(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2020년05월12일
(11) 등록번호 10-2110049
(24) 등록일자 2020년05월06일

(51) 국제특허분류(Int. Cl.)
G06F 21/56 (2013.01) *G06F 21/36* (2013.01)
(52) CPC특허분류
G06F 21/56 (2013.01)
G06F 21/36 (2013.01)
(21) 출원번호 10-2018-0126279
(22) 출원일자 2018년10월22일
심사청구일자 2018년10월22일
(65) 공개번호 10-2019-0129672
(43) 공개일자 2019년11월20일
(30) 우선권주장
1020180053965 2018년05월10일 대한민국(KR)
(56) 선행기술조사문헌
KR1020150092441 A*
Muhammad Shahzad et al, "Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures", Proceedings of the 19th Annual International Conference on Mobile Computing & Networking(2013.10.)
Vincent Huang et al, "Enhanced Experience Replay Generation for Efficient Reinforcement Learning"(2017.06.)
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
김용국
경기도 성남시 분당구 정자일로 15, 102동 1203호(금곡동, 분당하우스토리)
신상윤
서울특별시 노원구 덕릉로 459-18, 101동 511호(상계동, 미도아파트)
(74) 대리인
송인호, 윤형근, 최영중, 최관락

전체 청구항 수 : 총 15 항 심사관 : 정성훈

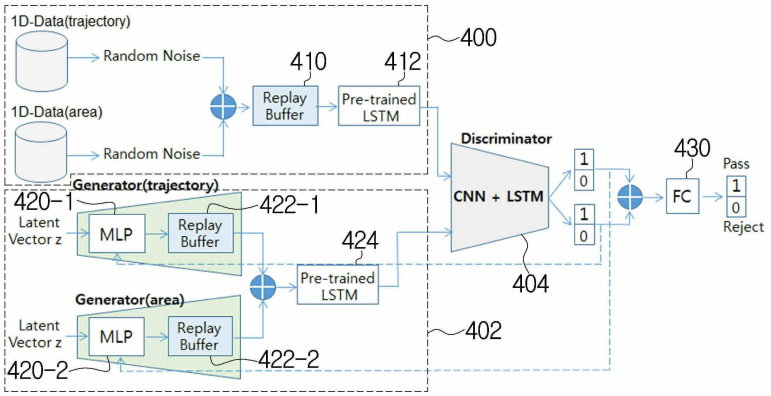
(54) 발명의 명칭 **신경망 기반 패턴 인증 방법 및 장치**

(57) 요 약

본 발명은 신경망 기반 패턴 인증 장치 및 방법을 개시한다. 본 발명에 따르면, 제1 패턴에 대해 사용자가 복수회 입력한 패턴 데이터인 원본 데이터의 특징값을 입력하는 원본 데이터 입력부, 임의의 노이즈를 이용하여 상기 원본 데이터에 대응되는 비교 데이터를 생성하는 비교 데이터 생성부 및 상기 원본 데이터의 특징값과 상기 비교

(뒷면에 계속)

대 표 도 - 도4



데이터의 특징값을 통해 학습이 수행되어 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값 및 상기 제1 패턴에 대해 상기 사용자가 입력한 패턴 데이터와 제3자가 입력한 패턴 데이터에 대한 통과 여부를 결정하는 판별부를 포함하되, 상기 비교 데이터 생성부는 상기 판별부의 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값을 피드백 받아 갱신된 비교 데이터를 생성하는 신경망 기반 패턴 인증 장치가 제공된다.

이 발명을 지원한 국가연구개발사업

과제고유번호	1711065881
부처명	과학기술정보통신부
연구관리전문기관	정보통신기술진흥센터
연구사업명	정보보호핵심원천기술개발
연구과제명	(창조씨앗 2단계)딥러닝 기반 사용자 행동정보 분석을 통한 인증 및 시스템 내 이상행동 탐지 기술 개발
기 여 율	1/1
주관기관	세종대학교 산학협력단
연구기간	2018.01.01 ~ 2018.12.31

명 세 서

청구범위

청구항 1

신경망 기반 패턴 인증 장치로서,

제1 패턴에 대해 사용자가 복수 회 입력한 패턴 데이터인 원본 데이터의 특징값을 입력하는 원본 데이터 입력부;

임의의 노이즈를 이용하여 상기 원본 데이터에 대응되는 비교 데이터를 생성하는 비교 데이터 생성부; 및

상기 원본 데이터의 특징값과 상기 비교 데이터의 특징값을 통해 학습이 수행되어 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값 및 상기 제1 패턴에 대해 상기 사용자가 입력한 패턴 데이터와 제3자가 입력한 패턴 데이터에 대한 통과 여부를 결정하는 판별부를 포함하되,

상기 비교 데이터 생성부는 상기 판별부의 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값을 피드백 받아 갱신된 비교 데이터를 생성하되,

상기 원본 데이터 입력부는,

상기 패턴 데이터에 임의의 노이즈가 부가된 데이터를 임시 저장하는 리플레이 버퍼; 및

상기 리플레이 버퍼에 저장된 데이터에서 미리 설정된 구간의 샘플 포인트에서의 특징값을 이용하여 상기 구간의 다음 샘플 포인트에서의 특징값을 예측하는 예측부를 포함하는 신경망 기반 패턴 인증 장치.

청구항 2

제1항에 있어서,

상기 패턴 데이터는 터치스크린에 표시되는 복수의 포인트 중 일부 포인트를 지나가도록 연속적으로 터치하는 동안의 터치 궤적 및 터치 면적 중 적어도 하나를 포함하는 신경망 기반 패턴 인증 장치.

청구항 3

제2항에 있어서,

상기 터치 면적은 상기 연속적으로 터치하는 동안 복수의 샘플 포인트 각각에서 소정 방향으로의 터치 길이로 정의되는 신경망 기반 패턴 인증 장치.

청구항 4

제1항에 있어서,

상기 원본 데이터 입력부는,

상기 패턴 데이터가 터치 궤적 데이터인 경우, 상기 터치 궤적 데이터를 복수의 샘플 포인트 각각에서 방향 및 속도를 포함하는 1-D 데이터로 전처리하는 전처리부를 포함하는 신경망 기반 패턴 인증 장치.

청구항 5

삭제

청구항 6

제4항에 있어서,

상기 복수의 샘플 포인트는 터치 궤적에 관계 없이 미리 설정된 개수를 갖는 신경망 기반 패턴 인증 장치.

청구항 7

제1항에 있어서,

상기 예측부는 LSTM(Long-Short Term Memory)인 신경망 기반 패턴 인증 장치.

청구항 8

제1항에 있어서,

상기 비교 데이터 생성부는,

상기 임의의 노이즈를 입력 받고, 상기 판별부의 상기 결과값을 피드백 받아 비교 데이터를 출력하는 다층 신경망;

상기 비교 데이터를 임시 저장하는 리플레이 버퍼; 및

상기 비교 데이터의 미리 설정된 구간의 특징값들을 이용하여 상기 구간의 다음 특징값을 예측하는 예측부를 포함하는 신경망 기반 패턴 인증 장치.

청구항 9

제1항에 있어서,

상기 패턴 데이터는 터치스크린에 표시되는 복수의 포인트 중 일부 포인트를 지나가도록 연속적으로 터치하는 동안의 터치 궤적 및 터치 면적을 포함하며,

상기 원본 데이터 입력부는, 상기 터치 궤적 및 터치 면적을 하나의 1-D 데이터로 합치며,

상기 비교 데이터 생성부는, 상기 터치 궤적 및 터치 면적 각각에 대한 비교 데이터를 개별적으로 생성하고 개별적으로 생성된 터치 궤적 및 터치 면적의 비교 데이터를 하나의 1-D 데이터로 합치는 신경망 기반 패턴 인증 장치.

청구항 10

제1항에 있어서,

상기 패턴 데이터는 네트워크를 통해 연결된 사용자 단말로부터 수신되며,

상기 판별부의 학습이 완료되고, 상기 통과 여부에 대한 정확도가 미리 설정된 임계치 이상이 된 이후, 상기 판별부의 파라미터가 상기 사용자의 단말로 전송되는 신경망 기반 패턴 인증 장치.

청구항 11

제10항에 있어서,

상기 사용자 단말은,

상기 제1 패턴에 대해 사용자가 입력한 패턴 데이터를 입력 받는 패턴 데이터 입력부; 및

상기 파라미터를 이용하여 상기 입력된 패턴 데이터가 상기 제1 패턴에 대해 미리 학습된 사용자의 패턴 데이터인지를 판별하는 판별부를 포함하는 신경망 기반 패턴 인증 장치.

청구항 12

제1항에 있어서,

상기 판별부는,

상기 비교 데이터가 상기 원본 데이터에 미리 설정된 수치만큼 근접한 경우에 학습이 완료되고, 상기 학습이 완료된 이후, 상기 제1 패턴에 대해 제3자가 입력한 패턴 데이터를 미리 설정된 비율로 거절하는 경우 테스트가 완료되는 신경망 기반 패턴 인증 장치.

청구항 13

제12항에 있어서,

상기 판별부는 테스트 과정에서 상기 제3자가 입력한 패턴 데이터에 포함된 터치 궤적 또는 터치 면적에 대한 특징값을 이용하여 거절 여부를 결정하는 신경망 기반 패턴 인증 장치.

청구항 14

신경망 기반 패턴 인증 방법으로서,

(a) 제1 패턴에 대해 사용자가 복수 회 입력한 패턴 데이터인 원본 데이터의 특징값을 입력하는 단계;

(b) 임의의 노이즈를 이용하여 상기 원본 데이터에 대응되는 비교 데이터를 생성하는 단계; 및

(c) 상기 원본 데이터의 특징값과 상기 비교 데이터의 특징값을 통해 학습을 수행하여 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값 및 상기 제1 패턴에 대해 상기 사용자가 입력한 패턴 데이터와 제3자가 입력한 패턴 데이터에 대한 통과 여부를 결정하는 단계를 포함하되,

상기 (b) 단계는, 상기 (c) 단계에서의 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값을 피드백 받아 갱신된 비교 데이터를 생성하되,

상기 원본 데이터의 특징값 입력 단계는,

상기 패턴 데이터에 임의의 노이즈가 부가된 데이터를 리플레이 버퍼에 임시 저장하는 단계; 및

상기 리플레이 버퍼에 저장된 데이터에서 미리 설정된 구간의 샘플 포인트에서의 특징값을 이용하여 상기 구간의 다음 샘플 포인트에서의 특징값을 예측하는 단계를 포함하는 신경망 기반 패턴 인증 방법.

청구항 15

삭제

청구항 16

제14항에 있어서,

상기 비교 데이터 생성 단계는,

상기 임의의 노이즈를 입력 받고, 상기 (c) 단계에서의 상기 결과값을 피드백 받아 비교 데이터를 출력하는 단계;

상기 비교 데이터를 임시 저장하는 단계; 및

상기 비교 데이터의 미리 설정된 구간의 특징값들을 이용하여 상기 구간의 다음 특징값을 예측하는 단계를 포함하는 신경망 기반 패턴 인증 방법.

청구항 17

제14항에 따른 방법을 수행하기 위한 일련의 명령어들을 포함하는 매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 신경망 기반 패턴 인증 방법 및 장치에 관한 것으로서, 보다 상세하게는 대립쌍 신경망 기반으로 패턴 잠금의 보안성을 강화할 수 있는 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 안드로이드 패턴 잠금 시스템은 오늘날 휴대 전화에서 일반적으로 사용되는 가장 보편적인 사용자 인증 형태로서, PIN 입력, 생체 인증에 비해 사용자 친화적 인증으로 인식되고 있다.

[0003] 그러나, 패턴 잠금 시스템은 훔쳐보기(shoulder surfing), 카메라 공격(camera attack) 및 얼룩 공격(smudge attack)에 취약한 단점이 있다.

[0004] 이러한 취약한 문제를 해결하기 위해 얼굴 인증, 지문 인증과 같은 생체 인증 기술이 제안되고 있다.

[0005] 그러나, 얼굴 인증은 카메라 각도, 밝기, 표정 및 안경 등에 따라 인식률이 낮아지는 문제점이 있다. 또한, 지문 인증의 경우, 지문 정보의 도난이 발생하는 경우 사용자에게 더 큰 피해가 발생하는 문제가 있다.

[0006] 따라서, 사용자의 선호도가 높은 패턴 잠금이 아직도 일반적으로 사용되고 있다. 이러한 패턴 잠금의 보안성을 높이기 위해, 키 스트로크 패턴를 식별하고, 시도한 인증 시간, 위치, 애플리케이션 작동 방식을 분석하여 패턴 공격을 방지하기 위한 연구가 진행되고 있다.

[0007] 이러한 연구가 진행되고 있음에도, 보안성을 높이기 위한 복잡도가 매우 높아지기 때문에 오히려 사용자의 불편을 초래하는 문제점이 있다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 한국등록공보 제10-153275호

발명의 내용

해결하려는 과제

[0009] 상기한 종래기술의 문제점을 해결하기 위해, 본 발명은 보안성은 높이면서 사용자의 불편을 최소화할 수 있는 신경망 기반 패턴 인증 방법 및 장치를 제안하고자 한다.

과제의 해결 수단

[0010] 상기한 바와 같은 목적을 달성하기 위하여, 본 발명의 일 실시예에 따르면, 신경망 기반 패턴 인증 장치로서, 제1 패턴에 대해 사용자가 복수 회 입력한 패턴 데이터인 원본 데이터의 특징값을 입력하는 원본 데이터 입력부; 임의의 노이즈를 이용하여 상기 원본 데이터에 대응되는 비교 데이터를 생성하는 비교 데이터 생성부; 및 상기 원본 데이터의 특징값과 상기 비교 데이터의 특징값을 통해 학습이 수행되어 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값 및 상기 제1 패턴에 대해 상기 사용자가 입력한 패턴 데이터와 제3자가 입력한 패턴 데이터에 대한 통과 여부를 결정하는 판별부를 포함하되, 상기 비교 데이터 생성부는 상기 판별부의 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값을 피드백 받아 갱신된 비교 데이터를 생성하는 신경망 기반 패턴 인증 장치가 제공된다.

[0011] 상기 특징값은 터치스크린에 표시되는 복수의 포인트 중 일부 포인트를 지나가도록 연속적으로 터치하는 동안의 터치 궤적 데이터 및 터치 면적 데이터 중 적어도 하나를 포함할 수 있다.

[0012] 상기 터치 면적은 상기 연속적으로 터치하는 동안 복수의 샘플 포인트 각각에서 소정 방향으로의 터치 길이로 정의될 수 있다.

[0013] 상기 원본 데이터 입력부는, 상기 특징값이 터치 궤적 데이터인 경우, 상기 터치 궤적 데이터를 복수의 샘플 포인트 각각에서 방향 및 속도를 포함하는 1-D 데이터로 전처리하는 전처리부를 포함할 수 있다.

[0014] 상기 원본 데이터 입력부는, 상기 패턴 데이터에 임의의 노이즈가 부가된 데이터를 임시 저장하는 리플레이 버퍼; 및 상기 리플레이 버퍼에 저장된 데이터에서 미리 설정된 구간의 샘플 포인트에서의 특징값을 이용하여 상기 구간의 다음 샘플 포인트에서의 특징값을 예측하는 예측부를 포함할 수 있다.

[0015] 상기 복수의 샘플 포인트는 터치 궤적에 관계 없이 미리 설정된 개수를 가질 수 있다.

[0016] 상기 예측부는 LSTM(Long-Short Term Memory)일 수 있다.

[0017] 상기 비교 데이터 생성부는, 상기 임의의 노이즈를 입력 받고, 상기 판별부의 상기 결과값을 피드백 받아 비교 데이터를 출력하는 다층 신경망; 상기 비교 데이터를 임시 저장하는 리플레이 버퍼; 및 상기 비교 데이터의 미리 설정된 구간의 특징값들을 이용하여 상기 구간의 다음 특징값을 예측하여 예측부를 포함할 수 있다.

[0018] 상기 패턴 데이터는 터치스크린에 표시되는 복수의 포인트 중 일부 포인트를 지나가도록 연속적으로 터치하는 동안의 터치 궤적 및 터치 면적을 포함하며, 상기 원본 데이터 입력부는, 상기 터치 궤적 및 터치 면적을 하나의 1-D 데이터로 합치며, 상기 비교 데이터 생성부는, 상기 터치 궤적 및 터치 면적 각각에 대한 비교 데이터를

개별적으로 생성하고 개별적으로 생성된 터치 궤적 및 터치 면적의 비교 데이터를 하나의 1-D 데이터로 합칠 수 있다.

[0019] 상기 패턴 데이터는 네트워크를 통해 연결된 사용자 단말로부터 수신되며, 상기 판별부의 학습이 완료되고, 상기 통과 여부에 대한 정확도가 미리 설정된 임계치 이상이 된 이후, 상기 판별부의 파라미터가 상기 사용자의 단말로 전송될 수 있다.

[0020] 상기 사용자 단말은, 상기 동일 패턴에 대해 사용자가 입력한 패턴 데이터를 입력 받는 패턴 데이터 입력부; 및 상기 파라미터를 이용하여 상기 입력된 패턴 데이터가 상기 제1 패턴에 대해 미리 학습된 사용자의 패턴 데이터인지를 판별하는 판별부를 포함할 수 있다.

[0021] 상기 판별부는 상기 비교 데이터가 상기 원본 데이터에 미리 설정된 수치만큼 근접한 경우에 학습이 완료되고, 상기 학습이 완료된 이후, 상기 제1 패턴에 대해 제3자가 입력한 패턴 데이터를 미리 설정된 비율로 거절하는 경우 테스트가 완료될 수 있다.

[0022] 상기 판별부는 테스트 과정에서 상기 제3자가 입력한 패턴 데이터에 포함된 터치 궤적 또는 터치 면적에 대한 특징값을 이용하여 거절 여부를 결정할 수 있다.

[0023] 본 발명의 다른 측면에 따르면, 신경망 기반 패턴 인증 방법으로서, (a) 제1 패턴에 대해 사용자가 복수 회 입력한 패턴 데이터인 원본 데이터의 특징값을 입력하는 단계; (b) 임의의 노이즈를 이용하여 상기 원본 데이터에 대응되는 비교 데이터를 생성하는 단계; 및 (c) 상기 원본 데이터의 특징값과 상기 비교 데이터의 특징값을 통해 학습을 수행하여 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값 및 상기 제1 패턴에 대해 상기 사용자가 입력한 패턴 데이터와 제3자가 입력한 패턴 데이터에 대한 통과 여부를 결정하는 단계를 포함하되, 상기 (b) 단계는, 상기 (d) 단계에서의 상기 비교 데이터가 상기 원본 데이터에 근접한 정도에 대한 결과값을 피드백 받아 갱신된 비교 데이터를 생성하는 신경망 기반 패턴 인증 방법이 제공된다.

[0024] 본 발명의 또 다른 측면에 따르면 상기한 방법을 수행하기 위한 일련의 명령어들을 포함하는 매체에 저장된 컴퓨터 프로그램이 제공된다.

발명의 효과

[0025] 본 발명에 따르면, GAN (Generative Adversarial Network)을 기반으로 하며 리플레이 버퍼와 결합한 후 임의의 노이즈에 기초한 비교 데이터를 생성하기 때문에 패턴 인증 네트워크의 빠른 훈련이 가능한 장점이 있다.

[0026] 또한, 본 발명에 따르면, 사용자가 입력한 패턴 데이터를 n차원의 1-D 데이터로 전처리하기 때문에 패턴을 그리는데 걸리는 시간이 다르더라도 네트워크 학습 및 판별이 가능한 장점이 있다.

도면의 간단한 설명

[0027] 도 1은 본 발명의 바람직한 일 실시예에 따른 신경망 기반 패턴 인증 시스템의 구성을 도시한 도면이다.

도 2는 일반적인 GAN의 구조를 도시한 도면이다.

도 3은 일반적인 강화 학습 구조를 도시한 도면이다.

도 4는 본 발명의 바람직한 일 실시예에 따른 서버에서의 패턴 인증 네트워크의 구조를 도시한 도면이다.

도 5는 본 발명의 일 실시예에 따른 사용자가 입력한 패턴 데이터를 전처리하는 과정을 설명하기 위한 도면이다.

도 6은 본 실시예에 따른 전처리 결과를 나타낸 도면이다.

도 7은 LSTM 네트워크의 구조를 도시한 도면이다.

도 8은 본 실시예에 따른 리플레이 버퍼의 수에 따른 효과를 나타낸 도면이다.

도 9는 본 실시예에 따른 사용자 단말에서의 패턴 인증 네트워크를 도시한 도면이다.

도 10은 본 실험에서 사용된 10개의 패턴 형태를 나타낸 도면이다.

도 11은 본 실시예에 따른 훈련 및 테스트 과정을 나타낸 도면이다.

도 12는 본 실시예에 따른 패턴 인증 방식과 기존 방식의 ROC(Receiver Operating Characteristic) 커브를 나타낸 것이다.

도 13은 사용자가 패턴을 그리는 동안 터치 면적의 변화를 나타낸 것이다.

도 14는 본 실시예에 따른 패턴 인증 네트워크에서 학습이 진행됨에 따라 비교 데이터가 원본 데이터에 근접하는 것을 나타낸 도면이다.

도 15는 사용자가 주로 이용하는 패턴에 대한 터치 궤적 및 터치 면적을 나타낸 것이다.

도 16은 본 실시예에 따른 각 패턴 종류에서 터치 궤적 및 터치 면적 중 적어도 하나를 이용한 경우의 AUC를 나타낸 것이다.

발명을 실시하기 위한 구체적인 내용

[0028] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세하게 설명하고자 한다.

[0029] 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조 부호를 유사한 구성요소에 대해 사용하였다.

[0030] 도 1은 본 발명의 바람직한 일 실시예에 따른 신경망 기반 패턴 인증 시스템의 구성을 도시한 도면이다.

[0031] 도 1에 도시된 바와 같이, 본 실시예에 따른 시스템은 서버(100) 및 사용자 단말(102)을 포함할 수 있다.

[0032] 본 실시예에 따른 서버(100)는 사용자 단말(102)로부터 사용자가 복수 회 입력한 패턴 데이터를 수신하여, 패턴 인증 네트워크를 학습한다.

[0033] 이하에서는 서버(100)가 사용자 단말(102)로부터 수신된 패턴 데이터를 학습하는 것을 중심으로 설명할 것이나, 비실시간으로 동일 패턴에 대해 복수 회 입력한 패턴 데이터를 수집하여 서버(100)가 학습하는 것도 본 발명의 범주에 포함될 수 있다.

[0034] 본 실시예에 따른 패턴 데이터는 터치스크린 상에 표시되는 사용자가 복수의 포인트(예를 들어, 안드로이드 패턴인 경우는 9개) 중 하나에서 시작해서 터치 상태를 유지하면서 다른 포인트를 지나면서 터치가 완료될 때까지의 터치 궤적 및/또는 터치 면적에 대한 정보일 수 있다.

[0035] 패턴 데이터에 대해서는 이하에서 다시 상세하게 설명될 것이다.

[0036] 서버(100)는 패턴 인증 네트워크의 학습이 완료된 이후, 사용자 단말(102)로 패턴 인증을 위한 파라미터를 사용자 단말(102)로 전송한다.

[0037] 사용자 단말(102)은 내부에 구비된 패턴 인증 알고리즘에 상기한 파라미터를 적용하여 부정 사용자의 액세스 시도를 차단할 수 있다.

[0038] 사용자 단말(102)은 터치 스크린을 구비하는 단말로서, 통상의 스마트폰, 태블릿 PC, 랩탑과 같이, 사용자의 터치를 통해 패턴을 그릴 수 있는 모바일 단말이다.

[0039] 여기서, 패턴 인증 네트워크는 사용자 단말(102)에서 사용자 또는 사용자가 아닌 제3자의 패턴이 입력되는 경우, 해당 패턴이 정상 사용자의 패턴인지 여부를 판별할 수 있도록 하는 판별부(Discriminator)를 포함할 수 있다. 패턴 인증 네트워크의 학습은 사용자 단말(102)에 적용되는 판별부의 파라미터(가중치 및 바이어스)를 결정하는 과정으로 정의될 수 있다.

[0040] 서버(100)에서 패턴 인증 네트워크를 학습하고, 그 결과를 사용자 단말(102)로 반환함에 따라 학습 과정을 단축하면서 사용자 단말(102)에서 다른 사용자의 무단 액세스를 방지할 수 있다. 본 실시예에 따르면 동일한 포인트를 지나가는 패턴 데이터를 입력하더라도 진정한 사용자와 다른 사용자의 패턴을 구분할 수 있다.

[0041] 제3자의 패턴 공격을 통한 무단 액세스 시도를 효과적으로 차단하기 위해, 본 실시예에 따른 패턴 인증 네트워크의 학습은 지도 학습(supervised learning), 비지도 학습(unsupervised learning) 및 강화 학습(reinforcement learning)의 3가지 주요 심층 학습을 포함한다.

[0042] 본 실시예에 따른 지도 학습은 LSTM(Long-Short Term Memory) 기법이 이용될 수 있고, 비지도 학습은 Actor-Critic (AC) 학습 방법에서 사용되는 ERB (Experience Replay Buffer)가 적용된 GAN(Generative Adversarial Network) 기법이 이용될 수 있다.

[0043] 본 실시예에 따른 패턴 인증 네트워크는 대립 신경망인 GAN(Generative Adversarial Network)를 기본 구조로 포함할 수 있다.

[0044] 도 2는 일반적인 GAN의 구조를 도시한 도면이다.

[0045] 도 2에 도시된 바와 같이, GAN은 판별 네트워크(Discriminator Network)에서 원본 데이터(real data)와 생성기 네트워크(Generator Network)에서 생성한 비교 데이터를 비교하여 참과 거짓을 구분한다.

[0046] 본 실시예에 따른 패턴 인증 네트워크의 학습에서, 원본 데이터는 사용자가 복수 회 입력한 패턴 데이터이고, 비교 데이터는 임의의 노이즈(Random Noise)를 이용하여 생성한 데이터이다.

[0047] 이때, 사용자가 입력한 패턴 데이터의 수가 많지 않고, 또한 임의의 노이즈로부터 생성되는 비교 데이터가 실제 패턴 데이터와의 유사성이 높지 않을 수 있기 때문에 학습 시간이 매우 오래 걸리는 문제점이 발생할 수 있다. 이를 위해, 본 실시예에 따른 패턴 인증 네트워크에는 도 3에 도시된 바와 같이, 강화 학습에서 사용되는 리플레이 버퍼(replay buffer)가 사용된다.

[0048] 도 4는 본 발명의 바람직한 일 실시예에 따른 서버에서의 패턴 인증 네트워크의 구조를 도시한 도면이다.

[0049] 본 실시예에 따르면, 사용자가 입력한 패턴 데이터에서 터치 궤적과 터치 면적 정보가 동시에 이용될 수 있다. 그러나 이에 한정됨이 없이, 터치 궤적과 터치 면적 중 하나가 패턴 모양의 복잡도에 따라 선택적으로 이용될 수도 있다. 도 4에 도시된 바와 같이, 본 실시예에 따른 서버(100)의 패턴 인증 네트워크는, 원본 데이터 입력부(400), 비교 데이터 생성부(402) 및 판별부(404)를 포함할 수 있다.

[0050] 원본 데이터 입력부(400)는 제1 패턴에 대해 사용자가 복수 회 입력한 패턴 데이터인 원본 데이터의 특징값을 예측한다.

[0051] 여기서, 패턴 학습을 위해 사용자는 동일한 패턴을 복수 회 입력하는 행위를 한다.

[0052] 패턴 데이터는 터치스크린에 표시되는 복수의 포인트 중 일부 포인트를 지나가도록 연속적으로 터치하는 동안(패턴을 그리는 동안)의 터치 궤적 또는 터치 면적일 수 있고, 터치 궤적 또는 터치 면적은 시간에 따라 연속되는 특징값(temporal feature)을 가질 수 있다.

[0053] 여기서, 연속되는 특징값은 이하에서 설명하는 패턴을 그리는 동안 복수의 샘플 포인트 각각에서의 터치 방향, 속도 및 면적일 수 있다.

[0054] 본 실시예에서, 사용자의 패턴 데이터는 1-D 데이터이며, 이때, 패턴의 모양에 관계없이 패턴 데이터는 n(예를 들어, 200개)개의 샘플 포인트로 샘플링되고, 연속적인 특징값은 n개 샘플 포인트 각각에서의 터치 궤적(터치 방향/속도) 및 면적으로 정의될 수 있다.

[0055] 원본 데이터 입력부(400)는 패턴 데이터가 소정 패턴에 대한 터치 궤적에 관한 데이터인 경우, 터치 궤적 데이터를 복수의 샘플 포인트에서의 방향 및 속도를 포함하는 1-D 데이터로 전처리하는 전처리부(미도시)를 포함할 수 있다.

[0056] 그리고, 터치 면적은 일부 포인트를 터치하는 동안 복수의 샘플 포인트 각각에서의 소정 방향으로의 터치 길이로 정의될 수 있다.

[0057] 즉, 특정 샘플 포인트에서 터치 면적이 넓을수록 샘플 포인트로 기준으로 수직 방향으로 터치 길이가 길어질 것이다.

[0058] 도 5는 본 발명의 일 실시예에 따른 터치 궤적의 전처리 과정을 설명하기 위한 도면이다.

[0059] 도 5에 도시된 바와 같이, 사용자가 사용자 단말(102)에서 소정 패턴을 입력하는 경우, 전처리부(미도시)는 패턴을 그리는 동안의 터치 궤적에 따른 복수의 샘플 포인트 각각에서의 터치 방향 및 속도를 포함하는 특징값을 추출한다.

[0060] 또한, 샘플 포인트는 학습 효율을 높이기 위해 패턴 모양에 따른 터치 궤적의 길이에 관계없이 미리 설정된 개수 (예를 들어, 200개)으로 설정된다.

[0061] 도 5에 도시된 바와 같이, 사용자가 터치 스크린 상에서 패턴을 그리는 동안 9개의 패턴 포인트 중 n번째 패턴 포인트에서의 좌표를 X_n, Y_n이라 할 때, 다음 터치 좌표인 X_{n+1}, Y_{n+1}로 8개의 방향으로 이동할 수 있다. 이때, 전처리된 데이터는 다음과 같이 표현된다.

수학식 1

[0062] $$D_n = w_{t=n} \cdot speed_{t=n}$$

[0063] 여기서 D_n은 샘플 포인트 n에서 처리된 데이터, $w_{t=n}$은 x_{n-1}, y_{n-1}이 샘플 포인트 n에서 이동하는 방향의 가중치, $speed_{t=n}$는 샘플 포인트 n에서의 속도이다.

[0064] 도 6은 본 실시예에 따른 전처리 결과를 나타낸 도면이다.

[0065] 도 6에 도시된 바와 같이, 전처리를 수행하는 경우, 터치스크린 상에서 동일하게 'ㄹ'모양으로 패턴을 그린다고 하더라도 이들의 전처리된 1-D 데이터는 사용자가 입력한 데이터와 차이가 두드러지게 된다.

[0066] 패턴을 그리는 데 걸리는 시간이 매번 다르므로 데이터의 크기가 달라질 수 있다. 이러한 점을 고려하여 본 실시예에서는, 학습 과정에서 Scipy 라이브러리를 사용하여 소정 차원(샘플 포인트의 수에 상응하는 차원)의 행벡터로 데이터의 크기를 조정한다.

[0067] 또한, 본 실시예에 따른 1-D 데이터는 패턴을 그리는 동안 복수의 샘플 포인트 각각에서의 터치 면적을 포함할 수 있다.

[0068] 터치 면적의 1-D 데이터는 별도의 전처리가 수행되지 않을 수 있고, 터치 면적에 따라 각 샘플 포인트에서 0에서 1 중 하나의 값을 가질 수 있다.

[0069] 다시 도 4를 참조하면, 원본 데이터 입력부(400)는 패턴 데이터에 임의의 노이즈가 부가된 데이터를 저장하는 제1 리플레이 버퍼(410), 제1 리플레이 버퍼(410)에 저장된 데이터에서 미리 설정된 구간의 샘플 포인트에서의 특징값을 예측하는 제1 예측부(412)를 포함할 수 있다.

[0070] 상기한 바와 같이, 본 실시예에 따른 패턴 데이터는 시간에 따라 연속되는 특징값을 가지게 되며, 패턴 인증 네트워크의 학습을 위해, 제1 예측부(412)는 미리 학습이 완료된 상태로 제공된다.

[0071] 제1 예측부(412)의 학습은 사용자가 복수 회 입력한 패턴 데이터를 통해 수행될 수 있다.

[0072] 여기서, 사용자가 입력한 패턴 데이터는 터치 궤적에 관한 데이터를 전처리하여 생성된 각 샘플 포인트에서의 터치 방향 및 속도와, 터치 면적일 수 있고, 터치 궤적 정보와 터치 면적이 동시에 이용되는 경우, 각각에 대해 노이즈가 부가될 수 있다.

[0073] 본 실시예에 따른 제1 예측부(412)는 제1 리플레이 버퍼(410)가 출력하는 노이즈 부가 데이터에서 미리 설정된 구간의 특징값을 이용하여 다음 구간의 특징값을 예측하여 판별부(404)로 출력한다.

[0074] 여기서, 서버(100)의 패턴 인증 네트워크에서의 판별부(404)는 사용자 단말(102)의 판별부와 구별되도록 제1 판별부(404)로 정의될 수 있다. 이하에서는 서버의 판별부를 제1 판별부로 기재하여 설명한다.

[0075] 제1 판별부(404)의 학습을 위해 비교 데이터 생성부(402)에서 비교 데이터를 생성한다.

[0076] 비교 데이터 생성부(402)는 임의의 노이즈를 이용하여 사용자가 복수 회 입력한 패턴 데이터인 원본 데이터에 대응되는 비교 데이터를 생성하고, 비교 데이터의 특징값을 예측하여 제1 판별부(404)로 출력한다.

[0077] 도 4에 도시된 바와 같이, 비교 데이터 생성부(402)는 터치 궤적에 대한 비교 데이터를 생성하기 위한 다층 신경망(420-1) 및 제2 리플레이 버퍼(422-1)와 터치 면적에 대한 비교 데이터를 생성하기 위한 다층 신경망(420-2)과 제2 리플레이 버퍼(422-2)를 포함한다.

[0078] 또한, 비교 데이터 생성부(402)는 각 리플레이 버퍼(422-2,422-3)의 출력에 연결되는 제2 예측부(424)를 포함할

수 있다.

[0079] 다층 신경망(420-1,420-2)은 임의의 노이즈를 입력 받고, 제1 판별부(404)의 출력을 피드백 받아 터치 궤적 및 터치 면적에 대한 비교 데이터를 출력한다.

[0080] 제2 리플레이 버퍼(422-1,422-2)를 다층 신경망이 생성한 비교 데이터를 임시 저장한다.

[0081] 터치 궤적 및 터치 면적에 대한 비교 데이터는 하나로 합쳐져 제2 예측부(424)로 입력된다. 제2 예측부(424)는 상기와 같이 합쳐진 데이터의 미리 설정된 구간의 특징값을 이용하여 다음 구간의 특징값을 예측한다.

[0082] 여기서, 비교 데이터는 미리 설정된 샘플 포인트의 수에 대응되는 특징값들을 가진다.

[0083] 이처럼 비교 데이터의 예측된 특징값은 제1 판별부(404)로 입력된다.

[0084] 본 실시예에서의 패턴 데이터는 시간에 따라 연속되는 순차적인 데이터 유형이기 때문에 갑자기 데이터가 변경될 수 있다. 따라서, 비교 데이터 생성부(402)가 제대로 학습되지 않으면 제1 판별부(404)의 정확성이 낮아지는 문제점이 있다.

[0085] 이를 위해, 본 발명에서는 제1 예측부(412) 및 제2 예측부(424)의 사전 학습을 수행한다.

[0086] 본 실시예에 따른 예측부는 소정 구간의 입력 데이터(특징값)를 기반으로 다음 구간에서의 특징값을 예측하는 것으로서, 입력 데이터에 작은 변화가 있더라도 실제 데이터와 매우 유사한 데이터를 출력할 수 있도록 설계된다.

[0087] 전술한 바와 같이, 본 실시예에 따른 예측부는 LSTM일 수 있다.

[0088] LSTM 네트워크는 긴 시퀀스를 가진 시간 도메인을 학습하기 위해 설계된 일종의 RNN이다. 전통적인 RNN 구조는 그라디언트 소실 문제가 발생하므로 역전파(backpropagation) 중에 오류가 기하 급수적으로 증가하거나 감소하게 된다.

[0089] LSTM 네트워크의 메모리 블록은 Recurrent 구조로 연결된 블록이다.

[0090] 도 7에 도시된 바와 같이, 각 블록은 입력 게이트, 출력 게이트 및 망각(forget) 게이트로 구성된다. 입력 데이터는 입력 게이트의 활성화 값에 추가된다. 출력값은 출력 게이트 및 망각 게이트의 활성화 값에 차례로 추가된다.

[0091] 네트워크는 이들 게이트를 통해 셀과 상호 작용한다.

[0092] 셀의 출력 y^c 는 현재 셀을 기반으로 계산된다. N_c 는 셀의 입력이다. N_i, N_f 및 N_o 는 각각 입력 게이트, 망각 게이트 및 출력 게이트에 대한 입력이다. T는 0부터 시작하는 이산 구간(시간 단계)를 나타낸다. j는 메모리 블록이고 v는 블록 j 내부의 메모리 셀이다. w_{ij} 는 i-j 사이의 유닛들의 가중치이다. 다른 매개 변수는 다음과 같다.

[0093] y^i = input gate activation

[0094] y^f = forget gate activation

[0095] s^c = cell input and cell state

[0096] y^o = output gate activations

[0097] y^c = cell output

[0098] 우선, y^i 및 y^t 는 다음을 통해 계산된다.

수학식 2

$$N_{i_j}(T) = \sum_m w_{i_j m} y^m(T-1) + \sum_{v=1}^{S_j} w_{i_j c_j^v} s_{c_j^v}(T-1),$$

[0099]

$$y^{i_j}(T) = f_{i_j}\left(N_{i_j}(T)\right)$$

[0100]

수학식 3

$$N_{t_j}(T) = \sum_m w_{t_j m} y^m(T-1) + \sum_{v=1}^{S_j} w_{t_j c_j^v} s_{c_j^v}(T-1),$$

[0101]

$$y^{t_j}(T) = f_{t_j}\left(N_{t_j}(T)\right)$$

[0102]

[0103] m의 범위는 전체 소스 유닛이다. 함수 f 은 [0,1] 범위의 로지스틱(logistic) 시그모이드(sigmoid) 함수이다.

[0104] 입력 게이트 및 망각 게이트는 수학식 2 및 3에 포함된다.

[0105] 메모리 셀 상태 $s_c(T)$ 는 셀 내부에서 밀어 넣어진다.

[0106] 아래와 같이, 게이팅 된 입력은 이전 시간 단계(time step) 상태 $s_c(T\text{-}1)(T>0)$ 에서 계산되고, 망각 게이트의 활성화 값($s_{c_j^v}(0)=0$, activation)이 곱해진다.

수학식 4

$$N_{c_j^v}(T) = \sum_m w_{c_j^v m} y^m(T-1),$$

[0107]

$$s_{c_j^v}(T) = y^{t_j}(T)s_{c_j^v}(T-1) + y^{i_j}(T)\ g\left(N_{c_j^v}(T)\right)$$

[0108]

[0109] 또한, 출력 게이트 활성화 값 y^o 은 다음과 같이 계산된다.

수학식 5

$$N_{o_k}(T) = \sum_m w_{o_j m} y^m(T-1) + \sum_{v=1}^{S_j} w_{o_j c_j^v}\, s_{c_j^v}(T-1),$$

[0110]

[0111] 수학식 5는 이전에 구현된 셀 상태 $s_c(T)$ 에서 메모리 블록 j 및 출력 게이트를 나타낸다.

[0112] c_j^v 는 j번째 메모리 블록의 v 번째 셀이다. 셀 출력 y^c 는 다음과 같이 계산된다.

수학식 6

$$y^{c_j^v}(T) = y^{o_j}(T)s_{c_j^v}(T)$$

[0113]

[0114] 정규화된 출력 레이어를 전제로 하는 정규화된 레이어드(layered) 네트워크, 히든 레이어들을 포함하는 메모리 블록들 및 출력 유닛 k의 최종식은 다음과 같다.

수학식 7

$$N_k(T) = \sum_n w_{km} y^m(T-1),$$
$$y^k(T) = f_k\left(N_k(T)\right)$$

[0115]

[0116] 여기서, m은 모든 출력 유닛들의 범위를 나타내고, f_k 는 출력 스쿼시 함수를 나타낸다. 이러한 방식으로 LSTM 네트워크는 그라이언트 소실 문제를 해결한다.

[0117] 본 실시예에서는 상기와 같은 특성을 갖는 LSTM을 패턴 인증 네트워크의 예측부에 적용하여 패턴 인증 시스템의 신뢰도를 개선한다.

[0118] 전처리를 통해 사용자가 입력한 패턴 데이터는 시간에 따라 연속되는 특징값(예를 들어, 200개 샘플 포인트에서의 방향 및 속도)을 갖게 된다.

[0119] 도 4에 도시된 바와 같이, 제1 예측부(412)는 노이즈가 부가된 패턴 데이터를 미리 설정된 구간의 특징값을 이용하여 다음 구간의 특징값을 예측하여 출력한다.

[0120] 미리 설정된 구간의 크기는 k(예를 들어, 10)으로 설정될 수 있으며, k개의 구간에서의 특징값들을 이용하여 k+1 샘플 포인트에서의 특징값을 예측하여 출력한다.

[0121] 200개의 샘플 포인트에서의 특징값이라 가정하면, 제1 예측부(412)는 1 내지 10번째 샘플 포인트에서의 특징값을 이용하여 11번째 샘플 포인트에서의 특징값을 예측하고, 또한, 2 내지 11번째 샘플 포인트에서의 특징값을 이용하여 12번째 샘플 포인트에서의 특징값을 예측한다.

[0122] 한편, 본 실시예에 따른 예측부는 비교 데이터 생성부(402)의 출력에도 포함된다.

[0123] 비교 데이터 생성부(402)의 다층 신경망(420-1,420-2)은 임의의 노이즈를 입력 받아 비교 데이터를 생성한다.

[0124] 터치 궤적 및 터치 면적에 대한 비교 데이터는 각각 제2 리플레이 버퍼(422-1,422-2)에 저장된다. 도 8은 본 실시예에 따른 리플레이 버퍼의 수에 따른 효과를 나타낸 도면이다.

[0125] 비교 데이터 생성부(402)의 출력이 실제 사용자가 입력한 패턴 데이터와 유사하지 않은 경우 훈련이 제대로 이루어지지 않는 문제점이 있다.

[0126] 이때, 리플레이 버퍼의 수가 증가할수록 이전에 생성했던 데이터가 리플레이 버퍼에 저장되므로 다층 신경망(420-1,420-2)은 제1 판별부(404)의 출력을 피드백 받아 사용자가 입력한 패턴 데이터와 유사한 비교 데이터를 생성할 수 있게 된다.

[0127] 다층 신경망(420-1,420-2)이 출력한 비교 데이터는 비교 데이터 생성부(402)의 제2 예측부(424)로 입력되며, 제2 예측부(424)는 비교 데이터의 미리 설정된 구간의 특징값을 이용하여 다음 구간의 특징값을 예측하여 제1 판별부(404)로 출력한다.

[0128] 제1 판별부(404)는 제1 예측부(412)에서 출력한 데이터와, 비교 데이터 생성부(402)의 제2 예측부(424)에서 출력한 데이터를 이용하여 비교 데이터가 원본 데이터에 근접한 정도에 대한 결과값을 출력한다.

[0129] 이때, 제1 판별부(404)는 CNN 및 LSTM의 조합으로 입력 데이터들의 비교를 통한 판별 과정을 수행할 수 있다.

[0130] 제1 판별부(404)는 터치 궤적 및 터치 면적 데이터 각각에 대해 판별 과정을 수행하여 2개의 판정 결과를 출력한다.

[0131] 최종 판단(0~1)을 위해서는 하나의 Fully connected layer(430)를 사용해서 2개의 제1 판별부(404)의 출력을 하나로 합치는 훈련을 진행한다.

[0132] 상기한 결과값은 다층 신경망(420-1,420-2)로 피드백되며, 다층 신경망(420-1,420-2)는 비교 데이터가 원본 데이터에 더욱 근접한 갱신된 비교 데이터를 생성한다.

[0133] 이와 같은 과정을 통해 학습이 완료되면 최종적으로 제1 판별부(404)는 제1 패턴에 대해 사용자가 입력한 패턴 데이터와 제3자가 입력한 패턴 데이터에 대한 통과 여부를 판별하는 과정을 수행한다.

[0134] 이때, 제1 판별부(404)는 사용자의 패턴 데이터의 통과 횟수가 높고 제3자의 패턴 데이터의 거절 횟수는 높아야 한다.

[0135] 통과 여부에 대해 미리 설정된 정확도가 확보되는 경우, 서버(100)는 사용자 단말(102)로 예측부 및 판별부의 파라미터를 전송한다.

[0136] 도 9는 본 실시예에 따른 사용자 단말에서의 패턴 인증 네트워크를 도시한 도면이다.

[0137] 도 9에 도시된 바와 같이, 본 실시예에 따른 사용자 단말에서의 패턴 인증 네트워크는 사용자의 패턴 데이터를 입력 받는 패턴 데이터 입력부(900) 및 제2 판별부(902)를 포함할 수 있다.

[0138] 패턴 데이터 입력부(900)는 터치 궤적 데이터를 전처리하는 전처리부(미도시) 및 제3 예측부(910)를 포함할 수 있다.

[0139] 이미 서버(100)에서 사용자 단말(102)에서 사용될 예측부 및 판별부의 학습이 완료되었으므로 사용자 단말(10

2)에는 비교 데이터 생성부가 포함되지 않으며, 사용자 또는 제3자의 패턴 데이터가 입력되는 경우, 제3 예측부(910)는 전처리된 패턴 데이터에서 미리 설정된 구간의 다음 구간에서의 특징값을 출력하고, 제2 판별부(904)는 입력된 특징값에 기초하여 해당 패턴이 정상적인 사용자의 입력인지 여부를 판별한다.

[0140] 즉, 제2 판별부(902)는 학습이 완료된 사용자의 패턴과 동일한 패턴이 입력되는 경우, 입력된 패턴 데이터가 진정한 사용자의 입력인지를 판별한다.

[0141] 패턴 인증 네트워크의 훈련은 판별부와 비교 데이터 생성부의 훈련이라는 두 부분으로 구성된다. 판별부는 사전 훈련 된 LSTM을 통과한 패턴 데이터 10 개를 무작위 노이즈를 추가하여 학습한다.

[0142] 판별부의 출력은 역전파를 수행하는데 사용된다.

[0143] 생성부의 목표는 판별부가 'true'로 분류할 데이터를 생성하는 것이다.

[0144] 따라서, 훈련이 진행됨에 따라 생성부는 판별부가 분류하기 점점 어려워지도록 실제 사용자가 입력한 데이터와 유사한 데이터를 생성한다.

[0145] 판별부는 true와 false에 따라 1에서 0 범위 내에서의 값을 출력한다. 테스트 데이터가 실제 데이터와 유사하면 판별부의 출력은 1에 가까우며, 유사하지 않은 경우 출력은 0에 가까워진다.

[0146] 각 패턴의 각 참가자 20 회 입력한 패턴 데이터 중 중 10 개의 세트가 훈련 데이터로 사용되었다. 나머지 10개는 테스트 데이터로 사용되었다. 본 실험에서 전 세계에서 가장 많이 사용되는 도 10과 같은 10개의 패턴을 실험에 사용하였다

[0147] 본 실시예에 따른 훈련과 테스트 과정은 도 11에 나타난 바와 같다. 정확도를 계산하기 위한 테스트는 판별부와 생성부가 모두 훈련을 끝내는 각 내부 훈련 단계마다 진행된다. 테스트 세트에 대해 아래의 수학식에 의해 계산된 정확도가 사전 정의 된 목표보다 높으면 테스트 과정이 종료된다.

수학식 8

[0148] $$\frac{1}{n}\left(\sum_{i=1}^{n-1}\sum_{j=1}^{m}\left(1-\frac{1}{1+e^{-D_{i,j}}}\right)+\sum_{j=1}^{m}\frac{1}{1+e^{-D_j}}\right)$$

[0149] 여기서, n은 사용자(대상)의 수, m은 테스트 세트의 수, $D_{i,j}$는 i번째 사용자의 j번째 데이터의 분류자 출력(classifier output)이다. D_j는 사용자 자신의 데이터의 분류자 출력이다.

[0150] 훈련을 위한 매개 변수의 스펙은 다음과 같다.

[0151] 최대 버퍼 크기 N_b = 1000, 최소 배치 크기 m = 50, 외부 훈련 단계 = 100, 내부 훈련 단계 = 20

[0152] 판별부와 생성부 모두의 훈련을 위한 학습 속도를 갖춘 Stochastic Gradient Descent(SGD) = 0.01

[0153] 도 12는 본 실시예에 따른 패턴 인증 방식과 기존 방식의 ROC(Receiver Operating Characteristic) 커브를 나타낸 것이다. 여기서 ROC Curve는 False positive rate(FPR), True positive rate(TPR) 을 통한 분류기의 성능 측정 지표이다.

[0154] 도 12에 도시된 바와 같이, 본 실시예에 따른 패턴 인증 방식은 기존 One class SVM, Elliptic Envelope, Isolation Forest에 비해 AUC(Area Under Curve)가 한층 높게 나타나는 것을 확인할 수 있다.

[0155] 또한, 도 12에 나타난 바와 같이, 본 실시예에 따른 신경만 기반 패턴 인증은 기존 학습 알고리즘에 비해 높은 정확도를 가지며, 나아가 터치 궤적과 터치 면적을 모두 이용하는 경우 매우 높은 정확도로 사용자의 패턴을 인식할 수 있다는 점을 알 수 있다.

[0156] 도 13은 사용자가 패턴을 그리는 동안 터치 면적의 변화를 나타낸 것이다.

[0157] 도 13을 참조하면, 시간의 경과에 따라 터치 면적이 달라지며 이를 통해 학습을 수행하는 패턴 인증의 정확도가 높아진다.

[0158] 또한, 도 14는 본 실시예에 따른 패턴 인증 네트워크에서 학습이 진행됨에 따라 비교 데이터가 원본 데이터에 근접하는 것을 나타낸 도면이다.

[0159] 이처럼 본 실시예에 따른 패턴 인증 네트워크의 학습은 비교 데이터가 원본 데이터가 근접하는 수준까지 반복 수행된다.

[0160] 도 15는 사용자가 주로 이용하는 패턴에 대한 터치 궤적 및 터치 면적을 나타낸 것으로서, 잠금을 위한 패턴의 복잡도는 사용자마다 크게 달라진다.

[0161] 도 16은 본 실시예에 따른 각 패턴 종류에서 터치 궤적 및 터치 면적 중 적어도 하나를 이용한 경우의 AUC를 나타낸 것이다.

[0162] 도 16을 참조하면, 패턴의 복잡도가 낮은 경우에는 터치 궤적만을 이용하더라도 높은 정확도를 가질 수 있으나, 패턴의 복잡도가 높은 경우에는 터치 궤적 및 터치 면적을 동시에 이용하는 경우에 높은 정확도를 가지는 점을 확인할 수 있다.

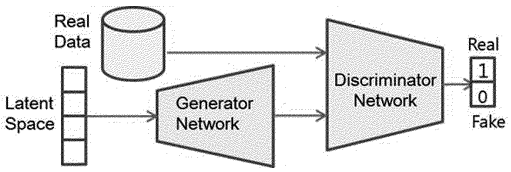
산업상 이용가능성

[0163] 상기한 본 발명의 실시예는 예시의 목적을 위해 개시된 것이고, 본 발명에 대한 통상의 지식을 가지는 당업자라면 본 발명의 사상과 범위 안에서 다양한 수정, 변경, 부가가 가능할 것이며, 이러한 수정, 변경 및 부가는 하기의 특허청구범위에 속하는 것으로 보아야 할 것이다.

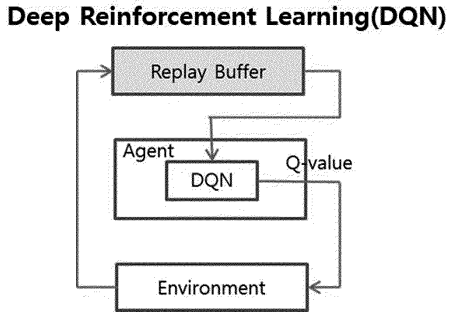
도면

도면1

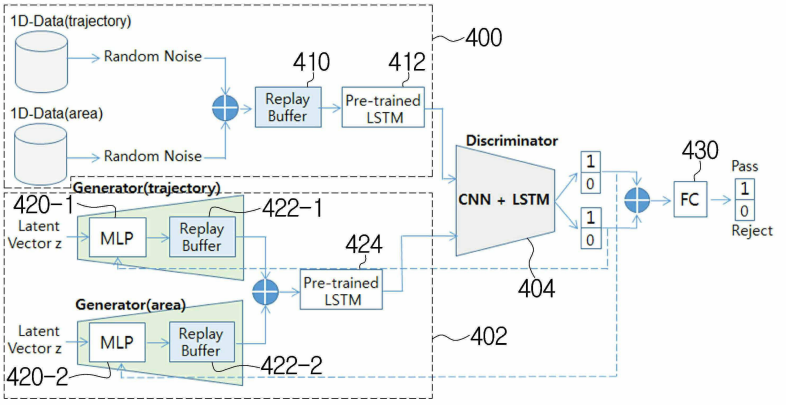
도면2



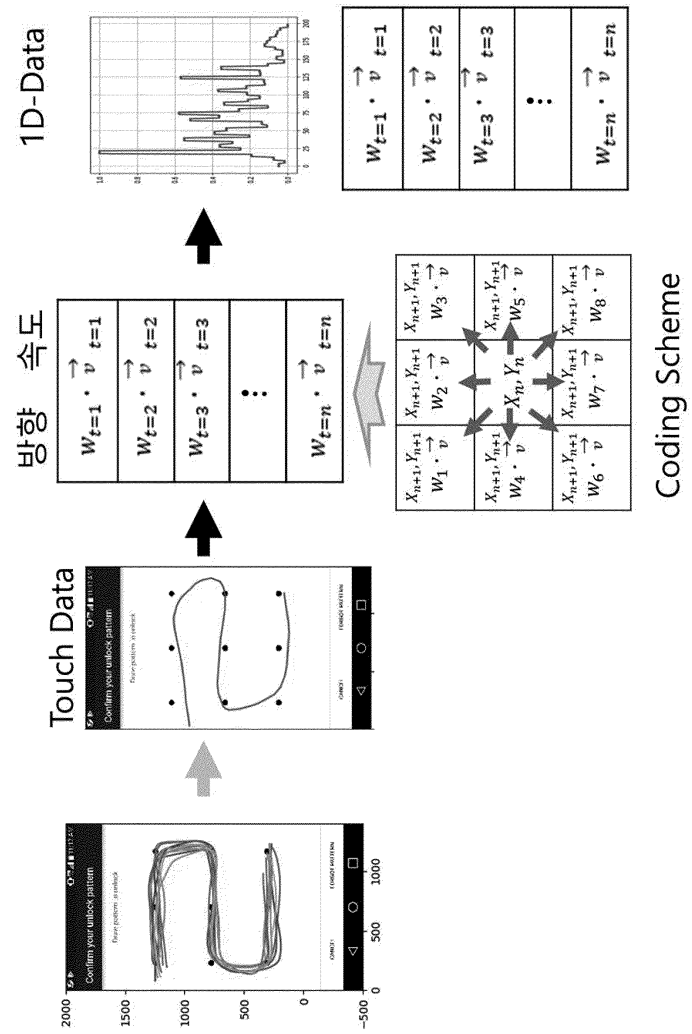
도면3


Deep Reinforcement Learning(DQN)
Replay Buffer
Agent
DQN
Q-value
Environment

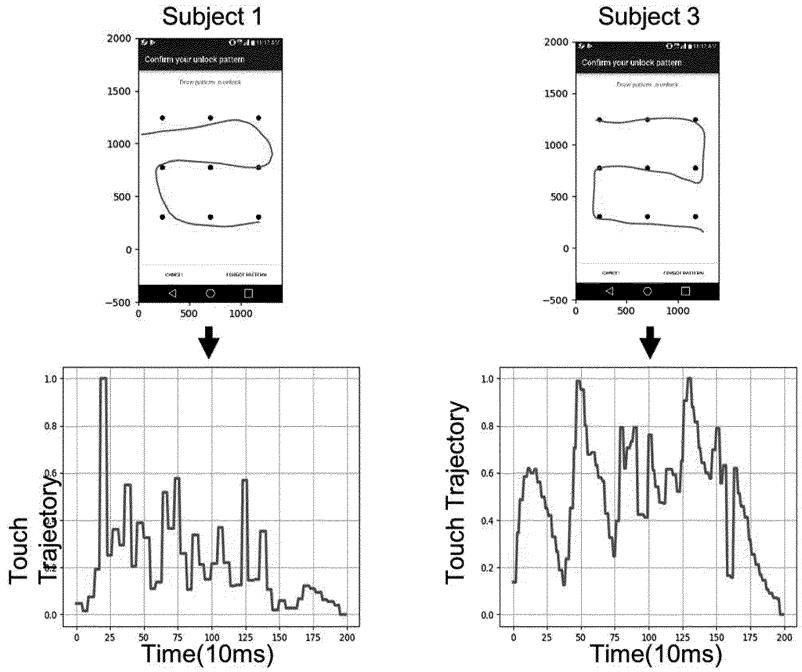
도면4


1D-Data(trajectory)
Random Noise
1D-Data(area)
Random Noise
410
412
400
Replay Buffer
Pre-trained LSTM
Discriminator
CNN + LSTM
430
FC
Pass
Reject
Generator(trajectory)
420-1
Latent Vector z
MLP
Replay Buffer
422-1
424
Pre-trained LSTM
404
Generator(area)
Latent Vector z
MLP
Replay Buffer
422-2
420-2
402

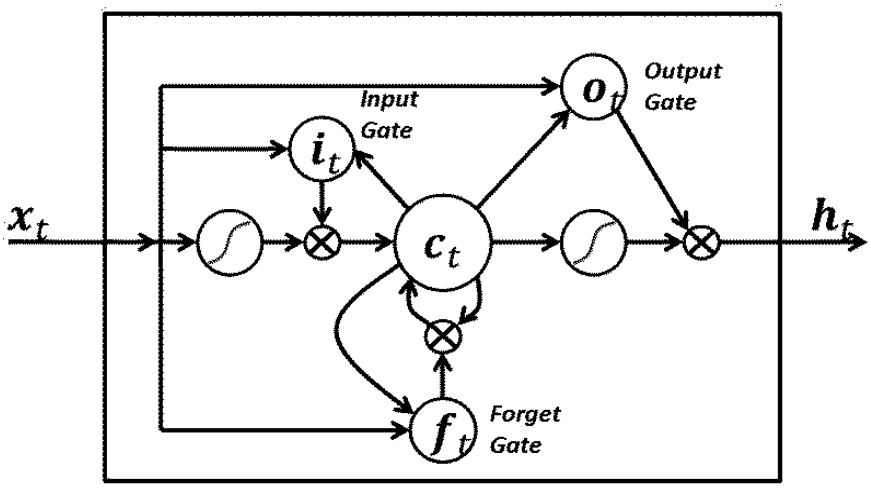
도면5



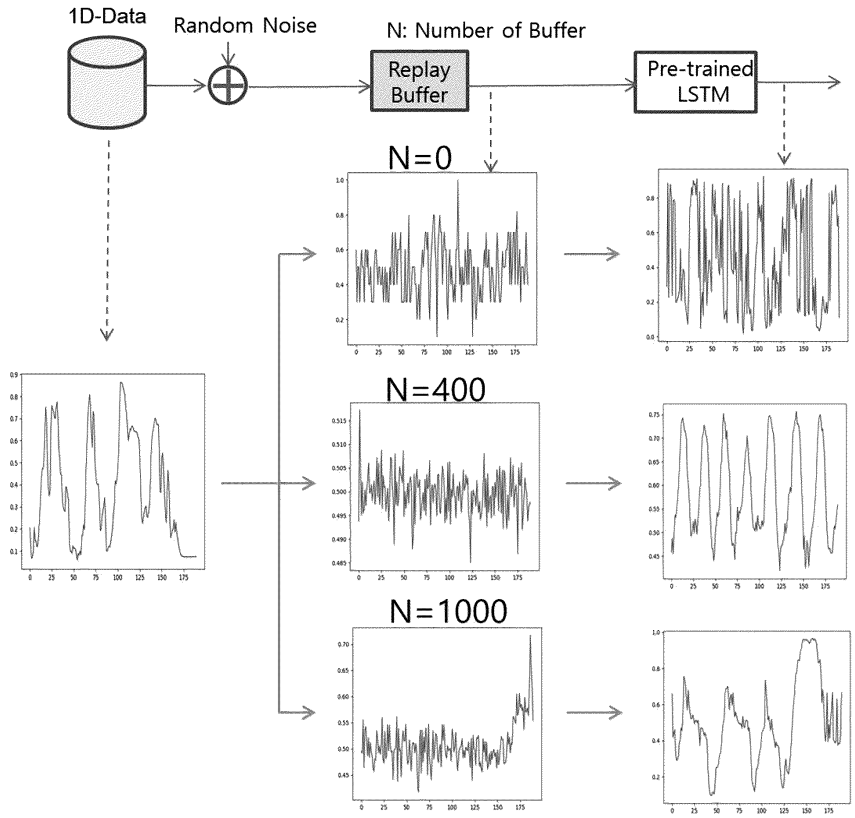
도면6


Subject 1
Subject 3
Touch Trajectory
Time(10ms)

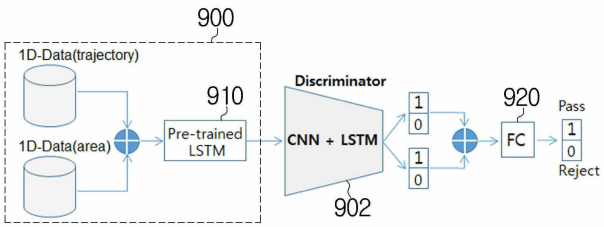
도면7


Input Gate
Output Gate
Forget Gate

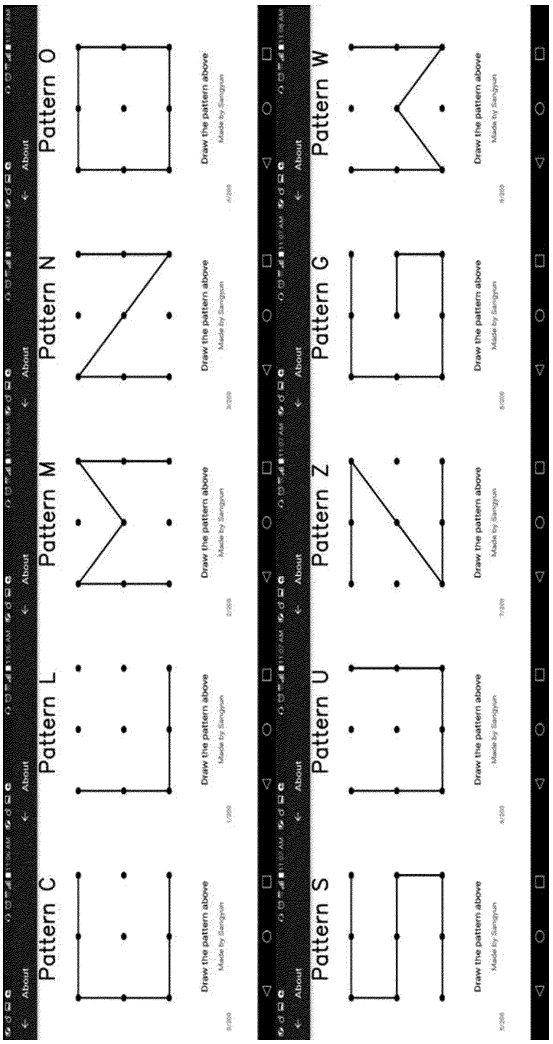
도면8


1D-Data
Random Noise
N: Number of Buffer
Replay Buffer
Pre-trained LSTM
N=0
N=400
N=1000

도면9


900
1D-Data(trajectory)
1D-Data(area)
910
Pre-trained LSTM
Discriminator
CNN + LSTM
902
920
FC
Pass
Reject

도면10

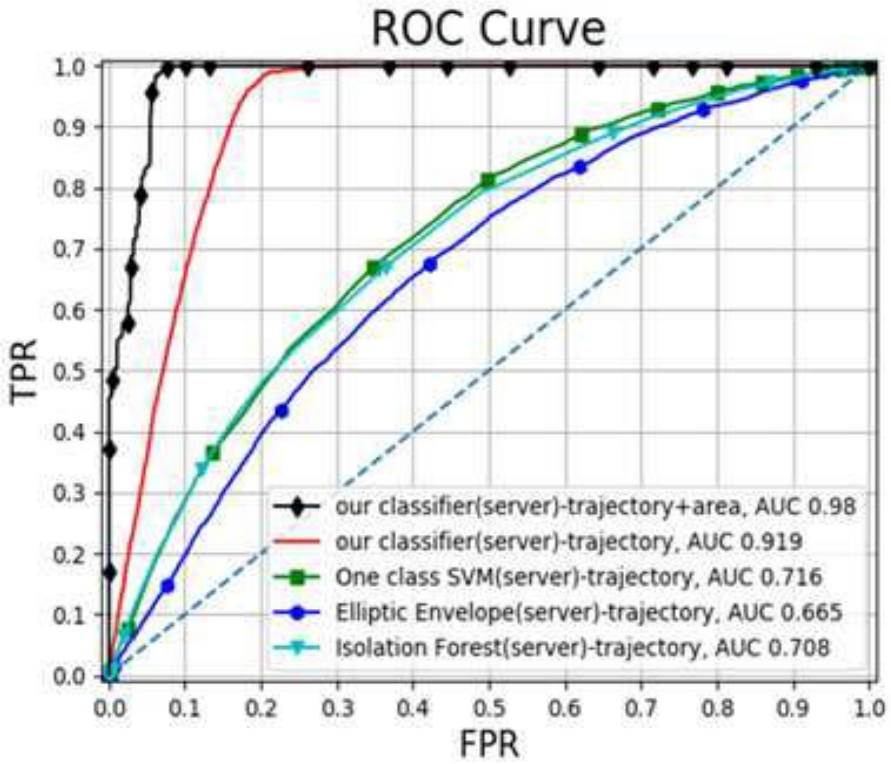

Pattern C
Pattern L
Pattern M
Pattern N
Pattern O
Pattern S
Pattern U
Pattern Z
Pattern G
Pattern W
About
Draw the pattern above
Made by Sangyun

도면11

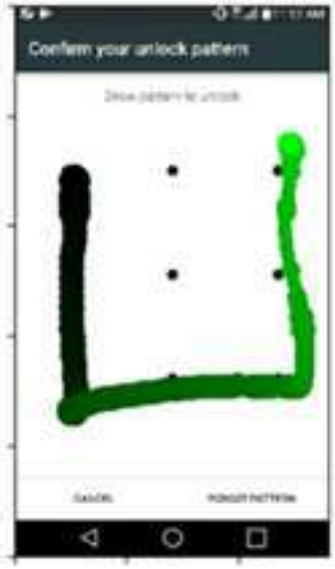
Algorithm 1 Training of our network

Input:D_p −Row vectors of pattern data from the user:
Input:D_o −Row vertors of test set
Input:$LSTM_p$ − pretrained LSTM model
Input: $B_d = buffer\ for\ the\ classifier$
Input:$B_g = buffer\ for\ the\ generator$
Input:$N_b = maximum\ buffer\ size$
Initialize classifier D and generator G
For external training steps do
  For internal training steps do
    x ← $D_p + Random\ noise$
    Store x into B_d
    x ← Sample minibatch of m from B_d
    x ← $LSTM_p(x)$
    if $|B_d| < N_b$
      Then delete oldest row vectors from B_d end
    $z \leftarrow LSTM_p$(G(m of random noise vectors))
    Update D with gradient:
      $\nabla_\theta \frac{1}{m}\sum_{i=1}^{m}[logD(x^{(i)}) + \log(1 - D\left(G(z^{(i)})\right))]$
  End
  For internal training steps do
    z← G(m of random noise vectors)
    Store z into B_g
    z ←Sample minibatch of m from B_g
    z ← $LSTM_p(z)$
    if $|B_g| < N_b$
      Then delete oldest row vectors from B_g end
    Update G with gradient:
      $\nabla_\theta \frac{1}{m}\sum_{i=1}^{m}\log(1 - D\left(G(z^{(i)})\right))$
  End
  Acc ← Calculate accuracy with D_o
  if Acc > goal
    Then terminate the training
End

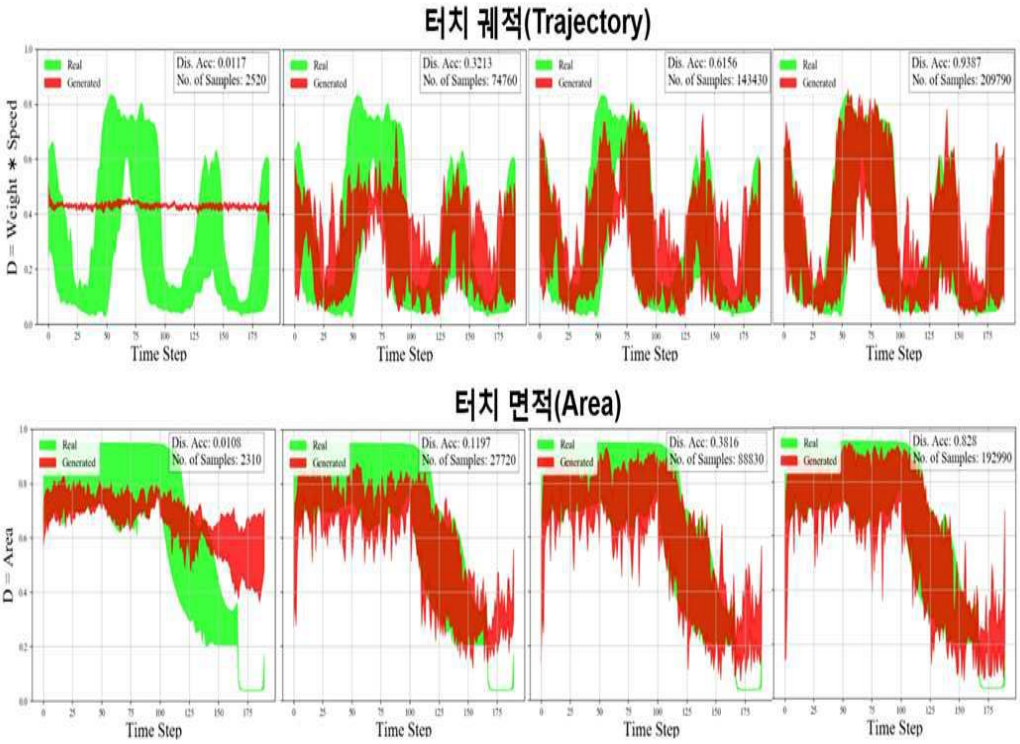
도면12



도면13


Confirm your unlock pattern

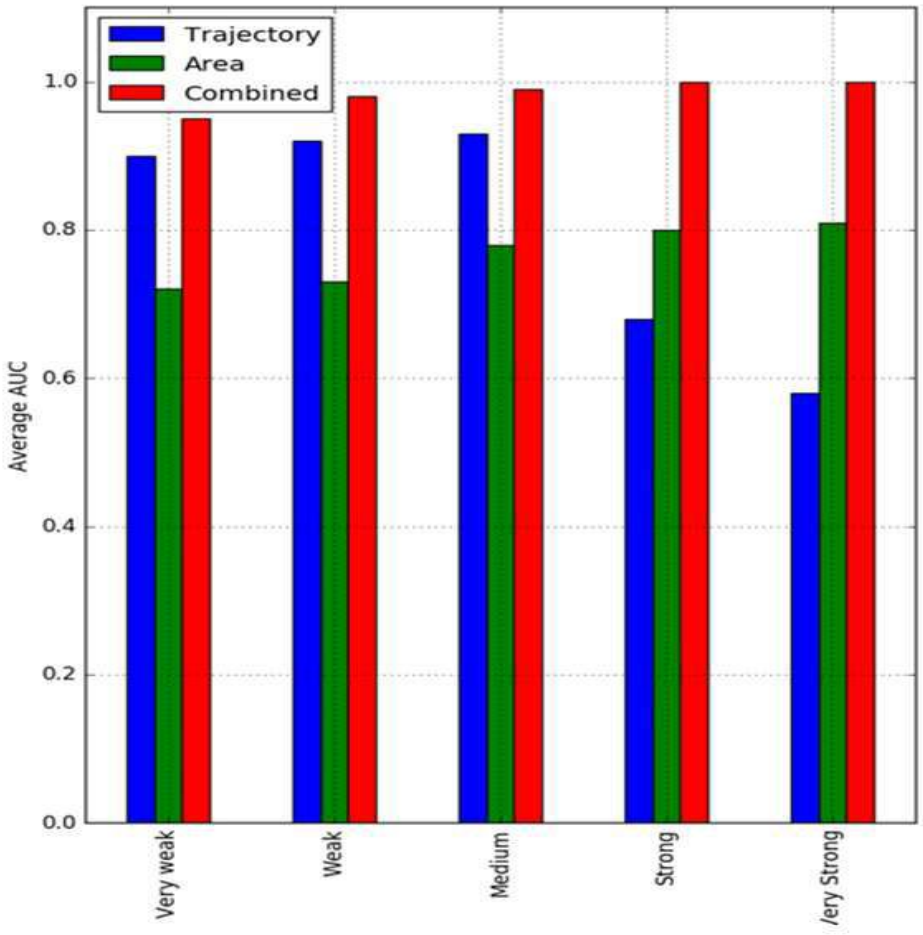
도면14


터치 궤적(Trajectory)
Real
Generated
Dis. Acc: 0.0117
No. of Samples: 2520
Dis. Acc: 0.3213
No. of Samples: 74760
Dis. Acc: 0.6156
No. of Samples: 143430
Dis. Acc: 0.9387
No. of Samples: 209790
D = Weight * Speed
Time Step
터치 면적(Area)
Dis. Acc: 0.0108
No. of Samples: 2310
Dis. Acc: 0.1197
No. of Samples: 27720
Dis. Acc: 0.3816
No. of Samples: 88830
Dis. Acc: 0.828
No. of Samples: 192990
D = Area

도면15


(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14)
(15)

도면16


Trajectory
Area
Combined
Average AUC
1.0
0.8
0.6
0.4
0.2
0.0
Very weak
Weak
Medium
Strong
/ery Strong