

생체인식 관련 연구동향

안도성* · 정용화** · 손승원***

1. 서론

인터넷기반의 현대 정보화 사회에서 개인의 신원 확인 및 인증에 대한 자동화된 수단의 필요성이 급증하고 있다. 개인고유번호(Personal Identification Number, PIN)와 암호를 이용한 기존의 인증기술은 도용, 망각의 위험이 상존하고 보안성이 미흡하여 최근의 정보보호에 대한 요구 수준을 만족시키지 못하고 있다. 따라서, 오늘날과 같이 네트워크화 된 환경에서 편의성과 보안성을 동시에 만족시킬 수 있는 신원 확인 방법으로 생체인식 기술이 도입되고 있는 것은 당연한 일이라 할 수 있다. 생체인식 기술이란 자동화된 장치를 통해 인간의 신체적/행동적 특징을 측정하여 개인 식별 및 인증의 수단으로 활용하는 기술이다. 이 기술은 지난 10여년간 기존의 신원 확인 수단을 대체할 것으로 주목받으며 많은 기술적 발전을 이어왔다. 생체인식 기술은 지속적인 성장이 예상되는 분야로서 Frost & Sullivan과 같은 시장조사 기관은 미국 테러사태 이후 세계 생체인식 산업이 연평균 50% 이상의 고성장을 하여, 2007년에 세계 시장규모가 5조원을 넘어설 것으로 전망하고

있다. 국내에서도 40~50여개의 생체인식 업체들이 지난해에는 800억원 가량의 시장을 형성한 것으로 추정하고 있다. 일부 업체는 원천 기술뿐 아니라 응용 기술까지 확보하고 적극적인 시장 확대를 도모하고 있다. 그러나 생체인식 기술은 그 필요성과 예상되는 효용성에도 불구하고 대규모 보급이 이루어진 실적은 부족한 것이 오늘의 상황이다.

이러한 생체인식 보급의 전제조건은 '기술적 완성도'와 '사회적 수용도'라 할 수 있다. 지금까지 생체인식이 갖는 장점과 발전 가능성을 다룬 많은 글이 있었기에 본 고에서는 지금까지 생체인식 연구가 이루어온 기술적 성과 중에서 아직도 부족한 것으로 지적되고 있는 이슈들을 고찰하고자 한다. 이와 함께 현 시점에서 논의되고 있는 생체인식의 적용 사례를 통해 정책 및 산업 동향과 생체인식의 발전 전망을 알아보하고자 한다.

2. 생체인식 기술 연구동향

지금까지 생체인식 기술은 편의성과 보안성의 관점에서 그 사용 범위를 확대하고자 하였다. 그러나 근래 편의성은 응용분야의 확대 과정에서 선택적으로 적용할 수 있는 기술에서 필수기술로 인식되고 있으며 보안성은 개인 프라이버시와 관련하여 몇 가지 취약점을 드러내고 있어, 이들로

* 한국전자통신연구원 정보보호연구본부 생체인식기술연구팀, 선임연구원
 ** 한국전자통신연구원 정보보호연구본부 생체인식기술연구팀 팀장, 책임연구원
 *** 생체인식포럼 의장 / 한국전자통신연구원 정보보호연구본부 네트워크보안연구부 부장, 책임연구원

부터 파생되는 문제점의 해결이 보급 확대의 선결 조건으로 요구되고 있다.

‘생체인식의 편의성’이란 생체인식 기술을 통하여 암호를 외우거나 열쇠를 가지고 다녀야하는 불편함을 해소하는 것으로 인식되어 왔다. 그러나 많은 부분이 자동화되고 시간과 공간을 초월하는 유무선 네트워크가 생활의 일부로 보급된 현 시점에서 시간과 공간에 제약받지 않고 자신의 신원을 입증하는 수단이 있어야 원하는 서비스의 혜택을 누릴 수 있다. 그러므로 24시간 어느곳에서나 관리자나 경비원의 개입 없이 자신의 신원을 자신만이 가지고있는 생체특징을 통해 입증하고 원하는 서비스에 접근 가능하다는 점에서 생체인식 기술은 편리성을 넘어 새로운 역할을 요구받고 있는 것이다. 생체인식 기술은 이러한 서비스 체제의 확립을 위해 반드시 필요한 요소로 받아들여지고 있다. 이는 향후 도래할 유비쿼터스 환경이 사용자를 인식하는 것에서 출발한다는 점에서 더욱 그 중요성을 높여가고 있다.

이와 함께 ‘생체인식의 보안성’이란 개개인이 갖는 생체 특성이 만인부동(萬人不同), 종생불변(終生不變)하여 유일한 개인을 식별할 수 있기에, 기존 토큰이나 패스워드 기반 개인 식별 방식보다 높은 보안강도를 얻을 수 있다는 것이 장점으로 받아들여져 왔다. 그러나 보급과 응용 분야의 확대에 걸림돌이 되고 있는 것은 생체인식 기술/제품간 상호운용성, 사생활 보호 측면에서 생체정보의 안전한 생산, 유통 및 폐기에 이르는 전 과정에서 안심하고 사용할 수 있는 방안이 요구되고 있다는 점이다. 이에 대한 대응 방향은 기술적 완성도의 향상과 표준화로 집약되고 있다. 본 고에서는 아래와 같은 내용을 언급하며 이로부터 파생되는 문제점과 관련 연구 동향을 정리해 보고자 한다.

• 인식율 및 인식 성능 항목

- 기기의 크기, 수행 속도, 가격 등의 사업적 항목
- 위조 등의 기술적 위협
- 생체정보의 호환성과 생체정보 자체의 보안성

2.1 인식율 및 인식 성능 항목

편의성과 보안성의 장점을 갖고, 혹은 이러한 장점을 기대하고 개발된 많은 생체인식 기술은 개개인이 갖고있는 특성을 입력 데이터로 하기 때문에 오류의 가능성이 상존하는 근본적 문제를 갖고 있다. 생체정보는 입력되는 시점에서 사용자의 감정, 자세, 주변 환경 등 시스템이 통제할 수 없는 변수가 너무 많기 때문이다. 생체인식의 성능을 언급할 때 반드시 언급되는 항목으로 동일인으로부터 획득한 생체정보를 다르다고 판정하여 발생하는 오류(False Non Match Rate, FNMR)와 서로 다른 사람의 생체정보를 동일인의 것이라고 판정하여 발생하는 오류(False Match Rate, FMR)가 있다(그림 1). 이것은 생체인식 시스템이 비교한 두 개의 생체정보가 갖게되는 유사도를 시스템이 설정한 임계치와 비교하며 수락과 거부를 판정하는 과정에서 발생하는 오류를 계량화하여 측정된다. 이때 FNMR, FMR 두 개의 측도를 다른 시스템과 동일하게 비교하기 어려우므로, 때로 오인식율을 하나의 변수로 표현하는 방법으로 이 두 오류가 같아지는 값(Equal Error Rate, EER)을 사용하기도 한다.

현재 대부분의 생체인식 시스템이 밝히고 있는 EER과 사용자가 체감으로 받아들이는 EER 사이에는 많은 차이가 있다는 것이 가장 커다란 불만으로 지적되고 있다. 이러한 괴리만을 놓고본다면 다소 주관적일 수 있으나 크게 다음과 같은 두 가지 이유에서 원인을 찾을 수 있을 것이다. 첫째, 충분한 실험이 가능하도록 지원하고, 객관적으로

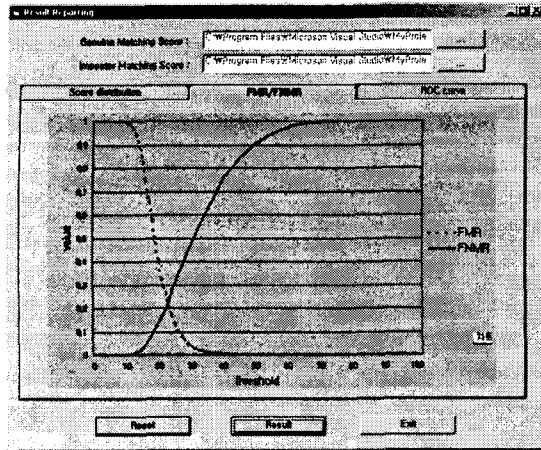


그림 1. FMR/FNMR curves

평가할 수 있는 공적 지원 기능의 부재와 둘째, 실제로 생체인식 시스템의 완성도가 부족하다는 점이다.

생체인식 시스템이 전체 사용자를 모델링하기 위해서는 다양한 생체정보를 접하고, 객관적인 결과를 도출할 수 있는 데이터베이스와 실험 환경이 제공되어야 하나, 이는 비용과 시간을 요구하는 일이기에 실험실 결과와 실제 사용결과 사이에서 인식을 차이가 있어왔다. 이러한 문제점을 인지하고 시스템 성능 평가에 있어 신중함을 기하는 최근의 현상은 긍정적이라 할 수 있으며, 생체인식 포럼에서도 시험, 평가 분과를 통해 많은 노력을 기울이고 있다. 또한 지난해 정보통신부의 지원으로 구축된 생체정보데이터베이스도 국내 생체인식 산업 발전에 커다란 도움이 될 것이다. 예를 들어, 0.0001%의 FMR는 백만번의 비교에서 한번 꼴로 오류가 발생할 수 있음을 의미하는 수치이나 이를 실증하기 위해서 백만번 이상의 실험이 필요하다. 그러나 이정도 규모의 데이터베이스가 없는 상황에서 이러한 수치를 성능 근거로 제시하는 것은 현실과 동떨어지기때, 데이터베이스 구축 사업은 더 큰 의미를 갖는다 하겠다. 현재까지 지문과 얼굴 데이터베이스가 구축되어 있으며, 특히

한국인 고유의 특성이 반영되는 얼굴에 대한 데이터베이스는 그동안 소규모 자체 데이터베이스나 체계적이더라도 외국인의 데이터베이스를 사용해왔던 얼굴인식 업계에서는 커다란 호응을 얻고 있어 활용도가 크게 기대되고 있다.

생체인식 시스템의 완성도와 관련하여 알고리즘의 성능을 평가하기 위한 공개경쟁인 Fingerprint Verification Competition(FVC2004), Face Recognition Vendor Test(FRVT2002), Face Verification Contest(FAC2004), Signature Verification Competition(SVC2004)[1-4]과 같은 행사가 꾸준히 이어지며 객관적인 성능 측정과 기술 개발을 촉진한 효과가 있었다. FVC에는 국내의 지문인식 업체인 슈프리마와 인하대학교에서 참여하여 소기의 성과를 보였으며, FRVT에서는 드림미르에서 참여하여 까다로운 평가를 거쳤다.

이밖에 생체인식 시스템은 다양한 성능 평가 항목이 존재하나 전체 개발 과정의 우선순위에서 뒤져 커다란 관심을 이끌어내지 못한 항목들이 있다. 그러나 근래 이러한 항목들이 시스템의 완성도를 높여주며 제품으로서의 필수 항목으로 인식되기 시작하여 많은 연구가 진행되고 있다. 대표적인 것들로서 생체정보의 획득 실패율 (Failure To Acquire Rate) 등이 있다. 이는 입력장치로부터 유의미한 생체정보를 획득할 수 없을 때 사용자는 원천적으로 본인확인이 불가능해지는 결과를 받게되어, 사용자 저변을 넓히는데 장애로 받아들여지고 있다. 이를 위해 입력 장치의 고성능화와 함께 전처리 기술의 발전을 위해 노력하고 있다. 획득 실패율을 보상하는 다른 접근 방법으로 얼굴 인식 기법과 홍채 인식 기법을 함께 사용 것과 같은 멀티모달 생체인식(Multi-modal biometrics)을 들 수 있다. 멀티모달 생체인식 시스템은 이러한 약점을 극복하는 동시에 보안 강도를

높일 수 있다는 측면에서 주목받고 있어, 국내 업체들도 이에 대한 투자와 연구를 지속적으로 전개하여 많은 신제품이 소개되고 있다.

이와 같은 노력에도 불구하고 아직도 기술적 완성도가 부족하다는 지적이 나오는 것은 국내 생체인식 업계의 영세성에도 기인한다. 표 1에 나타난 바와 같이 41%의 업체가 업력 2~3년으로 대부분 신생 벤처의 형태를 갖고 있으며 전체 직원 18명중 연구 개발 인력 12명의 평균치를 갖고 있다. 이러한 조사 결과가 시사하는 바가 많이 있겠으나, 국내 생체인식 산업 발전이 기술 발전을 그 토양으로 하고 있다면 현재보다 규모있고 체계

적인 기업형태가 절실하다 하겠다.

2.2 기기의 크기, 수행 속도, 가격 등의 사업적 항목

고전적이며 상업적 관점의 이슈로서 생체인식 시스템은 그 개발과정에서 인식 성능을 유지하면서 크기, 속도, 가격 등의 항목은 최소화 할 것을 지속적으로 요구 받아왔다. 입력 장치를 포함하는 생체인식 시스템의 크기를 살펴 보면, 얼굴 인식과 음성 인식등에 사용되는 카메라와 마이크는 이미 크기와 가격이 문제되지 않을 정도로 저렴해졌으며 지문 인식에 사용되는 입력장치의 경우도

표 1. 2002 국내 생체인식산업 현황 조사요약 (5)

(응답업체: 37개의 조사대상 중 34개 기관이 응답)

구 분		최다분포	평균	응답수	비고	
업체일반 현황	설립시기	2000년	1998년	34	-	
	소유구조	비공개 법인	88.2%	34	구 성 비	
	주력제품	지문인식	64.7%	34	"	
	자본금 규모	5억 이하	14억 6천만원	34	-	
	직원 규모	15인 이하	18명	34	생체위주	
	R&D 인력	6~10인	12명	34	"	
	생체인식분야 경력	2~3년	41.2%	34	구 성 비	
	향후 충원 계획	S/W(응용기술)분야	33.2%	31	"	
생 산 및 매출현황	연간 매출액	2억 이하(23.3%)	51억 4백만원	30	전체매출	
	2001년 매출액	금 액	2억 이하(34.6%)	22억3천6백만원	26	생체위주
		분 야	지문인식	69.2%	18	구 성 비
		수요처	민간(금융포함)분야	75.3%	25	"
	2002년(상) 매출액	금 액	2억 이하(38.1%)	13억1천8백만원	21	생체위주
		분 야	지문인식	76.2%	16	구 성 비
수요처		민간(금융포함)분야	83.4%	25	"	
생 산 및 매출전망	2002년(하) 예상매출	10억~30억(28.6%)	27억	28	생체위주	
	2003년 예상매출	100억 이상(31.3%)	81억3천6백	32	"	
	2004년 예상매출	100억 이상(56.7%)	158억4천9백	30	"	
해외진출 현황/전망	수출지역	아시아	31.1%	9	중복응답	
	수출분야	지문인식	46.5만달러	9	수출평균	
	수출애로사항	현지 마케팅 능력	5.0(6.0만점)	23	가중평균	
	2003년 예상수출	251만달러 이상(43.5%)	362만3천달러	23	수출평균	
생체인식 향후전망	신규개발 분야	얼굴인식	32.4%	34	중복응답	
	이용수준 전망(1년 후)	30%	64%	29	증 가 율	
	보급저조 이유	성능에 대한 신뢰성	34.2%	33	중복응답	
	정부지원 요구사항	내수기반 확대	4.0(5.0만점)	34	가중평균	

센서의 경박단소화에 많은 진전을 이루었다. 최근에는 스마트카드 위에 지문 인식용 센서를 실장하는 Sensor-on-Card 기술도 시도되고 있으며 ISO/IEC JTC1 SC17을 통해 규격제정이 진행되고 있다[6]. 많은 노력의 결과로 하드웨어의 개선은 이루고 있으나 무리하게 경박단소화 하는 과정에서 개발 원가와 생산 원가의 상승을 유발시키고 있다. 이러한 부담이 공급확대와 매출로 이어져 가격 인하를 이끄는 선순환이 이루어져야 하나, 매출 부진속에 지속적인 가격 하락으로 수익성이 저하될 소지가 있다는 점을 우려하고 있다.

수행 속도와 관련하여 지문 인식을 예로서 살펴보면, 지문 인식에 대한 성능평가 행사인 FVC2002에서는 31개 참가자들이 평균 0.92초의 등록시간과 1.04초의 비교시간을 보이고 있다. 이는 수행 메모리와 수행 속도 등 전산 자원에 제약을 두지 않고 인식율 향상에만 주안점을 둔 알고리즘들이 Pentium III 933 MHz의 범용 컴퓨터에서 수행된 결과임을 감안하면 충분히 수용 가능한 수치로 받아들일 수 있다. 나아가 2004년 1월에 결과가 발표될 FVC2004에서는 처음으로 표 2와 같이 두개의 분야로 나뉘어 경쟁하게 되었다. 기존과 같이 인식 성능에 주안점을 둔 Open Category 외에 제약적 환경아래 개발된 알고리즘을 대상으로하는 Light Category가 추가되었다 [1].

표 2. FVC2004 Categories

	Open category	Light category
Enroll time limit	10 seconds	0.5 seconds
Match time limit	5 seconds	0.3 seconds
Model size limit	No limit	2 KBytes
Allocated memory limit	No limit	4 MBytes

Light Category가 정하는 수행 속도와 메모리 상한의 규정 등은 AFIS(Automated Fingerprint Identification System)와 같은 대형 1:N 비교 시스템이나 스마트카드 상에서의 운영 등과 같이 우리가 접하는 실제 응용 환경과 유사한 결과를 제시할 것으로 기대된다. 또한 Light Category는 지금까지 Open Category에서 얻은 성능 지표가 만족할만 하므로 보다 실질적이고 상업적 응용이 가능한 분야로 관심이 옮겨가고 있음을 시사하고 있어 국내에서의 발빠른 대응이 촉구된다.

2.3 위조 등의 기술적 위협

요코하마 대학의 Matsumoto 교수는 젤라틴을 이용해 만들어진 위조 손가락이 일부 지문 입력기에서 사용될 수 있음을 실험적으로 확인한 결과를 지난해 서울에서 개최된 ITU-T회의에서 발표하여 많은 관심을 이끌어 내었다[7]. 이러한 생체인식 입력 장치에 대한 위협과 관련된 논의는 수용자 측면에서 의문시 되기도 하였고 개발자 내부에서도 그 가능성이 제기되어 왔으나, 크게 문제시 되지는 않았었다. 생체인식 시스템의 입력장치에 대한 위협에 대하여 생체신호 검출(Liveness check) 기능과 같은 대응이 가능하며, 이러한 기능을 탑재한 입력장치가 소개되고 있다.

이와 함께 획득된 생체정보의 무결성과 비밀성을 위협하는 시도가 있을 수 있다. 생체정보는 처리단계에 따라 2가지 기본형태로 되어 있다. 생체 특징의 원영상(Raw data)과, 생체인식과 인증의 기본을 이루는 비교과정에서 사용되는 생체 특징 정보만을 추출한 생체 템플릿(Template)이 있다. 템플릿은 사용자와 관계된 데이터를 추가로 포함할 수도 있다. 인증 과정의 무결성은 템플릿의 무결성에 의존한다. 만약 사용하는 템플릿이 신뢰할 수 없다면 결과인 인증 결과도 신뢰할 수 없게된

다. 신뢰할 수 없는 템플릿은 다음과 같은 몇 가지 이유에 의해 발생될 수 있다.

- 시스템 하드웨어 또는 소프트웨어의 고장에 의한 불의의 변조
- 공격자에 의한 템플릿의 의도적인 수정
- 승인된 등록자의 참조 템플릿을 대신하여 공격자의 생체 템플릿 삽입
- 공격자의 live 템플릿을 대신하여 승인된 등록자의 생체 템플릿 삽입

이러한 보안위협에 바탕에는 생체인식 알고리즘이 공개되지 않는다는 점에도 원인을 들 수 있다. 많은 암호화 알고리즘은 암호학자에게 암호화 강도의 분석과 검증이 가능하도록 공개적으로 사용할 수 있게 되어 있다. 생체인식 알고리즘은 이와 같이 공개되지 않았으므로 검토할 수 없으며, 그로 인해 알려지지 않은 요소가 있을 수 있다. 일반적으로 생체인식 알고리즘은 암호화 알고리즘과 같은 검증 요건을 만족시키지 못하고 있다. 오히려 시스템 사용자를 구분할 수 있는 특성을 추출하는 수단을 제공하는 방법을 주요 기능으로 하고 있다. 생체인식 알고리즘의 목적이 비록 보안기능을 함축하고 있다 하더라도, 근본적으로 정보보호에 연관된 것이 아니라 개인을 인식하는 기능에 있기 때문이다. 이러한 문제는 다음 절에서 보다 상세히 논의하기로 한다. 역설적으로 이 같은 문제점이 늘어나는 것은 개인인증 수단으로서 생체인식이 많은 것을 해낼 수 있다는 가능성이 있기에 위협의 기술적 강도 또한 증가하는 것으로 이해할 수도 있을 것이다.

2.4 생체정보의 호환성과 생체정보 자체의 보안성

생체인식을 이용한 서비스 범위의 확대를 위하

여 반드시 해결되어야 하는 부분이 상호운용성 확보 측면의 표준화와 획득된 생체정보의 오남용을 방지하는 프라이버시 보호 측면의 표준화일 것이다. 본 절에서는 이러한 두가지 문제를 고찰하고자 한다.

지금까지는 나름대로 최적의 인식 성능을 도출하기 위해 다양한 방식의 접근이 이루어져 왔다면, 오늘날은 이러한 기술적 발전을 바탕으로 생체인식 서비스의 저변 확대를 위한 표준화가 대두되고 있다. 현재 이러한 노력은 ISO/IEC JTC1 SC37을 통하여 활발히 진행되고 있다. 생체인식 포럼에서는 상호운용 분과를 중심으로 SC37에서의 분과위원장, 라포추어 등의 역할을 수행하며 적극적인 활동과 기고가 잇따르고 있어, 생체인식 표준화 분야에서 주도적인 역할을 수행하고 있다. ISO와 같은 국제표준화 기구 역시 그림 2와 같이 생체정보의 호환을 위한 표준이 가장 우선이며 핵심적인 위치에 있다고 이해하고 있으며, 국내에서는 표 3과 같이 TTA TC10 SC3을 통해 국내 표준 제정 활동이 활발히 진행되고 있다[8,9].

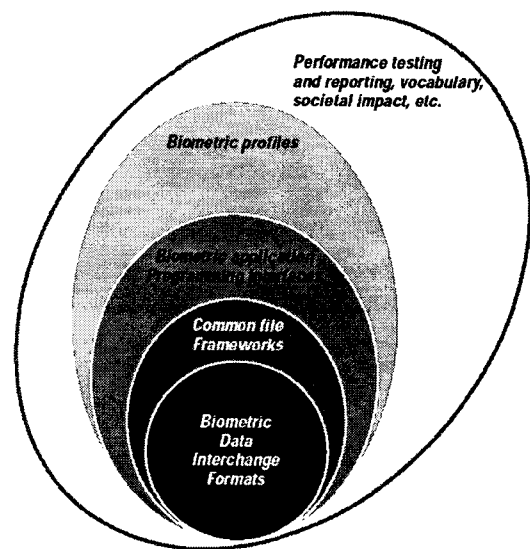


그림 2. 생체인식 표준화의 개발 단계

표 3. 생체인식 관련 국내 표준화 작업과제 목록

과제번호	과제명
2003-206	생체인증데이터 교환 형식 표준 (K-CBEFF)
2003-205	생체인식 기술용어 표준
2002-564	생체인식시스템 응용인터페이스 표준 규격 (K-BioAPI)
2002-563	생체인식 정보관리 및 보안표준 (K-X9.84)

본격적인 생체인식 보급기를 앞에 두고 있는 현 시점에서 생체정보 자체의 보호에 대한 문제가 최근 이슈로 대두되고 있다. 이는 개개인을 구별할 수 있도록 해주는 불변의 특성인 생체정보를 필요에 의해 변경할 수 없다는 한계로 인해 파생되는 문제로, 생체인식이 주는 효용성과 프라이버시와의 상충으로 이해할 수도 있다. 즉, 한번 노출된 현금카드 비밀번호는 번호를 다시 바꾸기만 하면 계속적으로 서비스를 제공받을 수 있으나 생체정보의 경우는 그렇지 않다는 점이다. 예를 들어, 어떠한 개인이 등록하여 사용중인 홍채정보가 노출된다면 그 사용자는 노출된 홍채정보를 평생 사용할 수 없으며 이를 대체할 수 있는 홍채는 다른 눈 하나만 남는다는 의미로 받아들일 수 있다.

이러한 생체정보의 경직성을 해소하기 위해 최근 생체정보로부터 추출한 생체 정보를 직접 개인 식별에 이용하는 것이 아니라 변환 함수를 적용하여 변환된 결과를 인식에 사용하여, 절취나 노출의 경우 이를 취소하고 새로이 구성할 수 있도록 하는 기술이 주목받고 있다. 이를 이용하면 생체정보 자체를 재구성하거나 원래의 생체정보로 역변환할 수 없도록 하는 기술이 적용되어 개인의 생체정보를 보호할 수 있을 것이다.

이밖에 생체정보의 오남용을 방지하는 차원에

서 생체정보를 보호하고자 하는 연구도 진행되고 있다. 획득된 생체 정보는 개인을 식별하는 것이 목적이므로 통상의 경우 응용 서비스와의 연계를 고민할 필요가 없으나, 이것이 절취되어 악의적으로 사용되는 상황을 상정할 경우 이러한 생체정보가 획득 목적에 어긋나게 부정 사용될 경우를 위한 대책을 세울 필요가 있다. 예로써, 비밀번호는 계좌별로 다르게 설정할 수 있으나 하나의 지문으로부터 생성된 생체특징 정보는 언제나 하나의 지문과 대응되기 때문에 모든 계좌의 비밀번호가 동일한 상황이 예상되기 때문이다. 이를 위해 응용목적이 추출된 생체정보와 결합되어 타 응용 서비스에서는 이 생체정보가 기능하지 않도록 하는 기술이 필요한 것이다.

생체정보의 보호와 안전한 관리를 위한 가이드가 생체인식포럼의 보안연동분과를 중심으로 연구되고 있으며 국내외에서도 생체인식과 관련한 정보 보호를 위한 표준 제정 노력을 기울이고 있다. 논의된 바와 같이 생체인식 정보가 프라이버시와 상충하는 문제는 향후 지속적으로 개선되어야 할 것이며, 이에 대한 많은 연구 테마가 있을 것으로 예상된다.

3. 정책 및 산업 동향

생체인식의 보급에서 적극적인 역할이 기대되는 부분이 공공 분야이며, 이러한 부분은 정부의 정책적인 판단이 가장 중요하게 작용하게 된다. 이와 관련하여 생체인식포럼의 조사 결과에서도 국내 생체 인식 업체가 응답한 정부지원의 최우선 희망과제는 표 4와 같이 내수기반 확대를 위한 정책적 지원으로 답하고 있다[5].

이미 지난 1996년 종이를 코팅한 형태의 주민등록증을 스마트카드로 교체하는 사업을 시도하는 과정에서 우수무지를 입력하여 지문템플릿을

표 4. 산업활성화를 위한 정부지원책

구분	가.	나.	다.	라.	마.
1위	13	7	0	4	0
2위	11	2	4	6	0
3위	8	7	7	4	0
4위	2	4	9	6	0
5위	0	0	0	0	34
가중평균	4.0	2.1	1.6	2.0	1.0

가. 내수기반 확대
 나. 기술개발 및 표준화
 다. 해외진출(수출) 지원
 라. 법제도 개선 등 산업기반 확충
 마. 기타
 (참조: 가중평균치가 5.0에 가까울수록 가장 필요한 정부지원책임.)

저장하고자 한 경험이 있는 우리나라는 지금 공공 분야 스마트카드 사업이 추진되는 과정에서 생체인식의 적용 기회를 맞고 있다. 현재, 공무원증을 스마트카드 방식으로 전면 전환하기 위한 시범 사업을 정보통신부, 행정자치부, 외교통상부 등 3부가 공동 추진하는 ‘공무원 전자카드 시범 도입 사업’, 국방부가 하사관 이상 15만명을 대상으로 발급 추진하고 있는 ‘국방전자카드’ 등의 사업에 생체인식을 통한 사용자 인식, 권한 관리 기능 등이 보다 적극적으로 고려될 필요가 있다고 생각한다. 생체인식 기능의 추가는 추진되는 사업의 서비스 범위를 획기적으로 넓힐 수 있으며 보안성도 높이는 기능을 제공할 것이기 때문이다.

이와 관련하여 예의 주시하여야 할 사항으로서 해외동향을 지적할 수 있다. 해외 사례의 경우 지금까지 생체인식 기술은 주로 사회복지 서비스의 제공과 효율적인 집행을 목적으로 많이 이루어져 왔다. 그러나 최근 신분증명에 생체인식기술을 도입하려는 시도가 잇따르며 이것이 국제사회에서 표준으로 제정되며 반드시 수용해야 하는 기술로 변하고 있는 추세에 있다. 대표적인 사례로서 미

국이 추진하고 있는 Patriot Act(P.L. 107-56), Customs Border Security Act of 2001 (H.R. 3129)와 Enhanced Border Security and Visa Reform Act (P.L. 107-173) 등에서 생체인식 기술의 도입과 일정을 제시하고 있다. 현 상황에서 100여개 이상의 국가에서 디지털 신분증을 구축함에 있어 생체인식을 포함하는 것은 개별 국가의 문제였으나[10], 이러한 사업이 발전하여 국가와 국가간에 활용되는 여권, 비자 등에 포함됨으로서 한번 획득된 생체정보의 활용범위는 전세계적으로 넓어지는 계기가 될 것으로 예상된다.

또한, International Civil Aviation Organization(ICAO)이 추진하고 있는 Machine Readable Travel Document[11]와 같은 사업은 직접적으로 국내 환경에 영향을 주게 될 것이다. 이미 선원수첩을 통한 보안 강화를 시도하고 있는 International Labour Organization(ILO)과 International Maritime Organisation (IMO)은 이러한 규정이 실시될때 ICAO의 규격을 준용하도록 각 국에 권고하고 있다[12]. 우리나라 해양수산부에서도 ILO의 연차총회에서 생체인식을 채택함에 따라 올해안에 선원법을 개정하고 내년 상반기 중에 1만 8000여명의 외항 선원에게 새 선원수첩을 발급할 예정이다. 이는 국내에서 공식적인 신분 증명에 생체인식을 적용하는 사업으로 최대 규모를 기록할 것이며, 향후 이러한 대규모 사업이 더욱 늘어날 것으로 예상되므로 적극적인 대응이 필요한 시기라 하겠다.

4. 결론

지금까지 생체인식 분야의 국내외 연구동향에 대하여 간략히 살펴보았다. 최근 이슈가 되고있는 몇 가지 항목들을 고찰하였으나 무엇보다 중요한 것은 이러한 일련의 이슈들이 보여주고있는 흐름

을 찾아내는 일일 것이다.

생체인식 분야는 국내 기술 동향과 국제 기술 동향이 불과 수개월의 차이를 두고 진행되는 상황으로, 특별히 국내외 상황을 나눌 필요가 없는 무한 경쟁의 시기를 보내고 있다. 따라서 앞으로의 1~2년이 지금까지 생체인식 분야가 산업화를 위해 걸어왔던 10여년의 기간을 완성하는 기간이 될것이다.

현재 국내 생체인식 분야는 사업규모가 영세하고 수익성이 낮은 상황이나, 경쟁국과 비교하여 상대적으로 기술 우위에 있으며 보다 높은 성능확보를 위한 지대한 노력을 기울이고 있다. 또한, 데이터베이스, 생체인식 평가 방법론 등과 같이 개별 기업이 수행하기 어려운 부분은 정부와 연구기관에서 지원을 계속하고 있다. 앞으로도 산업활성화를 위하여 정책기관과 산업계, 학계의 원활한 의사 소통이 더욱 절실하게 요구되고 있으며, 생체인식포럼을 통하여 이러한 요구를 만족시킬 수 있도록 노력할 예정이다.

참 고 문 헌

[1] Fingerprint Verification Competition, <http://bias.csr.unibo.it/fvc2004/>
 [2] Face Recognition Vendor Test, <http://www.frvt.org>
 [3] Face Verification Contest at ICBA2004, FAC2004, <http://www.ee.surrey.ac.uk/Research/VSSP/banca/icba2004/>
 [4] First International Signature Verification Competition, SVC2004, <http://www.cs.ust.hk/svc2004/>
 [5] 생체인식포럼, "국내 생체인식 산업현황 조사 보고서", 2002. 11.

[6] Information Technology Identification cards Integrated circuit cards with contacts Part 11: Personal verification through biometric methods, ISO/IEC 7816-11.
 [7] Tsutomu Matsumoto, "Importance of Open Discussion on Adversarial Analysis for Mobile Security Technologies A Case Study for User Identification", *ITU-T Workshop on Security*, Seoul, 2002. 5. 14.
 [8] Mike Hogan, "Are you who you claim to be?" *ISO Bulletin*, March 2003.
 [9] 한국정보통신기술협회, <http://www.tta.or.kr>
 [10] "Digital Citizen Identification Programs," *Biometric Market Intelligence Volume 1, Issue 5*, June 2002.
 [11] "Machine Readable Travel Document-Document 9303, Part 1, 2 and 3," *The International Civil Aviation Organization*, 2003.
 [12] "Improved security of seafarers' identification," ISBN 92-2-112885-7, *International Labour Office*, Geneva, 2003.



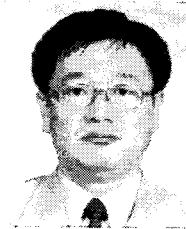
안 도 성

- 1992년 인하대학교 자동화공학과(학사)
- 1994년 인하대학교 기계공학과(석사)
- 2001년 인하대학교 자동화공학과(박사)
- 2001년 한국전자통신연구원 입소
- 현재 : 한국전자통신연구원 정보보호연구본부 생체인식 기술연구팀, 선임연구원
- 관심분야 : 생체인식, 지문인식, 정보보호



정 응 화

- 1984년 한양대학교 전자통신공학과(학사)
- 1986년 한양대학교 전자통신공학과(석사)
- 1997년 University of Southern California(박사)
- 1986년 한국전자통신연구원 입소
- 현재 : 한국전자통신연구원 정보보호연구본부 생체인식 기술연구팀장, 책임연구원
- 관심분야: 정보보호, 생체인식, 병렬처리



손 승 원

- 1984년 경북대학교 전자공학과(학사)
- 1994년 연세대학교 전자공학 전공(석사)
- 1999년 충북대학교 컴퓨터공학 전공(박사)
- 1983년 삼성전자(주) 연구원
- 1986년 LG 전자(주) 중앙연구소 HI8mm 캠코더 팀장
- 1991년 한국전자통신연구원 입소
- 1998년 한국전자통신연구원 교환전송기술연구소 NTB 팀장, 인터넷구조팀장
- 2000년 한국전자통신연구원 정보보호기술연구본부 정보 보호응용연구부장
- 현재 : 한국전자통신연구원 정보보호연구본부 네트워크 보안연구부장, 책임연구원, 한국정보보호학회 이사, 한국정보처리학회 이사, 생체인식포럼 의장