

웨어러블 디바이스를 활용한 ECG 인증 시스템 구현 및 평가

허재욱, 진선우, 전문석*
송실대학교 컴퓨터학과

Implementation and Evaluation of ECG Authentication System Using Wearable Device

Jae-Wook Heo, Sun-Woo Jin, Moon-Seog Jun*
Dept. of Computer Science and Engineering, Soongsil University

요약 IoT 기반의 스마트홈, 핀테크 등의 모바일 기술이 발달하면서 스마트 디바이스를 이용한 사용자 인증이 일상생활에서 널리 사용되고 있다. 이에 따라 기존의 비밀번호와 같은 지식 기반의 인증 방법에서 스마트 디바이스를 이용한 존재 기반의 생체인증이 새로운 주류가 되었고, 맥파, 지문, 얼굴, 홍채 등 다양한 생체인증 중에 신체적 특성상 위변조 가능성이 낮고 고유한 특징으로 개인 식별성이 높은 ECG(Electrocardiogram, 이하 ECG)를 이용한 생체인증이 헬스케어 및 핀테크와 맞물려 높은 관심을 받고 있다. 본 연구에서는 기존의 고가이면서 부피가 커 휴대가 불가능한 ECG 측정 디바이스가 아닌 소형화된 웨어러블 디바이스를 이용하여 손쉽게 사용자의 ECG 파형을 측정해 사용자 인증을 할 수 있는 ECG 인증 시스템을 구현하였다. 구현된 ECG 인증 시스템은 PQRST 고유 값 식별을 통해 ECG 특징점을 판별하고 이를 이용한 제안된 인증 프로토콜로 사용자 인증이 가능하였다. 최종적으로 성인 남성 다수를 통한 측정 평가를 통해 안정적인 정지 상태에서는 1.73%의 비교적 낮은 타인수락률과 4.14%의 본인거부율을 보였고 움직임이 있는 상태에서는 13.72%의 타인수락률과 21.68%의 높은 본인거부율을 보였다. 활동으로 인해 심박수가 상승한 정지 상태에서는 10.48%의 타인수락률과 11.21%의 본인거부율을 보였다.

Abstract As mobile technologies such as Internet of Things (IoT)-based smart homes and financial technologies (FinTech) are developed, authentication by smart devices is used everywhere. As a result, presence-based biometric authentication using smart devices has become a new mainstream in knowledge-based authentication methods like the existing passwords. The electrocardiogram (ECG) is less prone to forgery, and high-level personal identification is its unique feature from among various biometric authentication methods, such as the pulse, fingerprints, the face, and the iris. Biometric authentication using an ECG is receiving a great deal of attention due to its uses in healthcare and FinTech. In this study, we implemented an ECG authentication system that allows users to easily measure and authenticate their ECG waveforms using a miniaturized wearable device, rather than a large and expensive measurement device. The implemented ECG authentication system identifies ECG features through P-Q-R-S-T feature point identification, and was user-certified under the proposed authentication protocols. Finally, assessment of measurements in a majority of adult males showed a relatively low false acceptance rate of 1.73%, and a low false rejection rate of 4.14%, in a stable normal state. In a high-activity state, the false acceptance rate was 13.72%, and the false rejection rate was 21.68%. In a high-heart rate state, the false acceptance rate was 10.48%, and the false rejection rate was 11.21%.

Keywords : Electrocardiogram, Biometric Authentication, Wearable Device, Bio-Signals, Personal Authentication

*Corresponding Author : Moon-Seog Jun(Soongsil University)

email: mjun@ssu.ac.kr

Received July 11, 2019

Accepted October 4, 2019

Revised August 12, 2019

Published October 31, 2019

1. 서론

새로운 스마트 부품의 개발과 IoT 기술의 발전으로 인해 기존에 없던 다양한 스마트 디바이스들이 개발되었고, 모바일 결제 서비스와 같은 다양한 서비스 플랫폼에서 널리 사용되고 있다. 이러한 성장에 힘입어 보안에서 중요한 부분을 차지하고 있는 사용자 인증 분야도 기존의 비밀번호와 같은 지식 기반 인증에서 스마트폰과 같은 디바이스를 이용한 존재 기반의 생체인증이 대세가 되고 있다. 그러나 대표적으로 생체인증에 사용되는 지문, 얼굴, 등은 최근 발생한 위조지문 사례[1]와 같이 다양한 위변조 위협에 노출되어 그 위험성이 높아지고 있다. 따라서 본 연구에서는 기존의 신체인증 위변조 가능성을 낮추기 위해 신체적 특성상 위변조 가능성이 매우 적으며 고유한 사용자 식별성이 높고[2] 또한 피트니스, 헬스케어와 같이 활용이 가능한 ECG 인증을 구현하였다. 구현된 사용자 인증은 웨어러블 디바이스를 통해 사용자에게 부착하여 ECG 파형을 얻고, 이를 안드로이드 스마트폰에서 이용해 사용자 인증을 진행하는 방식으로 진행된다.

2. 관련 연구

2.1 생체인증

생체인증 기술은 사용자들에게 높은 편의성을 제공하기 위해서 사용자의 신원을 증명할 수 있는 인증을 온라인상에서 빠르게 진행할 수 있는 기술이다. 생체인증 방식은 홍채, 지문, 얼굴 등 다양한 종류의 고유 생체 정보를 기반으로 하며 카카오페이, 삼성페이, 알리페이 등 간편한 결제 방식을 제공하는 모바일 금융 서비스에서 활발하게 이용되고 있다. 생체인증에서 단순하고 가장 많이 사용되는 지문 인증 기술은 지문 융기의 분기점, 끝점 등으로 구성되는 고유 특징점의 속성과 위치를 추출해서 저장, 비교하는 알고리즘을 가지고 있다. 그러나 최근 실리콘을 이용한 지문 복제와 같은 위변조 문제가 발생하고 있는 만큼 주의가 필요하다. 얼굴 인증 기술은 비접촉으로 가장 자연스럽게 인증이 가능하다. 하지만 얼굴의 특성상 시간이 지나면 변화하거나 다른 외부적인 요인이 고유성에 크게 작용하게 된다. 홍채의 경우 개인마다 고유한 홍채 패턴의 형태를 가져 정확성이 높으며 변화가 적어 높은 보안성을 가지고 있다. 그러나 높은 비용과 거부감이 존재한다. 정맥 인증의 경우 손등의 피부로부터

정맥 패턴을 추출해 인증하는 방식으로 고유한 혈관 형태에 따라 높은 정확도를 가진다. 그러나 하드웨어 구성이 복잡하고 소형화가 어려워 매우 높은 비용을 가진다 [3].

Table 1. Pros and cons of biometric authentication

Biometric authentication	Advantages	Disadvantages
Fingerprint	Low cost, High stability	Fingerprint damage, Possibility of counterfeiting
Face	Low cost, fast, Simplicity	Environmental impact
Iris	Non-forgery	High cost
Vein	Non-forgery	Difficult to extract

2.2 ECG

ECG는 심장의 전압, 전류와 같은 전기적 활동을 나타내는 생체적 신호를 말한다. 피부에 부착된 전극과 신체 외부의 디바이스에 의해 기록되는 ECG는 심장 질환이나 의료적 진단 및 모니터링에 널리 사용되고 있다. ECG는 개인별로 고유한 특징을 가지고 있어 ECG를 이용해서 생체 인증이 가능하다는 장점이 있다. 또한 심장의 전기적 생체 신호가 가지는 특성상 위변조가 매우 어렵다는 특징을 가진다[2].

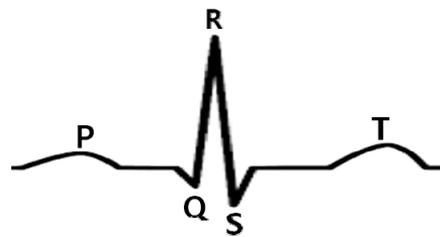


Fig. 1. PQRST according to ECG waveform

3. ECG 인증

3.1 ECG 특징점 추출

본 연구에서 구현된 ECG 기반의 생체 인증은 다음과 같은 ECG 특징점 추출을 기반으로 한다.

13000개의 전기적 생체신호 사이클을 기반으로 웨어러블 디바이스에서 125Hz로 전송된 특정 Byte의 16진수 Raw 데이터를 500 ~ 1000ms 간격으로 지속 수신한

다. 수신한 Raw 데이터의 수치 간격과 변화를 이용해 Fig. 2와 같이 각 PQRST의 고유 파라미터 값을 탐색한다. 기본적으로 한 사이클의 Raw 데이터에서 가장 큰 값이 R값이 되고 이를 기준으로 특정 간격 사이에 들어오는 이전 값이 Q값, 이후의 값이 S값이 된다.

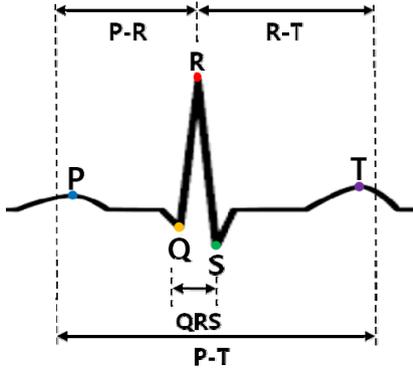


Fig. 2. PQRST feature point search

최종적으로 추출한 PQRST 파라미터 값을 특정하고 R-Peak을 기준으로 지속해서 측정되는 PQRST 고유 값의 평균을 바탕으로 해 사용자를 식별하게 된다. 이는 시간인 X축과 전기적 생체신호인 Y축으로 나누어 Fig. 3과 같이 표현된다.

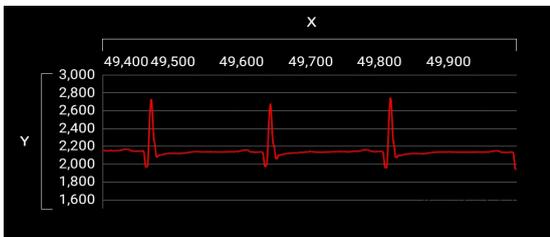


Fig. 3. ECG feature points along the X and Y axes

3.2 ECG 인증 프로토콜

다음과 같이 제안하는 인증 프로토콜을 이용해 ECG 파형을 기반으로 사용자가 인증하게 된다.

먼저 ECG 파형에서 추출된 특징점을 이용해 사용자를 신뢰받는 제3자에 등록하는 과정을 Fig. 4와 같이 진행한다. 등록 과정은 사용자와 CA(Certification Authority, 이하 CA)와의 통신으로 이루어진다.

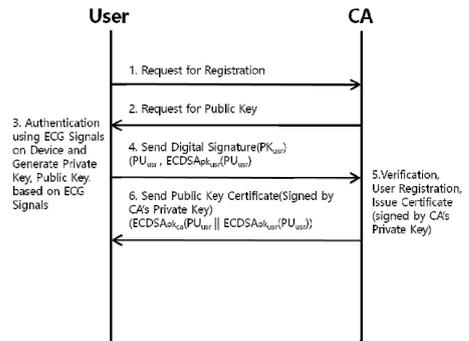


Fig. 4. User's public key registration protocol

Fig. 4에서 사용자는 CA에 사용자 등록을 요청하고 등록요청을 받은 CA는 사용자의 공개키인 PU_{usr} 를 요청한다. 인증기관의 요청을 받은 사용자는 개인의 ECG 특징점을 이용해 개인키인 SK_{usr} 와 공개키를 생성하고, 사용자의 공개키를 자신의 개인키로 전자서명한 결과와 공개키를 CA에 전송한다. CA는 전자서명으로 공개키의 주체를 검증하고 완료되면 CA의 개인키로 전자서명한 등록완료 데이터를 전송한다.

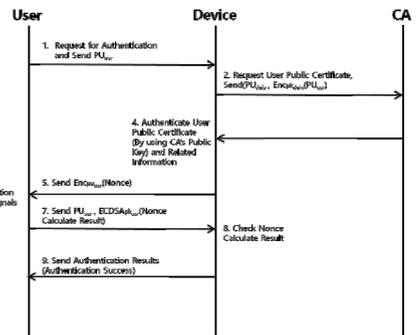


Fig. 5. ECG authentication protocol

Fig. 5에서 정보등록이 완료된 이후에 사용자가 인증을 요청하게 되면 요청 메시지와 공개키를 전송한다. 디바이스는 사용자의 공개키에 대해 자신의 개인키인 SK_{dev} 로 암호화하여 자신의 공개키인 PU_{dev} 와 함께 CA에 사용자 공개키 인증서를 요청하게 된다. CA는 사용자 공개키 정보를 통해 사용자 인증서와 자신의 공개키를 전송한다. 디바이스는 CA에게 받은 인증서 기반으로 사용자를 검증한 뒤, 사용자의 공개키를 사용해 Nonce값을 암호화해 전송하게 된다. 인증을 요청한 사용자는 Nonce값을 계산하여 결과값과 사용자의 PU_{usr} 와 함께 디바이스에 전송하게 된다. 이후 디바이스에서 이 Nonce값이 받아 들여지게 되면 인증이 완료되었다는 결과를 수신한다[4].

3.3 ECG 인증 시스템 구현

본 연구에서는 대중적으로 사용되는 Android OS 기반의 Application으로 ECG 인증 시스템을 구현하였다. ECG 수신 웨어러블 디바이스는 Fig. 6의 Maxim integrated 사의 고해상도 데이터 컨버터를 포함한 Maxim Integrated MAX30003 Biopotential Analog Front-End를 사용하는 MAX-ECG-MONITOR를 이용하였다. MAX-ECG-MONITOR는 2개의 전극 패드를 이용해 사용자의 상체에 부착하여 사용자의 ECG 파형을 효과적으로 얻을 수 있다.



Fig. 6. Monitoring electrode and ECG measurement device

Fig. 7에서 작은 크기의 데이터 전송 단위와 저전력을 제공하는 블루투스 4.0 + LE 통신을 이용해 웨어러블 디바이스와 스마트폰이 서로 연결되어 통신하게 된다.

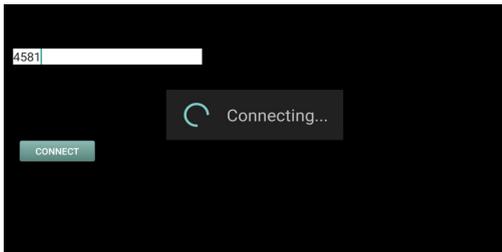


Fig. 7. Bluetooth communication process between mobile device and ECG wearable device

연결이 완료되면 사용자의 고유 ECG 파형이 기록되고 ECG 고유 특징점을 추출해 개인키를 생성 후 로컬에 저장하게 된다. 본 시스템에서는 Fig. 8과 같이 기본 120sec을 기준으로 특징점을 추출 저장해 인증을 진행하였다.

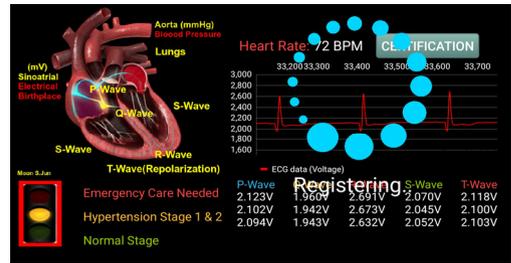


Fig. 8. User's ECG feature point registration process

사용자 인증 시 사용자의 고유한 ECG 데이터를 기반으로 하는 인증 프로토콜을 Fig. 9와 같이 진행하게 된다.

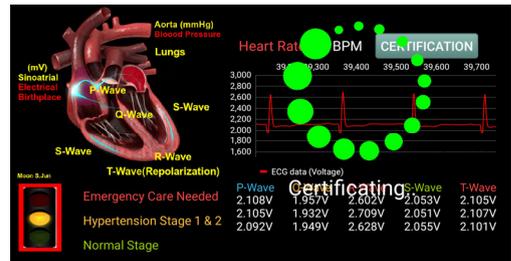


Fig. 9. User Authentication Process

등록된 사용자가 일치할 경우, ECG 특징점이 오차범위 내에서 동일하여 생성된 SK_{usr}가 같아 인증 프로토콜을 거쳐 사용자를 인증하게 되면 Fig. 10과 같이 인증이 성공하게 된다.

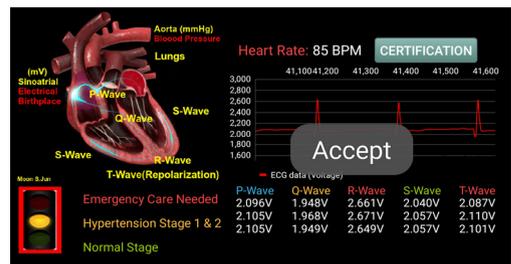


Fig. 10. User authentication successful

등록된 사용자와 다른 사용자가 인증할 경우, ECG 특징점이 달라지기 때문에 생성된 SK_{usr}와 상이하게 된다. 이의 경우 인증 프로토콜에 의해 Fig. 11과 같이 최종적으로 인증이 거부되고 등록된 사용자와 다른 사용자를 인증을 통해 식별할 수 있다.

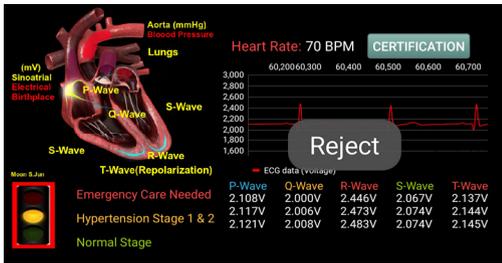


Fig. 11. User authentication failed

4. 인증 시스템 평가

본 연구에서 구현한 ECG 인증 시스템을 평가하기 위해 만 20세에서 만 35세 사이의 건강한 성인 남성 20명을 대상으로 FAR(False Acceptance Rate, 이하 FAR)과 FRR(False Rejection Rate, 이하 FRR)의 측정을 진행하였다. ECG 인증의 특성상 움직임에 따라 다른 인증 결과를 보이므로 정상 심박수의 안정적인 정지 상태, 신체 일부를 30% 이상 움직이는 다수의 활동이 있는 상태, 활동으로 인해 심박수가 120 bpm 가량 증가했으나 측정 시 움직임이 없는 정지 상태, 총 3가지의 경우로 구분해 진행하였고 측정된 값은 Fig. 12, 13에서 그래프로 표현하였다.

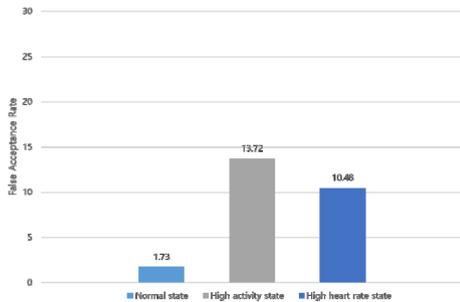


Fig. 12. False Acceptance Rate

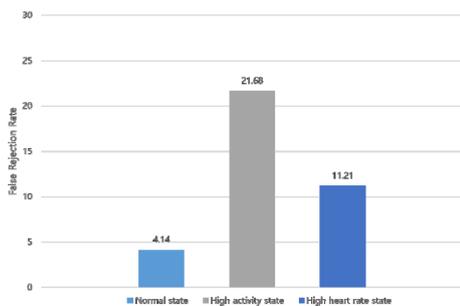


Fig. 13. False Rejection Rate

측정 결과, FAR의 경우 안정적인 정지 상태에서는 1.73%의 FAR을 보여 비교적 낮은 타인수락률을 보였으나 움직임이 있는 상태에서는 13.72%의 FAR로 높은 타인수락률을 보였다. 활동으로 인해 심박수가 120 bpm 가량 올라갔으나 가만히 정지된 상태에서는 비교적 덜 높은 10.48%의 타인수락률을 보였다.

FRR의 경우 안정적인 정지 상태에서는 4.14%의 낮은 본인거부율을 보였으나 움직임이 많은 상태에서는 21.68%의 높은 본인거부율을 보였다. 심박수가 올라간 이후에 정지 상태에선 움직임이 많은 상태보다 비교적 낮은 11.21%를 보였다.

본 연구에서 구현한 ECG 인증 시스템은 FAR과 FRR이 전체적으로 흉채, 지문, 얼굴 등 다른 생체인증 시스템보다 비교적 높았다[5]. 또한 ECG 인증 기술의 고유한 특성상 과도한 움직임이 있을 시 ECG 파형이 급격하게 변경되어 사용자 인증이 어려움을 보여주었다. 이는 ECG 특징점을 추출하는 알고리즘의 고도화로 더 낮은 FAR과 FRR 측정 결과가 필요하며, ECG 측정 디바이스의 부착 후 움직임에 따라 달라지는 웨어러블 디바이스의 ECG 전기적 신호를 개선하는 방안이 필요함을 보여주고 있다.

5. 결론

심전도 인증은 위변조가 매우 어렵다는 장점이 있지만, 기존에 높은 비용과 디바이스의 크기 제약으로 인해 범용적으로 사용되지 못하였다. 웨어러블 디바이스 시장의 발달[6]로 인해 다양한 피트니스, 헬스케어 웨어러블 디바이스가 주류가 된 지금에는 이러한 디바이스를 이용해 쉽게 ECG 파형을 얻을 수가 있다. 본 연구에선 ECG 파형을 측정 가능한 웨어러블 디바이스를 이용해 기존의 생체인증보다 한 단계 더 나아가 보다 많은 장점이 있는 심전도 인증을 구현하였다. 구현된 ECG 인증 시스템은 각 사용자의 PQRST 고유 값을 식별해 사용자를 효과적으로 인증하고, 부가적으로 ECG 파형과 하드웨어적으로 측정이 가능한 심박수, 체온 등의 측정으로 헬스케어 디바이스로의 역할도 제공이 가능한 것을 알 수 있었다.

향후 연구에서는 심박수, 체온 등의 부가적 데이터를 적극적으로 활용하여 헬스케어 디바이스의 역할 향상과 심박수, 운동량의 수치를 이용해 인증의 정확성을 향상시키는 방향으로 나아갈 것이다. 또한, 심전도 인증의 특성상 과도한 움직임이 있을 시 인증이 어려운 문제를 극복해 나가는 것이 추가 연구 과제이다.

References

- [1] The Guardian, <https://www.theguardian.com/technology/2018/nov/15/fake-fingerprints-can-imitate-real-fingerprints-in-biometric-systems-research> (accessed May. 15. 2019)
- [2] Ji-Hoon Kim, Kwang-seok Park, TTA Journal, Personal authentication using bio-signals Technology and DB construction, Vol.165 Special Report, Korea, May. 2016.
- [3] Ki-Young Moon, TTA Journal, Biometrics Technology Status and Prospects, Special Report, No.98, Korea, 2015.
- [4] Sun-Woo Jin, Sung-Soo Kim, Moon-Seog Jun, "Suggestion of User Authentication System for Safe Vehicle Control With ECG Waveform", *The KIPS Fall Conference 2018 on Korea Information Processing Society*, Vol.25, No.2 pp.227-230, November. 2018.
- [5] Byungchul Cho, Jong-man Park, "Technology Review on Multimodal Biometric Authentication", *The Journal of Korean Institute of Communications and Information Sciences*, Vol.40, No.1 pp132-141, January. 2015. DOI: <https://doi.org/10.7840/kics.2015.40.1.132>
- [6] Jin-Suk Hwang, In-Soon Jang, Ki-Su Jeong, "Wearable Technology Trend and Countermeasures against Cyber Attack" *The Journal of Korean Institute of Communications and Information Sciences*, Vol.44, No.4, pp765-773, April. 2019. DOI: <https://doi.org/10.7840/kics.2019.44.4.765>

허 재 욱(Jae-Wook Heo)

[준(학생)회원]



- 2017년 8월 : 국가평생교육진흥원 컴퓨터공학 (공학사)
- 2018년 3월 ~ 현재 : 송실대학교 컴퓨터학과 (석사과정)

<관심분야>

정보보호, 블록체인, 인공지능

진 선 우(Sun-Woo Jin)

[준(학생)회원]



- 2016년 8월 : 국가평생교육진흥원 컴퓨터공학 (공학사)
- 2018년 3월 ~ 현재 : 송실대학교 컴퓨터학과 (석사과정)

<관심분야>

ISMS, 개인정보보호, 정보시스템관리

전 문 석(Moon-Seog Jun)

[정회원]



- 1981년 2월 : 송실대학교 전자계산학과 (공학사)
- 1986년 2월 : University of Maryland Computer Science (공학석사)
- 1989년 2월 : University of Maryland Computer Science (공학박사)

- 1986년 9월 ~ 1989년 12월 : University of Mary 강사
- 1989년 3월 ~ 7월 : Morgan State University 조교수
- 1989년 9월 ~ 1991년 2월 : NMSU, PSL 연구소 책임연구원
- 1991년 3월 ~ 현재 : 송실대학교 정교수

<관심분야>

정보보호, 네트워크 보안, 전자여권, 암호학