

다중 생체인식 기반의 인증기술과 과제

조병철*, 박종만^o

Technology Review on Multimodal Biometric Authentication

Byungchul Cho*, Jong-man Park^o

요약

기존의 단일 생체인증 방법들은 인식과 식별이 주 용도이며 서비스 용도별 실시간 개인 인증보안은 취약하다. 이에 다중 생체인식기반의 실시간 인증 및 인증 기술을 통해 보안성능을 향상시키는 방법의 연구와 개발이 필수적이다. 본 논문은 생체인식기술의 다중 생체인식 파라미터를 조합하여 인증하는 선진 기술 및 특허동향 분석을 통해 국내 기술개발 전략과 과제를 제시하는데 중점을 둔다.

Key Words : unimodal biometric, multimodal biometric, authentication, patents analysis, strategic assignment

ABSTRACT

There might have been weakness in securing user authentication or verification with real time service approach, while existing unimodal biometric authentication has been used mainly for user identification and recognition. Accordingly, it is essential to research and develop ways that upgrade security performance with multi biometric based real time authentication and verification technology. This paper focused to suggest binding assignment and strategy for developing multi biometric authentication technology through investigation of advanced study and patents. Description includes introduction, technology outline, technology trend, patent analysis, and conclusion.

I. 서론

생체인식(biometric) 인증기술은 지문, 홍채, 얼굴, 음성, 정맥과 같은 개인의 신체 고유 정보를 활용하여 인증하는 방식을 지칭한다. 개인의 유일한 신체 고유 특성을 이용하여 기존의 카드번호나 패스워드 같은 단일 인증보다 보안성이 향상된 기술이지만 인식된 생체정보의 저장 및 관리방식이 기존방식과 유사하여 여전히 보안위협이 존재한다. 최근 세계적으로 단일 생체인식 기술의 성숙도가 높아지고 생체인식기술의

인식생체의 범위가 확대되면서, 스마트기기와의 융합을 통한 다중 생체인식기반의 인증기술 개발과 시장 선점 경쟁이 치열하다. 글로벌 생체인식 시장도 2019년 61억5000만 달러(약 6조 2800억 원)로 커질 전망이다¹⁾. 그러나 현재 국내 연구 및 기술개발과 상용화 수준은 열위이며 대응전략이 시급한 상황이다. 이에 대한 해결책으로 논문에서 다중생체인식 알고리즘 및 인증기술에 대한 기술동향분석과 대응전략 제시를 통해 국내 관련기술의 연구개발 가속화와 성장 산업을 요구하고자 한다.

※ 이 논문은 미래창조과학부 과학기술진흥기금, 복원기금의 지원을 받아 KISTI ReSEAT 프로그램의 지원으로 수행된 연구결과임.
 * First Author : Korea Institute of Science and Technology Information, ReSEAT, Senior Research Fellow, bcho@reseat.re.kr, 정희원
 o Corresponding Author : Korea Institute of Science and Technology Information, ReSEAT, Senior Research Fellow, jmp21c2008@reseat.re.kr (jmp21c2012@daum.net), 정희원
 논문번호 : KICS2014-10-432, Received October 27, 2014; Revised December 15, 2014; Accepted January 6, 2015

II. 기술개요

2.1 기술배경과 이슈

생체인식은 생리적, 행동적 특성을 기반으로 개인을 식별 및 입증하기 위한 자동 인증기법^[2]이며, 다양한 생체인식 특성들이 연구되고 있다^[3]. 생체인식시스템은 단일 및 다중시스템으로 분류된다. 다중 생체인식은 단일 생체인식에 비해 특정개인의 속성이 매치되지 않는에도 매치되는 것으로 인식하는 오류비율(FAR)과, 매치되는데도 매치되지 않는 것으로 인식하는 오류비율(FRR)을 줄이는데 도움을 줄 수 있다. 인식알고리즘은 입력속성의 매치 의사결정 과정과 수준별로 다양한 결정 기법을 통해 정보를 통합(fusion)하여 최종 인증여부를 결정하는 방법을 포함한다. 다중형태(multimodal)기반의 개인인증시스템(PAS: personal authentication system)^[4]은 다종의 센서별 인식 알고리즘과 통합수준별 효율성을 필요로 한다. 다중생체인식시스템은 1)동일생체에 대한 다종의 이중센서정보 활용, 2)다종의 이중생체인식을 위한 복수센서정보 활용, 3)동일생체의 다중인식 정보 활용, 4)동일생체의 다중 스냅사진 정보 활용, 5)동일생체에 대한 다중 표현이나 매칭 정보 활용 등의 5가지 범주로 분류^[5] 가능하다. 4), 5)의 방식은 2), 3)방식에 비해 정확도 개선이 크지 않고 계산 및 저장량이 더 요구되나 비용 효율적이다. 최근 생체인식시스템의 기술적 이슈는, 단일 생체인식시스템의 성능개선과 이중의 단일생체인식 시스템과의 비교사례를 통한 성능향상 및 알고리즘 개선보다 보안성이 향상된 다중 생체인식 융합시스템의 제시에 관한 것이다. 아직 기술적 완성도나 비용경제적인 측면에서 상용화를 위한 검증 이슈가 남아 있으나 다중센서 및 다중 형태의 생체인식 파라미터 기반의 효율적인 인식 및 인증 알고리즘 개발의 가속화가 필요하다.

2.2 기술 구성

다중 생체인식의 기술구성은 단일 생체인식의 비보편성문제 해결, 보안성의 향상, 불필요 데이터의 처리, 시스템 결함발생시 전체시스템의 무 정지 처리, 대규모 생체인식 데이터베이스의 필터링과 인덱싱의 편리성, 지속적 개인 추적과 모니터링 등^[6]이 해결 가능한 기술로 구성되어야 한다. PAS를 설계하기 위해서는 표 1.^[7]과 같이 생체인식 기술 분야별 FAR와 FRR, 수단별 장단점을 기반으로 다중인증을 위한 개선 아이디어와 알고리즘의 구성이 필요하다.

다중생체인식 시스템은 전형적으로 등록 및 인증모

표 1. 생체인식 수단별 비교
Table 1. Comparison by biometric measure

수단	A%	B%	장 점	단 점
지문	0.5	10 ⁻²	기술성숙/다양성	신뢰감 저하
홍채	10 ⁻⁴	10 ⁻⁴	고 신뢰성/비접촉	절차 복잡
서명	0.2	0.6	변경 내환경성	문자 의존
안면	1.0	1.0	비접촉/원격인증	민감/저인증도
음성	1.0	10 ⁻¹	별도장치 불필요	노이즈
손	0.2	0.2	고속 처리	기기 크기
정맥	10 ⁻¹	10 ⁻³	고 신뢰성	기기 크기

* 자료 [7] 참조 재작성
* A=FRR %, B= FAR %

드로 구성된다. 인식을 위해 채집된 생체인식 정보의 품질은 실측치와 기준치와의 매치여부를 결정하는 기법으로 통합수준별 전략에 의해 결정되며 데이터 통합모델의 하나인 JDL(Joint Director of Labs)모델을 활용할 수 있다. 본 연구에서 통합 프레임은 아래 그림 1.과 같이 특징 추출, 점수화, 의사결정수준을 기반으로 재구성되어 다중 소스로부터 데이터 및 정보의 자동감지, 조합, 상관, 추정, 결합에 대한 다중 처리과정으로 정의될 수 있다. JDL 데이터 통합모델은 소스, 데이터베이스관리, 사용자인터페이스, 프로세싱의 4 요소로 구성되며, 프로세싱 요소는 하위객체 데이터평가, 객체평가, 상황평가, 영향평가, 프로세스 개선 단계로 구성 된다^[8].

일반적 생체인식시스템은 생체인식 센서, 이미지 프로세싱 알고리즘, 데이터스토리지 모듈, 매칭 알고리즘과 결정모듈로 구성된다. 다중 센서들은 생체인식 데이터를 획득하고 정보를 디지털 데이터로 변환^[9]시키며, 시스템은 이중의 센서들을 복수로 채택할 수 있도록 구성 가능하다. 이미지프로세싱 알고리즘은 센서의 출력이미지로부터 유의미한 정보를 추출하고 생체인식 지표를 개발하는 프로세스로 구성된다. 매칭 알고리즘은 저장된 참조데이터를 기반으로 저장지표를 비교하고 매칭점수를 생성하며 최종적으로 시스템 수

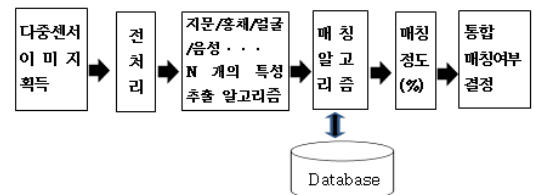


그림 1. 다중 생체인식 인증 프로세스
Fig. 1. Process of multi biometric authentication

준별 인식결정을 위해 이 매칭결과를 사용하는 단계로 구성된다.

2.3 선행 알고리즘

다중 생체인식 시스템에서의 정보통합은 센서 및 특징수준에서의 통합과 점수수준 및 결정수준에 대한 통합으로 분류된다. 통합기법들은 복수의 형태 및 알고리즘과 다양한 조건하에서 결합이 가능하다. 선행 연구조사에서 다중 생체인식에 활용된 기법으로 Fuzzy Commitment와 Fuzzy Vault, 토큰기반 혼합기법 등 다양한 기법 등이 있다²¹. 표 2.는 다양한 통합수준과 생체인식에 관한 선행연구 분류⁴⁴와 최근의 연구 상에서 나타난 생체인식형태별 데이터 통합결정 근거를 나타내 준다. 생체인식대상의 결합 형태는 주로 3개 이하이며 데이터통합의 근거로 매칭 점수화와 특이점 수준에 따른 FAR과 FRR이 사용되고 있다. 다중 생체인식인증의 목적이 단지 보안성만의 향상이라면 생체인식의 다중 요소나 형태의 증가로 목적이 충족될 수 있으나, 사용자입장에서 향상된 보안기술의 선택은 사용편리성이나 경제성의 레버리지 평가가 수반되어 결정되므로 다중 생체인식인증을 위한 파라미터 수는 중요하다. 현재 생체인식의 결합파라미터를 3개 이상 사용하는 실증연구는 소수인 것으로 판단되나, 생체인식기술 대상의 증가와 시장의 향상된 인증

알고리즘 요구에 의해 신규 다중 생체인식 지표에 의한 인증 알고리즘은 증가하고 있다.

2.4 알고리즘 확대

사용빈도가 많은 생체인식특성별 비교 요소는 표 3.^[13]과 같으며, 가치측면에서 경제성과 보안성의 비중 이외에 상황인식 환경에 따른 가변적 알고리즘의 확대가 요구된다. 다중 생체인식 시스템 설계를 위해 인증 프레임의 생성, 생체인식표준의 조정, 다양한 생체인식 형태의 조합, 특성의 표현, 시스템 수준의 인증에 대한 기존의 다양한 연구²¹를 활용할 수 있다. 본 연구에서 개별 생체인식 특성들을 기반으로 한 다중 생체인증 알고리즘⁴⁴과 같이 JDL 통합모델을 참조하여 개별모델들을 통합한 다중 생체인식 인증모델의 프레임을 제안한다. JDL 통합모델을 기반으로 기본 알고리즘의 확대는 그림 2.와 같이 다수(N)의 생체인식 파라미터를 가진 통합모델로 확대 가능하다. 통합모델의 상용화는 사용자 기기나 시스템에 대한 사용편리성, 처리속도, 경제성 및 효율성 등과 보안성 설정수준과의 trade off가 긍정적인일 경우 성공 가능성이 있다고 판단된다.

표 2. 다중 생체인증의 선행 연구
Table 2. Existing study about multi biometric authentication

연구 수 행	생체인식 형태
Marsico 외	귀, 얼굴, 손가락
Raghavendra 외	손바닥, 얼굴
Karthik 외	얼굴, 홍채
Dakshina 외	얼굴, 손바닥
Xiao 외	손바닥, 얼굴
Hui 외	손가락, 얼굴, 말
Lau 외	손가락, 얼굴, 음성
Kumar, Zhang	얼굴, 손바닥
Kumar, Zhang	손 모양
Chang 외	얼굴, 귀
Sakharovich 외	얼굴, 걸음걸이
Ross와 Jain	얼굴, 손, 지문
Frischholz 외	얼굴, 음성, 입술
R.VINOTHKANNA 외 ^[10]	지문(귀), 손바닥, 팔 정맥
Ola M. Aly 외 ^[11]	홍채, 손바닥, 손가락 관절
S.Brindha 외 ^[12]	눈 핏줄, 손가락 정맥

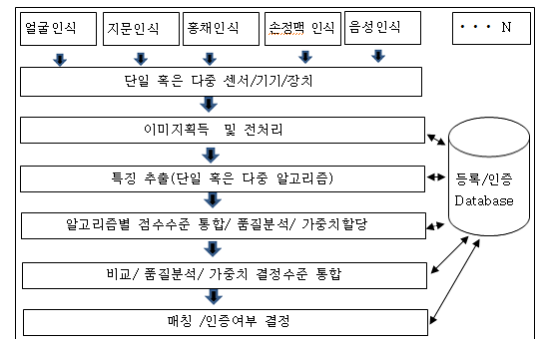


그림 2. 다중 생체인식 인증 프로세스
Fig. 2. Multi Biometric Authentication Process

표 3. 생체 인식 특성 비교
Table 3. Comparison by biometric features

생체	장점	단점	보안	센서	비용
음성	편리함	노이즈	보통	비접촉	저
얼굴	원격 수집	광조건	보통	비접촉	저
지문	광범위적용	피부조건	양호	접촉	저
홍채	고 정밀도	안경착용	상급	비접촉	고
정맥	고 보안수준	적음	상급	비접촉	저

III. 기술동향

3.1 특허동향

단일 생체인식기술로 지문, 장문, 손가락모양 및 길이, 손가락 주름, 얼굴인식, 눈동자 홍채, 음성, 서명, 손 움직임 등이 이용되고 있으며, 최근 진입 기술로 골격, 보행형태, 포즈와 제스처, 귀 모양, 자판 키 입력 형태, 심전도, 뇌파, 손톱무늬, DNA, 얼굴온도, 구취, 입술움직임, 핏줄형태, 망막, 공막, 사진 등을 인식하는 기술의 연구 개발이 가속화되고 있다. 미국의 경우 습관이나 행동특성, 생리 및 생물학적 특성, 정서적 특성기반의 움직임까지도 인식하여 개인의 인증에 활용하려는 연구개발 및 특허출원이 활발하다.

다중 생체인식 인증관련 2014년 이전 10년 동안의 세계(PCT)특허 주요 출원국 및 업체별 출원건수는 표 4와 같다.

키워드 “biometric authentication”로 검색한 최근 3년간의 국가별 특허 출원건수는 증가추세이며, 미국, 일본, EU, 한국, 중국, 캐나다, 독일 순이다. 중국의 출

표 4. 생체인식 인증에 대한 국별 출원건수
Table 4. Comparison of patents application about biometric authentication

검색 키워드	국별 출원건수(2004~2014.7)
Biometric Authentication	미국 1187, PCT 557, 일본 521, EPO 433, 한국 263, 중국 250, 캐나다 109
Multi biometric Authentication	미국 8221, PCT 2698, 캐나다 623, EPO 620, 남아프리카 30, 이스라엘 16, 일본 13, 중국 11, 한국 6
Multifactor Biometric Authentication	미국 168, PCT 65, 캐나다 28, EPO 12, 남아프리카 1, 이스라엘 1
Multimodal Biometric Authentication	미국 542, PCT 140, 캐나다 47, EPO 29, 한국 4, 중국 2, 일본 1
Finger-print Authentication	일본 755, 미국 462, 한국 367, 중국 364, PCT 219, EPO 141, 캐나다 40
Face Authentication	일본 646, 한국 186, 미국 177, 중국 174, PCT 116, EPO 83, 캐나다 7
Iris Authentication	일본 137, 미국 83, 한국 77, PCT 55, 중국 52, EPO 28, 캐나다 5
Vein Authentication	일본 247, 중국 83, 미국 59, 한국 47, EPO 31, PCT 26
Voice Authentication	한국 539, 미국 479, 일본 332, 중국 218, PCT 172, EPO 133, 캐나다 50

원속도로 볼 때 2015년 이후 한국의 출원건수를 추월할 것임이 분명하다. 주요 출원기업은 후지쓰, 히타치, 소니, 오키 같은 일본기업들의 출원이 강세이다. 그림 3.에서 보듯이 주요기술은 특허분류 코드(IPC)기준으로 디지털 데이터 프로세싱기술(G06F)이 26%로 가장 많으며 세부적으로는 컴퓨터보안 기술 분야(G06F 21) 중 보안 및 신원인증(G06F 21/30), 사용자 인증 (G06F 21/31), 사용자 생체인식 데이터의 활용(G06F 21/32)기술 등에 집중도가 높다. 신원 및 보안인증 분야에서는 1회용 암호, 변동암호, 문답식 인증, 블러핑 Bluffing), PW분실 처리, 상호인증, 보안계수측정 (metering), 접근제한, 반복인증, 공격시 메모리 삭제, 타임스탬프 기술관련 특허가 있다. 사용자 인증 분야에서는 인증메커니즘(H04L 29/06755) 관련 기술이 있으며, 특히 사용자 생체인식 데이터의 기술 분야에서 사용자의 행위패턴인증(G0 8F 21/1316), 특이한 사용자 등록(G06F 2 221/2117), 생체특징을 통한 사용자 인증(H0 4L 29/06809)기술이 특징적이다.

한국에서의 대표적 출원은 후지쓰, ETRI, 소니, 히타치, 비즈모델라인, 니트젠, SK, 삼성 등이며, 국내 출원자는 ETRI 19건과 삼성 4건 등으로 출원건수가 열세이다. 세계특허 PCT의 주요 출원자는 후지쓰, 히타치, NEC, 필립스, 인텔, 지멘스, 프리센스, 다운홀딩스 등이며, 한국의 경우 특이하게 개인이 5(2010년)건으로 상위 10위권에 있으며 국내특허를 소수 보유한 에트리 같은 연구기관이나 삼성같은 대기업의 세계특허 역시 소수로 국내의 모두 열위이다.

단일 생체인식기술 5개중 지문, 얼굴, 홍채, 정맥기술에 대한 국가별 출원건수는 일본이 최상위이다. 한국은 음성기술에서 출원건수가 최상위이며 지문, 얼굴 기술에서 2위, 홍채기술에서 3위이며 정맥기술 출원건수는 중국에 이어 4위이다. 그러나 다중생체인식 인

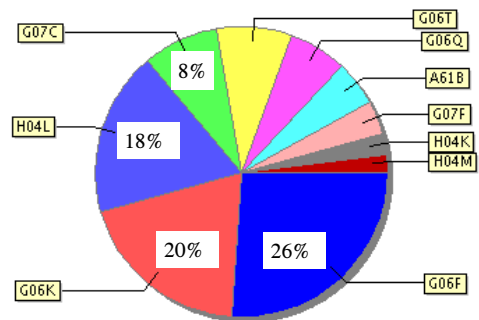


그림 3. 생체인식 인증기술의 IPC 비중
Fig. 3. IPC(%) in Biometric Authentication

증 기술에 대한 국가별 및 PCT 출원건수는 미국이 압도적이다.

키워드 “Multi Biometric Authentication”으로 검색한 출원국별 출원건수는 표 5.와 같으며 한국의 출원건수는 선진 국가와 격차가 크다. PCT 출원건수는 그림 4.와 같이 최근 3년간 급격히 증가하고 있으며 특히 2014년 다중 생체인식 인증관련 PCT출원이 증가하고 있다. 출원건수로 본 10개 주요업체는 그림 5.와 같이 빅플레이어들의 참여가 특징적이다. Digimarc가 문서보안업체로서의 높은 기술력을 시현하고 있으며 게임관리 및 솔루션 업체 IGT가 1위이나 마이크로소프트사의 특허 인용이나 의존도가 높은 점은 기술 네트워크와 일부 방향성을 암시하기도 한다. 특히 최근 그림 6.과 같이 점유율이 작았지만 증가율이 급격해진 Intel, Citrix, Apple의 동향과 출원내용을 IoT 및 웨어러블 컴퓨팅의 접근성 보안과 식별, 인증의 기술기반으로 추적할 필요가 있다. PCT 주요 특허내용은 표 6.과 같다. 기술내용은 IPC 코드 G06F 21내용이 주 대

표 5. 다중생체인식 인증에 대한 국가별 특허 출원건수
Table 5. Number of patents by country about multi biometric authentication

미국	PCT	캐나다	EPO	S. AF	이스라엘	일본	중국	한국
8221	2698	623	620	30	16	13	11	6

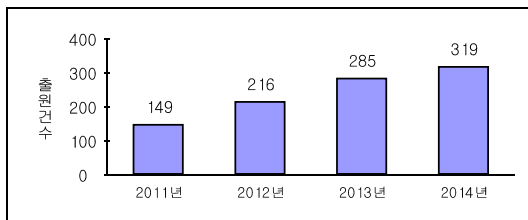


그림 4. PCT특허 출원추이
Fig. 4. PCT Patents Trend

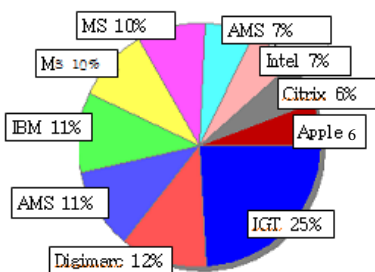


그림 5. PCT특허 주요 출원인
Fig. 5. Main Assignee of PCT Patents

상이며 다중생체인식 인증관련 기술비중이 높다.

기술적 판단에 의하면 단일 생체인식 인증기술 생

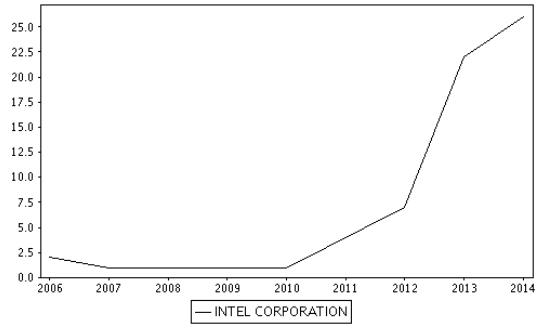


그림 6. Intel의 PCT특허 출원
Fig. 6. PCT Patents Application of Intel

표 6. 생체인식 인증에 관한 PCT와 미국 특허(2014년)
Table 6. PCT and US patents about biometric authentication(2014)

주요 특허 내용	
Key Words: multi/multifactor/multimodal biometric authentication	
WO2014111760	통합 전자거래 터미널의 다중 생체 인증
WO2014092665	셀프서비스 머신의 사용자 통합인증시스템
WO2014075734	주변기반의 다중요소 인증
WO2014052838	생체인식데이터를 사용하는 다중요소 인증
WO2104099355	융합보안엔진을 통한 프라이버시 강화 키관리
WO2014102294	리소스 사용 제3자 인가를 위한 다중요소 인가
WO2014111760	다중수준 인증을 위한 통합거래 터미널
WO2014005004	다중 인증요소를 가진 근거리 인식 보안시스템
WO2014011026	다중형태 인증플랫폼에 대한 시스템 및 방법
WO2014135409	컴퓨터 실행 다중요소 인증
WO2014046857	멀티 테넌트 환경의 단일서명
WO2014160853	복수 객체의 단절 없는 인증
WO2014052507	생체인식 식별자 생성을 위한 NFC
WO2014053509	웨어러블 센서 ID인증을 위한 생체인식 인증
WO2014022778	모바일인증을 통한 사용자의 편리한 인증방법
WO2014004556	생체인식을 통한 인증신용의 자동연계
WO2014105343	통신기간 다중요소 인증방법과 도구
WO2014052505	웨어러블 디바이스 사용자의 생체인증 방법
WO2014004135	상호 근접사용자 인증기법
WO2014025839	화자 인증 개선 및 자동 적용방법과 시스템
WO2014144964	다중사이트 영상기반 컴퓨터진단 분석 플랫폼
WO2014035696	퀵터 통신을 이용한 다중요소 인증
WO2014165416	생체인식과 터치 판별을 위한 레버리지
WO2014075734	근거리 기반 다중요소 인증
WO2014152576	전자 지불 인증요소와 신원 속성 확장시스템
WO2014140426	다중요소 인증기법
WO2014038732	카메라 탑재기와 연계한 생체인식 인증
WO2014051695	모바일 보안 상황 인증방법
WO2014117242	무선기기 사용패턴 감지로 보안강화 방법
WO2014097339	등록데이터 모음으로 생체인식 인증
WO2014105263	네트워크의 다중요소 인증과 로그인 시스템
WO2014144404	개인정보의 전차적 배포
WO2014105914	유저디바이스의 가장 보안 확장을 위한 보안 기기
WO2014153462	발전된 인증 기법과 응용
WO2014053748	웹브라우저 응용과 웹 대상 접근제어 방법/sys.
WO20140031983	다수 지문과 BIO-PIN에 의한 인증 방법

태계의 파편화가 이미 진행되고 있으며, 아직은 진입 장벽이 높은 IoT와 웨어러블 컴퓨팅기술에 대한 생태계 형성 환경도 다중 생체인식 인증기술의 선행개발 및 특허선점을 촉진하게 하고 있다. 다중생체인식 인증기술에 대한 특허출원이 증가하는 추세는 생태계의 요구와 기술융합의 속성에 의해 투자가 확산되는 결과로 판단된다.

다중 생체인식 인증관련 최근의 대표적 주요PCT 특허 WO2014/031983의 기술은 지문, 생체인식 파라미터 등 다중요소와 다중생체인식 메커니즘에 의한 개인 식별 및 인증방법과 도구를 제공하며 인증을 위해 다수 지문과 입력 순서(BIO-PIN)방법을 이용한다. 중요한 것은 미리 설정된 생체인식 기준치와 실제 사용 시 생체인식 값과의 공차(tolerance)범위 인정과 순서인식의 정확성이다. 열악한 이미지 기준치에 대한 오류 허용율(FAR)과 기각률(FRR)이 기술구현의 핵심이며 BIO-PIN과 같은 방식으로 오류감소를 추진한다. 이 기술은 자연적 기억법으로 기억 정보량이 기준보다 적어 기억하기 쉽고 생체인식 파라미터를 다양하고 독특하게 구성할 수 있으며 다중 생체인식 파라미터의 활용방법으로 보안성을 증가시킬 수 있다. 알고리즘은 그림 7.에서 보듯이 다중요소(3개의 지문과 1개의 눈동자)에 인증을 위해 가중치가 생체패턴의 인식결과에 주어지고 인증대상자 왼손의 다섯째(L5), 셋째(L3), 첫째(L1) 손가락과 오른쪽 눈동자(RE)의 인식샘플이 저장 및 정의된다. 정상인식 가중치는 40%, 순서표현 정확성의 가중치는 60% 이다. 인식과 순서 정확도의 80% 초과 시 실패범위로 결정한다. 아래 첫째 그림에서 L3과 L1은 정상인식 하였으나 순서는 잘못되었다. 더욱이 L3은 인식하지 못했다. 눈동자 인식에 40%, 손가락 인식에 20%의 가중치가 주어졌고

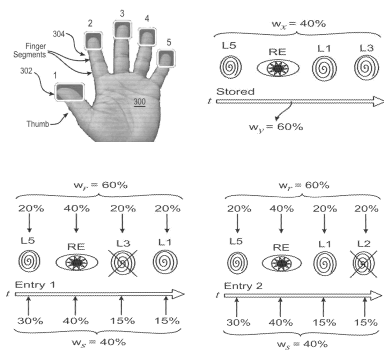


그림 7. 생체인식 다중요소와 가중치
Fig. 7. Multi factor biometric and Weight

순서의 정확성에 첫 번째 순서 30%, 두 번째 순서 40%, 나머지는 각각 15%씩 가중치가 주어졌다. 이를 합산하면, 인식정확도는 80%, 순서인식 정확도는 70%, 각각 가중치를 반영한 결과는 76%인데 사전에 설정된 임계 기준치 80%이하로 이 경우는 인증되지 않는 알고리즘이다. 다중요소의 생체인식 파라미터를 이용한 생체인식 알고리즘 개발과 상품개발에 응용할 만한 가치가 있다.

WO2014/052505의 기술은 기존의 단일 생체인식 기술에 의한 인증방법을 보완하고 발전시키기 위해 그림 8.과 같이 다중 생체인식 기술뿐만 아니라 복합적 파라미터로서 개인의 습관 활동, 생리적 특성, 움직임 패턴 등을 응용하여 기기 및 서비스, 네트워크의 인증 및 비즈니스 신뢰성을 향상시키고자 하는데 기술가치가 있다. 기존의 단일 생체인식기술과 단일 기준에 의한 인증형태를 벗어나 다중생체인식기술을 접목하고 상황별 감지 데이터의 동적인 분석과 시간경과에 따른 패턴 검증을 통해, 복합적 종합적 실시간 유일 인증방법을 구현한다는 면에서 기존 기술대비 비교 우위적이다. 향후 이와 유사기술을 활용하여 웨어러블 컴퓨팅기기와 IoT의 분야에서의 개인인증에 다양하게 응용할 수 있다. 응용을 위해서는 제시된 인

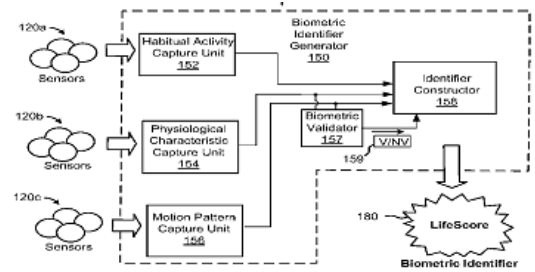


그림 8. 다중생체인식 식별자 생성
Fig. 8. Creating Multi biometric Identifier

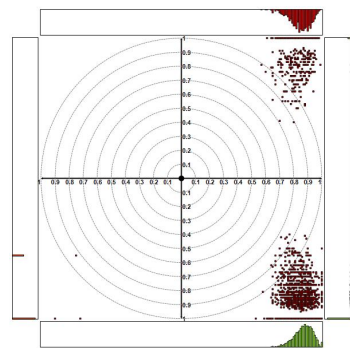


그림 9. 특허 유사도 분석
Fig. 9. Patents Similarity Analysis

증방법에 대한 인식오차의 허용 가능한 공차와 타당성, 시나리오별 대비를 감안한 일반화 신뢰수준, 비용 대 효과의 검토가 관건이며, 실제 개인 보안 및 인증을 위한 기술적 공인과 사업화 가능성에 대한 검증이 필요하다.

다중 생체인식 인증관련 특허의 심층 분석과 전략 수립을 위해 상기 PCT 특허 WO2014 /031983의 유사특허 분석 예는 그림 9와 같다. 관심 특허(원점)를 기준으로 분석 모집단 속 특허에 대해 청구항의 기술 키워드 유사성(x축)과 특허분류의 유사성(y축)을 측정한다. 유사도 상위 50개 이상의 분석결과 US 62299 06/7394919/753 9654/831038/8692875 등이 주요 추천대상으로 분석되었다.

특허 피 인용수와 패밀리 특허수로 본 한국의 특허 수준은 세계 평균 이하이다. 국내 특허 경쟁자 분석결과 학교 및 연구소의 정부과제 중심의 결과 출원이나 일부 대기업 중심의 과제성 연구가 많은 것으로 판단된다. 상용화를 전제로 한 개발과 생활 보안 기기와 관리체계에 대한 연구는 절대량이 부족한 것으로 보인다. 연도별 출원추이도 다른 선진국들의 출원 패턴이 달라진 2008년 이후 피크에 이른 2013년에도 증감이 별로 없는 것으로 나타나 분발이 필요한 상황이다.

3.2 연구 동향

기존의 실증적 연구와 달리 다중 생체인식의 주요 이점을 보안수준 향상 이외에 HCI기반의 사용자 편의성 향상으로 보는 연구¹⁴⁾도 있으며, 행위적 생체인식 정보에 대한 관찰과 축적된 특성으로 평가하는 SVM(support vector machine)기반의 상황인식 모바일인증시스템¹⁵⁾의 연구도 부각되고 있다. SVM은 인증의 필요여부와 인증요소의 결정에 사용된다. 최근 생체인식의 방법으로 사용자 신원 인식을 위한 다중 생체인식 정보통합 방법의 처리범위 연구¹⁶⁾, 생리 및 행위적 특징 파악과 이상 행동을 식별하기 위한 측정치의 개발¹⁷⁾, 인증 시 생체인식의 무효화¹⁸⁾처리 범위를 통보해 주는 알고리즘 등의 관련된 연구가 있다. 무효화 기준생성 알고리즘은 신규 생체인식정보의 변동에도 원래 생체인식의 판별능력을 잃지 않으면서 신규 생체인식기준을 생성할 수 있어 사용자 인증의 전체 신뢰성을 향상시킬 수 있다.

연구개발 이슈는 효율적인 보안, 대규모 인식 데이터의 실시간 처리, 프라이버시, 데이터베이스의 빈번한 변동의 처리방안, 생체인식 특성 과 동시에 획득된 상황정보의 활용능력, 발전된 정보통합 방법 등이 있다. 향후 이미지 패턴분석과 행위분석으로 사용자의

온라인행동에 대한 정상 및 이상여부 감지 방법, 생체인식의 새로운 특성으로 온라인상의 사회적 네트워크에서 활동하는 형태, 온라인 커뮤니티에 대한 시공간적 생체인식의 접근 형태, 아바타를 통한 인공적 생체인식 영역의 개발 등이 연구과제이다¹⁹⁾. 도전과제로 다중 생체인식 인증을 위한 통합보안 생성 프레임, 참조 템플릿과 특징 진단벡터의 조절, 다중 및 단일 생체인식 modality 조합, 생체특징 벡터의 통합표현과 보안 스킴, 통합수준에 따른 개별 및 전체 시스템의 보안 분야에 대한 연구가 확대되고 있다.

3.3 표준화 동향

생체인식기술의 안전성과 호환 및 연동기능, 생체인식시스템 평가방법, 생체데이터 포맷, 응용인터페이스(BioAPI) 및 생체정보 파일교환 포맷(CBEFF)등 관련 표준들이 국제표준화기구(ISO/IEC JTC1 SC37)에서 활발히 논의되고 있다. 2014년 10월 국내 KISA는 EC BioAPI v2.0을 준용하는 바이오인식 제품(BSP)들에 대한 정상구현 여부 시험과 국제표준화기구에서 권고하는 성능시험 기준 및 절차를 기반으로 바이오인식 제품의 인식알고리즘에 대한 인증 및 성능시험 서비스 실시를 발표했다.

최근 마이크로소프트나 구글 등이 글로벌 플랫폼으로 FIDO(fast identity online 연합)의 보안인증 기술인 '파이드 레디' 도입을 검토하면서 국내스마트폰 제조사, 금융권들도 생체인식 인증 기술의 전자결제 적용을 계획하고 있다. 생체인증솔루션 BioPay도 개발되고 있으며 HTML5 기반의 인증서비스도 개발되고 있다.

3.4 기술시장 전망

상용화 보안을 위한 기존의 기술시장은 2요소 모델이 다중요소 인증시장의 90%를 커버하며, 3~5요소 인증 모델은 2요소에 비해 적은 편이다. 3요소 인증은 pin과 생체인식기술과 결합한 스마트카드, 2개의 생체인식기술과 결합한 스마트카드나 pin 형태, 3개의 생체인식 인증의 형태이다. 5요소 인증은 다중 생체인식 기술과 스마트카드 및 pin을 포함하며 3요소 인증은 대부분 은행라커, 기밀보호, 국방 여권 등에 사용되고 있으며, 4~5요소 인증 모델은 고비용으로 정부, 연구, 국방 응용에 사용된다. 다중 생체인식 인증(MFA)기술은 보안의 가장 중요한 부분이며 고 신뢰도와 함께 모든 보안 부분으로 확대될 예정이다. 2020년 까지 연평균 19.87%씩 성장예측이 있다.

PCT 특허동향 및 출원업체 분석결과, 생체인식기

술 기반의 솔루션기업, 생체인식 어플 개발 전문기업, 단일 생체인식 기술이외에 다중 생체인식 기술개발을 추진하거나 모바일 결제기술을 접목하려는 스마트폰 제조기업, 플랫폼의 주도권을 가지려는 칩 제조기업, 특허사업 전문기업, 사업다각화를 추진하는 이동통신 기업 등 다수의 글로벌기업들이 주력업종에 관계없이 다중 생체인식 인증기술의 개발에 참여하고 있다. 특히 모바일 보안 분야에서 주목할 부분은 모바일 위협 관리, 모바일 정보보호 및 제어, 모바일 사설망, 모바일 ID 및 접속 관리, 모바일 보안 및 취약점 관리 분야이다. IDC에 의하면 MSVM 분야는 년 평균 22% 이상씩 성장할 전망이며 기존 보안 솔루션 사업자들 보다 신생벤처들이 빠르게 시장에 진출하는 상황이다^[20]. Goode Intelligence는 모바일 생체인식보안시장에서 스마트폰 제조 기업들이 2018년까지 주력 스마트폰 기기에 지문인식기능을 탑재해 갈 것이며 2015년 이후에는 저가 모바일기기에도 탑재도 일반화 될 것으로 전망 한다. 생체인식 기업들에게는 기존의 서비스와 MFA 서비스와의 균형점을 찾는 것이 핵심이다. 2018년까지 34억 모바일 기기사용자가 생체인식기능을 사용하게 될 것이라는 전망^[21]은 정확성여부에도 불구하고 생체인식 인증기술의 방향성을 시사해 준다.

Goode Intelligence는 향후 모바일 및 웨어러블 디바이스에서의 생체인식기능의 탑재가 세계적으로 표준적인 개인인증 수단이 될 것^[22]으로 전망한다. 관련된 기술발전 단계로 우선 고 사양 스마트폰과 태블릿의 지문센서들이 통합될 것이며, 이후 혁신적 생체인식 인증기술들이 FIDO표준에 의한 생체인식솔루션이나 지문인식 기기들의 MFA 플랫폼으로 통합되어 탑재되는 형태로 천이될 것이다. 5년 이내에 생체인식 인증기술이 사용자인증의 자연스러운 방법이 될 것이며 모바일과 웨어러블 기술은 생체인식 인증을 지원하는 핵심적 배경기술이 될 것으로 전망한다.

Apple은 Touch ID 지문솔루션과 심장박동과 같은 다른 생체인식 기능을 스마트 워치 등에 통합하는 것과 같이 헬스부문이나 의료부문, 공공부문에서도 다중 생체인식에 대한 관심과 응용증가가 예상된다. 금융권의 모바일 거래 및 결제에 대한 핀테크(Fintech)기술과 애플의 페이, 이베이의 페이펄, 스타벅스의 스케어 월렛, 카카오의뱅크월렛카카오 등 NFC기반의 모바일 결제시스템 시장에서도 다중 생체인식기술의 활용이 증가할 것으로 전망된다. 출입 신원관리 등 응용분야에서의 상용화도 가속화 될 것으로 예상된다. 현재 30개 정도의 생리적 행위적 생체인식 인증대상도 확대될 것으로 예상된다.

향후 5년간 모바일 및 웨어러블 기기에 생체인식 인증을 채택하려는 기술적인 동인은 첫째, 모바일 및 웨어러블 기기에서의 생체인식을 통한 사용자 인증의 편리성 추구, 둘째, 기존의 불편하고 보안성이 떨어지는 패스워드와 PIN의 대체 의지, 셋째, 모바일 지불과 결제 및 전자지갑에 생체인식 인증 채택, 넷째, 기업 모바일 솔루션 제공자들의 생체인식 인증방법 전환 시작, 다섯째, 모바일 및 웨어러블 기기의 다중 생체인식을 IoT기술의 사용자 인터페이스(HCI)에 대한 인증표준으로 인식하려는 경향 등이다.

IV. 대응전략 및 실천과제

다중 생체인식 인증기술 관련 기술이슈와 동향 분석결과를 토대로 한국의 대응전략 구축과 실천해야할 과제를 제시한다.

- 1) 다중 생체인식 인증을 위한 개인 생체인식 인증정보의 관리주체와 시스템 구축에 대한 연구와 개발 과제의 활성화 조치가 필요하다.
- 2) 국내 생체인식산업의 육성을 위한 로드맵 수정과 마스터플랜의 재정립이 필요하다.
- 3) 다중 생체인식기반의 사용자 인증기술에 대한 국내 산학연의 심층연구와 상용화 개발의 촉진정책 전개와 가속화가 필요하다.
- 4) 다중 생체인식 인증기술을 활용한 시범서비스 및 시범사업의 지속적 추진과 사후관리가 필요하다.
- 5) 다중 생체인식기술 관련 인터페이스 표준규격, 생체정보호환 파일 및 데이터 포맷, 생체인식제품 성능시험 방법, 생체인식정보 템플릿 보호, 생체인식 제품 보안성 평가방법 등 생체인식 관련 보안기술에 관한 특허출원 지원, 국제표준화 선도와 주도권 유지활동이 필요하다.
- 6) 국내외 다중 생체인식 표준 및 시험 관련 기구 및 조직 간의 협력 채널 유지와 협력 활동이 필요하다. 국내 우수기술의 국내외 표준화 선도를 위한 표준화 활동조직의 강화와 활동 지원, 업체중심의 자발적 표준화 전문가 양성과 지원책이 필요하다.
- 7) 다중 생체인식 인증제품의 성능시험 및 국제표준 규격에 준거한 상호연동과 국제표준 적합성 시험 서비스 운영 활성화가 필요하다.
- 8) 다중 생체인식 인증기술을 이용한 대국민 신원확인 수단 등의 신규 사업화와 공공부문의 추진이 필요하다. 다중생체인식 인증기술 및 제품 상용화 기술 개발을 위한 중소기업 지원정책 전개 및 관련 과제의 확대가 필요하다.

- 9) 다중 생체인식 인증관련 전문가에 의한 첨단기술 모니터링과 특허 내용분석에 따른 특허전략 수립과 지원, 전문적 내용분석이 필요하다.
- 10) 다중생체인식 인증기술에 대한 국내외 개발자 포럼이나 경진대회 등을 통한 생태계 형성과 산업 활성화 촉진대책이 필요하다. 특히 중소기업과 연계한 다중생체인식 인증기술의 전후방 산업 활성화 정책 전개와 지원이 필요하다.

V. 결 론

국내 다중 생체인식 인증기술의 연구개발 가속화와 산업발전을 위한 기술동향 정보와 대응전략을 제시하였다. 특히 관련 특허기술의 동향분석에 중점을 두었다. 내용은 첫째 다중 생체인식기술의 배경 및 이슈의 고찰과 기술구성 및 선행 알고리즘을 조사하여 상용화 개발 알고리즘의 확대가능성을 제시하였고, 둘째 다중 생체인식기술에 대한 특허동향 및 내역을 분석하고, 관련 연구 및 표준화 동향, 기술시장동향과 전망을 통해 국내 신규 진입기술 연구 및 개발요소의 방향성과 대응전략을 제시하였으며, 마지막으로 실천과제를 강조하여 실질적인 기술발전을 도모하고자 하였다.

References

- [1] http://biz.chosun.com/site/data/html_dir/2014/06/26/2014062602815.html
- [2] C. Rathgeb and C. Busch, *Multi-biometric template protection: issues and challenges*, Da/sec Biometrics and Internet Security Research Group, Center for Advanced Security Research Darmstadt (CASED) D-64283, pp. 173-190, Nov. 2012.
- [3] A. K. Jain, P. J. Flynn, and A. A. Ross, *Handbook of Biometrics*, Springer-Verlag, 2008.
- [4] A. A. Fathima, S. Vasuhi, N. T. Naresh Babu, V. Vaidehi, and T. M. Treesa, "Fusion framework for multimodal biometric person authentication system," *IA ENG Int. J. Comput. Sci.*, vol. 41, no. 1, (Advance online publication: 13 Feb. 2014)
- [5] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits and Syst. for Video Technol.*,

- vol. 14, no. 1, pp. 4-20, Jan. 2004.
- [6] A. Ross, "An introduction to multi biometrics," in *Proc. 15th European Signal Process. Conf.*, Poznam, Poland, Sept. 2007, Retrieved from http://www.cse.msu.edu/~rossarun/pubs/RossIntroMultibio_EUSIPCO07.pdf, Oct. 2014.
- [7] Small & Medium Business Administration, Small & Medium Business Corporation, *Biometric technology & market report*, Oct. 2009.
- [8] E. F. Nakamura, A. F. Loureiro, and A. C. Frery, "Information fusion for wireless sensor networks: Methods, models, and classifications," *ACM Computing Surveys*, vol. 39, no. 3, Article 9, 2007.
- [9] K. Hurst, "Biometrics overview," *NSTC Subcommittee on Biometrics*, Article 6 of the Data Protection Directive, 2006.
- [10] R. Vinothkanna and A. W. Ahi, "Fuzzy vault fusion based multimodal biometric human recognition system with fingerprint and ear," *J. Theoretical and Appl. Inf. Technol.*, vol. 59, no. 2, pp. 304-316, Jan. 2014.
- [11] O. M. Aly, H. M. Onsi, G. I. Salama, and T. A. Mahmoud, "A multimodal biometric recognition system using feature fusion based on PSO," *Int. J. Advanced Research in Comput. Commun. Eng.*, vol. 2, no. 11, pp. 4336-4343, Nov. 2013.
- [12] S. Brindha, I. Vennila, and B. Nivedetha, "Performance analysis of fused eye vein and finger vein multimodal biometric system," *Int. J. Eng. Research and Development*, vol. 10, no. 7, pp. 69-75, Jul. 2014.
- [13] S. A. Radzi, M. H. Khalil-Hani, and R. Bakhteri, *Finger-vein biometric identification using convolutional neural network*, Retrieved from file:///C:/Users/user/Downloads/LK-1311-43_manuscript_2.pdf, Nov. 2014.
- [14] R. R. Heckle, A. S. Patrick, and A. Ozok, "Perception and acceptance of fingerprint biometric technology," in *Proc. Symp. Usable Privacy and Security (SOUPS'07)*, pp. 153-154, 2007.
- [15] H. Witte, C. Rathgeb, and C. Busch, "Context-

aware mobile biometric authentication based on support vector machines,” in *Proc. Int. Conf. Emerging Security Technol. (ES T13)*, pp. 29-32, Retrieved from <http://ieeexplore.ieee.org>, Oct. 2014.

- [16] M. L. Gavrilva and R. V. Yampolskiy, “Applying biometric principles to avatar recognition,” *2010 Int. Conf. Cyberworlds (CW)*, pp. 179-186, Singapore, Oct. 2010.
- [17] S. Yanushkevich, M. Gavrilova, P. Wang, and S. Srihari, *Image pattern recognition: Synthesis and analysis in biometrics*, World Scientific Publishers, 2007.
- [18] P. P. Paul and M. Gavrilova, “Multi modal cancellable biometric,” *IEEE 10th Int. Conf. Cognitive Informatics & Cognitive Computing ICCI*CC 2012*, pp. 43-49, Kyoto, 2012.
- [19] M. L. Gavrilova, “Biometric-based authentication cyberworld security: Challenges and opportunities,” *Canadian Defence & Foreign Affairs Inst.*, pp. 1-9, Jun. 2014,
- [20] KISA, “Investigation for trend of global information protection industry in america,” *Issue no. 3*, pp. 1-25, 2013.
- [21] Goode Intelligence, *Fingerprint Biometrics Market Intelligence*, 1st Ed., Retrieved from <http://www.goodeintelligence.com>, Nov./ Dec. 2103.
- [22] JRM Research, *Biometrics on mobile and wearable devices set to become the universal personal authenticator*, Retrieved from <https://jrminfo.wordpress.com/2014/10/08/jrm-research>

조 병 철 (Byungchul Cho)



1994년 2월 : KAIST 산업공학 박사
 1982년 2월 : KAIST 산업공학 석사
 1980년 2월 : 고려대학교 산업공학 학사
 현재 : KISTI(ReSEAT ICT) 전문연구위원

<관심분야> 정보보안, Digital Forensics

박 종 만 (Jong-man Park)



1997년 2월 : 인하대학교 산업공학 박사
 1987년 2월 : Lehigh Univ. 산업공학 석사
 1983년 8월 : 연세대학교 경영학 석사
 1978년 2월 : 인하대학교 산업공학과 학사

현재 : KISTI(ReSEAT ICT) 전문연구위원
 <관심분야> IoT, 생체인식 인증, 웨어러블 컴퓨팅, 조립식스마트기기, 빅데이터, RFID/USN