FSR Array 마우스 패드를 이용한 사용자 인증 시스템

권승호*, 김태연*, 서승현*
한양대학교 ERICA 전자공학부
rnjs9232@hanyang.ac.kr, kty24898@hanyang.ac.kr

User Authentication System using FSR Array Mouse Pad

Seung-Ho Gwon*, Tae-Yeon Kim*, Seung-Hyun Seo*
*Division of Electrical Engineering, Hanyang University ERICA Campus

요 약

현재 PC 환경에 대한 보안시스템은 PIN 번호 인증 방식과 지문, 홍채와 같은 생체정보 인증방식에 머물러 있다. 하지만 취약한 PIN 번호는 도용이 쉽고, 생체정보는 누출되었을 경우 갱신이 불가능하다는 단점을 가지고 있어 이를 악용한 해킹 사례가 발생하고 있다. 기존 인증방식의 문제점을 개선하기 위해 최근, 개인의 행동습관을 통해 사용자를 인증하는 '행위적 특징 기반 인증기술'이 주목 받고 있다. 본 논문에서는 사용자마다 마우스 사용습관이 다르다는 특성에 기반한 PC 사용자 인증 방식을 제안한다. 인증 성공률을 높이기 위하여 Mouse dynamics 방식에 압력의 분포, 모양과 같은 새로운 특징적 요소를 추가한다. 또한, 마우스 사용 시 손의 모양, 압력의 분포 등을 수집하여 특징점을 추출할 수 있도록 FSR Array로 마우스패드를 구현하여 새로운 PC 인증 시스템의 프로토 타입을 구현하였다.

1. 서론

PC, 스마트폰과 같이 다량의 개인정보를 저장하고 있는 전자기기들이 늘어나면서 자연스럽게 개인정보에 대한 보안의 중요도가 증가하고 있다. 스마트폰의 경우 PIN 번호를 이용한 인증방식부터 홍채, 지문과 같은 보다 높은 안전성을 지닌 생체정보를 이용한 인증방식까지 꾸준히 개발되고 있다. 하지만 PIN 번호는 도용이 쉽고 개인정보를 통해 추측이 가능하다는 점에서 보안 위협에 굉장히 취약한 모습을 보인다. 또, 생체정보의 경우 임의로 갱신할 수 없어서 한번 유출되면 악의를 가진 타인도 쉽게 도용 가능하다는 치명적인 단점을 가지고 있다. 이에 걸음걸이, 키 스트로크와 같이 모방하기 어려운 사용자의 행동 습관을 기반으로 한 '행위적 특징 기반 인증기술'이 주목받고 있다. 실제로 2016년 구글은 사용자의 걸음걸이, 말하는 속도 등을 종합적으로 수집하여 분석을 거쳐 신뢰 점수를 측정하는 스마트폰 보안 인터페이스, 'Trust API'를 발표하였다. [1]

반면, PC 환경에서는 행위적 특징 기반 인증 기술에 관한 연구가 비교적 활발하지 않고, 여전히 PIN 번호 인증방식에 머물러 있다. 본 논문에서는 PC에 적용 가능한 행위적 특징 중 하나인 Mouse dynamics를 이용한 기존의 특징점 추출방식에 압력이라는 새로운 특징적 요소를 추가하여 사용자 인증 성공률을 높이는 방안을 제안한다. PC 환경에서 각 개인이 마우스를 사용하는 습관을 새로운 특징점으로 활용하는 시스템을 구현하기 위하여 FSR(Force-Sensing Resistor) Array를 마우스 패드로 제작하였다. 제작한 마우스 패드에 가해지는 압력의 분포, 모양 등을 감지하여 특징점을 추출하는 방법을 제시하고 실험을 통해 시스템의 상용화 가능성을 검증한다.

2. 관련 연구

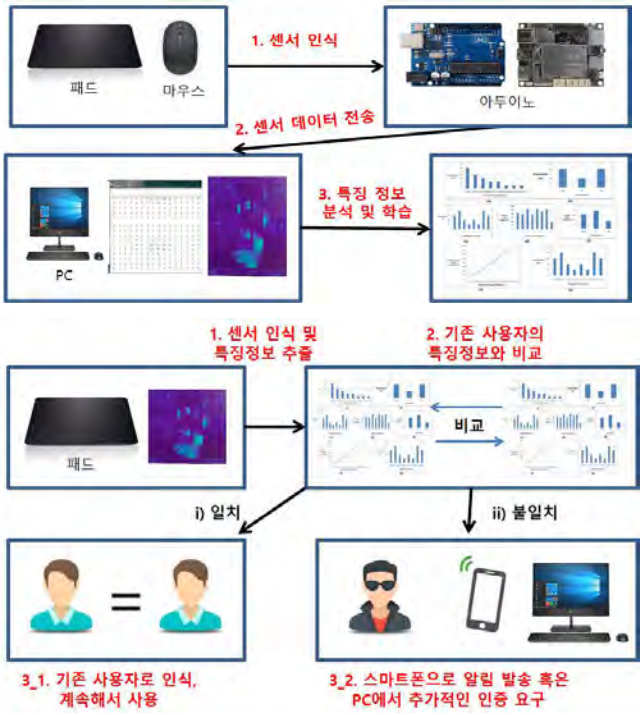
PC 환경에서 행위적 특징 기반 인증기술에 관한 연구는 크게 키보드를 눌렀다 떼는 시차를 행동특징으로 수집하는 Keyboard Stroke[2]와 마우스의 움직임을 기반으로 하는 Mouse dynamics[3],[4]로 나뉜다. 그러나 Keyboard Stroke의 경우, 사용자의 몸 상태 등에 따라 많은 편차가 있어 오류율이 다소 크다는 단점을 가진다. 반면, Mouse dynamics의 경우 다양한 특징점을 추출할 수 있어 인증 오류율이 비교적 작다는 장점이 있어 관련 특허도 꾸준히 출원되고 있다. 2019년 Victor Gorelik가 등록한 특허[5]

에서는 마우스에 카메라와 마이크를 내장하여 사용자의 손바닥 사진을 촬영하고, 맥박 소리를 등록하여 특징으로 추출한다. Clint Feher가 발표한 논문[6]에서는 마우스의 이동, 버튼 클릭, 드래그 등과 같은 움직임을 4가지 종류로 규정하여 종류마다 평균 이동 거리, 방향, 횟수 등을 통계적으로 분석하여 특징점을 추출하는 알고리즘을 제시하였다. 하지만 이러한 연구들도 상용화할 만큼 완벽한 인증 성공률을 보이지는 못하였다.

본 연구는 기존의 Mouse Dynamics 인증방식에 압력이라는 특징적 요소를 추가하여 더 많은 특징점을 추출하고 인증 성공률을 높이는 것을 목표로 한다.

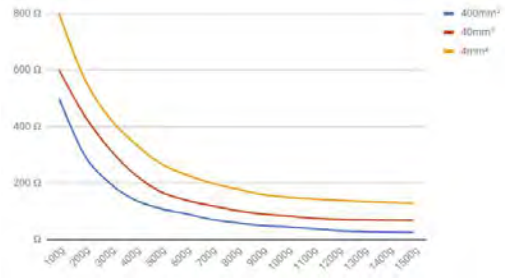
3. FSR Array를 이용한 마우스 패드 설계

본 논문에서 제안하는 방식은 FSR Array를 통해 압력의 분포, 모양 등의 특징점을 얻는 방식으로 현재 문제가 되는 원격해킹방식의 침입을 인지하고 예방한다는 점에서 차별된 장점이 있다. 실제 재택근무가 활발히 시행되는 요즘, 원격 상황에서 기업 내부망으로 접속하여 개인정보를 빼내는 해킹 사고[7]가 발생하고 있다. 마우스패드에서는 마우스의 움직임이 인식되지 않는데, 마우스 커서가 움직이는 등 특이점이 생기면 PC 사용을 자동으로 중단시키거나 본 소유자에게 위험 메시지를 전송하는 방식 등으로 응용될 수 있다.



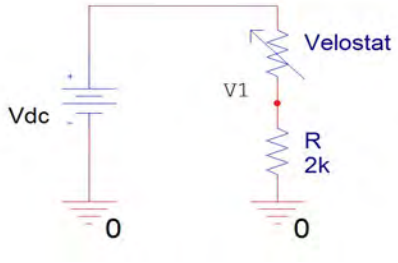
(그림 1) 시스템 구성도

3.1 Velostat을 활용한 FSR Array 설계



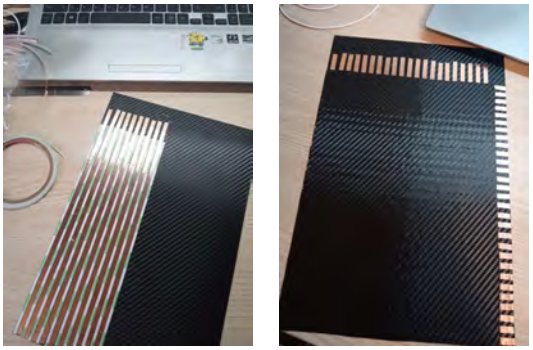
(표 1) Velostat 압력에 대한 저항의 크기 변화[8]

전도성 필름 Velostat의 성질을 이용해 Voltage Divider 회로(그림 2)를 설계하였다. Velostat은 (표 1)과 같이 가해지는 압력이 클수록 저항의 크기가 작아지는 일종의 가변저항이다. 가변저항으로 달라지는 전압 V1을 수치로 나타내도록 설계하였다.



(그림 2) Voltage Divider

구리테이프를 top layer에 가로로, bottom layer에 세로로 각각 배열하고, 그 사이에 Velostat을 부착하는 방식으로 FSR Array를 구현하였다. 구리테이프가 겹치는 면적이 하나의 압력 센서가 되며, Velostat에 압력이 전해지면 저항이 변하여 센서값도 변하는 원리로 작동한다.



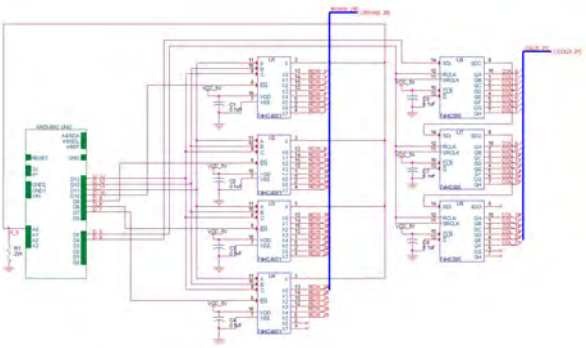
(그림 3) 29×20 센서 Array

3.2 FSR Array 구동을 위한 아두이노 기반 회로

아두이노를 통해 FSR Array를 제어하며, 압력 센서의 각 행과 열의 값을 얻기 위해 Shift Register와 Multiplexer를 이용해 회로를 구성한다.

Shift Register에 Clock 신호를 인가하여 Column

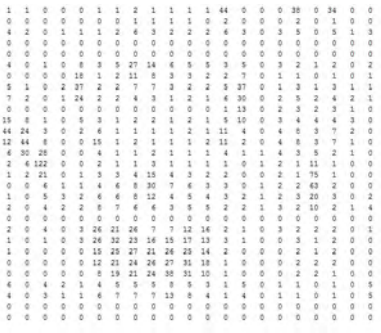
layer에서 검출된 29개의 전압값을 차례로 Multiplexer에서 받고, 다음 Column으로 넘어가도록 회로를 설계하였다.



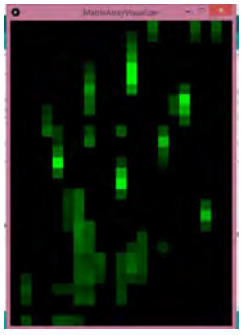
(그림 4) 4개의 MUX(74HC4051), 3개의 SR(74HC595)를 활용한 회로도

(그림 5) 완성된 FSR Array

가해지는 압력에 따라 변하는 압력센서의 값들을 그림 6과 같이 29×21의 숫자 행렬 형태로 아두이노 시리얼 모니터에 출력하도록 코드를 작성하였다. 그림 7과 같이 센서값의 크기를 색깔의 밝기로 나타내도록 java 코드를 작성하였다.



(그림 6) 시리얼모니터



(그림 7) Processing 출력

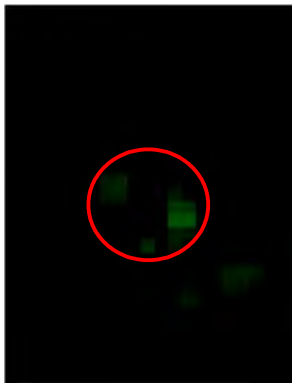
	센서값의 크기
압력이 가해지지 않았을 때	0 ~ 15
마우스를 올렸을 때	30 ~ 50
압력이 세게 가해질 때 (손목 등)	50 이상

(표 2) 센서값의 크기

4. 실험 결과

(그림 8) 사용자 A

(그림 9) 사용자 B



(그림 10) 사용자 C

- A : 마우스의 왼쪽과 아래쪽으로 압력이 분포
- B : 손목 부위에 집중적으로 압력이 분포
- C : 사용자의 약지, 소지가 패드에 닿아 압력이 가해진다

3명의 사용자가 평소에 마우스를 사용하듯이 마우스 패드 위에서 마우스를 사용하였다. 사용자 A는 마우스의 좌측 하단에 무게가 실리는 것을 확인할 수 있었고, 사용자 B의 경우, 마우스보다는 잡은 손의 손목 부위에 비교적 큰 센서값이 출력되었다. 사용자 C는 잡은 손의 약지, 소지가 패드에 닿아 그림 10과 같은 센서값이 확인되었다. 이 같은 실험을 통해 압력의 세기, 모양, 위치 등이 개인마다 차이가 있고, 행위적 특징 기반 인증 방식에 특징적 요소로 활용이 가능한 것을 확인했다.

5. 특징점 추출 - 유클리드 거리변환

FSR Array에서 출력한 센서값은 29×21의 숫자 행렬로 단순한 숫자 행렬끼리의 유사도를 판별하는데 자주 쓰이는 '유클리드 거리변환'을 본 시스템에 적용하려고 한다.

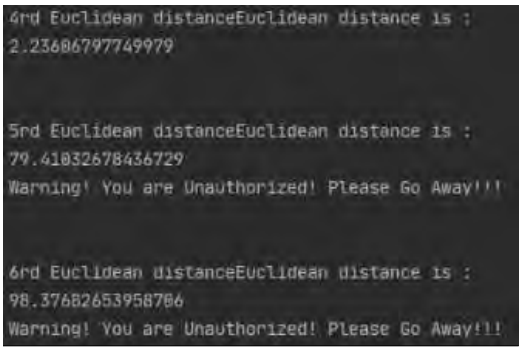
유사도란 두 데이터가 얼마나 같은지 나타내는 척도이다. 어떤 데이터가 n차원 상의 벡터로 표현된다면, 두 데이터의 유사도는 n차원 상에서 두 벡터 사이의 거리라고도 볼 수 있다. 만약 거리가 가깝다면 두 데이터는 꽤 유사하다고 생각할 수 있다.

$$d(\mathbf{p},\mathbf{q}) = d(\mathbf{q},\mathbf{p}) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \cdots + (q_n - p_n)^2}$$
$$= \sqrt{\sum_{i=1}^{n}(q_i - p_i)^2}.$$

이와 같은 방식으로 마우스패드의 센서값과 미리 학습한 사용자의 센서값 사이의 유클리드 거리를 계산한다. 거리가 일정 수준 이상 가까운 센서값이라면 PC를 사용할 수 있도록 하고, 차이가 크게 발생하면 침입자로 판단해 PC 사용을 중단시키도록 하는 등의 사용자 인증 시스템을 구현할 수 있다.

5.1 유클리드 거리 측정을 위한 코드 작성

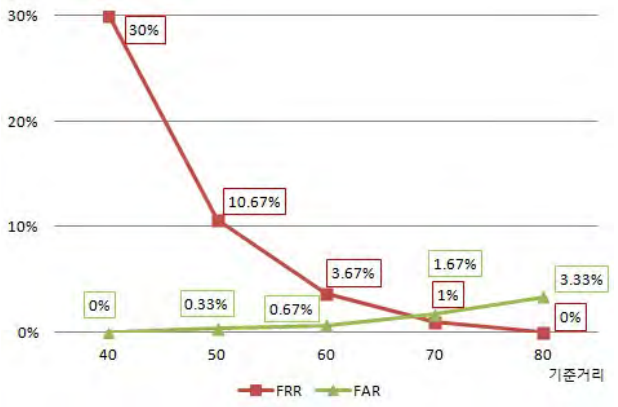
위와 같은 알고리즘으로 작동하는 파이썬 코드를 작성하였다. 인증단계에서는 학습된 데이터와 실시간으로 패드를 통해 얻어지는 센서값의 유클리드 거리를 계산한다. 기준 거리 이상의 값이 입력될 경우 유클리드 거리와 에러 메시지를 출력한다.



(그림 11) 결과 출력값

5.2 적절한 유클리드 기준 거리 조정

사용자 인증의 기준이 되는 적절한 유클리드 거리를 찾기 위해 기준 거리를 바꿔가며(40 ~ 80) 실험을 진행하였다. 각각 FAR(False Accept Rate, 비등록자를 등록자로 인식하여 잘못 수락하는 확률), FRR(False Rejection Rate, 등록자를 비등록자로 인식하여 접근을 거부하는 확률)을 측정하였다.



(표 3) 기준거리에 따른 FAR, FRR

기준 거리 70 이상에서 FAR, FRR 모두 5% 미만으로 만족스러운 인식률을 얻을 수 있었다.

6. 결론 및 향후 연구

본 논문에서는 마우스 패드를 FSR Array로 제작하여 센서에 가해지는 압력의 분포를 특징점으로 추출하여 사용자를 인식하는 Secondary 인증 시스템을 제안한다. 직접 하드웨어를 구상하고 제작하여 센서값을 얻을 수 있도록 하였고, 실험을 통해 개인마다 마우스 사용습관에 차이가 있고, 이를 특징점으로 활용할 수 있다는 가능성을 보였다. 제안한 시스템은 기존에 연구되어 온 Mouse dynamics 기반 인증 시스템에 추가적인 Secondary 인증방식으로써 정확도를 높이고 더욱 강력한 보안 시스템을 구현하는 데 도움이 될 것으로 기대된다. 향후 연구내용으로는 유클리드 거리변환을 적용한 인증 소프트웨어를 발전시킬 예정이다. 이외에도 여러 알고리즘을 적용하여 인식 성공률을 분석하고 가장 정확한 알고리즘을 찾아 활용해 완성도를 높이려 한다. 또, 하드웨어에서 노이즈를 줄이는 방안을 찾을 계획이다.

참고문헌

[1] 기사 “Google aims to kill passwords by the end of this year ”, The Guardian, https://www.theguardian.com/technology/2016/may/24/google-passwords-android, 2016.05.24

[2] 김원겸, “행위적 특징 기반 바이오 인증 기술 동향”, 정보통신기술진흥센터, 2017

[3] Chao Shen, “User Authentication Through Mouse Dynamics”, IEEE Transactions on Information Forensics and Security, 2013

[4] Maja Pusara, “User Re-Autehntication via Mouse Movements”, Vizsec/DMSEC'04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer securitty, 2004

[5] 등록번호 : 10210375 B2, 2019.02, Victor Gorelik, Alexander Fursenko

[6] Clint Feher, “User Identity Verification via Mouse Dynamics”, 2012

[7] 기사 “코로나19로 위장한 각종 해킹 공격 증가, '주의 필요'”, IT dongA, http://it.donga.com/30345/, 2020.04.07

[8] REPS.CC, https://reps.cc/?p=50