

바이오인식 기술과 원격의료 서비스의 융합 동향

문 호 건*, 류 희 수**, 김 재 성***

요 약

스마트폰과 태블릿 PC같은 스마트 기기의 보급 증가는 원격의료 서비스 분야의 활성화에 커다란 영향력을 미치고 있다. 그러나 환자와 의사가 직접 대면하지 않고 네트워크에 연결된 스마트 기기를 통해 진료 행위를 할 경우, 환자와 의사간에 상호 인식과 인증 등과 같은 보안 문제가 해결해야 할 가장 큰 걸림돌로 여전히 남아있다. 스마트 기기는 이동성과 편의성이 뛰어난 반면 각종 보안 침해 위협에 상대적으로 쉽게 노출될 수 있다는 단점이 있다. 스마트 기기를 원격의료 서비스에서 안전하게 활용하기 위해 바이오인식(Biometrics) 기술과의 융합 시도와 관련 표준화 작업이 적극 추진되고 있다. 본 논문에서는 안전한 원격의료 서비스 제공을 위해 바이오인식 기술의 융합 필요성과 기술 및 서비스 개발 사례를 분석하고, 원격의료 서비스 활성화를 위해 선결되어야 할 주요 과제를 모색하고자 한다.

I. 서 론

우리나라도 인구 고령화와 더불어 생활수준 향상에 따른 식생활 패턴의 변화로 과거에 비해 당뇨, 고혈압, 고지혈증 등 선진국형 만성질환이 급속도로 증가하고 있으며, 이에 따른 의료비용이 향후 사회적인 부담으로 크게 작용할 것으로 예상된다. 국민의 건강관리를 국가의 보편적 복지로 제공해야 한다는 사회적 요구가 증가하면서 정부는 국가 의료 체계를 선진화시키고 국민의 의료비 상승 부담은 억제하는 효과적인 대응방안의 하나로 원격의료 서비스의 활성화 방안을 지속적으로 검토해 왔다.

원격의료 서비스 분야는 이미 선진 각국과 국내의 정부 및 기업들에게 21세기를 선도할 주요 성장 동력으로 인식되고 있으며, 이에 따라 의료산업으로의 성장 기반을 마련하기 위한 기술적, 제도적 방안들이 활발하게 마련되고 있다[1][2]. 특히, ‘모바일 혁명’이라 불리는 스마트폰과 태블릿 PC 같은 스마트 기기의 보급 증가는 원격의료 서비스 분야의 활성화에 커다란 영향력을 미치고 있다.

스마트 기기를 활용한 원격의료 및 헬스 관련 시장이 급성장할 것으로 예상됨에 따라 의료기기 제조업체, 통

신사업자 및 의료기관 들 간에 기술 개발과 시장 공략을 위한 협력과 경쟁이 활발히 전개되고 있다[3]. 국내외 병원들도 자체적으로 스마트폰을 각종 의료 현장에 적용하거나 환자들을 위한 서비스에 활용하는 범위가 넓어지고 있어, 의료 현장에서 스마트폰의 활용은 그 끝을 알 수 없을 정도로 확대될 것으로 예상된다[4][5]. 그러나 환자와 의사가 직접적인 대면을 하지 않고 네트워크에 연결된 스마트 기기를 통해 진료 행위를 할 경우, 환자와 의사간에 상호 인식과 인증 등과 같은 보안 문제가 해결해야 할 가장 큰 과제로 남는다[6].

스마트 기기는 이동성과 편의성이 뛰어난 반면 PC나 전용기기에 비해 각종 보안 침해 위협에 상대적으로 쉽게 노출될 수 있다는 단점이 있다. 따라서 스마트 기기를 원격의료 서비스에서 안전하게 활용하기 위해서는 기존의 개인 확인 및 검증 방법의 한계를 극복할 수 있는 바이오인식(Biometrics) 기술의 적용과 표준화가 적극 추진되어야 한다[7].

2장에서는 원격의료의 다양한 서비스 유형을 분석하고 3장에서는 원격의료 서비스에 대한 보안 요구사항에 대해 소개한다. 4장에서는 바이오인식과 원격의료 융합 동향을 살펴보고 결론에서는 원격의료 서비스의 활성화를 위해 고려되어야 할 사항들에 대해 서술한다.

* KT 종합기술원 기술개발실 (hokun.moon@kt.com)

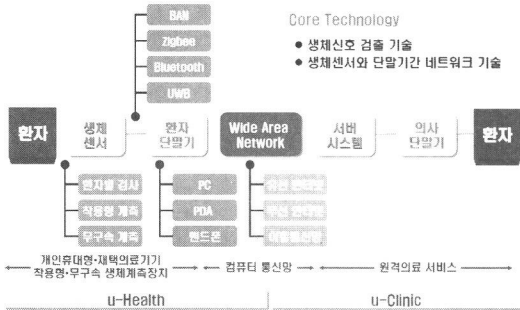
** 경인교육대학교 수학교육과 (hsryu@ginue.ac.kr)

*** 한국인터넷진흥원 (jskim@kisa.or.kr)

II. 원격의료의 정의와 서비스 유형

2.1 원격의료의 정의

원격의료(Telemedicine)는 광의로 “상호작용하는 정보통신 기술을 이용하여 원거리에 의료정보와 의료서비스를 전달하는 모든 활동”으로 정의되기도 하고, ‘원격보건(Telehealth)’ 또는 ‘원격건강관리(Tele-healthcare)’와 구별하여 협의로 “격지의 환자에 대한 의료의 제공 또는 그 지원을 위한 정보통신 기술의 활용”으로 정의되기도 한다. 원격의료 서비스는 [그림 1]과 같이 공간적, 시간적 제약을 없애고 환자가 생활공간 속에서 다양한 의료 센서 및 기기를 통해 수집된 생체 정보와 환경 정보를 기반으로 중앙의 원격의료 서비스 시스템을 통해 언제 어디서나 의료 피드백을 받을 수 있는 서비스를 총칭한다[8]. 국내의 경우, 공공부문 시범사업 대상자의 특성에 따라 원격의료(u-medical), 건강서비스산업(u-wellness) 및 고령친화사업(u-silver)이라는 이름으로 분류되기도 한다[9].



(그림 1) 원격의료 서비스 체계

2.2 원격의료 서비스 유형

원격의료 서비스 산업은 참여 집단들의 역할에 따라 원격의료 서비스 제공자, 서비스 수용자 및 환경 조성자로 나누어진다. 또한 각 참여집단 내에서도 개별 주체들의 역할 범위와 이해에 따라 다양한 형태의 서비스가 만들어 질 수 있다. [표 1]은 원격의료 서비스 산업의 참여 집단들에 포함되는 개별 주체들을 나타낸다[7].

원격의료 서비스 산업에 참여하는 집단의 요구에 따라 원격의료 서비스는 다양한 형태로 제공되고 있으며

[표 1] 원격의료 서비스 산업의 참여집단 분류

참여 집단	개별 주체
원격의료 서비스 제공자	의료기관
	케어서비스 사업자
	웰빙서비스 사업자
	정보통신 사업자
원격의료 서비스 수요자	장비/단말 사업자
	최종사용자(본인사용자)
	부양자(Care provider)
원격의료 조성자	정부 및 지방자치단체
	보험 사업자

세계 의사사회에서는 서비스 유형을 다음과 같이 분류하고 있다[10].

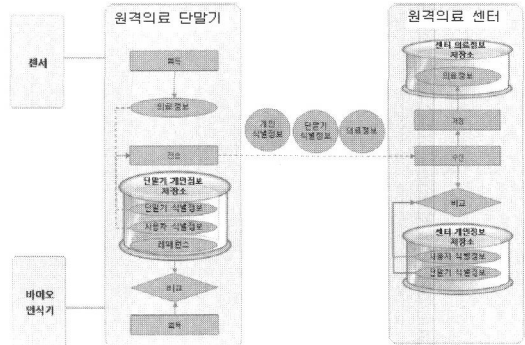
첫째, 원격지원(Tele-assistance)은 지리적으로 고통되어 있거나 열악한 환경에 놓여 있어 직접적인 진료를 받을 수는 없으나 현지에 있는 의료인이 원격지의 전문 의료인과 상호작용을 통해 환자가 치료를 받을 수 있는 의료 형태를 말한다. 둘째, 원격모니터링(Tele-monitoring)은 당뇨, 고혈압 또는 고위험 임신 등과 같은 만성질환자의 혈압이나 심전도 같은 환자의 의학적 정보가 의사에게 전자적으로 전달되는 상황에서 의사가 환자의 상태를 주기적으로 모니터할 수 있게 하는 의료 형태를 의미한다. 환자 본인이나 가족이 필요한 정보를 수집해서 전송할 수 있도록 훈련을 받을 수도 있으며 간호사나 의료기사, 혹은 전문 자격을 갖춘 사람이 신뢰할 수 있는 결과를 얻기 위해 개입할 수도 있다. 셋째, 원격상담(Tele-consultation)은 서비스 이용자인 환자가 인터넷을 비롯한 통신수단을 이용하여 서비스 제공자인 의사로부터 직접 건강 및 질병에 관한 의료 정보를 얻을 수 있는 형태의 의료 행위를 말한다. 이 경우, 온라인 상담이나 전화 상담을 통해 획득한 정보의 신뢰도나 비밀유지, 그리고 서비스 주체의 신원 및 자격여부 확인 등과 관련한 사전 준비가 필요하다. 넷째, 원격의료(Telemedicine)는 환자와 물리적으로 함께 있는 의사와 의료상의 문제에 대해 특별히 전문성을 갖고 있다고 판단되는 원격지의 의사 사이에 일어날 수 있는 서비스 유형이라 할 수 있다. 이 유형에 있어서는 지식자문 또는 지원을 위한 정보의 양과 질에 대한 판단이 중요하다. 우리나라의 대한병원협회에서는 원격医료를 ① 의사간 원격 상담에 의한 진료, ② 의사와 환자 간 원격 상담에 의한 진료 및 처방, ③ 의사와 환자 간 원격 상담, ④ 원격 검진, ⑤ 원격 수술, ⑥ 원격 간호, ⑦ 원격 의사 교육 등으로 좀 더 구체적으로 분류하고 있다.

III. 원격의료 서비스 보안 요구사항

3.1 바이오인식과 원격의료의 융합 필요성

의료서비스는 일반적으로 진료 지원(원무 및 행정), 질병의 판단, 처치, 요양의 4단계로 구분되는데, 이 중 원격의료는 진료 지원, 질병의 판단 및 처치 단계에서 IT의 활용이 필수적이다. 원격의료의 경우, 서비스가 원격으로 제공되기 때문에, 사용자 식별이 매우 중요한 요소로 꼽힌다. 그런데 기존의 패스워드 기반 사용자 인증 시스템은 개방형 네트워크에 잠재적으로 노출될 가능성을 가지고 있고, PKI 기반 사용자 인증은 보다 안전하기는 하지만, 키 관리 및 전자 서명 패스워드에 있어 불편함을 유발한다. 만성질환을 앓고 있는 환자가 원격의료 서비스를 위한 단말기에 접근할 때마다 전자 서명 패스워드를 입력해야 하는 것은 꽤 힘든 일이다. 따라서 정보의 입력 방식에서 편의성이 개선된다면 사용자의 안면 윤곽이나 지문과 같은 신체적 정보를 활용하는 바이오인식 기술의 활용은 원격의료 서비스의 안전성 확보에 필수적이라 할 수 있다. 바이오인식 기반 원격의료 서비스 인프라를 구축하기 위해서는 프라이버시 정보인 바이오정보를 보호하기 위한 보안 프레임워크 구축이 필수적이다[11]. [그림 2]는 사용자, 센서, 원격의료 센터, 단말기, 원격의료 센터의 5가지 구성 요소를 갖는 통합모델로서 각 구성 요소는 다음과 같은 기능을 갖는다.

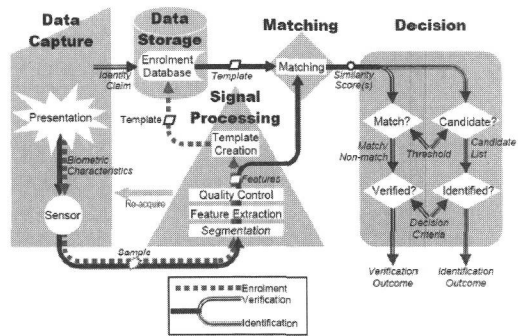
- 원격의료 단말기: 유·무선 네트워크에 연결되어 바이오인식 기반의 사용자 인증을 한다. 이 단말기는 원격의료 센터로부터 획득한 정보를 원격의료 센터로 안전하게 전송한다.
- 바이오인식 센서: 얼굴 및 지문 인식 등의 방법을 통해 사용자 편의와 개인 식별을 강화할 수 있어 강력한 보안 기능을 제공한다.
- 원격의료 센터: 사용자의 건강·의료정보를 수집하여 유·무선 통신을 통해 원격의료 단말기로 전달한다.
- 원격의료 센터: 원격의료 단말기와 사용자를 인증하고, 건강·의료정보를 저장 및 보존하며 이전에 축적한 정보와 비교, 분석한 다음 후속 의료조치를 처리한다. 센터에는 의료 이력정보와 사용자의 식별정보를 저장한다. 단, 개인정보보호를 위해 사용자의 생체인식 참조 데이터는 원격의료센터가 아닌 원격의료용 단말기에만 저장한다.



(그림 2) 바이오인식 기반 원격의료 통합모델

3.2 바이오인식 기반 원격의료 보안 요구사항

바이오인식 시스템은 신원 확인을 바라는 대상자의 바이오정보를 기초로 신원 확인을 원하는 대상자가 본인이 맞는지 확인하는 시스템이라고 할 수 있다. [그림 3]은 국제표준기구(ISO)의 기준에 따른 바이오인식 시스템의 구성도이다. 바이오인식 시스템은 크게 3가지의 기능을 수행한다. 그 첫 번째는 등록 과정이다.



(그림 3) 바이오인식 시스템 구성도

이 기능은 서비스 대상자의 바이오 정보로부터 개인 식별(Identification)과정이나 개인 인증(Verification)과정에서 필요로 하는 바이오인식 템플릿을 생성하고 저장하는 과정을 의미한다. 개인 식별 과정은 주어진 바이오인식 템플릿에 대해 이것이 누구의 것인지 신원을 밝히는데 목적이 있다. 이때 바이오인식 시스템은 저장장치 내의 모든 바이오인식 템플릿과의 비교를 통해 가장 유사도가 높은 대상자의 식별 정보를 제공하게 된다. 개인 인증 과정은 대상자가 본인의 바이오인식 템플릿과 함께 개인 식별용 ID를 제시하게 되면, 주어진 바이오

인식 템플릿에 대해 본인이 맞는지를 판별하는데 목적이 있다.

[그림 2]의 원격의료 시스템 통합모델에서 보안대상 요소별 보안위협과 대응 방안을 [표 2]와 같이 정리할 수 있다[12].

[표 2] 원격의료 통합모델의 위협 대응 방안

구성요소	위험요소	주요 대응방안
원격의료단 말기	취약한 개인인증	-바이오 기반 개인인증 제공 -TSM Local 모델 표준채택
	단말기 개인정보 유출	-단말 개인정보 암호화 적용 -MDM 솔루션 적용
바이오 센서	비인가 바이오인식 센서 사용	-ACBio 표준 채택 (인증서 기반의 신뢰성 제공)
원격의료 센서	비인가 센서사용	-기기인증서 표준 채택 (인증서 기반의 신뢰성 제공)
통신 프로토콜	보안인증 프로토콜의 가용성저하	-경량화된 통신프로토콜 적용 -경량화된 개인 및 기기 인증
원격의료 센터	개인정보 유출	-센터의 개인정보 저장소 보호 기술적용(개인/기기 접근제어)
	의료정보 유출	-상용 DB보안 기술 도입

- * TSM(Telebiometric System Mechanism)
- * MDM(Mobile Device Management)
- * ACBio(Authentication Context for Biometrics)

[그림 2]의 원격의료 통합 모델을 기반으로 일반적인 보안 요구사항인 정보의 기밀성, 무결성 및 가용성의 측면을 포함하여 다음과 같은 부가적인 보안 요구사항도 함께 고려해야 할 필요가 있다.

- 유·무선 네트워크를 이용하는 원격의료 서비스는 원격의료 센서와 통신단말에 취합되는 정보가 대용량이므로 서비스 성능 향상을 위해 경량화된 인증이 필요하다.
- 송·수신하는 의료정보는 디바이스 인증서를 기반으로 한 키 관리 및 인증서 상태 확인 방식에서 통신부하를 최소화하면서도 무결성을 제공할 수 있는 MAC(Message Access Control)과 기밀성을 위한 Diffie-Hellman 방식의 키교환을 제공해야 한다.
- 원격의료와 관련된 개인정보의 유출로 인한 피해 방지와 유출경로 추적을 위해 워터마킹 및 디지털 권한 관리 기능을 제공해야 한다.
- 원격의료 센터에 수집된 개인의 의료정보는 생성,

전송, 저장, 폐기되는 전 과정에 걸쳐 서 로그 형태의 감사기록을 제공해야 하며 의료인, 운영자 등이 개인 의료정보를 열람하는 경우, 권한관리와 감사 추적을 통해 안전성이 보장되어야 한다.

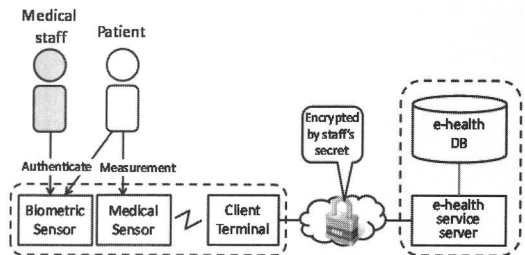
- 원격의료 데이터 중 특히 수치 데이터는 환자의 생명과 직접적인 연관 관계가 있는 데이터이므로 측정치, 투약량 등 전송 데이터의 정확성이 보장되어야 한다.

IV. 바이오인식과 원격의료 융합 동향

4.1 기술 적용 사례

[그림 2]의 원격의료 시스템 통합모델의 적용 사례로 다음과 같은 세 가지 경우를 생각해 볼 수 있다[13][14].

- 사례 1: 의료진이 원격의료 단말기를 보유하고 운영하는 경우이다. 예를 들어, 의료진은 방문 간호사가 돌보는 만성질환 환자나 일반 환자를 모바일 클리닉에서 검사한다. 이 경우, 환자는 관찰자(의료진) 때문에 ID/PW 입력을 망설일 것이다. 이런 이유로 이 상황에서는 생체인식이 적합하다.



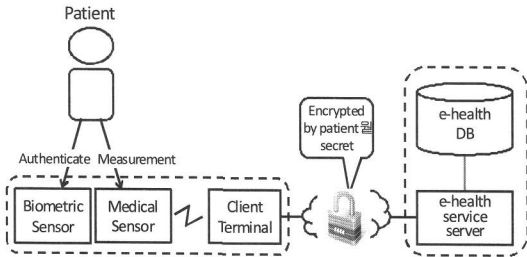
[그림 4] 바이오인식 기술적용 사례 1

[그림 4]에서 바이오인식 기반 원격의료 서비스의 사용자 인증 단계는 다음과 같다.

- 1) 의료진은 바이오인식, ID/PW나 다른 인증 방법을 사용해 단말기를 통해 원격의료 시스템에 로그인 한다.
- 2) 환자는 바이오인식을 사용해 위와 동일한 단말기를 통해 원격의료 시스템에 로그인 한다.
- 3) 의료진은 환자의 의료 및 건강정보의 측정을 도와 준다.
- 4) 의료진은 환자의 의료이력이나 기타 정보를 확인

한다.

- 5) 의료진과 원격의료 시스템 간에 전달되는 모든 정보를 안전하게 암호화한다.
- 사례 2: 만성질환 환자가 원격의료 단말기를 보유하고 운영하는 경우이다. 만성질환 환자의 경우, 원격의료 단말기를 규칙적으로 사용한다. 이 경우, 단말기를 사용할 때마다 ID/PW를 입력하는 것이 귀찮은 일일 것이다. 따라서 이와 같은 번거로움을 없애기 위해 생체인식을 사용하는 것이 적합하다.



(그림 5) 바이오인식 기술적용 사례 2

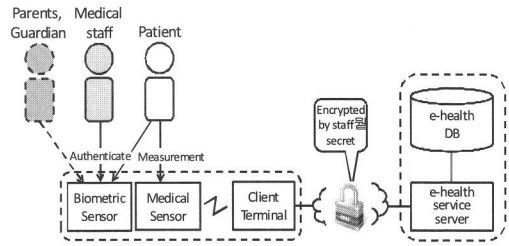
[그림 5]에서 바이오인식 기반 원격의료 서비스의 사용자 인증 단계는 다음과 같다.

- 1) 환자는 생체인식을 사용해 동일한 단말기를 통해 원격의료 시스템에 로그인 한다.
- 2) 환자는 스스로 의료정보를 취한다.
- 3) 환자는 자신의 의료이력이나 기타 정보를 확인해야 한다.
- 4) 의료진과 원격의료 시스템 간에 전달되는 모든 정보를 안전하게 암호화한다.

- 사례 3: 원격의료 단말기가 앰블런스나 의료 서비스 차량에 장착되어 있는 경우이다. 이 경우는, 의료진이 원격의료 단말기를 운영한다. 예를 들어, 환자가 앰블런스에 타고 있는 상황에서, 환자가 무의식 상태이거나 ID/PW를 입력할 충분한 시간이 없는 경우가 있을 수 있다. 따라서 이러한 상황에서는 생체인식이 적절한 해결책이 될 수 있다. 그러나 환자가 의식이 없는 경우에는 ID/PW를 알고 있는 환자나 보호자가 단말기에 대신 로그인할 필요가 있다.

[그림 6]에서 바이오인식 기반 원격의료 서비스의 사용자 인증 단계는 다음과 같다.

- 1) 의료진은 생체인식, ID/PW 또는 기타 인증을 사용해 단말을 통해 원격의료 시스템에 로그인 한다.



(그림 6) 바이오인식 기술적용 사례 2

- 2) 환자가(가능하다면 환자가 하되 어쩔 수 없는 경우에는 부모나 보호자가 대신)는 생체인식, ID/PW 또는 기타 인증을 사용해 동일한 단말을 통해 원격의료 시스템에 로그인 한다.
- 3) 의료진은 환자의 의료정보 측정을 도와준다.
- 4) 의료진은 환자의 의료이력이나 기타 정보를 확인해야 한다.
- 5) 전달된 모든 정보는 의료진과 원격의료 시스템 간에서 암호화된다.

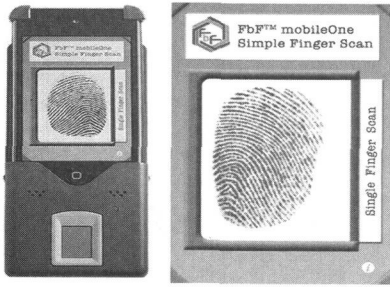
이상에서 제시된 적용 사례는 바이오인식 기술을 원격의료 서비스에 적용하는 가장 일반적인 경우이다. 그러나 어떤 경우, 특히 ‘응급 상황’에서는 환자 인증을 수행하는 것이 어렵다.

4.2 모바일 의료기기의 바이오인식 융합 동향

스마트폰과 태블릿 PC 같은 스마트 기기의 보급 증가는 원격의료 서비스 분야의 활성화에 커다란 영향력을 미치고 있다. 의료와 건강관리 분야의 앱들이 개발, 보급되면서 개인의 모바일 스마트 기기를 통해 원격의료 서비스를 제공할 수 있는 환경이 조성되고 있다. 기존의 바이오인식 기술 중 모바일 스마트 기기에 적용된 사례들은 다음과 같다[15][16].

4.2.1 지문인식 적용 사례

가장 널리 적용되고 있는 방식은 휴대전화에 지문 스캐너를 장착함으로써 사용자 인증을 수행하는 방식으로서 상대적으로 좋은 성능을 갖는다. [그림 7]의 FbF® mobileOne은 특히 아이팟 터치(제 2, 3, 4 세대)를 위한 휴대용 바이오 인식 지문 수집 액세서리이다. mobileOne은 애플의 30핀 커넥터와 연결하여 안전하게 iPod과 통신한다.



(그림 7) FbF® mobileOne

바이오 인식 어플리케이션 기반 표준의 요구에 부합하기 위해 mobileOne은 AuthenTec으로부터 FIPS 201/PIV 준수 지문 센서가 장착되어 제공된다. 지문 센서의 내장은 전체 256 비트 그레이 스케일과 가장 까다로운 1:N 식별에 적합한 508 DPI 이미지를 제공한다. 지문 캡처는 아이팟으로 이미지를 전송하고 화질 검사를 위해 센서 표면에 손가락을 대략 700밀리초 정도 대고 있다. 이밖에도 Excel-tek 사의 F960, BioSystemTM, L1사의 IBIS, 크로스매치사의 CATSA Program, 모토롤라사의 Atrix, MC75, Lumidigm사의 Analogics Rider Bio, MorphoTrak, Cogent, NEC의 Mobile Biometric ID System 등이 있다.

4.2.2 얼굴인식 적용 사례

구글의 안드로이드 운영 체제 중 최신 버전인 안드로이드 4.0(아이스크림 샌드위치)을 탑재한 삼성전자의 갤럭시 넥서스 스마트폰은 휴대전화 잠금을 해제하기 위한 새로운 방법을 제공한다. [그림 8]에서 얼굴 잠금 해제는 갤럭시 넥서스의 전면 카메라에서 휴대전화 사용자를 인식하기 위해 얼굴 인식 소프트웨어를 사용해서 화면의 잠금을 해제한다.

플라르츠사의 얼굴 인식 솔루션인 ‘레커그나이저 (Recognizer)’, Omron 사의 OKAO Vision, TAT사의



(그림 8) 안드로이드 4.0이 탑재된 삼성의 구글 넥서스에서 얼굴 잠금 해제 시연

Recognizr, L-1사의 HIDE TM, Cognitec사의 FaceVACS®, FaceR MobileID, FaceRTM, FaceCell등이 있다.

4.2.3 음성인식 적용 사례

음성 신호를 이용한 자동 화자 인식(ASR : Automatic speaker recognition)은 음성 신호 처리를 통해 신원을 확인하고 검증할 수 있는 바이오 인식 방법이다. 음성 특성은 높은 부분과 낮은 부분을 포괄한다. 높은 부분의 특성이 항상 추출의 어려움으로 인해 채택되지 않은 사투리, 화자의 말하는 습성, 감정 상태와 관련된 반면, 낮은 수준의 특성은 스펙트럼에 관련되어서 쉽게 추출이 가능하고 항상 ASR에 적용된다[5].

4.2.4 홍채인식 적용 사례

홍채 이미지 품질은 실험실 환경에서 촬영한 것 보다 일반적인 사용자에 의해 찍힌 사진이 제어하기 힘들기 때문에, 홍채 이미지 사진 처리 단계는 모바일 어플리케이션에 적용하기 위해서 매우 중요하다. 최근 연구에서 새 동공 및 홍채 세분화 방법은 휴대 전화로 촬영한 홍채 이미지에서 홍채 세분화를 위해 제안되었다. 이밖에도 L-1사의 PIER-TM, MORISTM, Cross Match Technologies의 I SCANTM 2, SEEK® II, Mobile-Eyes TM 등이 있다.



(그림 9) 모바일 터미널을 위한 홍채 인식(OKI)

4.3 모바일 기기의 바이오 인식 표준화 동향

모바일 기기에 바이오인식 기술을 융합하는 분야는 시장 진입 초기 단계이며 관련 업계를 중심으로 기술개발 및 표준화 기획이 진행되고 있다. 국내에서도 최근에 한국인터넷진흥원(KISA)을 중심으로 통신사업자·스마트폰제조업체·바이오인식업체·금융보안 및 원격의

료 보안관련 산·학·연 전문가로 구성되는 “모바일 바이오인식 신융합기술 표준연구회”(이하 표준연구회)를 발족하여 활동을 하고 있다.

바이오인식 융합기술에 대한 표준화 연구 영역은 다음과 같다[16][17].

- 모바일 기기인증을 위한 바이오인식 융합기술 표준화 연구
- 바이오인식기반 모바일 지급결제서비스 사용자인증 융합기술 표준화 연구
- 모바일 바이오인식기반 원격진료서비스 사용자인증 융합기술 표준화 연구
- 모바일 바이오 정보보호 및 시험기술 표준화 연구

V. 결 론

지난 수년간 원격의료 서비스 분야의 시범사업을 통해 의료서비스의 패러다임을 변화시킬 수 있는 기술적 발전이 이어지고 있다. 특히 스마트폰과 태블릿 PC 같은 스마트 기기의 보급 증가는 원격의료가 국민들에게 보편적 서비스로 제공될 수 있는 가능성을 증대시키고 있다. 하지만 원격의료 서비스가 활성화되기 위해서는 다음과 같이 개선해야 할 문제들이 여전히 남아있다.

첫째, 스마트폰을 통신 수단으로 활용한 각종 의료 서비스 앱들이 개발되고 있으나 서비스 이용자에 대한 신원 확인과 같이 인증에 대한 기술적 고려가 부족한 상황이다. 이때 가장 유용한 인증 수단이 바이오 기술을 이용한 생체인증 기술로 인식되고 있다. 하지만, 스마트 기기에서 앱 또는 내장 기능의 형태로 제공되는 각종 바이오인식 기반 인증 방식의 정확성, 신뢰성 및 전송 과정의 안전성을 체계적으로 검증할 필요가 있다. 이미 2010년 8월 미국 펜실베니아 주립대학교에서 스마트폰 스크린터치에 대한 해킹시연 연구 결과가 발표됨에 따라, 모바일 바이오 정보보호 및 시험기술에 대한 표준화도 수반되어야 할 것이다.

둘째, 현재 원격의료와 관련하여 정부, 학계 및 기업들이 개별적으로 사용하고 있는 용어의 개념 정립 및 표준화가 시급한 상황이다. 전문용어의 무분별한 남발과 오용으로 인해 서비스의 이해에 대한 혼란을 가중시키고, 이로 인해 의료 분야와 IT 분야의 기술적인 융합에 커다란 장애 요인이 되고 있다.

셋째, 동일본 대지진의 경우에서와 같이 원자력 발전소의 파괴 등 대형 재난, 재해의 발생으로 인해 주변 지

역에 대한 의료 및 구조 인력의 접근이 어려워진 상황에 대비하여 모바일 기기에 의한 인력 구조 및 진료 지원 서비스의 개발이 필요하다. 현재 국내에도 10여기가 넘는 원자력 발전소가 가동 중이고, 이 중 하나라도 재난으로 인한 방사능 유출 사태가 발생할 경우에 일본의 사례에서도 알 수 있듯이 의료진이나 구조대의 현장 접근이 어려워지는 사태가 예상된다. 이 경우, 재난 발생 지역의 주민들에 대한 직접적인 지원이 어려운 상황에서 가장 효과적인 소통 수단이 스마트폰과 같은 모바일 기기로 예상된다.

Goode Intelligence의 최근 보고서에 따르면 특히 모바일 보안에서 바이오인식 분야는 앞으로 중요한 성장세를 유지할 것으로 전망된다. 2011년 휴대전화 바이오인식 시장은 약 3000만 달러에 도달하고, 2015년까지는 시장 예측을 1억 6천 1백만 달러 이상으로 예상하고 있다.

이와 같은 시장 전망에 따라, 국내에서도 표준연구회를 통해 원격진료와 관련한 모바일 바이오정보 보호기술 및 시험기술에 대한 국내의 표준의 개발이 진행되고 있다.

모바일 스마트기기의 이용 확산과 원격의료 서비스 수요의 증가는 필연적으로 모바일 바이오인식 분야의 신규 시장창출로 이어질 것이다. 국내 바이오인식 산업 육성과 관련 시장의 선점을 위해서는 모바일 바이오인식 시장이 태동하는 시점부터 정부, 연구기관, 바이오인식업체 및 모바일 스마트기기 관련 업체의 지속적인 협력 노력이 필요하다.

참고문헌

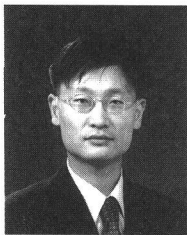
- [1] 고대영, 조현승, 강민성. “u-health 서비스 수요분석 및 시장 활성화 방안”, 산업연구원 연구보고서, Dec, 2010.
- [2] “서비스산업 선진화 방안의 주요 추진실적과 향후 과제”, 정부관계부처 합동보고, Aug. 2011
- [3] 백인수, 김정민. “IT기반 산업간 융합 현황과 국가 정보화 전략방향”, Nov, 2010.
- [4] “홈헬스케어 의료기기 표준화 가이드라인”, 식품의약품안전청, Nov, 2007.
- [5] “원격의료 정보통신서비스 추진현황분석서”, 한국인터넷진흥원, Nov. 2011.
- [6] 신용녀, 전명근. “바이오인식을 이용한 원격의료에

- 서의 개인정보보호”, 한국지능시스템학회 논문지, Vol 20, No. 5, pp 659-664.
- [7] 안무업, 최기훈., “원격진료, 이헬스 및 유헬스로의 발전과정”, 대한의사협회지, 2009, 52(12): 1131-1140.
- [8] 이의훈, “정보통신사업자들의 관점에서 본 *u-health* 산업의 현황과 전망”, www.ktoa.or.kr.
- [9] 이규환, “국내.외 *u-health* 동향 분석”, 한국보건산업진흥원, April. 2012.
- [10] “*u-health* 서비스 배경 및 추진현황”, 한국정보사회진흥원. April. 2011.
- [11] “스마트 공공보건의료 서비스 도입 방안”, 한국정보화진흥원, IT정책연구시리즈 제7호, June. 2011.
- [12] 이유리, 박동규, “유비쿼터스 환경에서의 원격의료서비스를 위한 보안 프로세스 설계”, 한국정보기술학회논문지 제7권 제3호, June. 2009.
- [13] 김재성. “*e-health* 및 전세계 원격진료에서 원격생체인식 데이터 보호를 위한 통합 프레임워크”, 인터넷진흥원, Dec. 2011.
- [14] “원격의료용 바이오 인증 기술 및 표준개발”, 한국정보보호진흥원, Dec. 2007.
- [15] 한승진, 김재성. “모바일 바이오인식 기술동향 및 표준화 추진전략”, 한국정보보호학회 동계학술대회, Dec. 2011.
- [16] Dr. Jason Kim, *The 3rd revised text for Draft Recommendation of X.tif, Integrated framework for telebiometric data protection in e-Health and worldwide telemedicine*, ITU-T SG17 Q.9, Aug., 2011.
- [17] Prof Yong-nyuo Shin and Dr. Jason Kim, *New work item Proposal for X.tam : A guideline to technical and operational countermeasures for telebiometric applications using mobile devices*, ITU-T SG17 Q9, Aug., 2011.

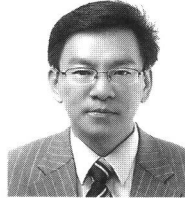
〈著者紹介〉



문호건 (Hokun Moon)
 정회원
 1985년 2월: 숭실대학교 전자공학과 학사
 1987년 2월: 중앙대학교 전자공학과 석사
 2005년 2월: 부산대학교 전자공학과 박사
 1987년 2월~현재: KT 종합기술원 보안솔루션 R&D 팀장
 2008년 2월~현재: TTA IT 국제표준화 전문가
 2008년 2월~현재: ASTAP 부의장, WG on Industry Relations 의장
 <관심분야> 위험분석, 사이버 공격 조기경보, 클라우드 보안, 정보보호 교육 등



류희수 (Heuisu Ryu)
 정회원
 1990년 2월: 고려대학교 수학과 학사
 1992년 2월: 고려대학교 수학과 석사
 1999년 5월: Johns Hopkins University 수학과 Ph. D.
 1999년 9월~2000년 6월: 홍익대학교 박사 후 연구원
 2000년 7월~2003년 8월: 한국전자통신연구원(ETRI) 정보보호기반연구팀 팀장
 2003년 9월~현재: 경인교육대학교 수학교육과 부교수
 2003년 2월~현재: TTA IT국제표준화 전문가
 2009년~현재: ASTAP forum ITAU vice-chairman & ISEG vice-chairman
 <관심분야> 암호 알고리즘, 암호 프로토콜, 개인 정보보호, 정보보호 교육 등



김재성 (Jason Kim)
 정회원
 1986년 3월: 인하대학교 전자계산학과 학사
 1989년 3월: 인하대학교 일반대학원 석사
 2005년 8월: 인하대학교 정보통신대학원 공학박사
 1989년 12월: LG 정보통신 중앙연구소 TDX-10 개발(연구원)
 1990년~1995년: 한국전자통신연구원(ETRI) 이동통신연구소(선임연구원)
 1996년 7월~현재: 한국인터넷진흥원(KISA) 바이오인식 표준연구 R&D 과제책임자
 2003년 2월~현재: TTA IT국제표준전문가, TTA PG505 의장, KBA(바이오인식협회) 부의장, 지경부 기표원 ISO SC37·TC68 전문위원, 금결원 금융보안기술위원장
 2003년 2월~현재: ISO SC37·ITU-T SG17 국제표준 프로젝트 에디터
 2010년 12월~현재: ABC(아시아 바이오인식컨소시움) 공동의장
 <관심분야> 바이오인식 국제표준화, 전자금융·원격의료 보안, 정보보호 보안성 평가 등