Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.4, Aug. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.4.841

바이오인식 정보의 안전한 활용 및 보호방안*

송 창 규,[1†] 김 영 진,[2] 전 명 근[3‡]
[1,3]충북대학교 (연구원, 교수), [2]금융결제원 (연구원)

Secure Biometric Data Utilization and Protection*

Chang-kyu Song,[1†] Young-jin Kim,[2] Myung-geun Chun[3‡]
[1,3]Chungbuk National University (Researcher, Professor),
[2]Korea Financial Telecommunications & Clearings Institute (Researcher)

요 약

바이오인식은 각 개인의 신체적, 생리적, 행동적 특성을 자동화된 장치로 측정하여 이를 등록한 후, 개인을 식별하거나 인증하는 기술을 말한다. 그런데, 여기서 사용되는 바이오인식 정보는 개인을 식별할 수 있으므로 개인정보에 해당된다. 따라서, 이것이 유출되거나 오용되었을 때 정보주체의 프라이버시에 부정적인 영향을 미치게 된다. 본 논문에서는 바이오인식 정보와 관련된 국내의 법적 현황을 살펴보고 이와 관련된 침해현황을 살펴본다. 이어서 대표적인 바이오인식 응용 모델을 도출하고, 각각에 대한 취약점 및 대책 방안을 논의한다. 최종적으로 바이오인식 시스템의 개발자와 서비스제공자를 위해 바이오인식 정보의 보호를 위한 수칙을 제시한다.

ABSTRACT

Biometric recognition refers to a technology that identifies or verifies an individual after registering each individual's physical, physiological, and behavioral characteristics with an automated device. However, the biometric data used here corresponds to personal information since it can identify an individual. Therefore, when it is compromised or misused, it negatively affects the privacy of the data subject. In this paper, we review the current status of domestic laws related to biometric information and the status of infringements related to this. And then, some biometric application models are derived and vulnerabilities and countermeasures for each model are discussed. Finally, for the developer and service provider of the biometric system, protection guidance is presented.

Keywords: Biometrics, Biometric Data, Biometric Authentication, Information Protection

I. 서 론

"바이오인식 정보"란 사람의 고유한 신체적, 생리적, 행동적 특징을 이용하여 개인의 신원을 확인할 수 있게 하는 정보로서 지문, 홍채, 망막, 정맥패턴, 얼굴, 음성, 서명패턴 등 개인을 구별할 수 있는 정보를 말한다. 이러한 바이오인식 정보는 일정한 목적하에 사람을 인식할 수 있음을 전제로 하여서만 그 목적에 따른 기능과 의미를 가지게 된다. 바이오인식은 각 개인의 신체적, 생리적, 행동적 특성을 자동화된 장치로 측정하여 이를 데이터베이스화하고, 이렇게 등록된 바이오인식 정보와의 비교를 통하여 개인을 식별하거나 인증하는 기술을 말한다. 바이오인식 정보는 신체적 특징(선천적)과 이들로부터 파생되는

Received(05. 25. 2021), Modified(06. 29. 2021), Accepted(06. 29. 2021)
* 본 연구는 "과학기술정보통신부 및 정보통신기획평가원의 지역지능화혁신인재양성(Grand ICT연구센터) 사업의 연구결과로 수행되었음" (IITP-2021-2020-0-01462)
* 본 연구는 "한국인터넷진흥원 용역(안전한 바이오정보 활용 및 보호방안 연구)의 연구결과임
† 주저자, sckyu@cbnu.ac.kr
‡ 교신저자, mgchun@cbnu.ac.kr(Corresponding author)

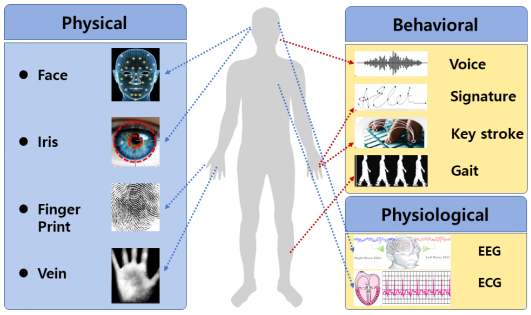

Fig. 1. Biometric characteristics

생리적신호, 그리고 행동적(후천적) 특징으로 구분할 수 있다[1].

신체적 특징으로는 지문, 홍채, 망막, 정맥 등이 대표적인 예이고, 생리적인 특징으로는 뇌파나 심전도 등이 있고 행동적 특징으로는 서명, 음성, 타이핑 리듬, 걸음걸이 등이 있다.

바이오인식 정보 중에서 가장 대표적인 것은 지문(Fingerprint)이라고 할 수 있다. 지문은 태아시기에 생성되어 평생 변하지 않는 특성을 가진다. 모든 사람이 서로 다르고, 평생 변하지 않는 지문이 가지는 장점은 그동안 가장 정확하고 효율적으로 개인의 신원을 확인할 수 있는 수단으로서 인정되어 왔다. 한편, 홍채(Iris)는 생후 18개월 전후 완성된 후 평생 변하지 않는 특성을 가지고 있으며, 홍채의 내측연 가까이에 융기되어 있는 원형의 홍채 패턴은 사람마다 모양이 모두 다르고, 손상으로 인한 변화 확률도 희박하여 최근 IT기기에서 활용되고 있다.

얼굴(Face)도 신체적 특징을 나타내는 대표적인 바이오인식 정보라고 할 수 있다. 다만, 조명이라든지 각도, 표정이나 화장, 헤어스타일 등에 따라 특징점의 변화가 큰 특징이 있다. 또한, 정맥(Vein)인식 기술은 손등이나 손바닥의 정맥 모양으로 신원을 식별하는 방법으로 적외선을 이용하여 혈관을 투시한 영상으로 신원을 확인하는 바이오인식기술이다.

음성이나 걸음걸이(Gait) 등의 행동적 특징을 이용한 바이오인식 기술은 원격에서의 사용자 로그인이나 지능형 CCTV 등에서 개인을 식별하는 데 사용되고 있다[2]. 최근에는 센싱 기술의 발전으로 뇌파(EEG)나 심전도(ECG)와 같이 신체로 유기되는 생리적 신호에 기반하여 개인을 인증하는 연구도 진행되고 있다[3].

바이오인식 정보보호에 관한 기존의 가이드라인[4][5]이 프라이버시 보호원칙에 따라 선언적인 권고사항만을 나열하고 있는 한계가 있다. 이에, 본 논문에서는 바이오인식 정보의 보호와 관련된 국내의 법적 현황을 살펴보고 이와 관련된 침해현황을 살펴본 후, 이를 토대로 대표적인 바이오인식 응용 모델을 도출하고, 각각에 대한 취약점 및 대책 방안을 논의한다. 최종적으로는 바이오인식 시스템의 개발자를 위해 각 개발 단계별 바이오인식 정보의 보호를 위한 수칙을 제시함으로서 안전한 바이오인정보의 활용에 기여하고자 한다.

II. 바이오인식 정보 활용 및 침해 현황

2.1 바이오인식 정보 관련 법적 현황

바이오인식을 이용한 서비스에서 바이오인식 정보의 보호에 관한 문제가 중요한 이슈로 제기되는 이유는 독립적으로 또는 다른 정보와 결합하여 특정한 개인을 인식할 수 있도록 하는 바이오인식 정보들이 집적되어 서버에 저장되어 정보주체나 정보 관리자 외의 제3자에게 유출되어 정보주체에게 불리하게 된다. 또한 개인의 바이오인식 정보를 획득한 자에 의하여 정보가 이용되지 않는다고 하여도 바이오인식 정보의 특성상 정보주체나 정보 관리자 외의 제3자가 그 정보에 접근 가능한 것 자체만으로도 문제의 소지가 있다. 한편으론, 접근 가능한 상태에 있다는 것만으로도 잠재적으로 프라이버시 침해가 가능한 상태에 있다고 할 수 있기 때문이다.

2020년 8월 5일부터 데이터 3법의 개정에 이어 개인정보보호법 시행령이 개정되면서 홍채, 안면 등 바이오인식 정보가 개인정보보호법상 '민감정보'로 분류되어 엄격한 관리 하에 놓이게 되었다. 개인정보보호법 제23조 제1항은 민감정보의 처리와 관련하여 원칙적으로 그 처리를 금지하고, 예외적으로 정보주체로부터 다른 개인정보처리에 대한 동의와 별도로 동의를 받은 경우, 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에만 이에 대한 처리를 할 수 있도록 하고 있다.

개인정보보호법상 민감정보의 범위는 시행령에서 규정하도록 되어 있다. 종래에는 민감정보가 '유전자 정보'와 '범죄경력자료에 해당하는 정보'로 규정되어 있었으나, 2020년 8월 시행령의 개정을 통하여 인종이나 민족에 관한 정보와 함께 '바이오인식 정보'가 민감정보에 포함되었다. 즉, 특정 개인을 알아볼 목적으로 사용하는 지문·홍채·안면 등 바이오인식

정보(Biometric Data)는 개인의 고유 정보로서 유출 시 되돌릴 수 없는 피해가 발생할 가능성이 매우 높기 때문에, 민감정보에 "개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보"를 포함하였다.

바이오인식 정보가 민감정보에 포함되면 별도의 동의를 받아야 하는 추가적인 부담이 생긴다는 우려가 있었으나, 바이오인식 정보가 본인인증이나 금융거래 등 개인에게 중요한 업무에 이용되고 침해 시 돌이킬 수 없는 피해가 예상됨에 따라 유럽 GDPR (General Data Protection Regulation)에 맞게 보호해야 할 필요성을 반영한 것이다[6]. 유럽연합의 GDPR 9조 4항에서 개인정보 중에서 유전정보, 바이오인식 정보 및 건강정보에 대해서는 회원국으로 하여금 더 엄격한 제한 기준을 추가적으로 설정할 수 있음을 명시하고 있다.

「개인정보 보호법」 제23조는 개인정보 처리에 관하여 특별한 규정으로 제15조, 제17조 및 제18조 등 개인정보 처리에 관한 다른 규정에 우선하여 적용되므로, 민감정보의 경우에는 제23조 제1항 각호에서 정하는 예외 사유가 존재하는 경우에 한하여 처리할 수 있다.

2.2 바이오인식 정보 침해 현황 및 시나리오

바이오인증 시스템은 바이오인식을 통하여 개인인증을 수행하는 정보시스템을 의미하며, Fig. 2.와 같이 크게 5개의 모듈로 구분된다.

- 데이터 취득(Data capture): 센서를 통해 바이오인식 원본정보를 취득
- 신호처리부(Signal processing): 취득된 바이오인식원보정보로 부터 특징정보를 추출
- 데이터 저장부(Data Storage): 특징정보 및 개인정보 등을 저장하는 저장소
- 비교부(Comparison): 저장된 특징정보와 새로 입력된 바이오인식 정보를 비교하여 매칭값을 계산
- 결정부(Decision) : 저장된 특징정보와 새로 입력된 특징정보를 비교하여 인증 여부를 결정

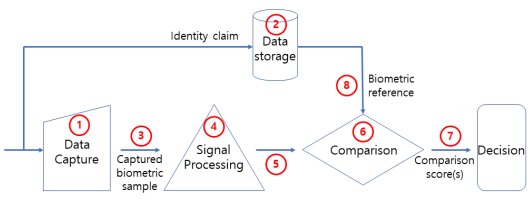

Fig. 2. Attack points within biometric system

공격자로부터 바이오인식 정보를 안전하게 보호하는 보안기술에 대한 관심이 높아지고 있으며, Fig. 2.에 보인 바와 같이 바이오인증 시스템의 취약점은 크게 8가지로 분류될 수 있다.

① 위조된 바이오인식 정보를 센서에 입력하여 인증을 우회하는 경우
② 저장소에 침투하여 저장되어 있는 바이오인식 정보를 조작, 삭제, 유출하는 경우
③ 불법 취득한 바이오인식 정보를 재생(replay)하여 인증하는 경우
④ 위조된 특징정보를 임의로 생성하는 경우
⑤ 정상적인 특징정보를 임의의 위조된 특징정보로 대체하는 경우
⑥ 특징 비교부에서 인증 결과값을 임의로 변경하는 경우
⑦ 최종 인증결과를 조작하는 경우
⑧ 저장소에서 정합부로 전송되는 특징정보를 절취 또는 타인의 정보로 대체하는 경우

바이오인식 정보를 이용한 인증에서의 공격은 ① PA(Presentation Attack)로 대상자의 바이오인식 정보를 도용하거나 ② PAI(Presentation Attack Instrument)를 이용하여 대상자의 바이오인식 정보로 정보를 도용하는 것이 주류를 이루고 있다. ③~⑧의 경우는 바이오인증 시스템을 해킹하여 침투할 경우 발생하는 취약점으로 해킹기술이 진화함에 따라 사고사례가 늘어날 것으로 예상된다[7].

III. 바이오인식 서비스 응용모델에 따른 바이오인식 정보보호 방안

앞서 설명된, 바이오인식시스템의 5개의 기능(데이터취득, 신호처리, 비교, 결정, 데이터저장부) 등이 시스템 상에 어디에 위치하느냐에 따라 Table 1.과 같은 바이오인식 서비스의 대표적인 응용 모델을 도출하였다. Table 1.에서 빈칸은 운용되고 있는 서비스가 없는 경우에 해당된다.

Table 1.에서 접근장치(Access device)는 금융분야에서의 예를 들면 현금지급기(ATM)나 키오스

Table 1. Application models of a biometric system

Capturing/Processing/Comparison/Decision						Storage	
						Server	Trusted Module
Capturing	Access device	Processing	Server	Comparison /Decision	Server	Model A	Model C
			Access Device		Server	Model B	Model D
	Trusted Module	Processing	Server	Comparison /Decision	Server		Model E
			Trusted Module	Comparison /Decision	Trusted Module		Model F

크(Kiosk) 등의 단말기로 바이오인식을 통하여 인증서비스를 받으려고 할 때 사용하는 단말기를 말한다. 또한 신뢰모듈(Trusted module)은 바이오인식 취득 센서를 포함하는 모바일장치, 스마트카드 또는 USB 형식의 모듈에서 신뢰할 수 있는 보안 영역을 가지고 있는 모듈이다. 스마트폰의 경우, 바이오인식 센서와 연결된 스마트폰 내의 신뢰 영역은 신뢰모듈로 간주될 수 있다[8].

3.1 모델 A

이 모델은 중앙 집중형 바이오인식 시스템이라고 할 수 있다. 이 경우 접근장치는 수집 능력만 있으며 처리 능력은 필요하지 않다. 따라서 서비스 기관과 고객은 처리 알고리즘을 구현하지 않고도 비교적 저렴한 접근장치를 채택할 수 있기 때문에 비용이 적게 든다. 또한 서비스 기관은 고객의 접근장치 업그레이드를 고려하지 않고도 필요할 때 서비스 기관의 서버만을 업그레이드 할 수 있는 장점이 있다.

이 모델은 ATM, 키오스크 또는 금융기관 창구직원의 단말기에서의 거래에 적용될 수 있다. 바이오인식 원보정보가 서비스 기관의 서버로 전달되어야 하기 때문에, 접근장치와 서버 간 보안 네트워크가 요구된다. 한편, 바이오인식 및 신원정보는 서비스 기관에 의해 처리되고 저장되기 때문에 데이터베이스 보안 및 네트워크 보안을 보장하는 신뢰할 만한 관리가 필요하다. 접근장치가 원격으로 연결되기 때문에 ISO/IEC 30107[9]에 명시된 위·변조된 바이오인식이 처리되지 않도록 하는 제시형 공격 탐지기법(Presentation attack detection) 등의 보안대책이 필요하다.

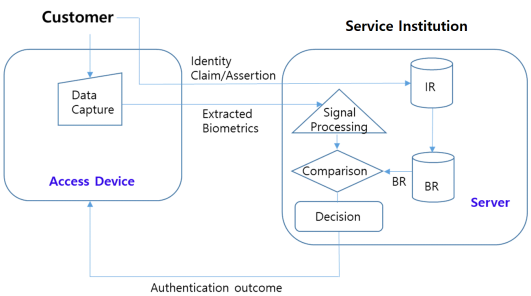

Fig. 3. Model A

3.2 모델 B

이 모델에서 바이오인식 정보는 접근장치에서 수집 및 신호처리 되는데, 접근장치는 개인용 장치이거나 공공장소에 설치된 장치일 수 있다. 여기에서 접근장치는 바이오센서뿐만 아니라 신호처리 능력을 가지고 있어야 한다. 추출된 바이오인식 특징 정보는 Fig. 4.에 보인 바와 같이 비교 및 결정을 위해 서비스 기관의 서버로 전송된다. 고객의 바이오인식 정보는 인증 전 등록 프로세스를 통해 서비스 기관의 서버로 전송된다. 서비스 시작을 위해 사용자의 추출된 바이오인식 정보 및 해당 신원정보(identity reference)를 요청한다. 이 모델은 서비스 기관의 중앙집중식 바이오인식 데이터베이스를 보호하기 위해 강력한 데이터베이스 및 네트워크 보안 관리가 필요하다.

이 모델은 고객이 인터넷 뱅킹을 위해 PC 또는 태블릿과 같은 개인용 접근장치를 사용할 때 금융거래에 적용될 수 있다. 접근장치가 ATM, 키오스크 또는 창구직원의 단말기와 같은 공용장치인 경우, 금융거래는 이 모델로 인증한 후 수행될 수 있다. 이 모델에서는 서비스 기관이 접근장치에 의해 수집되고

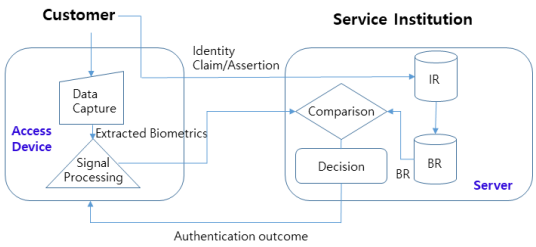

Fig. 4. Model B

처리된 바이오인식 데이터를 신뢰해야 한다. 바이오인식 정보 및 신원정보는 서비스 기관에 의해 처리되고 저장되기 때문에 데이터베이스 보안 및 네트워크 보안을 보장하는 신뢰할 만한 관리가 필요하다. 접근장치는 원격으로 연결되므로 모델 A와 동일한 제시형 공격 탐지기법 등의 보안대책이 필요하다.

3.3 모델 C

이 모델에서 바이오인식 정보는 신뢰모듈에 저장되며 바이오인식 데이터는 접근장치를 통해 추출된다. 그런 다음 신뢰 모듈의 바이오인식 정보와 취득된 바이오인식 원본정보는 비교를 위해 서버로 전송된다. 신원을 요청하고자 하는 고객은 신뢰 모듈을 가지고 있어야 하며 그것을 접근장치에 연결해야 한다. 비교 및 결정 후, 서버는 인증 결과를 접근장치로 전송한다.

이 모델에서는 서비스 기관이 접근장치에서 취득된 데이터를 신뢰해야 한다. 바이오인식 정보는 개인이 소지하고 있는 스마트카드 등의 신뢰모듈에 저장되어 있어야 한다. 그러나 이 모델에서는 저장된 바이오인식 정보 및 취득된 바이오인식 원본정보가 서버로 전송되므로 네트워크 보안이 필요하다. 접근장치는 원격으로 연결되므로 모델 A와 동일한 제시형 공격 탐지기법 등의 보안대책이 필요하다.

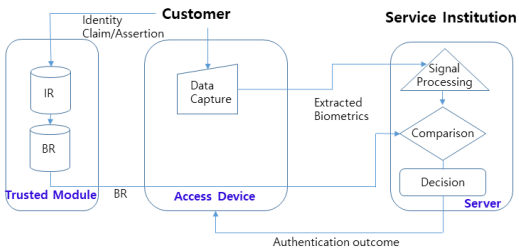

Fig. 5. Model C

3.4 모델 D

바이오인식 정보는 신뢰 모듈에 저장되며 바이오인식 데이터는 접근장치를 통해 취득된 후 특징점이 추출된다. 그런 다음 신뢰모듈의 바이오인식 정보는 비교 및 결정을 위해 서버로 전송된다. 그 후, 서버는 인증 결과를 접근장치로 전송한다. 이 모델을 채택하는 경우 등록된 바이오인식 정보와 추출된 바이오인식의 이동 경로를 최소화할 수 있다.

모델 B와 다르게 사용자의 바이오인식 정보가 서비스기관의 서버에 저장되지 않으므로, 대규모 중앙 데이터베이스에 의한 침해 위협은 피할 수 있다. 그러나 저장된 바이오인식 정보의 전송을 보호하기 위해 네트워크 보안이 필요하다. 또한 모델 A와 동일한 제시형 공격 탐지기법 등의 보안대책이 필요하다.

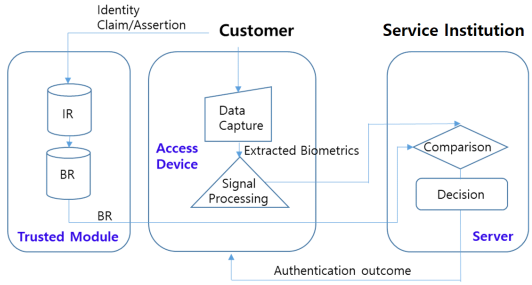

Fig. 6. Model D

3.5 모델 E

이 모델에서 바이오인식 정보는 신뢰모듈에 저장되며 바이오인식 정보는 신뢰모듈을 통해 취득된다. 그런 다음 등록된 바이오인식 정보 및 취득된 바이오인식 정보는 처리, 비교 및 결정을 위해 서버로 전송된다. 개인인증을 요청하고자 하는 고객은 신뢰모듈을 가지고 있어야 하며 그것을 접근장치에 연결해야 한다. 비교 및 결정 후, 서버는 인증 결과를 접근장치로 전송한다.

이 모델은 신뢰모듈이 저장 기능 및 취득 기능을 가지는 경우의 서비스에 사용될 수 있다. 이 모델은 ATM, POS 또는 키오스크에서의 거래와 같이 비교 및 결정이 서버에서 수행되어야 하는 서비스에 적용될 수 있다.

이 모델에서는 서비스 기관이 신뢰모듈에서 취득된 데이터를 신뢰해야 한다. 바이오인식 정보는 신뢰모듈에 안전하게 저장되어야 한다. 또한, 저장된 바

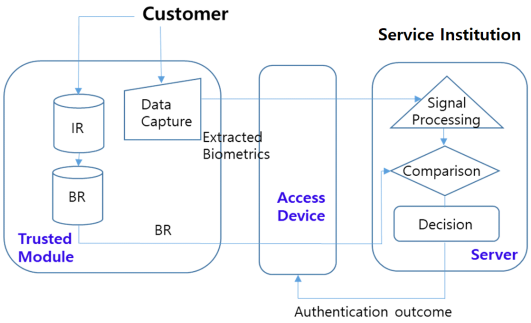

Fig. 7. Model E

이오인식 정보 및 취득된 바이오인식 원본정보의 전송이 필요하므로 이들을 보호하기 위한 네트워크 보안이 필요하다.

3.6 모델 F

이 모델에서 바이오인식 정보는 신뢰모듈에 저장되며, 바이오인식 데이터는 신뢰모듈의 바이오인식 센서를 통해 취득 및 특징점이 추출된다. 비교 및 결정 프로세스를 포함하여 모든 과정이 신뢰모듈에서 수행된다. 본 모델을 구현하려면, 신뢰모듈에는 수집, 처리, 저장, 비교 및 결정 기능이 있어야 한다. 신뢰모듈은 인증 결과를 접근장치로 전송하고 접근장치는 인증 결과를 서비스 기관의 서버로 전달한다.

본 모델은 삼성페이나 애플페이와 같이 바이오인식 센서가 내장되어 있는 스마트폰에서 이루어지는 모델에 해당된다. FIDO 프로토콜을 이용한 원격 개인인증에 널리 사용되고 있는 모델이다[10].

바이오인식 정보는 신뢰모듈에 안전하게 저장되어야 하며, 인증을 위한 바이오인식 정보가 신뢰모듈에서 수집 및 처리되고 비교되어야 한다. 모든 정보가 신뢰모듈 내에서 이루어지므로 가장 안전한 바이오인식 시스템이라고 할 수 있다. 다만, 신뢰모듈의 바이오인식 센서는 ISO/IEC 30107[9]에 명시된 제시

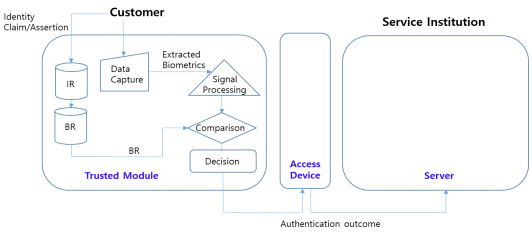

Fig. 8. Model F

형 공격 탐지기법 등의 보안대책이 필요하다.

IV. 바이오인식 정보 보호를 위한 수칙 도출

앞서 기술된 바이오인식 시스템의 응용모델을 개발하는 개발자에 공통적으로 적용할 수 있는 바이오인식 정보 보호 수칙을 바이오인식 정보의 처리 과정 및 이를 활용하는 절차에 따라서 제시하고자 한다.

- 개념설정
- 분석/설계
- 개발
- 테스트
- 적용

정보보호 수칙을 도출함에 있어서 다음과 같은 바이오인식보호 국제표준 및 국내 가이드라인뿐만 아니라 개인정보보호에 관한 국제표준 및 가이드라인을 참조하여 국내 실정에 맞게 수정 보완하였다.

- ISO/IEC 24745 Biometric Information Protection[8]
- KS X ISO/IEC 29100 프라이버시 프레임워크[11]
- 바이오인식보호 가이드라인[12]
- Ethical Principles for the Biometrics, Biometric Institute[13]

4.1 바이오인식 시스템 개발자를 위한 수칙

1. 개념설정 단계

□ (원칙 1) 바이오인식 정보의 이용에 있어서, 서비스 목적에 맞는 바이오인식 정보를 선택하여 적용하되, 이것을 제공 할 수 없는 사용자에 대한 대안도 마련하여야 한다.

2. 분석/설계 단계

□ (원칙 2) 바이오인식 시스템을 5개의 기본적인 부분요소로 나눈 후, 각 부분별 바이오인식 정보에 대한 침해 대응 요구사항을 반영한다.

□ (원칙 3) 바이오인식 정보보호가 전체 서비스시스템의 아키텍처 안에 내재 되어 기본 기능으로 제공되어야 한다.

3. 개발단계

□ (원칙 4) 바이오인식 정보 수집을 위한 동의 절차를 구현하고, 사용자 기기 내에 바이오인식 정보가 저장되는 구조로 개발하되, 바이오인식 정보의 저장이 필요한 경우 분할저장 방식을 채택하도록 한다.

□ (원칙 5) 바이오인식 정보의 활용에 있어서 시스템의 특별한 요구 조건이 없으면 바이오인식 특징정보 추출 후 바이오인식 원본정보를 폐기한다.

4. 테스트 단계
□ (원칙 6) 바이오인식 시스템의 성능을 테스트하기 위해 수집되는 바이오인식 정보도 적절한 동의절차를 거쳐서 수집되어야 한다.
□ (원칙 7) 테스트를 위해 수집된 바이오인식 정보는 연계된 개인식별 정보와 별도로 안전하게 보관되어 관리되어야 한다.

5. 적용 단계
□ (원칙 8) 개발된 바이오인식 시스템을 전달하기에 앞서서 개발 중에 사용된 바이오인식 정보 등의 저장 여부를 확인하고 폐기하는 절차를 마련하여야 한다.

4.1.1 개념설정 단계

□ (원칙 1) 바이오인식 정보의 이용에 있어서, 서비스 목적에 맞는 바이오인식 정보를 선택하여 적용하되, 이것을 제공 할 수 없는 사용자에 대한 대체 수단도 마련하여야 한다.
- ■ 바이오인식 서비스에 맞는 바이오인식 특징을 선택함에 있어서, 인식률과 더불어 사용자의 수용성과 편의성을 고려하여 선택한다.
- ■ 특정 바이오인식 특징, 예를 들어 지문인식을 채택 하였을 경우 전체 인구의 일정 비율은 이를 사용할 수 없을 정도의 지문을 가지고 있다. 따라서, 이로 인하여 특정 서비스에서 배제되는 이용자가 발생할 수 있으므로 지문이외의 대체수단을 제공하여야 한다.

4.1.2 분석/설계 단계

□ (원칙 2) 바이오인식 시스템을 5개의 기본적인 부분 요소로 나눈 후, 각 부분별 바이오인식 정보에 대한 침해 대응 요구사항을 반영한다.
- ■ 바이오인식 시스템을, 데이터 취득부, 신호처리부, 비교부 데이터 저장부, 결정부의 5개의 부분 요소로 나눈 후 각 부분별 침해 요소와 대응 방안을 반영한다. 3장의 바이오인식 서비스 응용모델에 따른 바이오인식 정보보호 방안 참조.

□ (원칙 3) 바이오인식 정보보호가 전체 서비스시스템의 아키텍처 안에 내재되어 기본 기능으로 제공되어야 한다.
- ■ 바이오인식시스템의 개발에 있어서, (원칙 2)에서 분석된 바이오인식 정보 대응 요구사항을 전체 서비스 시스템의 아키텍처 안에 정보보호 기능을 기본으로 내장하여 구현하도록 한다.
- ■ 저장 장치에 대해서는 암호화 등의 조치를 취하고, 바이오인식 정보의 전송 구간에서는 무결성과 기밀성을 보장할 수 있는 기술적 방안을 구현한다.
- ■ 센서 등의 장치를 통해 바이오인식이 수집·입력될 때, 제3자에 의해 위·변조된 바이오인식이 처리되지 않도록 제시형 공격 탐지 기능을 내장한다.
  - PAD: 실리콘 인공지문, 녹음된 음성, 캡처된 얼굴·홍채사진 등과 같이 위·변조된 바이오인식이 수집·입력될 경우, 이를 탐지하고 서비스 이용을 거부할 수 있도록 하는 메커니즘이다.

4.1.3 개발 단계

□ (원칙 4) 바이오인식 정보 수집을 위한 동의 절차를 구현하고, 사용자 기기 내에 바이오인식 정보가 저장되는 구조로 개발하되, 바이오인식 정보의 저장이 필요한 경우 분할저장 방식을 채택하도록 한다.
- ■ 「개인정보 보호법」 제23조제1항에 따라, 다른 개인정보의 처리에 대한 동의와 별도로 다음과 같은 내용을 포함한 바이오인식 정보 수집에 대한 동의 절차를 구현한다.
  - 바이오인식 정보의 수집·이용 목적
  - 바이오인식 정보의 보유 및 이용 기간
  - 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
- ■ 바이오인식 정보를 서버로 전송하여 처리할 경우 침해사고 발생 시, 대규모 바이오인식 유출 등 피해 범위가 커지므로, 스마트폰 내 안전한 영역 또는 보안토큰, 스마트카드 등 이용자가 자신의 바이오인식 정보를 통제할 수 있는 저장·처리하는 방식을 우선적으로 고려하여야 한다.
- ■ 바이오인식 정보를 서비스서버와 사용자기기에 분할하여 저장함으로서 어느 한곳에서 바이오

인식 정보가 유출되더라도 다른 한곳의 바이오인식 분할정보가 없으면 원래의 바이오인식 정보를 복구할 수 없게 함으로서 이용자의 바이오인식 정보를 보호할 수 있다[14].

□ (원칙 5) 바이오인식 정보의 활용에 있어서 시스템의 특별한 요구 조건이 없으면 바이오인식 특징정보 추출 후 바이오인식 원본정보를 폐기한다.

■ 바이오인식 원본정보는 개인을 식별하기 위해서 사용되는 바이오인식 특징 정보를 추출하기 위해서 사용되며, 이것이 유출 되었을 경우에는 이로부터 유사한 방법으로 바이오인식 특징점 정보를 불법으로 추출 할 가능성이 있다.

■ 개발자는 바이오인식 시스템을 개발함에 있어서, 특별한 요구 조건이 없을 경우에 바이오인식 특징점 추출 후 바이오인식 원본 정보를 즉시 폐기 하도록 설계 및 구현한다.

■ 시스템간의 호환성이나, 성능 향상 등을 위하여 바이오인식 원본을 저장할 경우에는 무결성과 기밀성을 위하여 안전성 확보조치를 구현한다.

4.1.4 테스트 단계

□ (원칙 6) 바이오인식 시스템의 성능을 테스트하기 위해 수집되는 바이오인식 정보도 적절한 동의절차를 거쳐서 수집되어야 한다.

■ 바이오인식 시스템의 성능을 테스트하기 위해서 해당기관(기업체) 내의 임직원을 대상으로 수집되어 사용되는 바이오인식 정보 및 개인정보에 대해서도 「개인정보 보호법」에 기술되어 있는 절차에 따라 합법적으로 수집되어야 한다.

■ 「개인정보 보호법」 제23조제1항에 따르면 바이오인식 정보를 다음과 같은 동의 절차에 따라 수집할 수 있다.

정보주체에게 다음의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도의 동의를 얻어야 한다.

- 바이오인식 정보의 수집·이용 목적
- 바이오인식 정보의 보유 및 이용 기간

□ (원칙 7) 테스트를 위해 수집된 바이오인식 정보는 연계된 개인식별 정보와 별도로 안전하게 보관되어 관리되어야 한다.

■ 바이오인식 시스템의 개발 성능 향상 및 테스트를 위하여 사용되는 바이오인식 정보와 이와 연계된 개인식별 정보가 같이 유출되는 경우에는 큰 개인정보 침해 요인이 될 수 있다.

■ 따라서, 바이오인식 정보와 개인을 식별할 수 있는 정보를 물리적 또는 논리적으로 분리하여 암호화 등의 안전조치 후 별도로 저장·관리하여야 한다.

4.1.5 적용단계

□ (원칙 8) 개발된 바이오인식 시스템을 전달하기 전에 개발 중에 사용된 바이오인식 정보 등의 저장 여부를 확인하고 폐기하는 절차를 마련한다.

■ 바이오인식 시스템의 성능 향상 및 테스트를 위해 제공된 바이오인식 정보와 이와 연계된 개인식별 정보를 개발완료 후 바이오인식 서비스 사업자에게 전달되는 시스템에 포함되어 넘기는 경우, 해당자들의 개인정보가 동의의 범위를 벗어나서 제 3자에게 넘어가는 것이 되므로, 이들을 안전하게 폐기하여야 한다.

■ 바이오인식 원본정보의 경우 유출이 되면, 변경이 불가능하며 건강·인종 등 부가적인 정보가 추출되어 개인의 프라이버시를 침해할 우려가 있으므로 강화된 보호 조치가 필요하다.

■ 바이오인식 서비스를 위한 시운전 등, 일부 바이오인식 정보 및 개인 식별정보가 필요한 경우, 해당자에게 이러한 사실을 고지 한 후, 별도의 동의를 받아야 한다.

4.2 바이오인식 서비스 제공자를 위한 수칙

1. 서비스 준비단계

□ (원칙 1) 바이오인식 정보의 이용목적이 합법적이며, 민감정보인 바이오인식 정보의 처리 필요성을 명확히 하여야 한다.

2. 수집 단계

□ (원칙 2) 바이오인식 정보의 처리에 대해 동의를 받는 절차를 마련하고, 바이오인식 원본 정보의 저장여부에 대해서도 별도의 동의를 받는다.

□ (원칙 3) 바이오인식 정보의 처리와 더불어 개인인증을 위해 수집되는 개인정보의 종류·접근권한·접근을 최소화 하여야 한다.

3. 이용·저장·관리 단계

□ (원칙 4) 바이오인식 정보는 전사차원에서 개인정보 보호 관리체계에 준하여 관리한다.

□ (원칙 5) 바이오인식 정보는 정확하고, 최신화 되고

인식성능 보증을 위해 일정 품질 이상이 되도록 하여야 한다.
□ (원칙 6) 바이오인식 정보 제공자가 자신의 바이오인식 원본정보가 저장되어 있는 경우 동의 철회, 삭제, 정정 등 정보주체의 기본권을 보장한다.
□ (원칙 7) 바이오인식 정보와 개인정보는 별도로 저장하여 함께 유출되는 일이 없도록 하여야 한다.
□ (원칙 8) 바이오인식 정보 처리에 있어서, 공개성, 투명성, 고지의 원칙을 준수한다.

4. 파기 단계
□ (원칙 9) 바이오인식 원본정보는 그 목적을 달성 하였을 경우, 즉시 파기한다. 서비스 중단 등의 경우에는 바이오인식 시스템의 테스트, 검증 등에 활용된 이용자의 바이오인식 정보를 파기하고 관련 개인정보를 파기 또는 비식별 처리하도록 한다.

4.2.1 서비스 준비단계

□ (원칙 1) 바이오인식 정보의 이용목적이 합법적이며, 민감정보인 바이오인식 정보의 처리 필요성을 명확히 하여야 한다.
- ■ 개인정보법 시행령에서 정의하고 있는 민감정보의 범위에 '개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보'인 바이오인식 정보를 포함하고 있다. 이러한 민감정보는 원칙적으로 그 처리를 금지하고, 예외적으로 정보주체로부터 다른 개인정보처리에 대한 동의와 별도로 동의를 받은 경우, 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에만 이에 대한 처리를 할 수 있도록 하고 있다.
- ■ 유럽연합의 GDPR은 안면 영상이나 지문 정보와 같이 개인 고유의 식별을 허용 또는 확인하는 해당 개인의 신체적, 생리적, 행동적 특성에 관한 특정 기술 처리로 발생하는 개인정보로 ′바이오인식 정보′를 정의하고 '민감정보(Special categories of personal data)'로 규정하고 있다.
- ■ 따라서, 사용자를 식별하기 위해서 적용할 수 있는 다양한 인증이나 식별 수단을 비교하여 바이오인식을 채택하여 얻을 수 있는 안전이나 편익이 기타의 수단보다 현저히 클 경우 이를 채택한다.

4.2.2 수집단계

□ (원칙 2) 바이오인식 정보의 처리에 대해 동의를 받는 절차를 마련하고, 바이오인식 원본 정보의 저장여부에 대해서도 별도의 동의를 받는다.
- ■ 「개인정보 보호법」 제23조제1항에 따라 바이오인식을 이용한 서비스 사업자는 바이오인식 정보를 다음과 같은 동의 절차 이후에 따라 처리할 수 있다.
  정보주체에게 다음의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도의 동의를 얻어야 한다.
  - 개인정보의 수집·이용 목적
  - 수집하려는 개인정보의 항목
  - 개인정보의 보유 및 이용 기간
  - 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용
- ■ 바이오인식 정보를 이용한 서비스 사업자는 민감정보인 바이오인식 정보를 처리하므로 이에 따라서 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 조치를 해야 한다(「개인정보 보호법」 제23조제2항).

□ (원칙 3) 바이오인식 정보의 처리와 더불어 개인인증을 위해 수집되는 개인정보에 종류·접근권한·접근을 최소화한다.
- ■ 바이오인식 정보와 결부하여 사용하려는 개인정보의 수집은 최소화 하고, 아울러 이들 정보에 접근 가능한 직원의 수를 최소한으로 통제 하여야 한다.
- ■ 개인정보를 보유해야 하는 법적 요구사항이 없고, 사제가 가능한 상태가 되거나 개인정보 처리 목적이 완수 될 때 마다 개인정보를 삭제하고 폐기함으로서 보유하고 있는 개인정보를 최소화한다.
- ■ "need-to-know(알아야 할 필요가 있을 때)"라는 원칙에 입각하여, 바이오인식 정보를 포함한 개인정보의 접근을 최소화 하여야 한다.

4.2.3 이용・저장・관리 단계

□ (원칙 4) 바이오인식 정보는 전사차원에서 정보보호 및 개인정보보호 관리체계(ISMS-P)에 준하여 관리한다.

■ 정보보호 및 개인정보보호 관리체계 인증의무 대상사업자인 경우에는, 이러한 관리체계에서 정의된 개인정보 취급 절차에 준하여 바이오인식 정보도 관리한다.

■ 인증 의무 대상자가 아니라도, 바이오인식 정보를 포함한 개인정보의 취급을 자율적으로 정보보호 및 개인정보보호 관리체계에 준하여 관리하도록 한다.

□ (원칙 5) 바이오인식 정보는 정확하고, 최신화되고 인식성능 보증을 위해 일정 품질 이상이 되도록 하여야 한다.

■ 안면 정보들의 바이오인식 정보는 시간에 따라, 인식률이 저하되는 것으로 알려져 있다. 따라서 바이오인식 시스템의 인식 성능을 유지하기 위해서 저장되어 있는 바이오인식 정보를 재수집하는 등의 절차를 마련하여야 한다.

■ 지문・얼굴・홍채 등의 바이오인식 정보를 취득 시에, 영상의 품질 검사 등을 통하여 일정 수준 이상이 되는 것만 취득되도록 하여 본인거부율이나 타인수락률 등이 높아지지 않도록 하여야 한다.

□ (원칙 6) 바이오인식 정보 제공자가 자신의 바이오인식 원본정보가 저장되어 있는 경우 동의 철회, 삭제, 정정 등 정보주체의 기본권을 보장한다.

■ 바이오인식 원본 정보는 별도의 동의에 의해 저장되므로, 서비스 이용자가 자신의 바이오인식 원본 정보의 저장에 더 이상 동의하지 않고 이를 철회, 삭제, 정정할 수 있는 절차를 마련하여 놓아야 한다.

□ (원칙 7) 바이오인식 정보와 개인정보는 별도로 저장하여 함께 유출되는 일이 없도록 하여야 한다.

■ 바이오인식 정보 중에서 특징점 정보의 경우, 이와 관련된 개인식별 정보가 같이 제공 되지 않은 경우에는 어떤 한 개인을 특정하기가 어려울 수 있다. 그러나, 바이오인식 원본정보나 특징정보가 개인식별 정보가 같이 유출되는 경우에는 대상자에게 큰 개인정보 침해 요인이 될 수 있다.

■ 따라서, 바이오인식 정보와 성명·주소 등 해당 이용자의 다른 개인정보와 분리하여 별도로 저장·관리하여야 한다.

- 물리적으로 분리하여 별도로 저장·관리하는 것이 바람직하나, 부득이한 경우 물리적 분리와 동등한 수준으로 논리적으로 분리하여 저장·관리하도록 한다.
- 원본정보와 이용자의 다른 개인정보를 상호 연결하는 공통식별자는 임의 값을 활용하여 직접적으로 해당 이용자가 나타나지 않도록 조치한다.

□ (원칙 8) 바이오인식 정보 처리에 있어서, 공개성, 투명성, 고지의 원칙을 준수한다.

■ 바이오인식 제공자에게 바이오인식 정보 처리에 대한 정책, 절차에 대해서 분명하고 쉽게 관련 정보를 제공한다.

■ 바이오인식 정보를 포함한 개인정보 처리의 책임자에 관한 연락처를 포함한 정보를 공개한다.

■ 사업자는 이용자에게 수집·이용되는 바이오정보의 종류, 보호조치, 통제권행사 방법, 처리방법 등을 적극적으로 안내하여야 하고, 이용자가 언제든지 이를 확인할 수 있도록 하여야 한다.

4.2.4 파기 단계

□ (원칙 9) 바이오인식 원본정보는 그 목적을 달성하였을 경우, 즉시 파기한다. 서비스 중단 등의 경우에는 바이오인식 시스템의 테스트, 검증 등에 활용된 바이오인식 정보를 파기하고 관련 개인정보를 파기 또는 비식별 처리 한다.

■ 바이오인식 정보를 활용한 인증 및 식별은 일반적으로 특징정보 비교를 통해 이루어지므로 바이오인식 원본정보에서 특징정보가 생성되면 원본정보의 수집·이용 목적은 달성된 것으로 볼 수 있다.

- 이에 따라, 원칙적으로 원본정보는 특징정보 생성 시, 지체 없이 복구 또는 재생되지 않도록 파기하여야 한다.
- 다만, 사업자의 필요에 의해 이용자 동의를 받아 원본정보를 이용하는 때에는 동의 받은 목적이 달성되거나, 보유·이용기간이 끝난 경우 지체 없이 원본정보를 파기하여야 한다.

■ 계약해지 등으로 바이오인식 서비스가 종료 되었을 경우에는 바이오인식 시스템의 테스트, 검증 단계 등에서 활용된 이용자의 바이오인식 정보를 안전한 방법으로 파기하여야 하며, 이와 연계된 개인 식별정보도 폐기 또는 비식별

처리 하도록 한다. 개인정보를 파기할 때에는 복구·재생되지 않도록 안전한 방법으로 파기하여야 한다.

V. 결 론

본 논문에서는 각 개인의 신체적, 생리적, 행동적 특성을 이용하는 바이오인식 시스템에 있어서 바이오인식 정보에 대한 보안 위협과 법률적 요구사항들을 살펴보았다. 바이오인식 정보는 유출되거나 오용되었을 때 정보주체의 프라이버시에 지속적인 영향을 미칠 수 있으므로 법률적으로도 민감정보에 해당하는 개인정보로 분류하여 보호하고 있다. 각 응용모델 별 취약점과 보안요구사항을 제시하였으며, 최종적으로 바이오인식 시스템의 개발이나 설계자가 지켜야할 수칙을 개념설정, 분석/설계, 개발, 테스트, 적용 단계별로 나누어 제시하였다. 바이오인식 정보는 안전한 사용이 담보된다면 원격 비대면 상황에서 가장 확실한 개인인증 수단으로 다양한 분야에서 적용될 수 있으리라 생각된다.

References

[1] "Information technology - Biometrics - Overview and application," ISO/IEC TR 24741, 2018.

[2] Sa Mun Kim, Dae Jong Lee, and Myung Geun Chun, "Infrared Gait Recognition using Wavelet Transform and Linear Discriminant Analysis," Journal of Korean Institute of Intelligent Systems, 294(6), pp. 622-627, Dec. 2014.

[3] Ju Hee Cho, Byeong Jun Cho, Dae Jong Lee, and Myung Geun Chun, "ECG based Personal Authentication using Principal Component Analysis," Transaction of the Korean Institute of Electrical Engineers P, 66P(4), pp. 258-262, Dec. 2017.

[4] Best Predictive Recommendations for Commercial Biometric Use, International Biometrics & Identification Association, 2014.

[5] Biometrics Privacy Guidelines, Biometrics Institute, 2019.

[6] Boo Geum Jung, Hun Yeong Kwon, Hea Sook Park, and Jong In Lim, "Biometrics Service Trends and Improvement of Bio Data Protection Law referring to GDPR," Journal of Korean Institute of Communications and Information Sciences, 43(1), pp. 201-208, Jan. 2018.

[7] Wencheng Yang, et al., "A cancelable biometric authentication system based on feature-adaptive random projection," Journal of Information Security and Applications, https://www.sciencedirect.com/science/article/abs/pii/S2214212620308504, May 2021.

[8] "Information security, cyber security and privacy protection - Biometric information protection," ISO/IEC FDIS 24745, 2021.

[9] "Information technology - Biometric presentation attack detection," ISO/IEC 30107, 2016.

[10] https://fidoalliance.org/specifications

[11] "Information technology - Security techniques - Privacy framework," KS X ISO/IEC 29100, 2011.

[12] Biometric Information Protection Guideline, Korea Communications Commission, 2017.

[13] Ethical principles for the biometrics, Biometrics Institute, 2019.

[14] Myung Geun Chun, "Biometric information protection and personal authentication using information splitting," International Symposium on Advanced Intelligent Systems (ISIS), Dec. 2019.

〈저자소개〉

송 창 규 (Chang-kyu Song) 정회원
1995년 2월: 충북대학교 전기공학과 학사
1997년 2월: 충북대학교 전기공학과 석사
2006년 2월: 충북대학교 전기공학과 박사
2006년~2010년: 충북대학교 충북정보기술 사업단 Post Doc.
〈관심분야〉 Biometrics, Recognition, Intelligent system

김 영 진 (Young-jin Kim) 정회원
1996년 2월: 연세대학교 영어영문학과 학사
2005년 2월: 서울대학교 행정대학원 석사
2016년 2월: George Washington Univ. MBA
2000년~현재: 금융결제원 금융결제연구소 팀장
2000년~현재: 금융정보(ISO TC68) 전문위원회 전문위원

전 명 근 (Myung-geun Chun) 종신회원
1987년: 부산대학교 전자공학과 학사
1989년: KAIST 전기 및 전자공학과 석사
1993년: KAIST 전기 및 전자공학과 박사
1996년: 삼성전자 자동화연구소 선임연구원
1996년~현재: 충북대학교 전자공학부 교수
2007년~현재: ISO/IEC SC27 정보보호 표준화 전문위원
2008년~현재: TTA PG505 전문위원
〈관심분야〉 지능시스템, 정보보호, 영상처리