모바일 터치스트로크 데이터를 이용한 2-class Maxtreme Learning Machine(MLM)

최석민, 테오벵진*
*연세대학교 전기전자공학부
e-mail : smchoi90@yonsei.ac.kr

2-class Maxtreme Learning Machine(MLM) for Mobile Touchstroke using Sequential Fusion

Seok-Min Choi, Andrew Beng-Jin Teoh*
*School of Electrical and Electronic Engineering, Yonsei University

요 약

핸드폰 사용자가 늘어나면서 이와 관련하여 개인 정보 보안에 대한 중요성이 대두되고 있다. 이에 따라 제안된 알고리즘은 Extreme learning machine 으로부터 착안하여 변형하여 고안한 Maxtreme Learning Machine(MLM)으로, 사용자들의 터치 스트로크 특성 벡터를 제안 알고리즘으로 학습하여 사용자들을 검증한다. 또한 특성 벡터의 순차적 융합 기법을 이용하여 더 많은 정보를 바탕으로 사용자를 높은 정확도로 검증 할 수 있다.

1. 서론

처음 스마트 폰이 나온 지 10 년 정도가 지난 지금, 휴대폰은 우리의 삶과 밀접하게 연관되어 있다. 예전의 휴대폰 보안은 주로 비밀번호, 패턴 등 주로 로그인 화면에서 한번만 인증을 하면 되었다. 하지만, 첫 화면에서만 인증을 하는 것의 한계가 야기되었고, 그에 따라 연속적 검증이라는 절차가 제기됐다. 특별한 추가 장치가 필요한 홍채 인식[1], 지문 인식[2]과는 달리 사용자가 휴대폰을 사용하는 매 순간 압력센서, 휴대폰의 터치 좌표 등 내재된 API 를 이용하여 연속적으로 검증 할 수 있는 터치 스트로크가 새로운 모바일 보안 메커니즘 중 하나로 떠오르고 있다. 사용자의 가공되지 않은 터치 데이터를 제공 받아 특징 추출을 하여 분류기를 통해 실 사용자인지 아닌지를 검증한다. 하지만 터치 데이터는 지문 혹은 홍채인식보다 취약한 정보를 제공하기 때문에, 우리는 더 많은 연속적인 스트로크를(특성 벡터) 받아 융합을 하여 더 많은 정보를 바탕으로 검증을 시도하였다.

2. 본론

이 연구는 Touchanalytic dataset[3]을 이용하여 진행하였다. 우선 28 개의 특징들이 가공되지 않은 터치 데이터로부터 추출되어 28 차원을 형성하였다. 한 개 이상의 데이터가 연속적으로 들어오면, 순차적 융합 기술을 적용하여 더 풍성한 정보를 얻을 수 있었고, 그 후 2 클래스 분류 단계로 넘어간다.

2.1 Maxtreme Learning Machine

Maxtreme Learning Machine(MLM)은 Extreme Learning Machine(ELM)[4]으로부터 영감을 받아 만들게 되었다. 이 것은 단일 은닉 층으로 구성되어 있으며, 반복적 훈련 알고리즘으로부터 자유롭다. 입력층과 은닉 층은 가우시안 분포의 임의 숫자를 할당하여 웨이트를 준다. 은닉 층에서의 활성 함수는 흔히 쓰는 시그모이드 혹은 하이퍼볼릭 함수 대신 맥스 아웃[5] 활성 함수를 사용하였다. 즉 랜덤 맥스 아웃 활성 함수를 이용하여 28 차원의 데이터를 보다 더 높은 차원으로 투영한다. 고차원으로 투영 된 값들은 맥스 아웃 활성 함수를 이용하여 각 깊이의 가장 큰 값들을 선택하고, 그 값들은 정규화와 비례 축소 과정을 통해 최종 출력 층의 입력이 된다. 은닉 층과 출력 층의 사이 웨이트는 최소 제곱법을 이용하여 해석학적으로 측정하였다. 반복적 훈련 알고리즘을 사용하지 않는 MLM 모델을 이용하여 검증할 때에는 훈련 단계 때 쓰이지 않았던 실험 데이터를 사용하여 이전의 학습 된 웨이트를 이용하여 2 클래스 분류작업을 시행하였다. 실 사용자의 목표 라벨은 1 로, 그 외 목표 라벨은 0 으로 설정하였다. 기준치를 정하여 1 에 가까우면 시험 데이터는 실 사용자로 판별되고, 0 에 가까우면 거짓 사용자로 판별이 된다.

2.2 특징 벡터의 순차적 융합 기술

논리적으로, 오직 하나의 스트로크만을 이용하여 검증하는 것은 결과를 신뢰 할 수 없기에 여러 개의 순차적 스트로크를 사용하는 것이 이 작업에 적절하다. [4]에서는 출력 층에서 나온 순차적인 결과 값들을 모아서 평균을 냄으로써 융합을 하였다. 하지만 여기에서는 출력 층이 아닌 입력 층에서 순차적인 스트로

크 자체를 모아 평균을 냄으로써 융합을 하였다. 사용자로부터 얻어지는 터치 스트로크는 시간 의존적인 경향이 있기 때문에, 출력 단에서 순차적 융합 기술을 적용 하는 것 보다는 입력 단 이전의 특성 벡터를 (터치 스트로크) 사용하여 순차적 융합 기술을 적용하는 것이 더 풍성한 정보를 제공하기 때문이다. 우리는 연속적인 p 스트로크 벡터들을 모아 특성 벡터들의 평균을 내는 방향으로 실험을 진행하였다. 실험에서는 p 를 1 부터 15 까지 순차적으로 변화시키며 결과를 관찰하였다.

2.3 실험 설정과 데이터 세트

앞에서 언급했던 Touchanalytic dataset[1]가 터치 데이터 중 널리 사용되는 데이터이며, 충분한 스트로크와 피험자가 있어 선택을 하였다. 데이터 세트는 총 21,158 개의 터치 스트로크와 41 명의 피험자로 구성되어있다. 그리고, 이 데이터 셋은 7 개의 세션과 3 가지의 시나리오로 구성되어 있는데, 이번 실험은 그 중 5 개의 세션과 하나의 시나리오만 채택하여 진행하였다. 각각의 스트로크에는, 28 개의 기능적인 특성들이 있다. 하지만 28 개의 특징들이 전부 다 같은 단위를 같는 것이 아니기 때문에, 정규화와 비례 축소 과정을 거칠 할 필요가 있다. 우리는 모든 특징의 값들을 최소-최대 비례축소법과 L2 정규화 과정을 통해 [0 1] 범위에 있도록 하였다.

MLM 에는 은닉 노드의 개수 (N), 맥스아웃 활성함수의 깊이 (d), 그리고 최소 제곱 원리에 사용되는 정규화 상수 (λ), 이렇게 3 개의 조작 가능한 변수가 있다. 이 실험에서 λ는 0.01 로 고정을 시켰고, d={1,30,50}, 그리고 N={10, 100, 300} 으로 설정하여 최적의 변수를 찾고자 하였다..

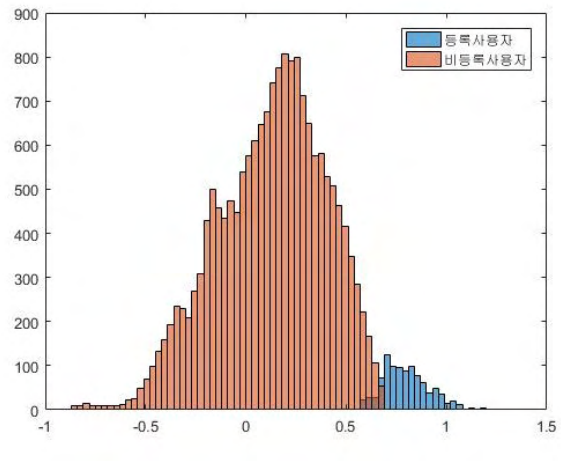
성능의 지표로는 생체 인식 시스템에서 가장 널리 사용되는 동일 오류율, 오수락률과 오거부율을 사용하였다. 동일 오류율은 오수락률과 오거부율이 일치하는 지점으로 생체 인식 시스템의 정확성 지표로 사용된다. 주로 동일 오류율이 낮을수록 시스템이 견고하다고 말 할 수 있다. 오수락률과 오거부율의 수식은 다음 수식과 같다.

오수락률(%) =
잘못 수락한 것의 갯수 / 비등록자 샘플 개수 (1)
오거부율(%) =
잘못 거부한 것의 개수 / 등록자 샘플 개수 (2)

MLM 은 입력-은닉 층에서 가우시안 분포로 이루어진 임의 숫자를 웨이트에 할당하기 때문에, 우연히 좋은 결과를 얻을 수 있는 경우를 배제하기 위해 서로 다른 임의 숫자를 세 번 할당하여 반복 진행하였다. 그렇게 해서 나온 세 번의 결과값과 전체 사용자의 결과값을 중앙값으로 평균을 내어 전체적인 퍼포먼스를 측정 할 수 있었다.

2.4 실험 결과

이번 실험 결과에 사용된 5 개의 세션과 그에 따른 시나리오는 피험자가 진행한 세션과 세션 사이 비교적 적은 시간간격을 가지고 있거나 전체 세션 내의

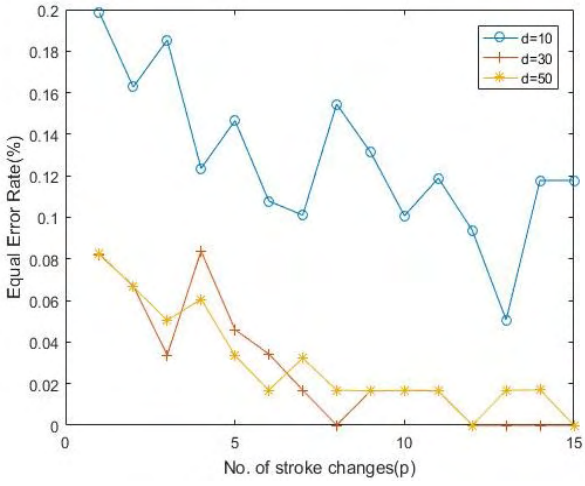


(그림 1). MLM 으로 학습한 후 등록 사용자와 비 등록 사용자의 히스토그램

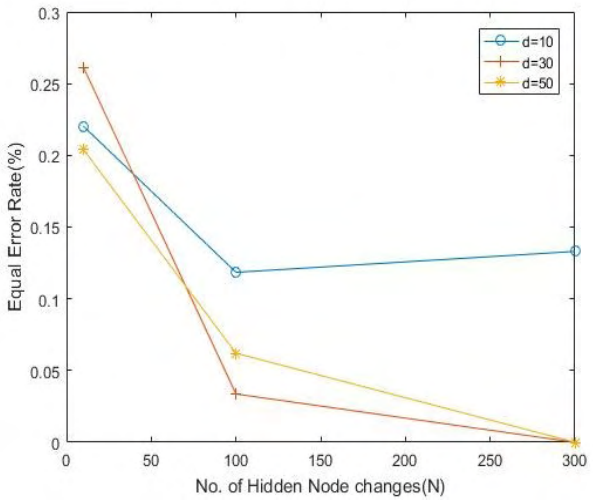
상황에서도 제안된 알고리즘이 검증을 제대로 할 수 있는지가 주된 관심 사항이었다. (그림 1)은 특정 사용자를(14 번 사용자) 등록하고 MLM 으로 학습을 시킨 후의 14 번 사용자의 시험 데이터와 비 등록 사용자들의(14 번 제외한 사용자들) 히스토그램을 나타낸다.

이와 같이 사용자들의 터치 스트로크를 사용해서 MLM 으로 학습시킨 후 **2.3** 에서 정한 변수를 이용하여 은닉 노드(N)를 변화시켜 총 9 가지의 결과를 얻었다. (N = {10,100,300} 과 d = {1,30,50}의 9 가지 경우) 그리고 연속적인 스트로크(p)를 변화시켰을 때는 총 45 가지의 결과값이 나오게 된다. (p = {1,2,…,15}와 d = {1,30,50}의 15 가지 경우). 아래의 (그림 2) 와 (그림 3)은 각각의 p 에 대해 d 와 N 이 달라짐에 따라 동일 오류율 양상이 어떻게 나타나는지 눈으로 확인 할 수 있도록 그래프화 시켰다.

(그림 2)를 실험하는 데에 걸린 총 경과시간은 12312.15 초다. (그림 2)을 보면 (d=30, p=12)에서 동일 오류율이 0 에 도달했음을 알 수 있다. d = 30 일 때의 12 개이상의 순차적인 터치 스트로크를 사용해서 융합 기술을 이용하면 동일 오류율이 0 에 수렴



(그림 2). 연속적인 스트로크 (p)에 따른 동일 오류율의 변화 (λ=0.01, N=200)



(그림 3) 은닉 노드 (N)에 따른 동일 오류율의 변화 (λ=0.01, p=11)

한다. d = 10 일 때에는 깊이가 상대적으로 얕기 때문에 맥스 아웃 활성 함수가 잘 작동하지 않기에 동일 오류율이 다른 경우보다 높음을 확인 할 수 있었다. d = 50 일 때에는 깊이가 상대적으로 깊고, 특정 p 이후부터는 융합되어진 정보가 많기 때문에, 과적합의 문제가 발생하여 동일 오류율이 어느 수준 이하로는 떨어지지 않는 경향을 보인다.

(그림 3)은 연속적인 스트로크를 p = 11 로 고정시키고 은닉 노드가 달라졌을 때의 동일 오류율이다. (그림 3)에 소요된 전체 경과 시간은 3697.55 초이다. 은닉 노드를 증가시켰을 때 N = 100 까지는 모두가 감소하는 경향을 보인다. 하지만 N = 100 에서 N = 300 까지의 경향을 보면 d=10 일 때는 동일오류율이 0.1185 에서 0.1330 으로 다시 증가한다. 이는 깊이가 상대적으로 얕기 때문에 더 높은 차원으로 투영시켜도 시험 데이터에 대하여 제대로 검증을 못하기 때문이다. 남은 두 가지의 경우엔 동일 오류율이 0 에 수렴하는 것을 알 수 있다.

3. 결론

이 학술지에서는 우리는 ELM 으로부터 영감을 받아 새로운 활성 함수를 이용한 MLM 모델을 만들게 되었다. 또한 입력 층 이전의 하나 이상의 특성 벡터를 순차적 융합 기술을 이용하여 분류 단계에서의 의사 결정을 좀 더 많은 정보를 바탕으로 할 수 있게끔 설계하였다. 더 많은 순차적 터치 스트로크를 모을수록 더 낮은 동일 오류율을 보임을 확인하였다. 입력층과 은닉 층 사이는 지엽적 선형의 임의 투영하는 맥스 아웃 활성 함수를 사용하였다. 은닉 층과 출력층은 최소 제곱 원리를 이용하여 학습할 때에 오차역전파법과 같은 반복적 학습이 필요하지 않다. 이번 실험을 토대로 은닉 층을 하나 더 추가하거나, 융합 기술을 은닉 층에 적용시켜보는 등 여러 가지 방향으로 발전시킨다며 더 적은 정보를 바탕으로 높은 성능을 낼 것으로 기대된다.

참고문헌

[1] R. P. Wildes, “Iris recognition: an emerging biometric technology,” Proceedings of the IEEE, vol. 85, no. 9, pp. 1348–1363, Sep. 1997.

[2] L. Coetzee and E. C. Botha, “Fingerprint recognition in low quality images,” Pattern Recognition, vol. 26, no. 10, pp. 1441–1460, Oct. 1993.

[3] M. Frank, R. Biedert, E. Ma, I. Martinovic and D. Song, "Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication", IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, pp. 136-148, 2013.

[4] G. Huang, Q. Zhu and C. Siew, "Extreme learning machine: Theory and applications", Neurocomputing, vol. 70, no. 1-3, pp. 489-501, 2006.

[5] I. J. Goodfellow, D. Warde-farley, M. Mirza, A. Courville, and Y. Bengio, “Maxout networks,” in In ICML, 2013.