," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 544-560, 2007.

[4] A. K. Jain, U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 25, no. 11, pp. 1494-1498, 2003.

[5] 이욱재, 이대종, 문기영, 전명근, "웨이블렛을 이용한 생체정보의 강인한 워터마킹 알고리즘," *한국퍼지 및 지능시스템 학회 논문지*, 제17권, 5호, pp. 632-639, 2007.

[6] J. Kim, C. Lee, J. 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.

[7] N. Ratha, J. Connell, R. M. Bolle, S. Chikkerur, "Cancellable Biometrics: A case study in fingerprint," *Int. Conference on Pattern Recognition*,

vol. 4, pp. 370-373, 2006.
[8] 신용녀, 이용준, 전명근, "개인정보보호를 위한 바이오인식 템플릿 보안," *한국지능시스템학회 논문지*, 제18권, 4호, pp. 437-444, 2008.
[9] M. G. Chun, P. J. Lee, J. H. Moon, ISO/IEC JTC 1 SC27 N6755, *Biometric template protection*, 2008.
[10] 문지현, "전자여권 관련 바이오인식기술, 표준기술 동향," *TTA Journal*, no. 144, pp. 88-94, 2007.
[11] X9.84-2003, *Biometric information management and security for the financial services industry*, America National Standards Institute.
[12] J. Larmouth, *ASN.1 Complete*, Morgan Kaufmann, 1999.
[13] 전명근, *프라이버시 친화적 생체인식 시스템 구축 방안 최종연구보고서*, 한국전자통신연구원, 2005.

저 자 소 개

신용녀(Yong Nyuo Shin)
1999년 2월 : 숭실대학교 컴퓨터학과 졸업
2001년 9월 : 고려대학교 컴퓨터학과 석사
2008년 2월 : 고려대학교 컴퓨터학과 박사
2002년 1월 ~ 현재 : 한국정보보호진흥원 암호응용팀 주임연구원
2005년 ~ 현재 : TTA PG505(바이오인식 프로젝트 그룹) 간사

관심분야 : 정보보호, 바이오인식, 정형기법
E-mail : ynshin@kisa.or.kr

권만준(Man-Jun Kwon)
1989년 : 부산대 전자공학과 학사졸업.
1991년 : 한국과학기술원 전기및전자공학과 (공학석사)
2008년 : 충북대 제어계측공학과 박사
현재 : 아주자동차대학 자동차계열 교수

관심분야 : 퍼지이론, 생체인식, 얼굴인식, 임베디드 프로그래밍
E-mail : mjkwonkr@yahoo.co.kr

이용준(Yong Jun Lee)
1999년 : 강남대학교 전자계산학과 졸업
2001년 : 숭실대학교 컴퓨터학과 석사
2005년 : 숭실대학교 컴퓨터학과 박사
2006년 ~ 현재 : LG CNS 기술연구부문 책임연구원

관심분야 : 개인정보 보호, 바이오인식
E-mail : bigman2u@korea.com

박진일(Jin Il Park)
2001년 : 한밭대학교 제어계측공학과(학사)
2003년 : 한밭대학교 제어계측공학과 (공학석사)
2005년 ~ 현재 : 충북대학교 제어계측공학과 박사과정

관심분야 : 지능시스템, 다중생체인식, 퍼지이론
E-mail : moralskr@yahoo.co.kr

전명근(Myung Geun Chun)
1987년 : 부산대학교 전자공학과(학사)
1989년 : KAIST 전기 및 전자공학과 (공학석사)
1993년 : KAIST 전기 및 전자공학과 (공학박사)
1993년 ~ 1996년 : 삼성전자 자동화연구소 선임연구원
2000년 ~ 2001년 : University of Alberta 방문교수
1996년 ~ 현재 : 충북대학교 전기전자컴퓨터공학부 교수
2008년 ~ 현재 : TTA PG505 의장
2007년~ 현재 : ISO/IEC SC27 정보보호 표준화 전문위원

관심분야 : 바이오인식, 개인정보보호, 데이터마이닝, 지능시스템
E-mail : mgchun@chungbuk.ac.kr