Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.5, Oct. 2016 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2016.26.5.1161

모바일환경에서 위조서명에 강건한 딥러닝 기반의 핑거서명검증 연구*

남 승 수,† 서 창 호, 최 대 선‡
공주대학교

Mobile Finger Signature Verification Robust to Skilled Forgery*

Seng-soo Nam,† Chang-ho Seo, Dae-seon Choi‡
Kongju National University

요 약

본 논문에서는 스마트폰에서 손가락으로 서명하는 동적서명에서 위조서명에 강건한 검증 방법을 제안한다. 본 논문에서는 위조서명을 효과적으로 구분할 수 있도록 재생산 신경망의 일종인 1 class Auto-Encoder 모델을 사용한다. 핑거서명에서는 지원되지 않는 펜 압력 등 기존의 특징 정보 대신 대부분의 스마트폰에서 지원하는 가속도센서를 추가로 활용하여 서명이 이루어지고 있는 동안 스마트폰의 동적인 움직임의 특징정보를 추출한다. 서명 데이터는 리샘플링을 통해 길이를 맞추고, 일정한 크기로 정규화하여 사용한다. 제안 방법의 성능을 평가하기 위해 테스트셋을 구축하여 단일세션검증, 시간차 검증, 위조서명 검증의 3가지 실험을 실시하였다. 실험결과 위조서명 구분에 있어서 제안방법은 기존 방법보다 EER이 최대 6.9% 더 낮았다. 또한, 서명의 모양과 속도만 사용한 기존의 방식보다 가속도센서를 추가한 방식이 1.5% 나은 성능을 보였고, 최고 3.5%의 에러율을 얻었다.

ABSTRACT

In this paper, we provide an authentication technology for verifying dynamic signature made by finger on smart phone. In the proposed method, we are using the Auto-Encoder-based 1 class model in order to effectively distinguish skilled forgery signature. In addition to the basic dynamic signature characteristic information such as appearance and velocity of a signature, we use accelerometer value supported by most of the smartphone. Signed data is re-sampled to give the same length and is normalized to a constant size. We built a test set for evaluation and conducted experiment in three ways. As results of the experiment, the proposed acceleration sensor value and 1 class model shows 6.9% less EER than previous method.

Keywords: Deep learning, AE, Mobile Signature, One Class, Biometric Recognition

I. 서 론

스마트폰이나 스마트패드와 같은 모바일기기에서 생체인증이 많이 연구되고 있다. 지문이나 목소리, 얼굴 등 정적인 바이오 정보를 이용한 인증에서는 3D프린터로 만들어진 지문[1]이나 녹음된 목소리[2], 사진[3]등을 이용한 위조가 가능하며 한번 노출되면 변경할 수 없다는 문제가 있어, 걸음걸이인식[4], 제스처인식[5] 등 쉽게 흉내 내기 어려운 동적 행위기반 인증에 대한 연구가 활발하다. 스마트폰에

Received(07. 28. 2016), Modified(1st: 09. 19. 2016, 2nd: 10. 05. 2016), Accepted(10. 05. 2016)
* 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No. B0717-16-0084, (K-GSS) 부인방지를 제공하는 FIDO 기반 동적 전자서명 기술)과 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. 2016R1A4A1011761, 핀테크 서비스를 위한 금융 보안 핵심 기술 개발)
† 주저자, tnfok815@kongju.ac.kr
‡ 교신저자, sunchoi@kongju.ac.kr(Corresponding author)

서 동적서명은 쉽게 할 수 있고, 직관적이며, 추가적인 장치를 필요로 하지 않는다. 또한 노출이 되더라도 자유롭게 변경이 가능한 장점이 있다.

모바일에서 동적서명은 스타일러스를 이용하는 방법[6][7]과 손가락을 이용하는 방법이 있다. 스타일러스를 사용하면 휴대 및 관리가 불편하고, 최신형 단말이 아닌 경우, 선을 그을 때 선 끊김 현상이 발생되어 정확하게 인식을 못하는 때가 많다. 따라서 손가락으로 서명하는 것이 편리하고 사용자에게 익숙하므로 최근 모바일 동적서명연구[8][9]는 주로 손가락을 이용한 핑거서명에 초점을 맞추고 있다.

동적서명에서도 어깨너머 훔쳐보기(Shoulder surfing)나, 서명의 자국을 따라 글씨를 본뜨는 얼룩공격(Smudge Attack)같은 위조서명(Skilled forgery)을 가려내는 것이 중요한 이슈이다[8]. 태블릿에서 스타일러스를 사용하는 서명기법[7]에는 위조서명에 대한 내용이 다루어져 있지만, 우리가 아는 범위에서는 핑거서명 방법에서 위조서명을 다룬 연구를 찾을 수 없었다.

우리는 모바일기기의 핑거서명에서 위조서명에 강건한 서명검증기법을 제안한다. 위조서명을 구분하기 위해서는 서명이 이뤄지는 동적인 행위에 대한 특징 정보가 많이 필요하다. 서명 시 서명의 모양, 속도, 펜 압력, 펜 각도 등 다양한 특징 정보를 획득할 수 있는 스타일러스 경우와 달리, 지금까지 모바일핑거서명[9]에서는 서명의 모양이나 속도만이 사용되었다. 스마트폰의 핑거서명에서는 펜 각도, 펜 압력 등의 정보를 얻을 수 없기 때문이다. 하지만 두 가지 정보만으로는 위조서명구분에 충분한 특징 정보를 획득하기 어려우므로 모바일기기에서 활용 가능한 추가적인 특징을 고려할 필요가 있으며, 우리는 거의 모든 스마트폰에서 지원하는 가속도계 정보를 추가적으로 사용한다.

본 논문의 기여점은 다음과 같다. 첫째는 위조서명구분에 강점을 보이는 딥러닝 기반의 1 class classification 기법을 사용한다. 일종의 재생산 네트워크(reproducing network)인 AE(Auto-Encoder)를 사용한 1 class 모델을 이용하여, 위조서명 구분능력을 향상시킨다. 둘째는 가속도센서를 활용한다. 사람마다 서명하는 동작의 특징에 따라 가속도가 다르게 나타나기 때문이다. 셋째 위의 두 방법을 이용해 원본서명, 시간차서명과 위조서명 성능평가를 실험한다. 기존 핑거서명 연구에서는 시간차서명, 위조서명에 대한 성능 평가가 미흡했다.

본 논문의 구성은 다음과 같다. 2장에서는 배경 및 관련연구, 3장에서는 제안 방법, 4장은 실험구성 및 실험결과를 서술했으며, 5장에서 결론 및 향후 연구계획에 대해 서술한다.

II. 배경 및 관련연구

서명이란 본인 고유의 필체로 자신의 서명을 제3자가 알아볼 수 있도록 기재하는 것을 의미한다. 서명은 입력방식에 따라 동적방식과 정적방식이 있다. 정적방식은 오프라인 환경을 말하며 볼펜, 만년필과 같은 서명입력장치를 통해 계약서나 은행거래, 신용카드사용 확인에서 자신을 나타낼 때 사용한다. 정적방식에서 서명인증은 문서에 입력도구(연필, 볼펜, 만년필)로 서명된 이미지를 분석해 검증한다[10][11].

동적방식은 디지털기기(컴퓨터, 디지타이저, 터치스크린)를 이용한 온라인에서 서명하는 방식으로 전자상거래, 전자문서, 출입국관리 용도로 사용된다. 동적방식은 장치별로 마우스, 사인패드, 터치스크린으로 나누어진다. 마우스로 사용하는 방식은 책상, 테이블이나 마우스패드위에서 가상으로 서명하는 방법이고, 사인패드는 서명전용패드에서 스타일러스로 서명하는 방식으로 서명검증을 위해서는 별도의 기기(PC)가 필요하다. 터치스크린은 스크린에 스타일러스나 손가락으로 서명을 하고 기기내부에서 서명검증을 한다.

모바일기기는 터치스크린으로 분류할 수 있으며 서명기구에 따라 스타일러스서명과 핑거서명이 있다. 스타일러스방법은 모바일기기에서 스타일러스도구로 서명하는 방법이다. 그동안 스타일러스를 이용한 서명검증 연구가 많이 실시되었다[12][13]. 핑거서명은 스타일러스 같은 입력도구 없이 손가락으로 서명하는 방법이며 스타일러스보다 이용자가 많고 편리한 장점을 가지고 있다. 핑거서명에서 대표적인 연구는 NYU에서 2014년에 발표한 것이다[8]. [8]에서는 웹브라우저에서 실험자가 1번에 5회를 서명하게 하고 1주일동안 실험샘플을 모았으며, HTML5 플랫폼을 통해 x, y좌표와 시간정보를 저장했으며 97%의 정확도를 보였다. 우리는 위의 논문에서 사용된 특징 정보 뿐만 아니라 가속도센서 정보를 추가해 위조서명 구분에 사용한다.

일반적으로 서명검증에서 위조는 고의위조 및 선택위조로 크게 나누어진다. 선택위조는 일반적으로

본인의 이름에 기반 한 패턴을 사용하는 경우가 많기 때문에 타인서명과의 구별은 비교적 쉬운 편이라 할 수 있다. 그러나 일정 수 이상 사용자가 있는 경우, 닮은 서명도 존재하여 구별하기 어려운 상황이 발생하기도 한다. 한편, 고의위조는 특정인의 서명을 고의적으로 흉내 내는 것으로 어느 정도 연습을 거치면 모양 만으로는 사실상 구별이 어려울 만큼 비슷한 경우도 많다.

서명 검증 방법은 시계열패턴과 전역패턴을 이용하는 방법으로 나눌 수 있다. 시계열 패턴은 구간의 흐름에 따라 서명데이터를 일정한 간격으로 나누어 분석하는 방법으로 DTW(Dynamic Time Warping)[14], RMS(Root Mean Square)[15], 그리고 HMM(Hidden Markov Model)[16] 알고리즘을 적용한 연구가 있었다.

전역패턴은 서명의 전체 데이터의 특징을 비교하여 검증하는 방법으로 SVM(Support Vector Machine)[17], MLP(Multi Layer Perceptron)[18], 그리고 AE(Auto Encoder)[19][20]를 사용한 연구가 있었다.

최근, 높은 성능으로 패턴인식 분야에 각광을 받고 있는 딥러닝 기법을 사용한 연구 중에 Iranmanesh[18]가 서명검증을 위해 2 class모델로 MLP를 사용하여 평균 82.42%의 정확도를 보여주었으나, 위조서명 검증 결과는 제시하지 않았다. Subject와 others를 구분하는 2 class 방법에서는 위조서명이 subject class에 더 가깝게 분류되므로 위조서명 구분에는 1 class 기법이 효과적이다[21]. 그리고 1 class 기법을 사용한 연구로는 Fayyaz[20]가 제안한 AE를 기반한 1 class 모델이 있다. Fayyza는 PDA에서 스타일러스로 서명하였으며, x, y좌표와 시간 그리고 압력센서 정보까지 사용하여 위조서명 구분에 92%의 정확도를 보였다. [20]은 스타일러스를 사용하는 방법으로 핑거서명을 사용하는 논문과 구분되며, 2 class와 1 class 모델의 차이를 제시하지 않고 있다.

본 논문은 모바일기기에서 핑거서명 했을 때 위조서명을 구분하기 위해 1 class 모델이 2 class 모델보다 효과적인 것을 보이고, 시간차서명에 대한 성능 분석을 함께 제시한다.

III. 제안 방법

Fig. 1.은 본 논문에서 구현된 동적서명인식의 처리흐름을 보여준다. 스마트기기의 앱에서 손가락으로 서명하면, 일정한 샘플링 주기로 현재 서명 포인트의 x, y좌표와 이 시점의 x, y, z축의 가속도 센서 값을 측정한다. 측정된 데이터는 같은 길이로 리샘플링하고, 같은 크기로 정규화 하여 데이터 가공을 한다.

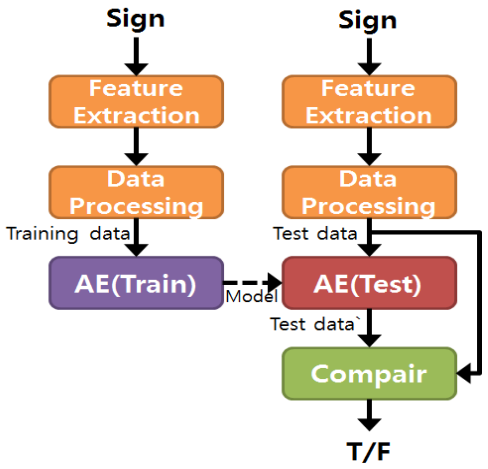


Fig. 1. Overall structure block diagram

서명 학습단계에서는 n개의 서명을 Training data로 이용하여 AE에 학습시켜 서명 모델(Model)을 생성한다. 서명 검증 단계에서는 서명데이터인 Test data를 AE모델에 입력하면 AE에서 이 서명의 재생성 값인 Test data`을 출력한다. Test data와 Test data`의 유사도를 정해진 임계값(Threshold Value)과 비교하여 서명 검증 성공, 실패를 판단한다.

각 단계에 대한 자세한 설명은 다음과 같다.

3.1 데이터 획득

모바일기기에서 서명정보를 획득하는 방법은 스마트폰 앱에서 사용자가 서명을 위해 화면을 터치하면 터치 디바이스 드라이버가 터치이벤트(x, y좌표, 가속도센서값)를 감지하고, 모바일매니저에 저장한다. 모바일매니저는 터치이벤트 정보를 갖게 되며, 서명자가 서명한 모습이 Fig. 2.와 같이 보이게 된다. 입력정보는 사용자가 서명을 입력하는 동안 32ms단위로 주기적으로 샘플링 되기 때문에 시간정보는 따로 필요하지 않다.

$$Sign = (Ax_i, Ay_i, Az_i, x_i, y_i), \; _{i=0,\ldots,n} \quad (1)$$

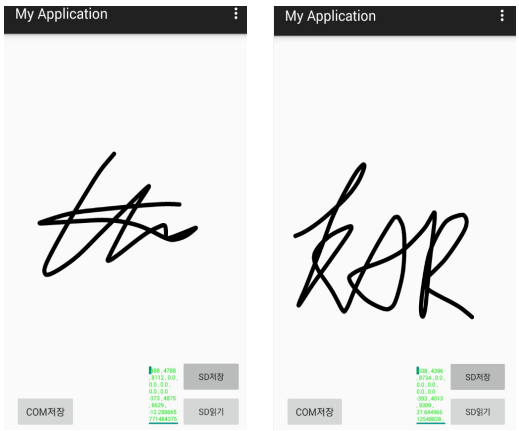


Fig. 2. Original signature

식 1은 32ms 단위로 획득한 센서값의 벡터로 구성된 서명을 보여준다. x,y는 x,y좌표이고, Ax, Ay, Az는 가속도센서의 x, y, z 값이다.

3.2 데이터 정규화

데이터 획득단계에서 획득된 서명 데이터를 가공하여 학습모델에 입력하기 위한 형태로 변환하기 위해 시작점 일치하기, 리샘플링, 크기 정규화를 수행한다. 먼저, 서로 다른 서명의 시작 좌표를 일치시키기 위해 x_i를 비롯한 각 센서값에서 초기값 $(Ax_0, Ay_0, Az_0, x_0, y_0)$을 빼주면 식(2)와 같다.

$$Sign' = (Ax_i - Ax_0,\ Ay_i - Ay_0,\ Az_i - Az_0,\ x_i - x_0,\ y_i - y_0),\ i = 0,\ldots,n \quad (2)$$

$$k_0 = k_1 = n/m$$
$$k_{j+2} = k_{j+1} + k_j,\ j = 0,\ldots,m-3 \quad (3)$$

리샘플링 단계[22][23]에서는 길이가 작은 데이터는 늘리고, 길이가 긴 데이터는 줄여 모든 서명의 길이를 맞추는 작업을 한다. 리샘플링 방법은 식 3, 4와 같이 기술된다.

$$\begin{aligned} &i = 1 \mid i \leq m-2 \\ &\text{if } t \leq k_i < t+1 \\ &x'_i = x_t + (x_{t+1} - x_t) \times (k_i - t) \\ &x'_0 = x_0 \\ &x'_{m-1} = x_{n-1} \end{aligned} \quad (4)$$

여기서, n은 원본 데이터 길이, m은 재생성 데이터 길이, k는 n을 m으로 균등하게 분할하기 위한 비율, t는 임의의 자연수이고 x는 원본서명데이터이다. x'_0와 x'_{m-1}는 처음과 끝에 서명위치를 맞추기 위해 원본 서명 데이터에서 처음과 끝을 그대로 넣어주고 x'_i는 x_i의 리샘플링한 데이터이다.

Fig. 3.은 데이터 정규화 예를 보여준다. (a)는 원본서명데이터이고 (b)는 원본서명에서 리샘플링으로 길이가 변화한 서명을 보여준다. 여기서 '•' 표시는 샘플링된 센서 값의 분포를 나타낸다. (b)는 (a)보다 센서 정보가 많아 분포도가 정밀하게 찍혀 있다. (c)는 (b)에서 0과 1사이로 크기를 정규화한 결과를 보여준다. (b)에서 (c)로 크기가 축소된 것을 볼 수 있다. Fig. 4.의 (a)는 시간 축 따른 X,Y 위치 변화 이고, (b)는 가속도 센서의 위치변화이다.

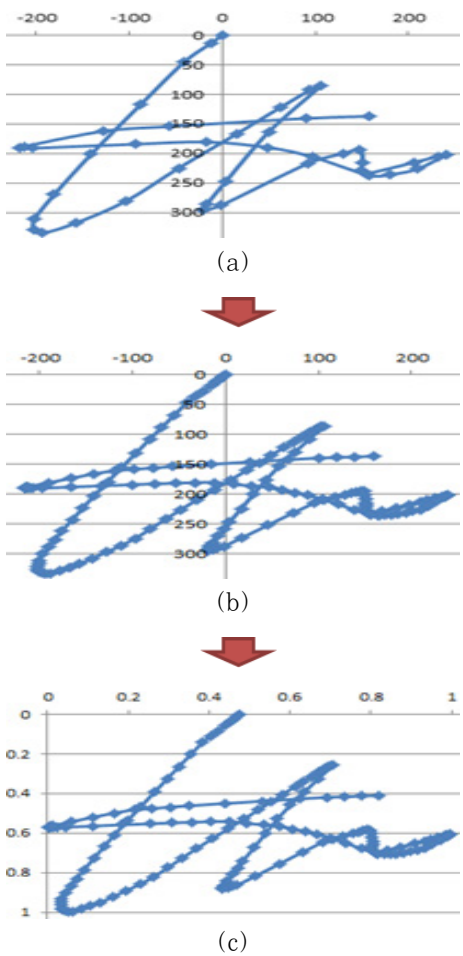
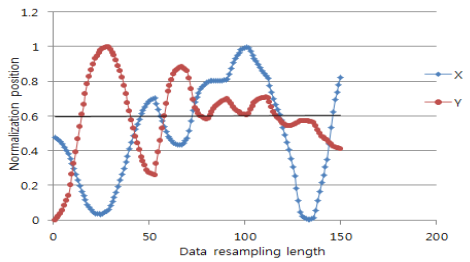
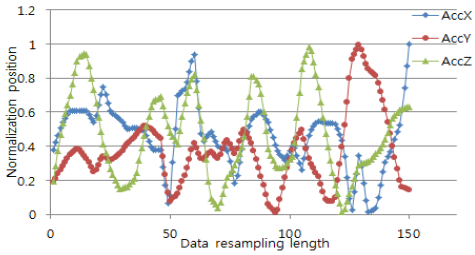


Fig. 3. Signature Preprocessing



(a) X, Y position data



(b)Accelerometer data

Fig. 4. Sample coordinates of position and accelerometer

X,Y좌표의 움직임에 따라서 가속도 센서의 기울기가 크게 변하는 것을 볼 수 있다.

3.3 Auto Encoder 기반 One class 분류모델

본 절에서는 3.2절에서 정규화된 데이터를 이용해 AE 모델을 학습하는 과정을 설명한다. AE는 FNN(Feedforward Neural Network)의 한 종류로 데이터의 내재된 특성을 학습하는 신경망이다. 입력에 유사한 출력을 생성하는데 학습된 데이터와 비슷한 입력에 대해서는 높은 유사도를 갖는 출력을 생성하지만, 그렇지 않은 입력에 대한 출력은 입력과 유사도가 낮다.

제안 방법에서 사용한 AE는 Fig. 5.와 같이 총 5계층으로 구성된다. 서명데이터를 입력받은 입력층 그리고 은닉계층에서 거쳐 새롭게 표현하는 출력계층으로 구성되는 Encoder와 Encoder의 출력계층을 입력계층으로 하여 은닉계층을 거쳐 데이터를 복원하여 출력하는 출력계층으로 구성된 Decoder가 결합된 형태로 구성된다.

AE는 학습(train) 단계에서는 subject의 서명데이터를 입력과 출력으로 동일하게 제공하여 학습하게 되고, 예측(predict) 단계에서는 주어진 서명값에 대해 출력값을 생성하게 된다.

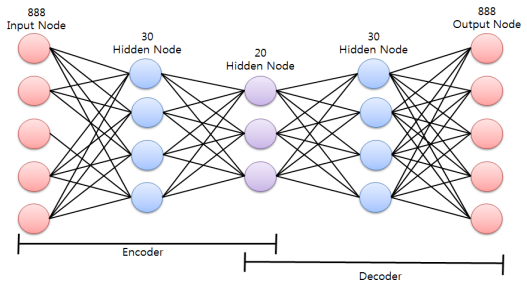


Fig. 5. Structure of Auto-encoder

$$z = \sigma_1(Wx + b) \tag{5}$$

$$x' = \sigma_2(W'z + b') \tag{6}$$

$$L(x,x') = \| x - \sigma_2(W'(\sigma_1(Wx+b)) + b \|^2 \tag{7}$$

식 5, 6, 7[26]은 AE의 학습 단계를 설명하는 식이다. 식 5의 z는 서명데이터 x로부터 AE를 통해 encoding된 결과이고, 식 6에서 x'는 z를 decoding한 결과이며, σ_1, σ_2는 활성화 함수이다. 식 7은 손실 함수(L:Loss Function)이며, AE의 학습 과정은 L을 최소화하는 W와 W'을 찾는 과정이다.

$$Diff = MSE(x,x') \tag{8}$$

$$Diff < t, \quad t : threshold \tag{9}$$

식 8, 9는 서명 검증을 위한 유사도 비교에 기준을 보여준다. AE는 입력된 서명 x에 대해 이를 재생성한 예측값인 x'를 출력하는데 이 둘의 차이인 MSE(Mean Square Error)를 계산하여 정해진 threshold()보다 작으면 검증에 성공하고, threshold보다 크면 검증에 실패하게 된다.

IV. 실 험

현재 국내 외에 다양한 동적 서명인식 연구가 소개되고 있지만, 사인패드나 PDA환경을 위한 테스트셋이 제공되고 있고, 스마트폰에서 손가락으로 서명한 테스트셋은 존재하지 않는다. 따라서 본 논문에서는 자체적으로 테스트DB(Data Base)를 구축하여 실험하였다.

본 장에서는 실험구성과 실험결과를 기술한다.

4.1 실험 구성

실험 데이터를 만들기 위해서 실험자에게 스마트폰을 들고 서명하도록 실시하였다. 실험은 다음과 같이 3가지로 구성된다.

1) 단일 세션
핑거서명에서 성능차이를 비교하기 위해 기존 서명수집방법과 가속도센서를 추가한 제안방법의 서명검증 성능을 비교하고, 제안방법인 SVM과 2 class 모델 그리고 1 class 모델의 성능차이도 비교한다.

2) 시간차 서명
단일 세션에서 서명한 사용자가 시간이 지난 뒤 같은 서명을 했을 때 서명검증의 정확도를 비교한다. 실제 인증이 수행되는 환경에서는 최초에 서명을 등록한 뒤 시차를 두고 사용자를 인증해야 하므로, 본 실험은 중요한 의미가 있다.

3) 위조 서명
다른 사용자가 원래 서명을 보고 따라하는 고의 위조서명을 한 뒤 서명검증에서 이를 구분하는 성능을 분석한다.

실험 데이터는 Table 1.과 같이 구성된다. 단일 세션은 10명에게 20번씩 서명을 받았다. 1 class모델의 경우 이 중 사람 당 10개를 개인별 서명모델 학습데이터로 사용하고 2 class 모델에서는 타인의 서명 10개를 others 학습데이터로 사용하였다. 학습데이터는 3개 실험에서 모두 동일하고, 테스트 데이터만 3개 실험에 따라 다르다. 단일 세션의 경우 나머지 10개의 본인 서명을 subject data로 타인의 서명 180개를 others data로 사용하였다. 시간차 서명에서는 1달 뒤 원본서명과 같은 방법으로 10명에게 20개의 샘플을 수집하여 테스트 데이터로 이용했다. 위조 서명은 원본서명을 본 위조 서명자 5명이 4번씩 서명하여 subject당 20개의 위조 서명을 획득하여 원본서명 중 10개와 함께 테스트 데이터로 사용해 실험하였다.

Table 1. Test Data Set

	Subject	Others
Original sign	10EA (Original sign)	9 User X 20EA (Original sign)
Time difference sign	20EA (1 Months after sign)	9 User X 20EA (1 Months after sign)
Skilled forgery sign	10EA (Original sign)	20EA (Skilled forgery sign)

실험환경은 Android GalaxyS3에서 서명데이터를 추출했고, 데이터 정규화 AE 모델 학습 및 테스트는 Ubuntu 15.04에서 Python으로 구현했다. AE 모델을 Python Theano기반의 Keras 라이브러리를 이용하였으며, Titan X GPU를 사용하여 학습속도를 높였다.

AE의 구조는 입력층에서 888개의 노드, 은닉층은 30개의 노드, 출력층은 20개의 노드로 구성된 encoder와 중간노드 20개, 은닉층은 30개의 노드, 출력층은 888개의 노드로 구성되어 있으며, 활성화함수(Activation function)는 relu[27]를 사용하였고 Training optimizer로는 RMSprop [28]을 사용하였다. Training 회수는 500 epoch을 수행하였다.

서명 검증에 대한 평가척도는 임계값을 변경하면서 EER(Equal Error Rate)을 측정하였다. FAR(False Acceptance Rate)은 본인의 것이 아닌 생체인식 정보를 본인의 것으로 잘못 판단할 확률을 의미하며, FRR(False Rejection Rate)은 본인의 생체정보를 본인이 아닌 것으로 잘못 판단할 확률을 말한다. EER은 FAR과 FRR이 같아지는 비율을 뜻하고 EER이 가장 낮은 지점을 측정하였다[29].

4.2 실험 결과

4.2.1 단일 세션

단일 세션에서 Data1은 x, y축 정보와 거리정보를 특징값으로 사용한 데이터이고, Data2는 여기에 가속도센서 값을 추가한 데이터이다. Table 1.은 제안 방법인 AE 모델을 이용하였을 때 가속도센서의 유무에 따른 서명검증 성능 실험결과를 보여준다. Data1에서는 Fig. 6.과 같이 EER 5%, Data2에서는 Fig. 7.과 같이 3.5%의 EER을 보여준다. 제안방법인 가속도계를 추가한 결과가 1.5% 더 나은 성능을 얻었다. 이러한 성능은 기존 연구[8]와 동등한 수준이다.

Table 2. Acceleration sensor comparison

	Data1	Data2
AE	5%	3.5%

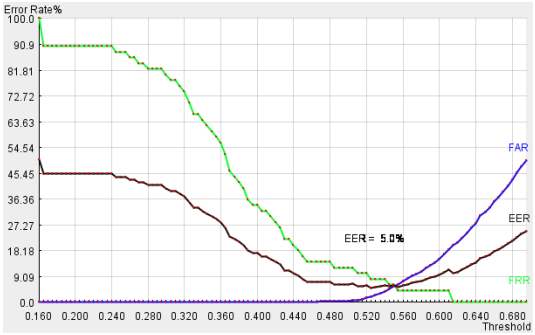


Fig. 6. Result of AE(Data 1)

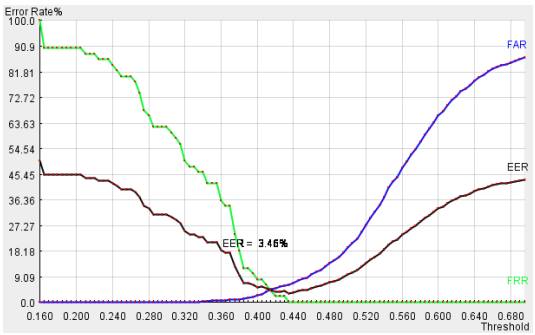


Fig. 7. Result of AE(Data 2)

Data1은 x, y축 정보와 거리정보를 특징값으로 사용한 데이터이고, Data2는 여기에 가속도센서 값을 추가한 데이터이다. Table 2.는 제안 방법인 AE 모델을 이용하였을 때 가속도센서의 유무에 따른 서명검증 성능 실험결과를 보여준다. Data1에서는 Fig. 6.과 같이 EER 5%, Data2에서는 Fig. 7.과 같이 3.5%의 EER을 보여준다. 제안방법인 가속도계를 추가한 결과가 1.5% 더 나은 성능을 얻었다. 이러한 성능은 기존 연구[8]와 비슷한 수준을 보여준다. 그리고 실험에 의해 얻어 ROC(Receiver Operation Characteristic) 곡선을 Fig. 8.에 나타냈다. 그림에서 보여 지는 것과같이 Data2가 Data1보다 EER이 작고 성능이 향상되어 진 것을 볼 수 있다.

다음 실험으로 2 class 모델인 SVM, MLP 그리고 제안방법인 1 class AE 모델의 서명 검증 정

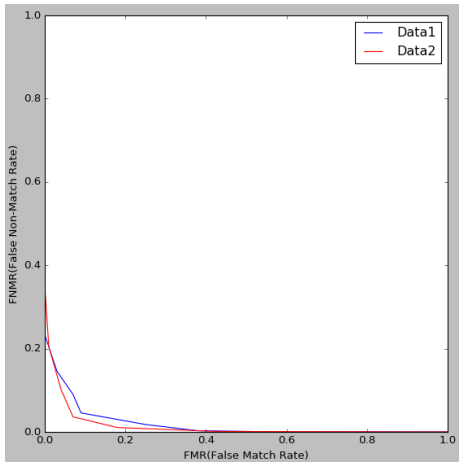


Fig. 8. ROC Curve of Data1, Data2

확도를 비교한다. SVM은 scikit learn 라이브러리를 사용하였으며, Gamma값으로 0.001을 사용하였다. MLP는 Keras 라이브러리를 사용했다. 888 노드의 입력 계층을 갖고 각 128개 노드를 갖는 7 개 은닉 계층을 사용했으며, 2개의 출력 계층을 갖는다. RMSprop을 optimizer로 relu를 activation함수로 각각 사용했다.

Table 3.에서 보는 바와 같이 SVM은 4.7%의 오류율을 보였으며, 2 class MLP는 3.8%의 오류율를 보였다. 1 class 모델인 AE는 3.5%의 오류율을 보여준다. 실험에서 보여준 결과는 AE가 SVM과 MLP보다 1.2%와 0.3%의 높은 정확도를 보여주었다.

Table 3. Comparison of SVM, MLP and AE

	SVM	MLP	AE
Data2	4.7%	3.8%	3.5%

4.2.2 시간차서명 비교

Table 4.는 시간차서명검증 결과를 보여준다. MLP에서는 Data1은 8.2%와 Data2는 9.1%의 오류율을 보였으며, AE는 Data1에서 9%, Data2

Table 4. Time different comparison

	Data1	Data2
MLP	8.2%	9.1%
AE	9%	7.7%

에서는 7.7%의 오류율을 보여준다. 시간차 서명에서는 Data2에서 AE가 1.4%의 나은 결과를 보였다.

4.2.3 위조서명 비교

위조서명에서 Table 5.는 위조서명 구분 실험 결과를 보여준다. MLP에서 Data1은 25%와 Data2는 18.1%의 EER을 나타냈으며, AE에서는 학습한 결과 Data1은 19.3% Data2는 13.7%의 EER을 보여준다. Data1과 Data2에서 모두 AE가 평균 5% 높은 정확도를 보여 주었다. 위조서명을 구분하는데 있어 제안방법인 1 class AE 모델이 기존의 2 class 모델 보다 높은 성능을 보여, 위조 서명 구분에는 1 class 모델이 효과적임을 알 수 있다. 또한 제안방법인 가속도센서값이 추가된 Data2가 Data1보다 5.6% 향상된 정확도를 보이고 있다.

Table 5. Skilled forgery comparison

	Data1	Data2
MLP	25%	18.1%
AE	19.3%	13.7%

V. 결론 및 향후 연구계획

본 논문에서는 모바일환경에서 손가락으로 서명한 동적서명을 검증하는 방법을 제안하였다. 특히, 위조서명 검증에 효과적으로 생각되는 방안으로 1) 가속도센서값의 활용 2) 1 class 모델 사용을 제안하였다. 첫 번째 제안 방안에 대한 결과로 스마트폰에서 활용할 수 있는 동적 서명의 특징 정보인 서명시 가속도센서값을 추가하여 위조서명 실험데이터 대해 가속도값을 활용하지 않았을 때보다 6% 향상된 정확도를 얻을 수 있었다. 스마트폰에서 핑거서명시 활용할 수 있는 동적 특징정보가 스타일러스 사용시 보다 부족한 상황에서, 가속도센서값의 활용이 위조서명 검증에 효과가 있음을 입증하였다. 두 번째 제안 방안인 1 class 모델의 사용결과, 위조서명 구분에 있어 1 class AE 모델은 2 class MLP모델 보다 5% 향상된 결과를 보여 제안방법의 효과를 보였다. 두가지 방안이 모두 사용된 경우 기존 방법보다 11%의 성능향상을 얻을 수 있었다.

향후 연구로는 가속도센서의 경우 파지상태에 따라 변화하기 때문에 손에 쥐고 있는 상태와 책상에 놓고 서명하는 미파지 상태를 구분하여 모델을 적용하는 방식과 모바일기기에서 활용할 수 있는 자이로센서를 추가하여 동적서명의 특징을 추가로 확보하고 주기적 샘플링 데이터로부터 획수, 멈춤 등의 동적 특징을 추가로 추출하는 방식으로 성능을 개선할 수 있을 것으로 기대된다. 또한, 서명의 부분 특징을 구조화하여 모델링할 수 있는 CNN(Convolutional Neural Network)와 위조서명에 강건한 AE 모델을 결합하는 방법을 시도해 볼 것이다.

References

[1] S.S. Arora, et al, "3D fingerprint phantoms," *Proc. of 22nd Int. Conf. on Pattern Recognition*, pp. 684 - 689, Sweden, Aug. 2014.

[2] H. Malik and H. Farid, "Audio Forensics from Acoustic Reverberation," *Proc. IEEE Int'l Conf. Acoustics, Speech, Signal Processing.* pp. 1710-1713, USA, March 2010.

[3] T. Fladsrud, "Face recognition in a border control environment: Non-zero effort attacks effect on false acceptance rate," Master thesis, Gjovik Univ. College, Norway, 2005.

[4] D. Kim and J. Paik, "Gait recognition using active shape model and motion prediction," *Computer Vision IET*, vol. 4, no. 1, pp. 25-36, March 2010.

[5] M. C. Thomas and A. P. M. S. Pradeepa, "A comprehensive review on vision based hand gesture recognition technology," *International Journal of Research in Advent Technology*, Vol. 2, no. 1, pp.303-310, January, 2014.

[6] R. P. Krish, J. Fierrez, J. Galbally and M. Martinez-Diaz, "Dynamic Signature Verification on Smart Phones," *In Communications in Computer and Information Science*, vol 365, pp.213-222. 2013.

[7] M. Martinez-Diaz, J. Fierrez, J. Galbally and J. Ortega-Garcia, "Towards mobile

authentication using dynamic signature verification: useful features and performance evaluation," *In Proceedings of the International Conference on Pattern Recognition, ICPR*, pp.1 - 5, Dec. 2008.

〔8〕 N. Sae-Bae and N. Memon, "Online signature verification on mobile devices," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 6, pp.933 - 947, Jun. 2014.

〔9〕 N. Paudel, M. Querini and G. F. Italiano, "Handwritten Signature Verification for Mobile Phones," *International Conference on Information Systems Security and Privacy(ICISSP)*, pp46-52, 2016.

〔10〕 M. A. Ferrer, J. B. Alonso, and C.M. Travieso, "Offline geometric parameters for automatic signature verification using fixed-point arithmetic," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 27, no. 6, pp.993 - 997, Jun. 2005.

〔11〕 R. Kumar, J.D. Sharma and B. Chanda, " Writer-independent off-line signature verification using surroundedness feature," *Pattern Recognition Letters*, vol. 33, no. 3, pp.301-308, Feb. 2012.

〔12〕 G. Dimauro, S. Impedovo, M.G.Lucchese, R.Modugno and G. Pirlo, "Recent Advancements in Automatic Signature Verification," *Int'l Workshop on Frontiers in Handwriting Recognition(IWFHR)*, pp. 179-184, Oct, 2004.

〔13〕 N. Li, J. Liu, Q. Li and X. Luo, "Online Signature Verification Based on Biometric Features," *International Conference on System Sciences*, pp. 5527-5534, Jan. 2016.

〔14〕 A. Fischer, M. Diaz, R. Plamondon and M.A. Ferrer, "Robust score normalization for DTW-based on-line signature verification," *International Conference on document analysis and recognition*, pp.241 - 245, Aug. 2015.

〔15〕 W.S. Wijesoma, M. Mingming and K. W. Yue, "On-line signature verification using a computational intelligence approach," *Lecture Notes in Computer Science Springer-Verlag*, vol. 2206, pp.699 - 711, Oct. 2001.

〔16〕 S.Y. Ryu, D.J. Lee, M.G. Chun, "A Robust On-line Signature Verification System," *International Journal of Fuzzy Logic and Intelligent Systems*, vol. 3, no. 1, pp.27-31, 2003.

〔17〕 C. Gruber, et al, "Online Signature Verification With Support Vector Machines Based on LCSS Kernel Functions," *IEEE Transactions on Systems Browse Journals & Magazines*, Vol. 40, No 4, pp.1088 - 1100, Aug. 2010.

〔18〕 V. Irnmanesh, et al. "Online Signature Verification Using Neural Network and Pearson Correlation Features", *IEEE Conference on Open Systems (ICOS)*, pp.18-21, Dec. 2014.

〔19〕 A. Makhzani and B.J. Frey, "Winner-take-all autoencoders," *Neural Information Processing Systems(NIPS)*, pp.2773-2781, CANADA, Dec. 2015.

〔20〕 M. Fayyza, et al. "Online Signature Verification Based on Feature Representation," *IEEE Artificial Intelligence and signal Processing*, pp.211-216, Mar. 2015.

〔21〕 D.I. Chae, et al, " Hidden Singer Contest: Auto-encoder based singer Identification," *Joint Conference on communications and Information (JCCI)*, pp.629-632, Apr. 2016.

〔22〕 P.O. Kristensson, T. Nicholson, and A. Quigley, "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.

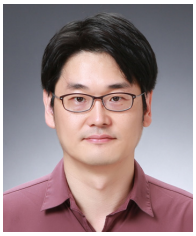
〔23〕 P.O. Kristensson and L.C. Denby,

"Continuous recognition and visualization of pen strokes and touch-screen gestures," *Proc. of Euro graphics Symposium on Sketch-Based Interfaces and Modeling*, pp.95-102, 2011.
〔24〕 R. Reed and R. Marks, "Neural smithing supervised learning in feedforward artificial neural networks," Cambridge MA: MIT press, 1999.
〔25〕 A. Krizhevsky and G.E. Hinton, "Using very deep autoencoders for content-based image retrieval", *In Proceedings of the European Symposium of Artifical Neural Networks*, pp.489-494, Belgium. 2011.
〔26〕 https://en.wikipedia.org/wiki/Autoencoder
〔27〕 A. Krizhevsky, I. Sutskever and G. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks", *In Neural Information Processiong Systems*. 2012.
〔28〕 Y. N. Dauphi, H. D. Vries and Y. Beigio, "Equilibrated adaptive learning rates for non-convex optimization", *arXiv preprint arXiv:2502.04390*, 2015.
〔29〕 https://en.wikipedia.org/wiki/Biometrics

〈저 자 소 개〉

남 승 수 (Sungsoo Nam) 학생회원
2012년 2월: 공주대학교 응용수학과(이학사)
2014년 8월: 공주대학교 융합과학과(공학석사)
2014년 8월~현재: 공주대학교 융합과학과 박사과정
〈관심분야〉 영상처리, 딥러닝, 정보보호

서 창 호 (Changho Seo) 종신회원
1990년 2월: 고려대학교 수학과 졸업(학사)공학석사
1992년 2월: 고려대학교 수학과(석사)
1996년 8월: 고려대학교 수학과(박사)
1996년 8월~2000년 2월: 한국전자통신연구원 선임연구원, 팀장
2000년 3월~현재: 공주대학교 응용수학과 교수
〈관심분야〉 암호알고리즘, PKI, 무선 인터넷 보안 등



최 대 선 (Daeseon Choi) 종신회원
1995년 2월: 동국대학교 컴퓨터공학과 학사
1997년 2월: 포항공과대학교 컴퓨터공학과 석사
2009년 1월: 한국과학기술원 전산학과 박사
1997년 1월~1999년 6월: 현대정보기술 선임
1999년 7월~2015년 8월: 한국전자통신연구원 인증기술연구실 실장/책임연구원
2015년 9월~현재: 공주대학교 의료정보학과 부교수
2016년 현재: 정보보호학회 이사
〈관심분야〉 인증, 개인정보보호, 이상거래탐지, 의료정보보안, 머신러닝