한국지능시스템학회 논문지 2008, Vol. 18, No. 4, pp. 437-444

개인정보 보호를 위한 바이오인식 템플릿 보안

Biometric Template Security for Personal Information Protection

신용녀* · 이용준** · 전명근***+

Yong-Nyuo Shin*, Yong Jun Lee**, and Myung Geun Chun***+

* 한국정보보호진흥원 산업지원팀

** (주)LG CNS 솔류션사업본부 기술연구부문

*** 충북대학교 전기전자컴퓨터공학부 컴퓨터정보통신연구소

요 약

본 논문에서는 개인인증 시스템으로 널리 사용되고 있는 바이오인식 시스템에서의 바이오인식 템플릿 보호에 대해서 다룬다. 먼저 바이오인식 시스템의 구성요소와 동작을 살펴보고 여기에서 사용되는 바이오인식 템플릿과 개인 식별정보(ID)에 대한 정의를 내린다. 이어서 바이오인식 시스템의 동작에 있어서 개인 식별 정보와 바이오인식 템플릿이 공격당할 수 있는 위협 요소와 공격의 예를 살펴봄으로서, 암호와 전자서명에 의해서 방지 될 수 있는 보안 위협의 유형을 찾아낸다. 이러한 위협 요인들이 실제의 바이오인식 시스템을 운영하면서 발생될 수 있는 예와 대책을 찾기 위하여, 지역모델, 다운로드, 첨부모델, 센터 모델 등의 4개의 운용유형에 대해서 취약성을 분석하여 각각의 경우에 개인 식별 정보와 바이오인식 템플릿의 보호를 위한 대책을 기술한다. 마지막으로 바이오 인식 시스템을 운영하는데 있어서 프라이버시 관점에서의 바이오인식 템플릿의 보호에 대해서 기술하고자 한다.

키워드 : 바이오 인식, 정보보호, 프라이버시

Abstract

This paper deals with the biometric template protection in the biometric system which has been widely used for personal authentication. First, we consider the structure of the biometric system and the function of its sub-systems and define the biometric template and identification(ID) information. And then, we describe the biometric template attack points of a biometric system and attack examples and provide their countermeasures. From this, we classify the vulnerability which can be protected by encryption and hashing techniques. For more detail investigation of these at real operating situations, we analyze them and suggest several protection methods for the typical application scheme of biometric systems such as local model, download model, attached model, and center model. Finally, we also handle the privacy problem which is most controversy issue related to the biometric systems and suggest some guidances of safeguarding procedures on establishing privacy sympathy biometric systems.

Key Words : Biometrics, Information Security, Privacy

1. 서 론

최근 정보통신 기술이 급속히 발달함에 따라 인간의 삶의 질은 향상되어 가고 있지만, 컴퓨터 간 정보의 불법 복제 및 삭제, 불법 정보유출 등에 의한 사회적 손실도 증가하고 있다. 이러한 문제점을 해결하기 위하여 해킹, 누출에 의해 정보가 도용될 수 없고, 또한 변경되거나 분실할 위험성이 없는 신분 검증 기법인 바이오인식 기술이 각광을 받고 있다[1]. 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][3].

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 ID처럼 사용자가 원하는 경우에 쉽게 변경하기가 어렵다는 치명적인 단점을 지니고 있다. 이런 이유로 바이오인식시스템의 개발에도 불구하고 사용자로 하여금 바이오인식정보의 유출에 따른 문제로 바이오 정보의 데이터베이스화 하거나 온라인상에서 바이오정보의 사용을 꺼려하고 있는 추세다[4].

더욱이 최근에 연구에 따르며, 지문영상과 같은 바이오정보의 원본 이미지에서 추출된 바이오인식 템플릿을 이용하여 역으로 원본영상을 만들어 낼 수 있다는 연구가 발표되어 바이오인식 시스템에서 사용하고 있는 바이오인식 템플릿에 대한 보호 연구가 활발히 이루어지고 있다[4]. 먼저, 기술적인 측면에서 보면, 바이오정보의 유출 및 불법적 사용에 대한 문제점을 해결하기 위하여 바이오인식정보를 은

접수일자 : 2008년 5월 30일
완료일자 : 2008년 6월 25일
이 논문은 KISA(정보보호진흥원)의 학술연구지원사업의 연구비지원에 의하여 연구되었음
+ : 교신저자

닉하여 불법 사용자가 은닉된 정보에 접근하지 못하도록 하는 워터마킹에 대한 연구들이 진행되고 있다. 미국 미시건 대학의 Jain 등은 지문 영상에 얼굴정보를 삽입할 수 있는 지문 영상 워터마킹기법을 제시하였다[5]. 이 기법은 얼굴의 특징인 고유 얼굴을 지문 영상에 워터마크로써 삽입한 후, 복원된 얼굴 영상은 얼굴 확인에 이용될 수 있음을 제안하였으나, 시스템 차원에서의 얼굴인증은 시도하지 않았다. 또한, 워터마킹에 따른 지문 영상과 지문 특징의 변형정도를 실험결과로 제시하였으나, 지문 및 복원된 얼굴 인식에 대한 실험은 제시되지 않았다. 국내에서는 웨이블렛을 이용하여 워터마크 삽입위치를 결정하고 배경영상의 특성을 고려한 적응적 가중치설정방법에 의해 워터마크를 효과적으로 은닉하고. 은닉된 워터마크 데이터는 워터마크가 삽입된 영상에 웨이블렛 역변환을 적용하여 효과적으로 바이오인식 특징을 추출하여 커버이미지에 대해서도 높은 인식률을 갖는 디지털 워터 마킹 기법이 제시되었다[6].

또 다른 기술적 기법으로는 변환 가능한 바이오 템플릿(changeable biometric template) 혹은, 취소 가능한 바이오 템플릿(cancellable biometric template) 기법이다[7][8]. 바이오 템플릿의 사용에 있어서 문제되는 부분이 바이오인식 템플릿이 불법 유출 되었을 때 이를 쉽게 바꿀 수 없다는데 있다. 따라서 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. 그러나 이 분야에 대한 연구는 실용화하기에는 아직 초기 단계로 이러한 기술을 응용할 수 있는 체계화된 방법이나 알고리즘의 정립이 필요한 단계라고 볼 수 있다.

이에, 본 연구에서는 실제 바이오 인식 시스템의 운영상에서 발생할 수 있는 위협요소를 분석하고 대책을 제시하며, 특히 사용자의 ID와 바이오인식 템플릿의 결합에 따르는 위협 및 결합된 바이오정보 패키지의 무결성(integrity), 기밀성(confidentiality)를 보호하기 위한 방안에 초점을 두어서 기술하고자 한다. 본 논문에서 주로 다루고자 하는 사항은 다음과 같다.

- 바이오인식 시스템에서 템플릿의 생성, 전송, 저장과 관련되는 각 단계별 위협 요소의 정의와 대책
- 바이오인식 시스템의 응용구성 별 바이오인식 템플릿과 사용자 정보의 결합과 이에 따른 위협과 바이오정보의 무결성(integrity), 기밀성(confidentiality) 보장 방안
- 프라이버시 보호 관점에서의 바이오인식 시스템 구성과 바이오 인식 템플릿 보호

2. 바이오 인식시스템과 바이오인식 템플릿

바이오인식 시스템은 신원인증을 바라는 대상자의 바이오정보를 기초로 신분확인을 원하는 대상자가 본인이 맞는지의 여부를 확인하는 시스템이라고 할 수 있다. 보통 많이 사용되고 있는 바이오정보로는 지문, 얼굴, 홍채, 손등정맥, 지정맥 등의 정적 바이오정보와 서명, 음성, 걸음새와 같은 대상자의 동적 바이오정보를 이용하는 것으로 나눌 수 있다. 이러한 생체인식시스템의 구성도를 국제표준기구(ISO)의 기준에 따라 나타낸 것이 그림 1이다.

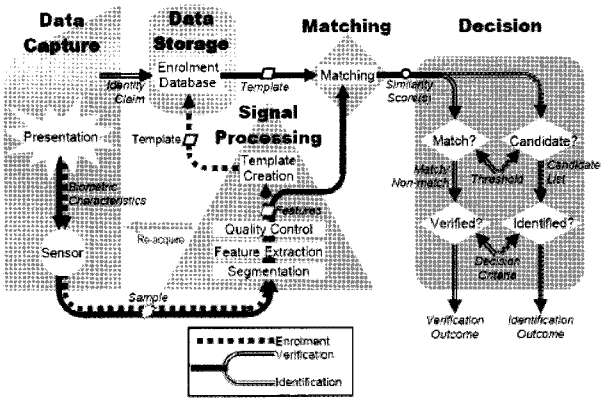

그림 1. 바이오인식 시스템의 구성도[9]
Figure 1. Biometric System Diagram

상기의 그림에서 볼 수 있듯이 바이오인식 시스템의 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 바이오인식템플릿을 생성하고 저장하는 과정을 의미한다. 개인식별과정은 주어진 바이오인식 템플릿에 대해서 이것이 누구의 것인지 신원을 밝히는데 목적이 있다. 이때 바이오인식시스템은 저장장치내의 모든 바이오인식 템플릿과의 비교를 통하여 가장 유사도가 높은 대상자의 식별정보를 제공하게 된다. 이러한 이유로 이를 1:N 비교라고도 부른다. 한편, 개인인증과정은 대상자가 본인의 바이오인식템플릿과 함께 개인식별용 ID를 제시하게 되면, 주어진 바이오인식 템플릿에 대해서 이것이 주장하고 있는 본인이 맞는지의 여부를 판별하는데 목적이 있다. 이때 바이오인식시스템은 저장장치내의 해당 ID의 바이오인식 템플릿과의 비교를 통하여 대상자의 인증여부를 결정하게 된다. 이러한 이유로 이를 1:1 비교라고도 부른다.

2.1 바이오인식 시스템의 구성

그림 1에 나타낸 바와 같이 바이오 인식 시스템은 크게 다섯 개의 부분으로 이루어져 있다. 각각에 대한 역할은 다음과 같다.

(a) 데이터취득부(Data Capture)

데이터 취득부는 대상자의 바이오인식 특징을 수집할 수 있는 입력장치를 포함한다. 이들 입력 장치는 사용자로부터 바이오인식 특징을 읽고 이 정보를 다른 부분이 처리하기에 적절한 형태로 변형한다.

데이터 수집 구성요소에 사용되는 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. 그러나 몇몇 바이오인식 정보들은 시간에 따라 천천히 변한다. 따라서 바이오인식 시스템은 이러한 변화에 대응하여 저장된 사용자의 템플릿을 최신 정보로 유지해야 한다.

(b) 신호처리부(Signal Processing)

신호 처리부는 데이터취득부로부터 얻어진 바이오인식데이터를 받아서 비교부가 요구하는 형태의 데이터로 변환하

여 주는 역할을 한다. 이 단계에서 입력 신호가 사용하기에 적당한지를 결정하기 위한 품질분석을 수행한다. 만약 입력 신호의 품질분석 결과가 적합하지 않다고 판단되면, 이 신호는 처리되지 않고, 등록(enroll) 정책에 따라서 대상자에게 다시 바이오 인식 정보를 요구해야 한다.

구체적으로 예를 들어보면, 지문인식의 경우에는 입력된 지문영상으로부터, 구간분할(segmentation), 이진화(binarization), 세선화(thinning) 등의 전처리 과정을 거친 후에 바이오인식용 특징정보로 미뉴셔(minutiae) 정보를 추출하게 된다. 얼굴인식의 경우에는 얼굴영상에서의 잡음제거, 영상 크기와 밝기 레벨의 정규화 과정 등의 전처리 과정을 거쳐서 특징정보로 고유얼굴(eigenface)계수 등을 구하게 된다.

(c) 데이터저장부(Data Storage)

데이터저장부는 기본적으로 등록된 사용자의 바이오인식 템플릿을 저장한다. 또한 등록된 템플릿의 추가, 삭제 그리고 복구 기능을 제공할 수 도 있다. 데이터저장부는 단일 대상자를 위한 단일 템플릿만을 저장할 수도 있고, 많은 사용자를 대상으로 수천 개의 템플릿들을 저장할 수도 있다. 구체적으로 바이오인식 템플릿이 저장되는 장소는 다음과 같은 곳이 있다.

- 대규모 바이오 템플릿 저장을 위한 컴퓨터 시스템 내의 데이터베이스
- 스마트 카드와 같은 휴대 가능한 토큰(token)
- 바이오인식용 디바이스내의 저장소

기본적으로 저장소에 저장된 데이터는 사용자의 템플릿과 사용자의 ID(개인식별정보)를 포함하고 있다. 이러한 개인식별정보는 개인확인(Identification)이나 개인인증(verification)시에 주어지는 바이오인식 템플릿과의 비교결과에 따라 같이 주어지게 된다.

(d) 비교부(Matching)

비교부는 신호처리부에서 처리된 대상자의 바이오인식특징값과 데이터저장부에 저장 되어 있는 바이오인식 템플릿을 비교하는 역할을 한다. 여기서 주로 사용되는 방법은 거리척도 등을 이용하여 특징값과 템플릿간의 거리척도 등을 이용하여 두개의 값이 얼마나 정확하게 일치하는가를 나타내는 수치 값을 계산하여 결정부에서 사용하기에 적절한 형태의 점수(score)를 산출하는 역할을 한다. 가장 간단한 개인인증과정은 다음과 같이 설명 될 수 있다. 비교부는 신호처리부에서 받은 바이오인식특징값을 데이터베이스내의 등록된 템플릿과 1대1로 비교하고 그 결과를 결정부로 전달한다. 결정 구성요소는 스코어와 바이오인식시스템 정책에 입각하여 대상자가 등록 템플릿의 해당되는 본인 인지애 이진 결정을 출력하는 것으로 볼 수 있다.

(e) 결정부(Decision)

결정부는 비교부로부터 스코어를 받고, 시스템 결정 정책에 입각하여 대상자를 식별 또는 검증하게 된다. 결정 구성요소는 정합 구성요소에서 계산된 스코어를 기반으로 대상자의 식별 결과로 "예" 또는 "아니오"의 이진 값을 반환한다. 간단한 방법으로, 결정은 단일 임계값을 기반으로 한다. 만약 스코어가 임계값을 넘을 경우, 시스템은 주장자가 정말 템플릿을 등록한 개인이라고 결론을 내린다. 만약 그렇지 않다면, 시스템은 사용자가 등록된 개인이 아니라고 결론을 내린다. 그러나 예를 들어 사회보장의 이중 혜택을 받으려는 대상자를 가려내는 경우와 같은 경우에 있어서는 어떤 시스템에 있어서는, 사용자의 템플릿이 해당 데이터베이스에 등록되어 있지 않다는 것을 확인하는 것이 주목적이 될 수 있다.

2.2 바이오인식 템플릿 보호

바이오인식 시스템의 각 구성 부분에서 언급되고 있는 것이 바로 바이오인식 템플릿이다. 국제 표준(ISO)에 따르면 바이오인식 템플릿을 정의하기 위해서는 다음과 같은 몇 가지 용어에 대한 정의가 필요하다[9].

-바이오인식 샘플(biometric sample): 바이오인식 특징점이 추출되기 전의 바이오인식 특징의 아날로그 및 디지털 표현으로 바이오인식 취득 디바이스나 바이오인식 데이터취득부에서 얻어 지는 것. 예를 들면 얼굴영상이나 취득된 지문영상이 여기에 해당 된다.
-바이오인식 특징(biometric feature): 바이오인식 샘플로부터 추출된 숫자나 레이블로 비교를 위해 사용된다. 예를 들면 얼굴영상에서 고유얼굴(eigenface)에 대한 계수값이나 지문인식에 있어서 미뉴셔(minutiae)의 위치와 각도값 등의 모임이 여기에 해당된다.

최종적으로 바이오인식 템플릿은 다음과 같이 정의된다.

-바이오인식 템플릿(biometric template): 인식하고자하는 바이오인식 샘플의 바이오인식 특징에 직접적으로 필적하는 저장된 형태의 바이오인식 특징점 집합. 예를 들면 얼굴영상에서 고유얼굴(eigenface)에 대한 계수값이나 지문인식에 있어서 미뉴셔(minutiae)의 위치와 각도값 등이 비교부를 위해서 보통 사용자 ID 정보 등과 함께 저장부에 저장되어 있는 것을 말한다.

위와 정의에서 알 수 있듯이, 바이오인식시스템에서 바이오인식 템플릿은 인증을 요구하는 대상자가 실제로 해당 식별 ID을 가진 본인인지의 여부를 가리는데 매우 중요한 역할을 함을 알 수 있다.

표 1. 바이오인식템플릿과 ID의 공격 유형
Table.1 Biometric Template and ID Attacks

공격대상	내용
개인식별자(ID)	ID를 조작하여 유효하지 않은(Invalid) ID로 변경
	ID를 변조하여 침입자의 사용자의 ID로 대체
	등록되어 있는 ID를 삭제
바이오인식템플릿(BT)	BT를 조작하여 해당 ID의 바이오 특징값과의 매칭값이 현저히 낮아지도록 변경
	해당 BT를 변조하여 침입자의 바이오 특징값으로 대체
	등록되어 있는 BT를 삭제

표 1에 나열되어 있는 공격은 바이오템플릿이 저장공간에 있을 시의 제한적 상황만을 기술하고 있다. 그러나 바이오 인식 템플릿의 활용이라는 측면에서 보면, 템플릿의 발

생, 저장, 비교, 판단 등의 각 바이오인식 시스템의 부시스템별로 다양한 공격이 존재함을 알 수 있다. 이들에 대한 자세한 사항은 다음 장에서 기술하고 대책을 논의하고자 한다.

3. 바이오인식 템플릿보호를 위한 취약성 분석 및 대책

바이오인식시스템에서 템플릿에 대한 공격위험이 있는 주요 지점을 나타내면 그림 2와 같으며 다음과 같다.

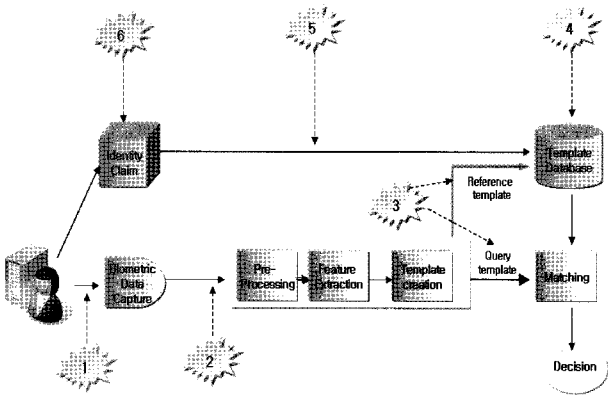

그림 2. 바이오인식 시스템에서의 템플릿 주요 공격지점[10]
Figure 2. Biometric template attack points of a biomtric system[10]

AT_P1: 가짜 바이오정보(Spoofing biometric identifier)에 의한 공격. 위조지문이나 복사된 얼굴사진 등을 통한 바이오정보의 등록이나 타인을 사칭하는 행위
AT_P2: 취득된 바이오인식 샘플의 변경. 바이오인식 데이터의 취득부로부터 얻어진 샘플을 임의로 변경
AT_P3: 만들어진 템플릿을 저장부에 이송 중에 변경
AT_P4: 저장되어진 템플릿에 대한 변경
AT_P5: 개인인증과정에서 ID에 대한 고의적 오차 삽입.조작된 ID나 잘못된 ID로의 변경
AT_P6: 등록이나 인증단계에서 변조된 ID의 제공

바이오인식 템플릿에 대한 주요 위협과 대책과 이에 해당되는 공격 포인트는 다음과 같다.

표 2. 바이오인식시스템에서의 공격과 대책
Table,2 Attacks and Countermeasure in the Biometric System

위협	공격의 예	공격위치	
위조 바이오인식샘플	모조지문,얼굴사진, 홍채사진	AT_P1	R1
날조된 바이오인식 템플릿	저장부에 저장되어 있거나, 등록시의 제공되어 생성되는 바이오인식 템플릿을 날조	AT_P1 AT_P4	R2
바이오인식 데이터/템플릿 전송위협	등록이나 데이터 전송시의 바이오인식 템플릿 가로채기	AT_P2 AT_P3	R3
사용자식별자	개인인증을 위해 제공되는 식별자의 가로채기나 변조	AT_P5 AT_P6	R4
등록이나 관리 사용상의 위협	등록, 관리, 사용상의 바이오인식샘플 변경	AT_P1 - AT_P6	R5
유사한 바이오인식 특징을 가진 사용자에 의한 공격	합법사용자와 유사한 바이오인식특징을 가진 비합법사용자의 인증시도	AT_P1	R6
무작위 공격	침입자가 시스템을 속이기 위해 계속적인 시도	AT_P1	R7
바이오인식 템플릿의 소실	하드 디스크나 하드웨어의 소실	AT_P4	R8

상기의 8가지 위협에 대한 대책을 살펴보면 다음과 같다.
(Ⅰ) 일반적인 정보보안 정책에 의한 위협방지의 대책이 될 수 있는 것: R5, R7[1], R8[2]
(Ⅱ) 하나의 바이오인식 정보가 아닌 여러개의 바이오인식 정보를 이용하는 다중 생체인식 기법을 이용한 대책: R1, R6
(Ⅲ) 바이오정보의 취득대상인 살아있는(Liveness)지의 여부로 위조나 사진 등의 복제를 검출하는 대책: R1
(Ⅳ) 암호와 전자서명 등의 보안 기법에 기반한 대책: R2,R3,R4

4. 바이오인식 시스템 구성별 바이오인식 템플릿 및 사용자 식별정보 보호

바이오 인식시스템은 다양한 형태로 구현이 가능하다. 그러나 이를 바이오인식 템플릿이 저장되고 비교되는 장소에 따라서 다음과 같은 4가지의 형태로 정의할 수 있다[11][12]. 본 논문에서는 각각의 응용 형태에 따라서 바이오인식 시스템이 인증시스템으로 사용될 경우 필수적으로 같이 사용하게 되는 개인식별정보(ID)와 바이오인식 템플릿의 보호를 기밀성(confidentiality)와 무결성(integrity)의 관점에서 살펴보고자 한다.

표 3. 바이오인식 시스템 응용 형태
Table 3. Application Models of Biometric System

비교 \ 저장	클라이언트(client)	서버(server)
클라이언트(client)	지역(local) 모델 (MOC)	Download 모델 (EMR)
서버(server)	Attached 모델 (전자여권)	Center Model (AFIS)

4.1 지역모델(local model)에서의 바이오인식 팻키지 보호

지역모델에서는 바이오인식 템플릿이 클라이언트에 저장

1) 시스템이 허용할 수 있는 인증실패 횟수를 설정한다.
2) 데이터 백업과 복구에 대한 대책을 강구한다.

되며 이에 대한 비교 역시 클라이언트에서 이루어지게 되는 구조이다. 이러한 경우의 대표적 경우가 MOC (Match on Card) 형태의 스마트 카드를 사용한 경우이다. 그림 2는 바이오인식 기능이 있는 스마트 카드를 이용한 시스템의 구성을 보여주고 있다. 여기에서는 개인식별정보(ID)가 스마트 카드 내에 위치하게 되어 카드 밖으로 데이터가 유출되지 않는 장점이 있다. 먼저 단말기(ATM)에 설치되어 있는 센서로부터 바이오인식영상이 얻어지고 여기에서 추출된 바이오인식 특징점이 MOC내로 보내져서 여기에서 비교가 이루어지게 된다. 비교의 결과인 인증여부가 서버로 보내져서 사용자가 원하는 거래의 허용여부가 결정되게 된다.

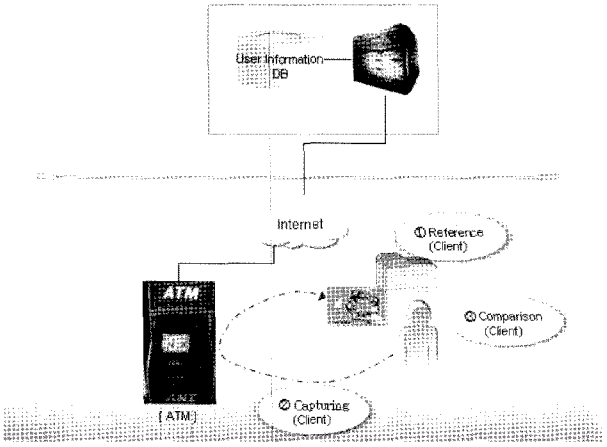

그림 3. 은행에 사용된 Local 모델
Figure 3. Local model applied in Banking system

센서에서 획득되어 얻어진 바이오인식 특징점이 MOC로 보내질 때 암호화 기능과 디지털서명 또는 MAC(message authentication code)의 생성기능을 제공해야한다. 즉, 센서로부터 수신된 데이터에 대한 무결성 검증 및 비교장치로 보내는 데이터에 대한 무결성 확인 기능을 제공해야하며, 센서와 획득 및 추출 장치간 그리고 획득장치와 비교장치간 링크에서 기밀성을 보장해야 한다.

4.2 Download 모델에서의 바이오인식 팻키지 보호

Download 모델에서는 바이오인식템플릿이 서버에 저장되어 있는 형태인다. 먼저 사용자는 자신의 ID를 서버로 보내서 여기에 해당되는 바이오인식템플릿을 가져오게 된다. 이것을 센서로부터 취득된 바이오인식 특징값과 비교하여 개인의 인증여부를 최종적으로 결정짓게 된다. 그림 4는 이를 채용한 전자의료기록시스템(Electronic Medical Record System)을 나타내고 있다. 서버와 클라이언트와의 통신을 통해서 개인식별정보와 바이오인식 템플릿이 주고 받게 되므로 다음가 같은 보안요소를 염두에 두어야한다.

초기에 ID 정보를 서버를 보낼 때, 이것과 바이오인식 템플릿과의 상호 연결을 막기 위한 고려가 있어야 한다. ID 정보를 서버에 보낼 때, 기밀성(confidentiality)와 무결성(integrity)을 위하여 암호화와 전자서명이 필요하다. 또한 서버로부터 클라이언트로 바이오인식템플릿을 전송할 시에 이의 누출을 막기 위하여 적절히 암호화 되어야 하며, 바이오인식 템프릿에 대한 다양한 변경기법에 대응하기 위한 전자 서명이 필요하다.

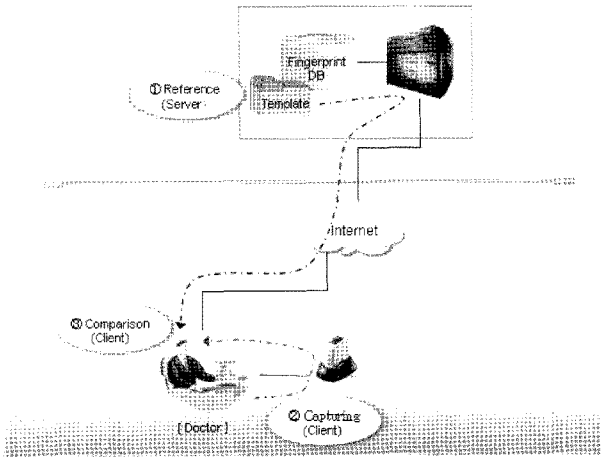

그림 4. EMR 시스템에 사용된 Download 모델
Figure 4. Download model applied in EMR system

4.3 Attached 모델에서의 바이오인식 팻키지 보호

Attached 모델에서는 바이오인식템플릿이 클라이언트에 저장되며 비교가 서버에서 이루어지는 형태이다. 그림5 에서와같은 전자여권을 이용한 출입국 통제 시스템을 보여주고 있다. 사용자는 Kiosk에서 전자여권을 제출하면서 자신의 바이오 데이터를 제공한다. 그러면 Kiosk에서 특징점을 뽑아내어 이를 전자여권상의 템플릿과 함께 서버로 보내게 된다. 그러면 서버에서는 비교기를 거쳐서 인증여부를 클라이언트에게 주게 된다. 이러한 바이오인식시스템의 구성 장점은 서버에 바이오인식 템플릿을 저장해야하는 위험 부담이 없을뿐더러 비교부가 서버에게만 있으면 되므로 클라이언트 시스템에서의 계산 부담을 줄여 줄 수 있다. 또한 비교부가 서버에 존재함으로서 고신뢰성을 갖는 단일의 비교부이므로 안정적인 인증 결과를 줄 수 있는 장점이 있다.

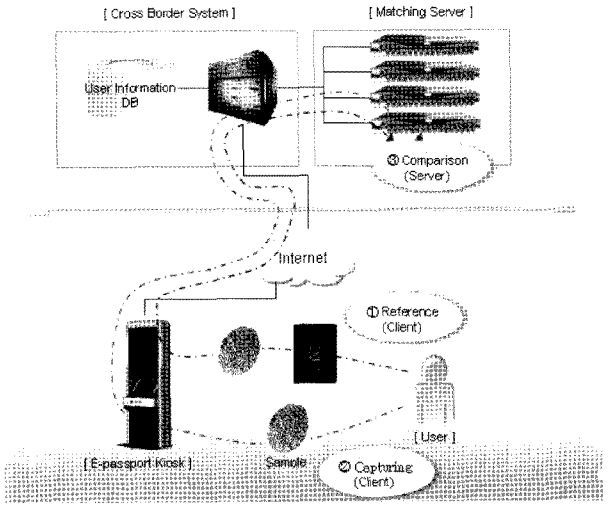

그림 5. 전자여권시스템에 사용된 Attached 모델
Figure 5. Attached model applied in E-passport

서버와 클라이언트 사이에 바이오인식 템플릿과 바이오인식 특징점이 전송되므로 이들간에는 기밀성(confidentiality)과 무결성(integrity)을 위하여 암호화와 전자서명이 필요하다. 이 경우 사용자 식별정보와 바이오 인

식 템플릿은 클라이언트에 저장되어 있으므로 이들 정보의 보호를 위하여 암호화와 전자서명이 필요하다. 전자여권과 같은 스템에 있어서는 여권내에 내재되어 있는 IC칩과 단말기 사이의 정보보호 및 보안을 위한 접근통제(Access Control) 및 권한인증 기술로 되어 있다[13]

4.4 Center모델에서의 바이오인식 팻키지 보호

Center 모델에서는 바이오인식템플릿이 서버에 저장되어 있고 비교 또한 서버에서 이루어지는 구조이다. 클라이언트에서는 단지 바이오인식 데이터를 취득하여 서버에 보내는 역할을 한다. 그러면 서버에서는 저장되어 있는 바이오인식 템플릿과의 비교를 통하여 인증 여부를 결정하게 된다. 그림 5는 이를 채용한 자동지문인식시스템 (Automatic Fingerprint Identification System)을 나타내고 있다. 서버와 클라이언트와의 통신을 통해서 개인식별정보와 바이오인식 템플릿이 주고 받게 되므로 다른 모델에 비해서 여러 가지 보안요소를 고려하여야 한다.

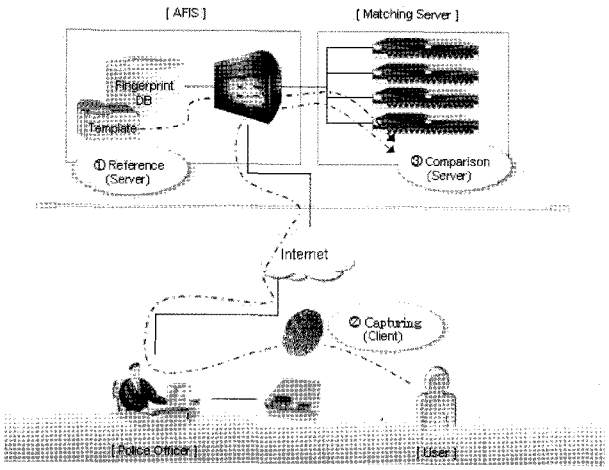

그림 6. AFIS에 사용된 center 모델
Figure 6. Center model applied in AFIS

상기 모델의 경우는 사용자가 대상자의 지문정보를 취득하여 이를 서보로 전송하는 단계에서, 기밀성과 무결성을 보장 하여야 한다. 특히 위의 AFIS 시스템의 경우는 서버에서 저장되어 있는 바이오인식 템플릿과의 비교를 통하여 매칭값이 높은 몇 개의 바이오인식 템플릿에 대해서 이와 연관된 개인 식별 정보를 서버에서 클라이언트로 전송하게 되는데 정보보호를 위하여 암호화와 전자서명이 필요하다.

5. 바이오인식 템플릿과 프라이버시 보호

5.1 바이오인식 시스템과 프라이버시

바이오인식기법은 정보보호를 위한 여러 가지 기법 가운데 하나라고 볼 수 있다. 그러나 바이오인식에서 사용되는 바이오인식 특징 즉, 지문이나 얼굴영상과 같은 것들은 또 다른 중요한 정보보호의 대상이 된다고 할 수 있다. 왜냐하면 이러한 것은 개인의 바이오인식 특징을 담고 있어서 언제든 다른 사람과 나를 구별 짓는 중요한 수단으로 사용 될 수 있는 개인 식별정보(Personal Identifiable Information)의 일부이기 때문이다. 어떤 시스템이 바이오인식시스템을 개인인증용으로 채택하였다면, 우리의 바이오정보는 나의 개인정보를 부당한 사용으로부터 보호하는 역할을 한다고 할 수 있다. 그러나 한편으로 바이오인식 정보가 유출 된다면 이것이 개인정보를 침해할 수 있는 요소가 되어 개인의 프라이버시를 침해하게 된다. 정보시스템의 관점에서 보면 프라이버시란 타인에 위한 부당한 침입이 없이 독자적인 삶을 영위하면서 개인의 정보에 대한 접근을 통제할 수 있는 능력을 말한다[14].

개인정보보호를 위해서 당사자의 바이오정보를 이용하는 경우를 언급했으나, 바이오정보가 개인의 식별자(identifier)로서 사용되는 경우에는 본인의 동의 여부와 관계없이 우리의 바이오정보가 사용될 수 있게 된다. 예를 들어, 사건 현장에 남은 유일한 증거가 지문이었다면, 필연적으로 그러한 지문과 유사도를 갖는 지문을 찾아내기 위해 불특정 다수의 지문이 검색되고 매칭되는 상황을 생각 할 수 있다. 이럴 경우 개인의 고유한 바이오정보가 본인의 동의 없이 사용될 수 있는 경우라 할 수 있다. 이럴 경우 개인의 신체적 자유에 해당되는 프라이버시 침해 문제를 야기하게 된다.

즉, 대규모의 바이오인식 템플릿을 구출하여 관리하게 되는 경우, 지문과 같은 바이오특징이 개인의 신분을 나타내는 하나의 개인식별자로 작용하여 특정인의 모든 거래를 추적하거나 엄청난 양의 개인적 정보를 그와 연관시키는데 사용될 수 있다는 것이다. 특히 앞장에서 언급된 바와 같이 바이오인식템플릿과 같이 사용되는 사용자식별정보(ID)[3]와 바이오인식 데이터/템플릿이 동시에 유출되었을 경우 그 피해정도는 더욱더 커질 수 있다. 따라서 앞의 4장에서 언급된 것 같이 바이오인식 시스템의 각 단계에서 데이터의 기밀성과 위/변조를 막을 수 있는 보안기법이 적용되어야 한다.

5.2 프라이버시를 고려한 바이오인식 템플릿 사용

개인식별정보에 대한 프라이버시를 위하여 각국의 의견을 모아서 ISO SC27에서는 프라이버시에 대한 국제 표준을 만들고 있다[15][16]. 이에 따르면 개인식별정보의 생명주기별 프라이버시 요구사항과 프라이버시 보호를 위한 안정보장방법이 그림7과 같이 나타낼 수 있다.

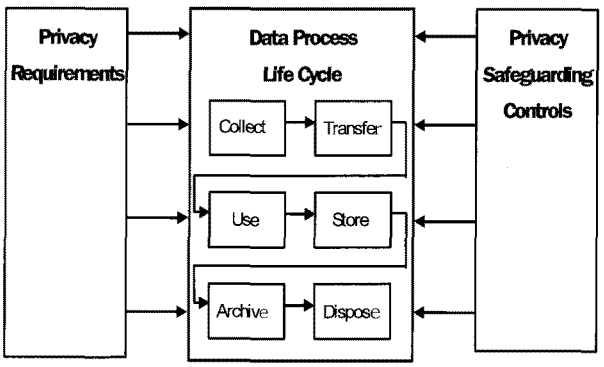

그림 7. 프리이버시 보호를 위한 프레임워크
Figure 7. Privacy Framework

3) 우리나라의 경우는 주민등록 번호나 개인의 은행계좌 번호 등이 여기에 해당된다. 더 넓게 보면 개인의 전화번호나 이메일 주소와 같은 것은 쉽게 변경이 가능하지만 이들이 바이오 인식 정보와 결합되어 사용될 경우에는 필요한 보안 조치를 취하여야 한다.

본 논문에서는 위의 표준안을 따라 개인의 프라이버시를 침해하지 않고 바이오인식 템플릿을 이용한 개인 인증을 위해 요구되는 다음 원칙들을 제시한다.

① 동의와 선택(Consent and Choice)

개인의 바이오 정보를 수집함에 있어서 특별히 법에 의해서 개인의 동의 없이 바이오정보를 수집할수 있도록 구정하지 않은 자신의 바이오 정보가 수집되고, 전달되고, 사용, 저장, 보존되는 각 단계의 수명주기(lifecycle) 에 대해서 그렇게 할지의 여부를 선택할 수 있어야 한다. 바이오인식 정보의 부당한 수집은 정보 프라이버시의 주된 관심사이다. 부당한 정보 수집은 바이오인식 데이터베이스와 개인의 동의가 없거나 개인이 알지 못하는 사이에 수행되는 비교 과정을 통하여 개인의 정보 프라이버시를 침해 할 수 있다.

② 책임규명과 목적의 명확성
(Accountability and Purpose Specification)

사용자가 제공하는 바이오인식 데이터의 수집, 전달, 사용, 저장, 보존되는 각 단계의 수명주기에 대한 관리 책임사항 및 책임자가 명확해야 한다. 이에는 앞장에서 설명된 암호와 전자서명등을 이용한 적적한 보안조치를 취해야 함을 위미한다. 한편, 바이오인식 시스템의 사용 목적을 명확하게 하여야 하여 바이오인식 정보에 대한 부당한 사용을 방지할 수 있어야 한다. 이를 위하여 수집단계에서부터 최초의 정의된 목적에 필요한 최소한의 생체정보만을 수집하는 것을 권고한다.

③ 사용, 유지와 공개의 제한
(Use, Retention and Disclosure Limitation)

바이오인식 정보를 필요 이상으로 오랜 기간 저장하고 있다면 이 또한 프라이버시의 침해 요소로 작용할 수 있다. 당초의 바이오인식 시스템에서 규정한 목적을 달성하였다면 저장하고 있던 바이오정보는 마땅히 파기해야 할 것이다. 그렇지 않은 경우 추후의 기술의 발전에 따라 다른 용도로 바이오정보가 이용될 가능성이 많아지고 이는 바이오정보 제공자에게 잠재적인 프라이버시 침해요소로 작용할 가능성이 많다. 바이오인식 정보를 다른 공공 기관이나 개인적 영역의 조직에 대하여 부당하게 공개하는 것은 개인이 자신의 데이터에 대하여 소유하고 있는 정보에 대한 통제권을 침해하는 것이다.

④ 정확도와 바이오인식 정보의 질
(Accuracy and Quality)

바이오인식정보를 처리하는 경우 사용 목적에 적절한 정확도와 신규성을 보장 할 수 있어야 한다. 얼굴인식에 사용되는 특징 정보의 경우대상자의 특징값이 시간의 변화에 따라 그 정확도가 떨어지므로 적절한 주기를 가지고 새로운 바이오인식 정보로 대체 될 수 있도록 바이오인식 템플릿을 등록 하여야 한다. 이를 준수하지 않아서 생기는 타인과의 비교 결과의 부정확성은 개인의 정보정보의 유출을 가져 올 수 도 있기 때문이다.

⑤ 개인참가와 접근허용
(Individual Participation and Access)

바이오인식 정보를 제공한 사람은 당초의 의도에 맞게 바이오인식 시스템이 동작하고 있는지 이를 알 수 있도록 해야 하며 본인의 바이오정보가 어디에 어떻게 사용되고 있는지에 대한 문의 사항이 있다면 이를 질의 하고 합리적인 시간내에 이에 대한 답변을 들을 수 있어야 한다.

5. 결 론

개인마다 타고난 신체적·행동적 특성을 이용한 바이오정보의 불변성은 보안시스템의 성능을 극대화하는 긍정적 측면을 가지고 있는 반면에 이러한 바이오 정보가 분실되거나 다른 사람에 의해서 도용되었을 경우에 비밀번호나 ID처럼 사용자가 원하는 경우에 쉽게 변경하기가 어렵다는 치명적인 단점을 지니고 있다. 이와 더불어 바이오인식 데이터를 취득하기 위해서는 개인의 신체적 프라이버시를 침해할 수 있는 소지가 많으므로 바이오인식 정보를 이용한 시스템 구축에 대해서 사회적 저항감이 있는 것 또한 사실이다.

이에 본 연구에서는 바이오인식 템플릿과 개인 식별정보(ID)에 대한 다양한 위협 요인들을 분석하고 이를 방지할 수 있는 대책을 다루었다. 특히, 실제 바이오인식 시스템을 운영하는데 사용되는 대표적인 4가지의 운영방식에 대하여 취약성을 분석하여 각각의 경우에 개인 식별 정보와 바이오인식 템플릿의 보호를 위해 암호와 전자서명에 의해서 방지될 수 있는 보안 위협의 유형 대책에 초점을 두어 기술하였다. 이러한 기술적 보안 대책과 함께 마지막 부분에서 기술된 프라이버시 친화적 바이오인식 시스템의 구현 방식을 따른다면 사용자의 개인정보를 보호함과 동시에 높은 보안능력을 갖는 고성능의 개인인증용 바이오인식 시스템을 구축할 수 있다.

참 고 문 헌

[1] 전명근, *생체인식(Biometrics) 총론*, 한국정보통신교육원, 2004.

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

[3] Arun A. Ross, K. Nandakumar, Anil K. Jain, *Handbook of Multibiometrics*, Springer, 2006.

[4] Arun Ross, Jidnya Shah, Anil K. Jain, "From template to image: Reconstucting fingerprints from minutiae points", *IEEE Tr. on Pattern Analysis and Machine Intelligence*, "Vol. 29, No.4, 2007

[5] Anil K. Jain, Umut Uludag, "Hiding biometric data," *IEEE Trans. Pattern Analysis and Machine Intelligence*, Vol. 25, No. 11, pp. 1494-1498, 2003.

[6] 이욱재, 이대종, 문기영, 전명근, "웨이블렛을 이용한 생체정보의 강인한 워터마킹 알고리즘", *한국퍼지 및 지능시스템학회* Vol. 17, No.5 pp.632-639, 2007.

[7] Jongsun Kim, Chulhan Lee, Jaihie 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.

[8] Ratha, N, Connell, J, Bolle R..M, Chikkerur. S, "Cancellable Biometrics: A case study in fingerprint" *Int. conference on pattern recognition*, Vol. 4, pp. 370-373, 2006.
[9] ISO/IEC JTC1 SC37 N2486, *Standing Document 2*, Harmonized Biometric Vocaburuary, 2008
[10] FIDIS(Future of Identity in the Information Society), *D3.10: Biometrics in identity management*, 2007."
[11] ITU-T draft Recommendation X.tsm-part1: Telebiometric system mechanism -General biometric authentication protocol and system model profile for telecommunication systems, ITU-T SG17 Q.8, 2007.
[12] Yong-Nyuo Shin, *Secure mechanism for biometric recognition technology in internet environment*, Ph.D. thesis, Korea University, 2007.
[13] 전은경, 이용준, 전자여권에 사용된 융합 보안기술 *정보보호학회지*, 제 17권 5호, pp 40-43, 2007.
[14] 전명근, 문기영, 생체정보 이용과 프라이버시 보호, *정보보호학회지*, 제 15권 6호, pp.11-18, 2005.
[15] ISO/IEC JTC1 SC27 N6258, Information technology-security techniques-A privacy framework, 2007
[16] ISO/IEC JTC1 SC27 N6259, Information technology-security techniques-A privacy reference architecture, 2007

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 산업지원팀 주임연구원
2005년 ~ 현재 : TTA PG505(바이오인식 프로젝트 그룹) 간사

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

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 부의장
2007년 ~ 현재 : ISO/IEC SC27 정보보호 표준화 전문위원

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