ECG 파형으로 안전한 차량 제어를 위한 사용자 인증 시스템 제안

진선우*, 김성수**, 강정호***, 전문석*
*숭실대학교 컴퓨터학과
**한국정보화진흥원
***배화여자대학교 정보보호과
e-mail : *jinsunw@soongsil.ac.kr **cryptoauth@nia.or.kr
***kangsamm@baewha.ac.kr *mjun@ssu.ac.kr

Suggestion of User Authentication System for Safe Vehicle Control With ECG Waveform

Sun-Woo Jin*, Sung-Soo Kim**, Jeong-Ho Kang***, Moon-Seog Jun*
*Dept. of Computer Science, Soongsil University
**National Information Society Agency
***Dept. of Information Protection, BaeWha Women's University

요 약

자동차는 현대사회에서 보편화한 편리한 운송수단으로써 사람이 생활하는 어느 곳에서나 활용되고 있다. 최근 ICT 와 차량을 융합한 커넥티드 카는 운전자에 의해 모든 동작이 결정되는 특징을 가지고 있어 도난 및 오용되지 않게 적합한 사용자 인증이 필요하다. 운전자가 음주를 하게 되면 정상적인 차량 운행이 불가능하여 교통사고가 발생할 수 있다. 이를 방지하기 위해 운전자의 현재 상태를 파악하여 차량을 운전하는데 이상이 없는지를 파악하고 부적합할 경우 차량 운행을 제어할 수 있는 수단이 필요하다. 스마트키, 지문 인식 등 차량에 대한 사용자 인증의 방식이 존재하지만, 인증과 동시에 사용자의 현재 상태를 파악하는 방법은 없는 상황이다. 본 논문에서는 고유한 생체정보인 ECG 파형의 특징을 이용하여 사용자 인증과 동시에 운전자의 현 상태를 파악하는 안전한 차량 제어 시스템을 제안하고자 한다.

1. 서론

자동차는 운전자가 원하는 위치로 안전하고 편안하게 이동할 수 있도록 도와주는 운송수단으로써 일상생활에 필수사항처럼 되었다. 최신 정보통신기술과 차량이 결합한 커넥티드 카는 차량 외부의 교통시설 혹은 내부에 장착된 장치와 무선 통신을 할 수 있다. 운전자는 차량의 모든 동작을 결정할 수 있는 권한을 가지고 있어 올바른 차량 제어를 위해선 전한 사용자 인증 방법이 필요하다. 이런 차량의 특징으로 인하여 운전자가 현재 술에 취해 있거나, 스스로 제어되지 않는 급박한 상황이 되어 자동차를 안전하게 운전할 수 없다면 운전자, 동승자 그리고 보행자 모두에게 위험한 사고가 발생할 수 있다. 교통사고를 유발하는 음주운전을 방지하기 위한 음주시동잠금장치가 존재하지만, 자동차에 장착하기 위한 큰 비용과 시간을 소모해야 하는 단점이 존재한다. 차량에서 사용하는 인증방법으론 RFID 기반의 스마트키와 지문, 홍채, 얼굴 등 생체 정보를 활용한 인증 방법 등이 있지만, 탈취 혹은 복제로 인한 오용이 가능하다는 문제점을 가지고 있다. 안전한 차량운행을 위해 인증과 동시에 운전자의 현 상태를 간단하게 파악하는 방법이 존재하지 않고, 부가적인 장치를 차량에 장착하여야 하며, 장비에 대한 일련의 과정을 거쳐야 운전자의 상태가 파악되는 불편함을 지니고 있다. 이러한 문제점을 해결하고자 사람의 고유 정보이자, 운전자의 생리학적 변화 상태를 파악할 수 있는 ECG(Electrocardiography) 파형을 웨어러블 장치와 스마트폰을 이용하여 안전한 사용자 인증을 통한 차량 제어 시스템을 제안하고자 한다. 논문의 구성은 2 장에서 음주운전을 방지할 수 있는 장비에 대해 살펴보고 차량 제어를 위한 사용자 인증 방법과 ECG 파형에 관한 연구 동향에 살펴본다. 3 장 본론에서 제안 기법과 제안 기법에 대한 평가에 대해 살펴보고, 마지막으로 4 장에서 논문의 결론을 맺고자 한다.

2. 관련 연구

운전자가 자동차를 주행하는 도중 사고를 유발할 수 있는 음주운전을 사전에 방지하려는 방법에 관한 동향, 사용자 인증 방법 관련 연구 동향 그리고 ECG 파형에 대해 살펴본다.

2.1 음주운전 방지를 위한 연구동향

운전자가 차량을 안정적으로 제어할 수 없는 음주운전을 방지하기 위한 음주시동장금장치에 대한 연구동향을 살펴본다. 현재 차량에서 음주측정을 할 수 있는 장치는 3 가지의 검지 방식을 사용한다. 장치를 통해 자동차의 시동을 걸기 전에 운전자의 호흡 중 알코올 농도를 측정해 규정치를 넘는 경우엔 엔진을 작동시키지 못하도록 하는 장치이다[1]. 먼저 반도체 방식은 응답성이 우수하고 가격이 저렴하지만, 외부 환경적 요인에 따라 정확도가 떨어진다. 전기 화학식은 반도체 방식보다 정밀도가 높지만, 검사를 위해 주변 환경을 내장 히터로 조절해 응답성이 떨어진다. 마지막으로 비분산형 적외선식은 외부 환경적 요인에 영향을 받지 않고, 장기간 측정이 가능하지만, 장치의 특성상 차량에 적용하기 어려운 단점이 있다.

<표 1> 음주측정에 사용되는 주요 검지방식 및 특성

검지방식	주요특성
반도체식	- 흡착·촉매 반응에 의한 전기 전도도의 변화를 이용한 것 - 응답성이 우수하고 가격이 저렴함 - 알코올 이외의 성분과 온도, 습도 등 외부 요인의 영향을 받기 쉬워 정확도가 떨어짐
전기 화학식	- 전기 화학 반응에 의한 기전력의 변화를 이용한 것 - 알코올에 대한 선택성과 정밀도가 높음 - 외부 요인의 영향을 받지 않기 위해 히터를 내장하여 정확성을 보장하나 응답성이 떨어짐
비분산형 적외선식	- 알코올 증기 분자가 특정 파장의 적외선을 흡수하는 특성을 이용한 것 - 광학적 측정 방법이라 외부 요인에 영향을 받지 않고 장기간 안정된 측정이 가능 - 구조상 크기가 크고, 진동에 약해 차량에 적합하지 않음

2.2 차량 제어와 사용자 인증 관련 연구 동향

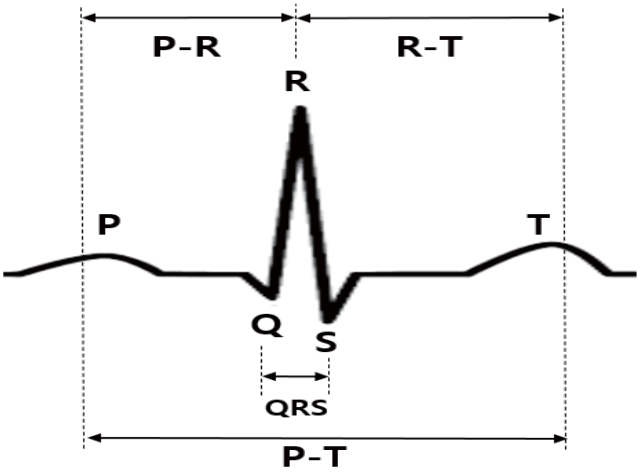
대부분의 사람이 사용하고 있는 스마트폰을 활용한 사용자 인증 기법에 관한 연구와 모바일 환경에서의 보안 기법에 관한 연구가 활발히 이루어지고 있다. 특히 스마트폰에서 생체 정보 인식이 가능한 센서와 기술이 대중화되면서 모바일 어플리케이션을 이용한 금융거래에서 간편한 사용자 인증으로는 FIDO 인증 프로토콜이 사용되고 있다. 모바일 환경에서 사용자 인증을 위해 지문, 홍채, 얼굴의 고유한 특성이 있는 생체 정보를 사용하고 있다[2]. FIDO 표준은 UAF(Universal Authentication Framework) 프로토콜과 U2F(Universal 2nd Factor) 프로토콜 2 가지를 제안한다. UAF 프로토콜은 사용자 디바이스에서 제공하는 인증 방법을 온라인 서비스와 연동해 인증하는 기술이다. U2F 프로토콜은 로그인 시 기존 패스워드를 사용하면서 다른 인증요소를 추가하여 안전한 인증이 가능하게 한다[3]. 최근 모바일 환경에 한정되었던 FIDO 프로토콜은 웹 브라우저 환경에서도 사용할 수 있으며 서버에서 정의한 자체 프로토콜을 사용할 수 있는 FIDO 2.0 이 발표되었다[4]. 현재 상용화되어 사용하고 있는 생체 정보는 사람마다 고유한 패턴을 생성할 수 있지만, 외부적 환경요인에 대한 인식률 저하, 인증 시 사용자의 거부감 발생 가능성, 생체 정보가 탈취되어 오용되는 문제가 발생한다. 지문, 홍채 얼굴과 같은 생체 정보는 차량에서 사용되고 있다. 지문의 경우 도어 개폐와 엔진을 작동시키는 동작을 할 때 사용되고 있다. 홍채와 얼굴은 차량 내부에 탑재된 인공지능과 카메라로 운전자의 현 상태를 파악하여 졸음운전 혹은 전방미주시 등의 교통사고를 유발할 수 있는 상황을 감지하여 진동, 경고음 등으로 안전한 차량 운행 환경을 마련한다.

<표 2> 기존 생체 정보의 특징과 단점

생체 정보	특징	단점
지문	지문 융기의 분기점, 끝점 등의 특징 정보를 이용	- 땀이나 물기가 존재하는 경우에 인식률이 저조함 - 지문이 닳아 없어진 사람의 경우 이용이 불가능
홍채	안구 배면에 위치한 모세혈관의 특징 정보를 이용	- 레이저를 이용한 기술로서 사용 거부감이 존재 - 백내장, 녹내장 같은 질병이 있는 경우 이용이 불가능
얼굴	얼굴의 열상 방식과 2 차원/3 차원의 얼굴 영상 방식을 통한 얼굴에 존재하는 특징 정보를 이용	- 대상자의 표정이나 얼굴의 상황에 영향을 받아 인식률이 저조함 - 주위의 조명에 영향을 많이 받아 인식률이 저조함

2.3 ECG 파형을 활용한 사용자 인증 연구동향

ECG(Electrocardiography) 파형은 정해진 시간 동안 심장의 전기적 활동을 해석하는 것으로, 이는 주기적으로 전기를 생성하여 심장의 수축을 유도함으로써 심장 박동을 조절하는 동방결절에서 생성된다. ECG 파형은 전압의 크기를 기준으로 P, Q, R, S, T 파형이 연속적으로 생성되며, 이런 파형은 사람마다 고유의 특징을 가진다[5].



(그림 1) 연속적인 ECG 그래프

심장은 1 분에 70~100 번 주기로 동일한 연속적인

파형을 형성한다. 일정 시간 동안 사람의 QRS 파형의 X, Y 패턴 정보를 측정하면 사용자별 고유한 값을 측정할 수 있다[6]. ECG 파형은 음주, 수면, 심장질환 등 사람의 현 상태가 정상적이지 아닌 경우 파형의 폭과 넓이가 변화할 수 있다[7]. 이러한 특징을 가진 ECG 파형의 고유한 값을 이용하여 기존 생체 정보로 사용중인 지문, 홍채, 얼굴 등의 취약점을 보완한 새로운 생체 정보를 사용하여 더욱 안전하고 정확한 사용자 인증과 음주 시 변화한 ECG 파형을 통한 차량 제어 시스템을 제안한다.

3. 본론

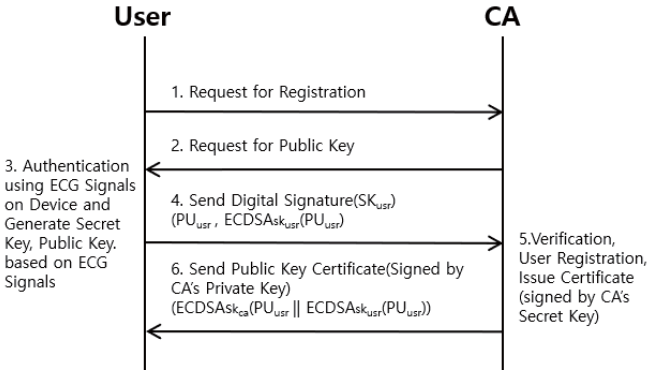
앞서 설명한 연구동향의 단점을 ECG 파형을 이용하여 사용자 인증과 동시에 운전자의 현 상태를 파악하여 안전한 차량 제어를 위한 사용자 인증 시스템 기법과 그에 대한 평가를 설명한다.

3.1 제안 기법

제안하는 기법은 사용자 인증을 위한 사용자 등록과정과 사용자 인증과 동시에 사용자의 현재 상태를 파악하여 보다 안전한 차량 제어를 할 수 있는 방법 2 가지로 나뉜다. 그리고 사용자의 현 상태에 따라 변할 수 있는 ECG 파형의 특성을 이용하여 주행중인 차량에 대한 차량 제어 기법 또한 제안하고자 한다.

3.1.1 사용자 등록과정

ECG 파형을 측정할 수 있는 웨어러블 장비는 블루투스 연결을 통하여 사용자의 스마트폰으로 측정한 데이터를 전송한다. 웨어러블 장비에서 전송을 받은 데이터는 스마트폰 어플리케이션에서 ECG 파형의 X, Y 패턴 정보를 추출할 수 있으며 사용자 인증을 위해 사용자의 평상시 X, Y 패턴 정보를 저장한다. 사용자 등록 과정은 ECG 인증 장치인 스마트폰과 신뢰할 수 있는 인증기관(Certification Authority, CA)과 통신으로 이루어지며 해당 과정은 아래 그림 2 와 같다.

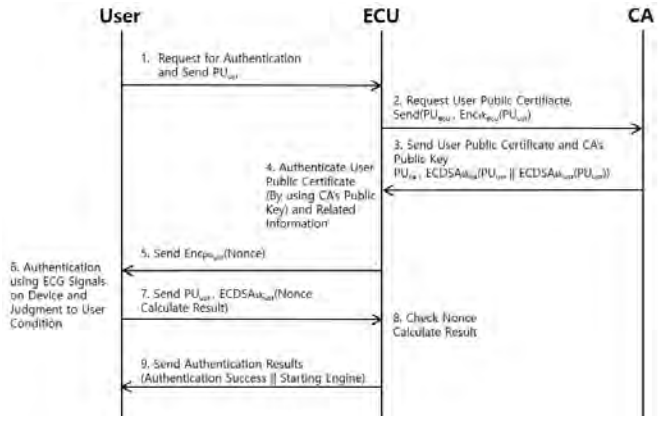


(그림 2) 제안 기법의 사용자 등록 과정

먼저, 사용자는 인증기관(CA)에게 사용자 등록을 요청하는 메시지를 전송한다. 사용자에게 등록요청을 받은 인증기관은 사용자의 공개키(PU_{usr})를 요청한다. 인증기관의 요청을 받은 사용자는 웨어러블 장치와 스마트폰을 통한 사용자 인증을 하여 자신의 개인키(SK_{usr})와 공개키를 생성한 다음 사용자의 공개키를 개인키 기반으로 전자 서명한 결과와 자신의 공개키를 인증기관에게 보낸다. 인증기관은 사용자의 공개키 정보와 전자 서명된 데이터에 대해 검증을 한다. 검증이 완료되면 인증기관의 개인키(SK_{ca})로 전자 서명한 데이터를 보냄으로써 등록과정이 완료된다.

3.1.2 사용자 인증과정

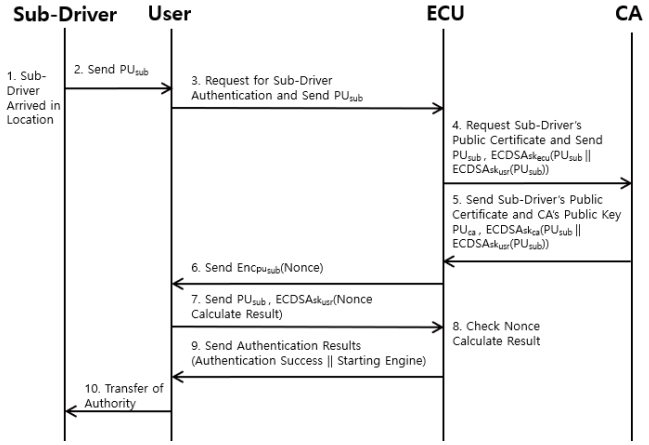
사용자 등록과정을 통해 사용자의 정보를 등록한 이후, 사용자 인증과 동시에 사용자의 현재 상태를 파악해 엔진의 작동 여부를 결정하는 과정 설명한다. 차량 제어권한을 얻고 싶은 사용자와 자동차의 장치들을 제어하는 ECU(Electronic Control Unit)간의 통신과 ECU 와 인증기관 간의 통신으로 구성된다. 사용자 인증을 하기 위해선 자신의 차량 ECU 에게 인증을 요청하는 메시지와 사용자의 공개키 정보를 전송하면, ECU 는 사용자의 공개키 정보에 대해 자신의 개인키(SK_{ecu})로 암호화한 뒤, 자신의 공개키(PU_{ecu})와 함께 인증기관에게 사용자 공개키 인증서 정보를 요청한다. 요청을 받은 인증기관은 사용자 공개키 정보를 통해 사용자의 인증서와 인증기관의 공개키를 ECU 에게 전송한다. ECU 는 인증기관에게 받은 인증서를 기반으로 사용자를 검증한 뒤, 사용자 공개키를 사용하여 Nonce 를 암호화하여 전송한다. ECU 로부터 암호문을 받은 사용자는 자신의 현 ECG 파형을 측정하여 스마트폰으로 인증을 시도한다. 만약 음주로 인하여 현 ECG 파형이 평소보다 좁은 폭으로 빠르게 생성되어 인증을 실패하게 된다면 스마트폰의 어플리케이션이 실행되어 음주 여부와 대리기사 요청 여부를 묻는다. 인증에 성공하면 Nonce 를 처리한다, 처리된 결과를 사용자의 개인키로 전자 서명한 후, 자신의 공개키 정보를 ECU 측에 전송한다. ECU 는 Nonce 의 처리 결과를 확인한 뒤, 인증 결과를 사용자에게 전송한다. 인증 결과를 받은 사용자는 차량 제어 권한을 얻게 되어 시동을 걸 수 있게 된다.



(그림 3) 제안 기법의 사용자 인증 과정

3.1.3 제 3 자에게 권한양도 과정

앞 절에서 음주로 사용자 인증을 실패한 경우 어플리케이션을 통해 호출된 대리기사(제 3 자)에게 사용자 권한양도와 인증 과정을 설명한다. 어플리케이션을 통해 호출된 대리기사가 차량에 도착하면 인증기관에 등록된 대리기사의 공개키(PU_{sub})를 사용자에게 전달한다. 인증에 실패한 사용자는 대리기사의 공개키를 받아 ECU 에게 대리기사 인증요청과 공개키를 전송한다. 요청을 받은 ECU 는 대리기사의 공개키 정보에 대해 ECU 의 개인키로 암호화하여 자신의 공개키와 함께 CA 에게 대리기사의 공개키 인증서를 요청한다. 요청을 받은 CA 는 대리기사의 공개키 정보를 통해 대리기사의 인증서와 CA 의 공개키를 ECU 에게 전송한다. ECU 는 대리기사의 공개키를 사용하여 Nonce 를 암호화하여 전송한다. 사용자는 Nonce 처리 결과를 사용자의 개인키로 전자 서명하여 대리기사의 공개키 정보를 ECU 측에 전송한다. ECU 는 Nonce 처리 결과를 확인하고, 인증 결과를 사용자에게 전송한다. 인증 결과를 받은 사용자는 대리기사에게 차량 제어권한을 양도함으로써 인증과정이 마무리가 된다. ECG 파형을 측정할 수 있는 웨어러블 장치와 인증과정을 처리할 수 있는 스마트폰을 이용한 제안 기법을 사용한다면 안전한 차량 제어를 위한 사용자 인증 과정과 동시에 음주운전을 방지하고, 제 3 자에게 차량 제어 권한을 양도할 수 있다.



(그림 3) 제안 기법의 제 3 자에게 권한양도 과정

3.2 제안 기법 평가

제안 기법을 평가하기 위해 기존에 사용되고 있는 RFID 방식을 이용한 스마트 키, 생체 정보(지문, 홍채, 얼굴)를 이용한 FIDO 인증 방식과 제안 기법을 비교 분석하였다. 보편적으로 사용하고 있는 스마트키의 장점은 차량 근처에 있으면 RFID 를 통해 간단하게 차량에 대한 사용자 인증과정이 이루어진다. 단점은 스마트키가 분실 혹은 탈취되면 복제할 수 있으며, 누구나 스마트키를 가지고 차량 근처에 있으면 차량을 제어할 수 있는 단점이 있다. 모바일 환경에서 지문, 홍채, 얼굴 등의 생체 정보를 사용하는 기존 FIDO 인증 방식은 스마트키보다 복제와 탈취가 어렵고 분실의 위험이 적지만, 복제로 인한 비인가자의 인증 사고가 매년 발생하고 있다. 기존에 사용 중인 생체 정보는 정적 정보로서 탈취될 경우 변경이 불가능하고, 제 3 자에 대한 사용 연계성을 제공하지 않는 단점이 존재한다. 이런 단점을 해결할 수 있는 제안 기법은 고유성을 가진 동적 생체 정보인 ECG 파형을 사용하여 복제 및 탈취가 기존의 생체 정보보다 어렵다. 제 3 자에 대한 사용 연계성을 지니고 있어, FIDO 인증 방식의 단점을 해결하고, 사용자 인증과 사용자의 현 상태를 파악할 수 있는 장점을 지닌다.

<표 3> 차량 제어를 위한 기존 사용자 인증 수단과 제안 기법 비교

	스마트키	FIDO 인증 방식	제안 기법
권한양도	O	X	O
부가 APP 사용	X	O	O
동적 정보 여부	X	X	O
사용자 상태 확인	X	X	O

4. 결론

차량의 사용자 인증과 동시에 운전자의 현 상태를 측정하여 안전한 차량 제어 기법을 제안하였다. 제안 기법을 통해 차량 제어를 위한 사용자 인증을 하나의 인증 수단만 사용하여 차량의 도난 및 오용을 방지할 수 있으며, 교통사고 발생의 주 원인인 음주운전에 대한 방지책을 마련했다. ECG 파형을 측정하고, 활용하기 위한 웨어러블 장치는 아직 많은 연구가 필요하지만, 기존에 사용중인 생체 정보보다 활용성이 무궁무진하다. 결론적으로, 기존에 사용되는 생체 정보보다 안전한 사용자 인증에 사용될 수 있음을 제안한다.

참고문헌

[1] 교통과학연구원. (2017) “음주시동장금장치 기술 동향”

[2] 조상래, 최대선, 진승헌, 이형효. (2015) “패스워드 없는 인증기술-FIDO”, ETRI 소프트웨어 기술동향 특집

[3] 조상래, 조영섭, 김수형. (2016) “FIDO 2.0 범용인증 기술 소개” 정보보호학회지, 26(2), 14-19.

[4] 금융보안원 (2017) “FIDO2.0 구조적 특징 소개”

[5] 조주희, 조병준, 이대종, 전명근. (2017). “주성분 분석기법을 이용한 심전도 기반 개인인증” 전기학회논문지 P, 66P(4), 258-262.

[6] 이재진, 한하영, 정하영, 곽근창. (2018) “심전도를 이용한 PCA 와 LDA 의 개인 식별 성능 비교” Proceedings of KIIT Summer Conference, 519-520.

[7] 문광수, 황경인, 최은주,·오세진. (2015) “심전도(LF/HF)를 활용한 졸음운전 예방 연구” Journal of the Korean Society of Safety, Vol. 30, No. 2, pp. 56-62