오토인코더와 변이형 오토인코더를 활용한 공유 킥보드 사용자 인증 시스템 강화

강예준*, 김현지**, 임세진*, 김원웅*, 서화정***
*한성대학교 컴퓨터공학과
**한성대학교 IT 융합공학부
***한성대학교 IT 융합공학부
etus1211@gmail.com, khj1594012@gmail.com, dlatpwls834@gmail.com,
dnjsdndeee@gmail.com, hwajeong84@gmail.com

Reinforcement of user authentication system of shared kick scooter using autoencoder and variational autoencoder

Yea-Jun Kang*, Hyun-Ji Kim**, Se-Jin Lim*, Won-Woong Kim*, Hwa-Jeong Seo***
*Dept. of Computer Science, Han-Sung University
**Dept. of IT Convergence Engineering, Han-Sung University
***Dept. of IT Convergence Engineering, Han-Sung University

요 약

경찰청에 따르면 도로교통법이 개정된 이후 3개월단 개인형 이동장치(PM)를 단속한 결과 무면허 운전이 3199건에 달하는 것으로 나타났다. 공유 킥보드 서비스의 경우 회원가입을 할 때 운전면허증 취득 여부를 확인하긴 하지만 서비스를 이용할 때는 별도의 확인 절차 없이 대여할 수 있기 때문에 운전면허증을 취득하지 않았어도 대여하는 경우가 발생한다. 본 논문에서는 공유 킥보드 서비스의 보안 취약점을 보완하기 위해 오토인코더와 변이형 오토인코더를 사용한 딥러닝 기반의 공유 킥보드 대리 대여 방지 시스템을 제안한다. 오토인코더는 지문 데이터로부터 특징만을 추출할 수 있어, 사용자의 지문 원본을 서버에게 노출시키지 않을 수 있다. 변이형 오토인코더는 생성형 모델로써, 사용자의 지문 데이터를 증폭 시켜 합성곱 신경망의 성능을 높이는데 도움을 준다. 이러한 오토인코더와 변이형 오토인코더의 특징을 이용해 사용자의 지문을 서버에 노출시키지 않으면서 적은 데이터로 신뢰성 높은 사용자 인증이 가능한 전동 킥보드 대여 시스템을 제안한다.

1. 서론

최근 전동 킥보드 대여 서비스가 증가함에 따라 도로교통법을 위반하는 사례가 증가하고 있다. 2021년 5월 13일부터 개정된 도로교통법에 따르면 전동 킥보드는 원동기면허 이상 취득해야만 운전을 할 수 있다. 하지만 경찰청에 따르면 도로교통법이 개정된 이후 3개월간 개인형 이동장치(PM)를 단속한 결과 무면허 운전은 3199건에 달했다. 공유 킥보드의 경우 회원가입을 할 때 운전면허증을 취득하였는지 확인한다. 하지만 회원가입을 한 뒤 서비스를 이용할 때는 별도의 확인 절차 없이 대여가 가능하기 때문에, 면허증이 없는 사용자가 다른 사람의 면허증을 빌려 회원가입한 뒤 전동 킥보드를 대여하는 취약점이 존재한다. 또한 이외에도 도난과 같은 문제점이 있다. 본 논문에서는 이에 대한 방안으로 기존보다 더 강화된 인증 시스템을 제안한다.

2. 관련연구

2.1 지문 인식을 통한 사용자 인증

지문은 선천적으로 개인마다 모두 다르고 인식할 때 편리하다는 특징을 가지고 있어 생체 인식을 할 때 가장 활발히 사용되고 있다. 하지만 지문은 유출 위험이 높고 유출되더라도 지문을 변경할 수 없다는 점과, 복제가 쉽다는 단점이 존재하기도 하다. 그럼에도 불구하고 지문 인식은 편리하고 정확하기 때문에 가장 활발히 이용되는 생체 인식 기술이다. 지문을 인식하는 과정은 크게 입력 단계와 인증 단계로 이루어진다. 입력 단계는 지문 인식 센서에 지문을 대어 촬영하는 단계이고, 인증 단계는 촬영된 지문을 미리 저장된 지문과 대조하여 일치 여부를 판단함으로써 개인을 식별하는 단계이다. 지문을 촬영하는 방식은 크게 정전식, 광학식, 초음파 방식 등이 있다.

2.2 오토인코더 (Autoencoder)

오토인코더란 출력값을 입력값의 근사로 하는 함수를 비지도 학습의 형태로 학습하는 네트워크다[1]. 오토인코더는 인코더와 디코더로 구성되어 있다. 인코더 과정에서는 입력한 데이터 X를 특징 값으로 변환하는 신경망으로 구성되어 있어, 입력된 데이터의 핵심 특징만 학습하고 나머지 정보는 손실시켜 데이터로부터 특징을 추출할 수 있다. 즉, 어떤 데이터를 효율적으로 나타내기 위해서 입력 데이터의 차원을 축소하거나 특징을 추출할 수 있다. 디코더 과정에서는 인코더 과정을 거쳐 나온 출력값을 디코더에 입력하면, 인코더 과정을 거치기 전 데이터인 X 값이 나오게 된다. 이러한 특징으로 오토인코더의 신경망 구조는 은닉층을 기준으로 좌우가 대칭이며 입출력이 동일하다. 따라서 오토인코더는 인코더를 통해 입력 데이터에 대한 특징을 추출하거나 차원을 축소하고, 디코더를 통해 원본 데이터를 재구성하는 학습 방식이다.

2.3 변이형 오토인코더 (Variational Auto-Encoder)

변이형 오토인코더는 확률 분포를 이용해 새로운 데이터를 생성하는 생성형 모델이다[2]. 변이형 오토인코더는 입력 데이터의 특징을 추출하는 오토인코더와 달리, 인코더가 입력 데이터를 평균과 표준 편차로 인코딩한 후, 두 벡터에 대응하는 정규 분포로부터 샘플링을 통해 잠재변수 z를 만든다. 디코더는 해당 z값을 통해 인코더에 입력했던 이미지 데이터의 분포와 유사한 새로운 데이터를 생성한다. 즉, 변이형 오토인코더는 인코더를 통해 샘플링한 후, 샘플링을 통해 얻은 값으로 디코더가 새로운 데이터를 생성하는 생성형 모델이다. 변이형 오토인코더는 대표적인 생성형 모델인 GAN(Generative Adversarial Network)과 비교하였을 때, 출력이 GAN에 비해 흐릿하고 평균값 형태로 표시되는 문제 등이 있지만 모델의 평가 기준이 명확하고 학습이 안정적이며 데이터에 내재한 잠재변수 z도 함께 학습할 수 있다는 장점이 있다.

2.4 합성곱 신경망 (Convolutional Neural Network)

합성곱 신경망은 컴퓨터 비전 분야에서 많이 쓰이는 신경망이다. 심층 신경망(Deep Neural Network)은 데이터를 1차원 형태로만 입력받을 수 있기 때문에, 3차원 데이터인 이미지를 입력하고자 해도 1차원 데이터로 반드시 평탄화해야 한다. 하지만 이미지 데이터의 경우 인접한 픽셀들끼리는 RGB 채널에 있어서 관련이 많고, 멀리 떨어져 있는 픽셀들과는 관련이 없는 정보를 가지고 있다. 심층 신경망에서 이러한 특징을 가지고 있는 3차원 데이터인 이미지를 1차원 데이터로 평탄화하면, 모든 입력 데이터를 동등한 뉴런으로 취급하여 형상에 담긴 정보를 살릴 수 없다. 즉, 이미지 공간 정보가 유실되어 공간적 특징을 살릴 수 없으며, 학습이 매우 비효율적이고 정확도를 높이는 데 한계가 있다. 하지만 합성곱 신경망은 데이터의 형상이 무시되는 심층 신경망과 다르게 이미지를 3차원 데이터로 입력받고 다음 계층에도 3차원 데이터로 전달하므로 데이터의 형상을 유지할 수 있다. 이러한 특징으로 인해 이미지의 공간적인 정보를 학습할 수 있으므로 이미지 인식 분야에서 주로 사용된다.

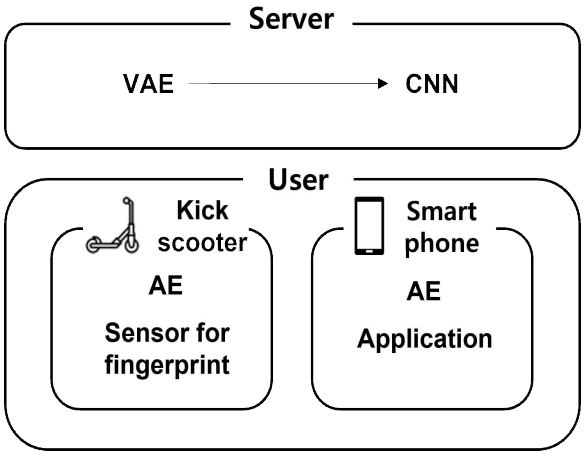
3. 제안기법

본 논문에서는 오토인코더와 변이형 오토인코더를 사용한 딥러닝 기반의 공유 킥보드 대리 대여 방지를 위한 강화된 인증 시스템을 제안한다. (그림 1)은 제안 시스템의 전체 동작 과정을 개략적으로 나타낸 구성도이다. 전체 시스템은 크게 전동 킥보드를 이용하는 사용자와 서버로 나뉜다. 사용자는 스마트폰을 통해 이용하려는 전동 킥보드 어플리케이션을 설치해야 하고, 공유 킥보드에는 지문 인식 센서와 오토인코더가 배포된 상태이다. 또한, 전동 킥보드 서버는 사용자 인증을 위한 분류기인 합성곱 신경망과 더 신뢰성 있는 인증시스템을 훈련시키기 위한 변이형 오토인코더로 구성된다.

변이형 오토인코더와 분류기의 학습을 위해 지문의 특징점을 추출할 수 있는 오토인코더를 사용자의 스마트폰에 배포한다. 배포 받은 오토인코더 모델을 통해 지문에서 특징을 추출한 후, 공유킥보드 어플리케이션을 통해 서버에게 보낸다. 서버는 해당 추출 값을 변이형 오토인코더에 입력하여 사용자의 지문 특징을 내포하는 새로운 데이터들을 생성한다. 생성된 데이터들은 사용자 인증을 위한 분류기 학습에 사용된다.

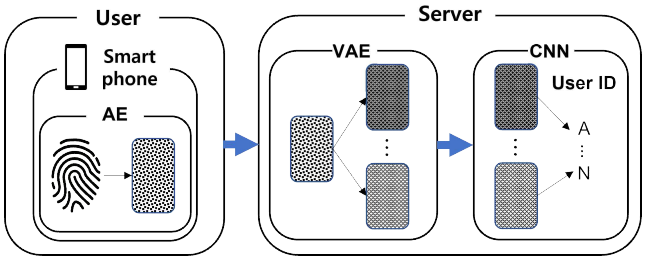
실제 사용 시에는 전동 킥보드의 지문인식 센서로부터 수집된 지문이 오토인코더를 거쳐 특징점으로 축소되고 해당 정보가 훈련된 합성곱 신경망 분류기로 전송되어 사용자 인증을 수행할 수 있도록 한다. 또한, 인증 과정을 임의의 시간마다 반복함으로써 탑승하고 있는 사용자가 본인이 아닐 경우 속도가

줄어들어 운행할 수 없도록 한다.



(그림 1) System diagram

3.1 사용자 인증 시스템 훈련



(그림 2) System diagram for training phase

제안 시스템은 훈련 단계에서 공유 킥보드 사용자와 공유 킥보드 서버로 나뉜다. (그림 2)는 훈련을 위한 전체 구성도이며, 3.1.1절과 3.1.2절에서 자세히 설명한다.

3.1.1 공유 킥보드 사용자

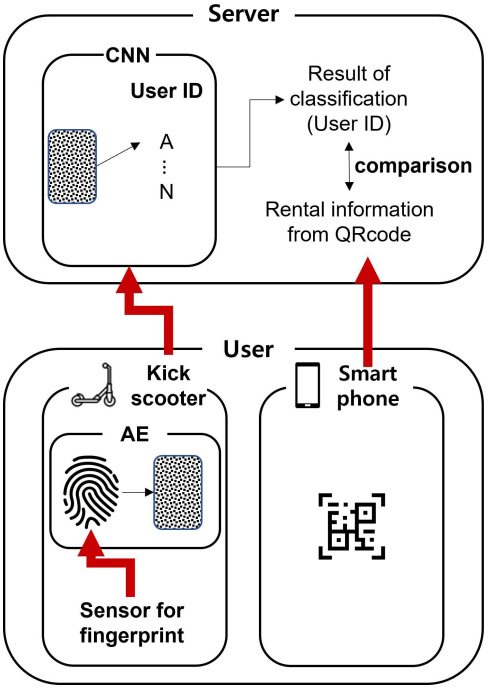
사용자가 스마트폰에 애플리케이션을 설치하여 전동 킥보드 공유 서비스에 가입하면 사용자 ID가 생성된다. 가입 초기에 사용자의 스마트폰에 저장된 지문 정보는 오토인코더를 거쳐 특징점만 추출된 상태로 애플리케이션에 등록된다. 해당 정보는 전동 킥보드 서버에서 변이형 오토인코더를 훈련하기 위해 사용된다.

3.1.2 공유 킥보드 서버

서버는 사용자 인증을 위한 합성곱 신경망을 학습하여 인증을 진행해야 하므로, 사용자의 지문 데이터가 필요하다. 그러나 지문 데이터를 그대로 학습에 사용할 경우, 사용자의 생체 정보가 노출되므로, 지문 데이터 원본을 서버에 제공하기 않기 위해 오토인코더를 사용한다. 오토인코더는 인코더 부분과 디코더 부분으로 구성되는데 원본 지문의 특징을 추출하는 부분인 인코더만을 사용한다. 학습이 완료된 오토인코더를 전동 킥보드와 사용자의 스마트폰에 배포한다. 3.1.1에 언급한 과정을 통해 사용자의 지문 특징 데이터를 수집한 후, 해당 데이터를 변이형 오토인코더에 입력한다. 변이형 오토인코더는 입력된 데이터에 잠재 변수를 추가하여 입력 데이터를 기반으로 변형된 데이터들을 생성한다. 생성된 데이터들을 합성곱 신경망의 학습 데이터로 사용하며, 해당 데이터를 사용자들의 ID로 분류하도록 학습시킨다. 따라서 적은 양의 생체 정보를 가지고 많은 데이터를 생성함으로써 합성곱 신경망 분류기에 입력될 학습 데이터의 수를 증폭 시킨다. 일반적으로 학습 데이터가 많을수록 신경망의 성능이 증가한다. 따라서 적은 생체 데이터로 신뢰성 높은 사용자 인증이 가능해진다.

3.2 사용자 인증

다음은 사용자가 실제로 전동 킥보드를 대여해서 이용하는 단계이다. (그림 3)은 사용자 인증 단계의 구성도이다.



(그림 3) System diagram for authentication phase

사용자는 전동 킥보드 사용을 위해 QR코드를 인식하여 대여한다. 전동 킥보드의 손잡이에는 지문 인식 센서가 부착되어 있어서 전동 킥보드 운행할 경우 자연스럽게 사용자의 지문이 주기적으로 수집

된다. 해당 지문을 전동 킥보드의 오토인코더에 입력하여 특징값을 추출한 후, 전동 킥보드 서버로 전송한다. 서버는 합성곱 신경망에 전송받은 데이터를 입력하여 추론을 진행하고, 등록된 사용자가 맞는지 확인한다. 예를 들어 A 사용자가 전동 킥보드를 탑승하였을 때, 지문이 수집 및 추출되어 전동 킥보드 서버로 전송된다. 서버에서는 해당 지문 추출 값을 합성곱 신경망에 입력하면, 입력 데이터가 각 클래스 (사용자 ID)로 분류될 확률이 계산되며, 특정 임계값 이상일 경우 해당 클래스로 분류한다. 또한, 이미 등록된 사용자가 다른 사용자의 명의를 도용하여 탑승할 경우를 방지하기 위해서 대여 시에 전동 킥보드에 등록된 사용자의 대여기록 정보와 비교한다. 만약 등록되지 않은 사용자가 이용하거나 실제 탑승자가 현재 대여한 사용자가 아닌 경우, 전동 킥보드의 속도가 점차 줄어들어 멈추게 된다. 따라서 전동 킥보드 무면허 사용 및 대리 대여 문제를 방지할 수 있다.

4. 결론

본 논문에서는 오토인코더와 변이형 오토인코더를 사용한 공유 킥보드 대리 대여 방지를 위한 강화된 인증 시스템을 제안한다. 제안 시스템은 변이형 오토인코더를 활용하여 적은 데이터로도 합성곱 신경망의 사용자 분류 성능을 향상 시킬 수 있다. 뿐만 아니라 오토인코더를 사용함으로써 사용자의 지문 원본 데이터를 서버에 노출시키지 않아도 된다는 장점이 있다. 또한, 제안 시스템 적용 시 현재 탑승자를 주기적으로 확인하므로, 면허증이 없는 사용자의 사용이나 대리 대여를 막을 수 있을 것으로 기대된다.

5. Acknowledgment

이 논문은 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2018-0-00264, IoT 융합형 블록체인 플랫폼 보안 원천 기술 연구, 50%) 그리고 부분적으로 2021년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. NRF-2020R1F1A1048478, 50%).

참고문헌

[1] Ng, Andrew. "Sparse autoencoder." CS294A Lecture notes 72.2011 (2011): 1-19.

[2] Pu, Yunchen, et al. "Variational autoencoder for deep learning of images, labels and captions." Advances in neural information processing systems 29 (2016): 2352-2360.

[3] Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E. Hinton. "Imagenet classification with deep convolutional neural networks." Advances in neural information processing systems 25 (2012): 1097-1105.