

숙련된 위조서명 구분이 가능한 딥러닝 기반의 모바일 동적 서명 인식

남승수*, 최대선**, 서창호*
*공주대학교 융합과학과
**공주대학교 의료정보학과
e-mail : sunchoi@kongju.ac.kr

Deep learning based mobile dynamic signature recognition for skilled forgery division

Seung-Soo Nam*, Dae-Seon Choi**, Chang-Ho Seo*
*Dept. of Conversions Science, Kongju University
**Dept. of Medical Information, Kongju University

요 약

본 논문에서는 모바일 환경에서 동적서명인식에 관해 원본서명과 숙련된 위조서명의 구분을 검증하는 방법을 제안한다. 속도/거리 정보 실험(Data1)과 속도/거리정보와 가속도계를 추가 실험(Data2)을 원본 서명과 위조서명에 대한 테이블을 만들고, 비교하여 원본 서명의 인식을 확인한다. 제시한 방법은 각각 모바일 환경에서 10 명이 20 번씩 손가락으로 테스트 하였다. 원본서명에서 딥러닝중의 하나인 MLP를 실험한 결과 원본 서명에서 Data1 은 92%, Data2 는 95%의 정확도를 보였으며, 위조서명에서 Data1 은 82%, Data2 는 85%를 보였다. 그리고 AE 에서 실험한 결과 Data1 은 원본 서명에서 Data1 은 95%, Data2 는 97%의 정확도를 보였으며, 위조서명에서 Data1 은 91.5%, Data2 는 93%의 정확도가 보였다. 실험결과 위조서명에 대해서는 MLP 로 위조서명을 분류하는 것보다 OAE 에서 분류하는 것이 더 좋은 정확도를 보여준다.

1. 서론

서명인식은 서명자마다 그 특성이 다르고, 동일한 필기자의 경우에도 필기 자세, 감정 상태나 사용된 서명 입력 장치 등에 따라 조금씩 다르게 나타나며 동일한 조건에서도 시간에 따라 다소 다르게 나타나게 된다. 서명인식 방법에는 오프라인 서명인식과 온라인 서명인식이 있다. 오프라인 서명은 필기된 서명 혹은 도장을 의미하며, 온라인 서명은 터치스크린 등의 장치를 이용해 실시간으로 입력하는 서명을 뜻한다. 그 중 온라인 서명인식은 모바일 환경에서 스타일러스가 아닌 손가락으로 서명한 동적서명인식에 대한 학계의 연구가 수행되고 있다[1]. 스타일러스 서명은 좌표, 속도, 압력과 같은 특징을 사용하지만, 손가락 서명은 압력에 대한 특징을 가용할 수 없어 가속도계(Accelormeter)를 사용한다. 그리고 온라인 서명에는 위조서명(Skilled forgery)이 일어날 수 있다 이것을 증명하기 위해 원본서명과 위조서명에 대한 비교를 제시한다.

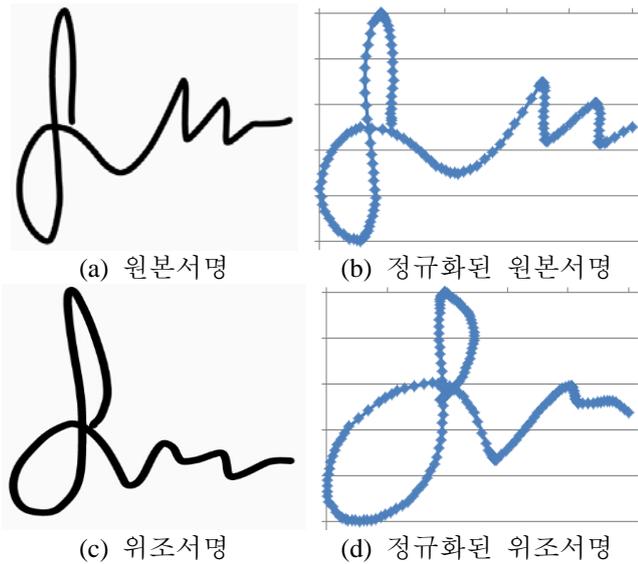
서명들의 특징을 비교하기 위해서는 RMS(Root Mean Square)방법 이나 HMM(Hidden Markov Model)등

이 사용된다. RMS 는 서로 다른 좌표의 차이를 누적 시간에 따라 비교하여 좌표의 차이를 누적시키는 방법이지만, 왜곡에서 오차율이 높다. HMM 은 관측 symbol 을 구성하는 확률로 구성하지만, 학습자료가 충분하지 않으면 학습과정을 정확히 수렴하지 못하거나 오히려 부정확한 모델을 만들어 낼 수 있는 단점이 있다[2]. 위의 문제를 해결 하기 위하여 현재 이슈로 떠오르고 있는 딥러닝(Deep Learning) 기법 중에서 MLP(Multi-Layer Perceptron)[3]를 활용하고, AE(Auto Encoder)[4]를 사용하여 정확도를 비교한다.

본 논문에서는 2 장 원본서명과 위조서명의 특징정보를 설명하고 딥러닝을 이용한 방법 3 장 실험구성과 결과 4 장은 결론 및 향후 연구과제에 대해 서술 할 것이다.

2. 서명 특징 정보

서명특징 정보를 분석하기 위해서는 1 절 원본서명과 위조서명에 대한 속도/거리정보의 특징을 설명하고, 2 절은 1 절에서 검출한 특징들을 딥러닝의 MLP 와 AE 를 이용한 방법을 서술한다.



(그림 1) 기존서명과 정규화된 서명비교

1. 속도/거리정보의 비교

본 연구에서 제안한 서명의 주요 특징 정보는, 서명할 때 손가락이 Touch Down 시에 나타나는 속도정보, 획 순서, 전체 획 수 등을 나타내는 속도/거리정보이며, 가속도계를 추가하여 사람의 특징을 보다 더 상세하게 나타낼 수 있다. 그리고 모바일에 장착된 가속도센서에서 나온 가속도계를 추출하여 개인고유의 특성에 대한 정보를 보여준다. 개인정보를 쉽게 노출될 가능성을 낮게 만들고, 상대적으로는 다른 사람에게 쉽게 노출이 되지 않아 보안성이 높은 특징을 지니고 있다. 그림 1 에서 (a)와 (c)는 원본서명과 위조서명을 보여주며 (b)와 (d)는 정규화(Normalization)와 일정한 간격으로 리샘플링(Resampling)한 서명 데이터를 보여준다[5]. 원본서명과 위조서명의 위치와 거리차이를 볼 수 있다. 원본서명과 위조서명에서 정규화로 인해 잃어버린 좌표를 추적 탐지하여 인식의 정확도를 높일 수 있도록 하였다.

2. 딥러닝을 이용한 비교

1 절은 서명에 추출되는 두 점 사이의 속도/거리정보를 계산하였고, 가속도계정보를 추가해 전체 에러율에 영향을 주지 않으면서 보안성은 높아졌다. 하지만 메모리 용량이 늘어나고, 처리속도가 낮은 단점이 발생할 수 있다. 이를 개선하기 위해 복잡한 자료를 효율성 있게 적용할 수 있는 딥러닝의 기법중에서 MLP 와 AE 를 이용하여 분석하였다. 딥러닝은 여러 비선형 변환기법의 조합을 통해 높은 수준의 추상화를 시도하는 기계학습(Machine learning) 알고리즘의 집합으로 정의 된다.

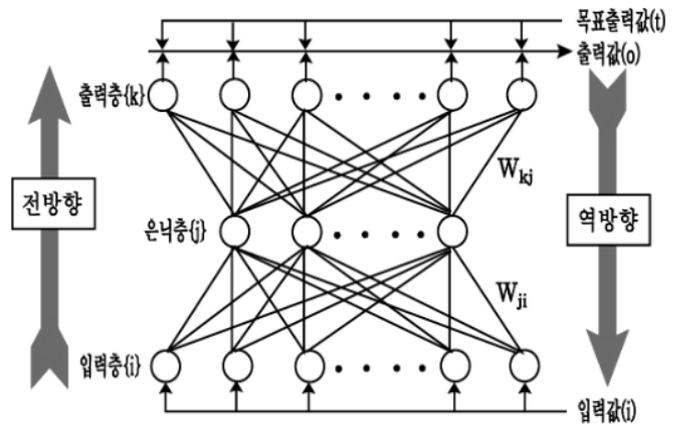
MLP 는 입력층과 출력층 사이에 하나 이상의 중간층이 존재하는 신경망으로 그림 2 에 나타낸 것과 같은 계층구조를 갖는다. 이 때 입력층과 출력층 사이의 중간층을 은닉층 (hidden layer) 이라 부른다. 단층 퍼셉트론(Perceptron)과 유사한 구조를 가지고 있지만

중간층과 각 구성(Unit)의 입출력 특성을 비선형으로 함으로써 네트워크의 능력을 향상시켜 단층 퍼셉트론의 여러 가지 단점들을 극복했다. MLP 는 층의 개수가 증가할수록 퍼셉트론 이 형성하는 결정 구역의 특성은 더욱 고급화된다. 즉 단층일 경우 패턴공간을 두 구역으로 나누어주고, 2 층인 경우 볼록한 (convex) 개구역 또는 오목한 폐구역을 형성하며, 3 층인 경우에는 이론상 어떠한 형태의 구역도 형성할 수 있다.

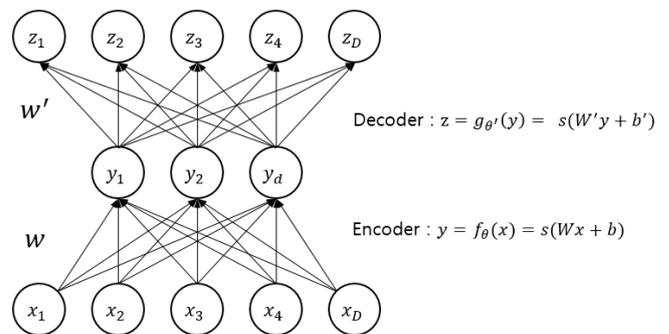
AE 는 입력과 출력을 동일하게 하여 둘 사이의 오차를 최소화하도록 학습하는 다층 신경망의 일종이며, 그림 3 과 같이 입력 계층, 1 개의 은닉 계층, 출력 계층의 총 3 계층으로 구성된다[6].

AE 가 입력받은 데이터를 은닉 계층에서 새롭게 표현하는 과정을 부호화(encoding), 은닉 계층에서 출력 계층을 거쳐 데이터가 복원되는 과정을 복호화(decoding)라고 한다. 은닉 계층의 노드 수를 입/ 출력 계층의 노드 수보다 적게 구성하면 부호화 과정에서 정보 손실이 발생하게 된다. 이렇게 부호화 된 입력이 온전히 복호화 되도록 학습되므로, 입력데이터가 갖는 내재적 특성은 보존하면서 불필요한 잡음 특성이 제거된 특징 추출이 이루어진다

AE 는 변환 규칙을 학습하는 변환기로도 활용될 수 있다. 입력을 일정 규칙으로 변환한 것을 출력으로 사용하면, Auto-encoder 는 데이터로부터 내재된 변환 규칙을 학습하여 새로운 입력에 대해서도 학습된 변환을 수행할 수 있게 된다.



(그림 2) MLP 의 구조



(그림 3) Auto-Encoder 의 구조

MLP 와 OA 기법을 활용하여 원본서명에 대해서 샘플을 학습하고 실험하여 정확도를 비교 한다.

3. 실험

1. 실험 구성

제안 방법의 성능을 측정하기 위한 실험 구성이다. 실험인원은 1 인당 20 번씩 총 10 명의 원본 서명을 얻어 200 개의 테스트 샘플을 수집했다. 그리고 4 명의 사람에게 원본서명을 1 인당 5 개씩 서명하도록 총 200 개의 숙련된 위조서명을 만들었다. 테스트 샘플은 원본 서명과 위조서명의 4 개 테스트군을 만들었다. Data1 은 좌표/시간정보, Data2 는 가속도계 + 좌표/시간정보로 이루어졌다. 서명은 GalaxyS3 에서 실험데이터를 추출했다. 실험환경은 Ubuntu 15.04 에서 Python 으로 구현했다. 3,072 개의 GPGPU 를 이용하여 MLP 와 OA 모델을 사용하여 학습하였다.

2. 실험 결과

획득한 10 명의 원본서명 샘플 중 10 개를 트레이닝으로 분류하고, 나머지 10 개는 테스트로 분류 한다. 위조서명샘플은 10 개의 원본서명을 트레이닝으로 위조샘플은 10 개의 테스트로 분류 했다.

<표 1> 좌표/시간정보와 가속도계+좌표/시간정보

	MLP	
	Data1	Data2
Original	92%	95%
Skilled Forgery	82%	85%

<표 2> 좌표/시간정보와 가속도계+좌표/시간정보

	AE	
	Data1	Data2
Original	95%	97%
Skilled Forgery	91.5%	93%

<표 3> 좌표/시간정보와 가속도계+좌표/시간정보

	Skilled Forgery	
	Data1	Data2
MLP	82%	85%
AE	91.5%	93%

<표 1> 과 <표 2>에서 보는 바와 같이 각각 Data1 은 좌표/시간정보만을 사용한 것이고, Data2 는 가속도계+ 좌표/시간정보의 데이터로 이루어져 있다.

MLP 로 학습한 결과 원본서명의 Data1 은 92%, Data2 는 95%의 정확도가 나온 것을 확인 했다. 위조서명의 Data1 은 82%, Data2 는 85%의 정확도를 보였다. 원본서명에서 보여주는 정확도 보다 위조서명을 추가한 정확도가 각각 13%, 7%차이가 났다. 그리고 AE 로 학습한 결과 원본서명의 Data1 은 95%, Data2 는 97%의 정확도가 나온 것을 확인 했다. 위조서명의 Data1 은 91.5%, Data2 는 93%의 정확도를 보였다. 원본서명에서 보여주는 정확도 보다 위조서명을 추가한 정확도가 각각 3.5%, 4%가 낮았다. 이를 비교하기 위해 <표 3>과 같이 정리해 놓았다. 위조서명을 판별하기 위해서는 MLP 보다 AE 기법으로 사용하는 것이 위조서명의 판별을 더욱 강인하다는 것을 뜻한다.

그리고 Data1 보다 Data2 의 정확도가 높은 것을 확인할 수 있다. 그 이유는 원본서명과 위조서명은 가속도계를 추가한 샘플에서 정확도가 높은 것을 보여주며, 가속도계의 정보가 개인특성에 따라 비슷한 가속도계를 저장하고 있기 때문에 높은 정확도를 보여준다.

4. 결론 및 향후 연구방향

본 논문은 원본서명과 위조서명을 검증하는 방법에서 MLP 와 AE 기법을제안하고 서로 비교하였다. MLP 로 확인한 결과 위조서명은 83.5%의 정확도를 보였으며, AE 에서는 92.25%의 정확도를 확인했다. MLP 보다 AE 의 기법으로 학습한 것에 대해 8.75%차이의 정확도를 보였다. 현재 위치 정보만을 사용한 모바일 서명인증의 최고 수준은 NYU 의 97%이다[7]. 향후 연구로는 모바일에서 가용할 수 있는 센서와 서명에 대한 데이터를 정확하게 수집하여 AE 기법으로 동적서명인증의 정확도를 높여야 할 것이다.

참고문헌

- [1]M. Priya, A. Kaur. "Handwritten Signature Verification using Instance Based Learning", *International Journal of Computer Trends and Technology*, Mar. 2011.
- [2] J.W. Kim, J.H Cho."동적 서명의 특징 정보에 대한 통계적 분석에 관한 연구", *한국해양정보통신학회 논문지*, 13.8, 1693-1698, 2009.
- [3] Q. Wu, et. al, "Cross-view and multi-view gait recognitions based on view transformation model using multi-layer perceptron", *ICPR*, Vol. 33, p882-889, 2010.
- [4] Autoencoder, <https://en.wikipedia.org/wiki/Autoencoder>
- [5] P. O. Kristensson, et.al, "Continuous recognition of one-handed and two-handed gestures using 3D full-body motion tracking sensors," *Proc. of ACM Int'l. Conf. on Intelligent User Interfaces*, pp. 89-92, 2012.
- [6] G. E. Hinton, et al., "Transforming auto-encoders," *Artificial Neural Networks and Machine Learning 2011, Springer Berlin Heidelberg*, pp. 44-51, 2011
- [7] Napa Sae-Bae, et.al, "Online Signature Verification on Mobile Devices", *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 6, 2014.