(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2024-0087337
(43) 공개일자 2024년06월19일

(51) 국제특허분류(Int. Cl.)
G06F 21/36 (2013.01) *G06F 18/2413* (2023.01)
G06F 21/31 (2013.01) *G06F 21/45* (2013.01)
G06N 20/00 (2019.01) *G06N 3/0455* (2023.01)
(52) CPC특허분류
G06F 21/36 (2013.01)
G06F 18/2413 (2023.01)
(21) 출원번호 10-2022-0172939
(22) 출원일자 2022년12월12일
심사청구일자 2022년12월12일

(71) 출원인
주식회사 카카오뱅크
경기도 성남시 분당구 분당내곡로 131, 판교테크원 11층 (백현동)
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
한대희
경기도 성남시 분당구 분당내곡로 131, 11층(백현동, 판교테크원)
신동화
경기도 성남시 분당구 분당내곡로 131, 11층(백현동, 판교테크원)
(뒷면에 계속)
(74) 대리인
카이특허법인(유한)

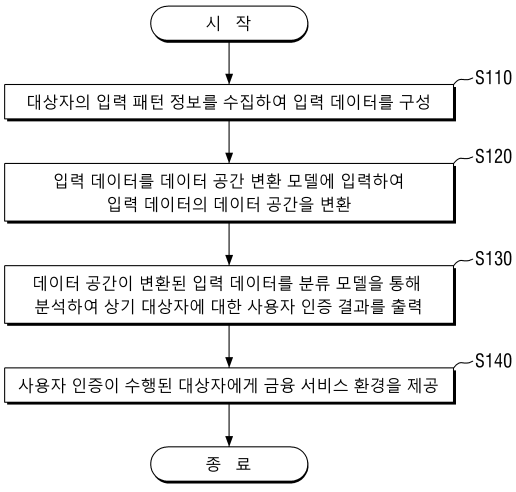
전체 청구항 수 : 총 14 항

(54) 발명의 명칭 **입력 패턴 정보를 이용한 사용자 인증 방법 및 장치**

(57) 요 약

본 발명은 입력 패턴 정보를 이용한 사용자 인증 방법 및 장치가 제공된다. 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법은 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계, 상기 입력 데이터를 데이터 공간 변환 모델에 입력하여 상기 입력 데이터의 데이터 공간을 변환하는 단계 및 상기 데이터 공간이 변환된 입력 데이터를 분류 모델을 통해 분석하여 상기 대상자에 대한 사용자 인증 결과를 출력하는 단계를 포함한다.

대 표 도 - 도3



(52) CPC특허분류
G06F 21/316 (2013.01)
G06F 21/45 (2013.01)
G06N 20/00 (2021.08)
G06N 3/0455 (2023.01)
(72) 발명자
강필성
서울특별시 양천구 목동동로 177 삼성쉐르빌2, 506호
허재혁
서울특별시 성북구 고려대로27길 47, 503호
김정섭
서울특별시 노원구 초안산로2라길 26, 106동 1406호
정의석
서울특별시 강남구 학동로68길 30 삼성동중앙하이츠빌리지아파트, 101동 1003호
김수빈
경기도 화성시 동탄중앙로 200 메타폴리스, D-3606

명 세 서

청구범위

청구항 1

사용자 장치에서 수행되는 사용자 인증 방법에 있어서,

상기 사용자 장치를 이용 중인 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계;

상기 입력 데이터를 데이터 공간 변환 모델에 입력하여 상기 입력 데이터의 데이터 공간을 변환하는 단계; 및

상기 데이터 공간이 변환된 입력 데이터를 분류 모델을 통해 분석하여 상기 대상자에 대한 사용자 인증 결과를 출력하는 단계를 포함하는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 2

제1 항에 있어서,

상기 입력 패턴 정보는,

입력 인터페이스 상에서 인증 정보가 입력되는 공간 정보; 및

상기 입력 인터페이스 상에서 상기 인증 정보가 입력되는 시간과 관련된 시간 정보를 포함하는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 3

제2 항에 있어서,

상기 입력 데이터를 구성하는 단계는,

상기 공간 정보 및 상기 시간 정보를 이용하여 시간 정규화 정보를 계산하는 단계; 및

상기 공간 정보, 상기 시간 정보 및 상기 시간 정규화 정보 중 적어도 하나를 이용하여 상기 입력 데이터를 구성하는 단계를 포함하는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 4

제1 항에 있어서,

상기 데이터 공간 변환 모델은, 사용자 데이터가 잠재 공간에서 특정 분포를 따르도록 미리 학습된 모델인

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 5

제4 항에 있어서,

상기 데이터 공간 변환 모델은, 상기 사용자 데이터가 상기 잠재 공간 상에서 정규 분포를 구성하도록 학습된 노말라이징 플로우(Normalizing Flow)로 구성되며,

상기 데이터 공간을 변환하는 단계에서, 상기 입력 데이터는 상기 데이터 공간 변환 모델의 상기 학습된 노말라

이징 플로우에 의해 상기 잠재 공간의 특정 위치로 투영되는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 6

제4 항에 있어서,

상기 데이터 공간 변환 모델은, 상기 사용자 데이터에서 추출된 피쳐를 잠재 공간으로 투영하고, 상기 투영된 피쳐를 기초로 상기 사용자 데이터와 동일 또는 유사한 데이터를 재구성하도록 학습된 오토 인코더로 구성되며,

상기 데이터 공간을 변환하는 단계에서,

상기 입력 데이터가 인가된 상기 학습된 오토 인코더로부터 피쳐가 추출되고, 상기 피쳐는 상기 잠재 공간의 특정 위치로 투영되는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 7

제1 항에 있어서,

상기 분류 모델은, 상기 데이터 공간이 변환된 입력 데이터에 기초하여 상기 대상자가 미리 등록된 사용자와 일치하는지 여부를 판단하도록 학습된 기계 학습 모델 기반의 분류 모델인

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 8

제1 항에 있어서,

상기 데이터 공간 변환 모델에 입력되는 상기 입력 데이터, 및 상기 입력 데이터에 대응하여 상기 데이터 공간 변환 모델에서 출력되는 출력 데이터를 제1 학습 데이터로 저장하는 단계; 및

상기 분류 모델에 입력되는 상기 변환된 입력 데이터, 및 상기 변환된 입력 데이터에 대응하여 상기 분류 모델에서 출력되는 출력 데이터를 제2 학습 데이터로 저장하는 단계를 더 포함하는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 9

제8 항에 있어서,

상기 데이터 공간 변환 모델과 상기 분류 모델을 포함하는 인증 모델이 학습 가능한 상태인지 여부를 판단하는 단계; 및

상기 인증 모델이 학습 가능한 상태인 경우, 상기 제1 학습 데이터로 상기 데이터 공간 변환 모델을 학습시키고, 상기 제2 학습 데이터로 상기 분류 모델을 학습시키는 단계를 더 포함하는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 10

제9 항에 있어서,

상기 데이터 공간 변환 모델에 대한 학습이 완료된 제1 학습 데이터와 상기 분류 모델에 대한 학습이 완료된 제

2 학습 데이터를 삭제하는 단계를 더 포함하는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 11

제1 항에 있어서,

상기 입력 패턴 정보를 이용한 사용자 인증 방법은, 상기 데이터 공간 변환 모델 및 상기 분류 모델을 메모리 또는 스토리지에 저장하여 이용하는 상기 사용자 장치에서 수행되는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 12

제1 항에 있어서,

상기 대상자의 사용자 인증이 완료되는 경우, 상기 대상자에게 상기 금융 서버로부터 제공되는 금융 서비스 환경을 제공하는 단계를 더 포함하는

입력 패턴 정보를 이용한 사용자 인증 방법.

청구항 13

프로세서;

상기 프로세서에 의해 실행되는 컴퓨터 프로그램을 로드하는 메모리; 및

상기 컴퓨터 프로그램을 저장하는 스토리지를 포함하되,

상기 컴퓨터 프로그램은,

대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계;

상기 입력 데이터를 데이터 공간 변환 모델에 입력하여 상기 입력 데이터의 데이터 공간을 변환하는 단계; 및

상기 데이터 공간이 변환된 입력 데이터를 분류 모델을 통해 분석하여 상기 대상자에 대한 사용자 인증 결과를 출력하는 단계를 포함하는

금융 서버.

청구항 14

제1 항 내지 제12 항 중 어느 하나에 기재된 방법을 실행할 수 있는 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

발명의 설명

기 술 분 야

[0001] 본 발명은 입력 패턴 정보를 이용한 사용자 인증 방법 및 장치에 관한 것이다. 구체적으로, 본 발명은 대상자가 인증 정보를 입력하는 과정에서 대상자의 입력 패턴 정보를 수집하고, 수집된 입력 패턴 정보를 기초로 대상자에 대한 사용자 인증을 수행함으로써, 더욱 보안성이 강화된 금융 서비스 환경을 제공할 수 있는 사용자 인증 방법 및 장치에 관한 것이다.

배 경 기 술

[0003] 이 부분에 기술된 내용은 단순히 본 실시예에 대한 배경 정보를 제공할 뿐 종래기술을 구성하는 것은 아니다.

[0004] 금융기관 또는 전자금융업자가 컴퓨팅 장치를 통하여 금융상품 및 서비스를 제공함에 따라, 이용자가 금융기관 또는 전자금융업자의 종사자와 직접 대면하지 않고, 온라인으로 수행되는 비대면 금융 업무 처리 방식이 점점 증가하고 있다.

[0005] 비대면 금융 업무 처리 방식은 고객이 컴퓨터 및 스마트폰 등의 자신의 단말을 통하여 금융 업무 처리를 요청하고, 금융 업무 처리 결과를 자신의 단말을 통하여 확인하게 된다. 이러한 비대면 금융 업무 처리 과정에는 보안과 안전을 위하여 비대면 금융 업무를 요청하는 주체에 대한 사용자 인증이 요구된다.

[0006] 통상적으로 사용자 인증은 사용자가 기설정한 인증 정보를 통해 수행될 수 있다. 예를 들어, 인증 정보는 비밀번호, 패턴, 인증서 정보 또는 지문 등의 생체 정보 등을 포함할 수 있다. 다만, 비대면 금융 업무 처리 기술의 발전과 함께 인증 수단을 해킹하거나, 복제하는 기술도 발전되었으며, 인증 수단이 타인에게 노출되거나, 해킹되는 위험성도 높아지고 있는 상황이다.

[0007] 특히, 복수의 사용자의 인증 수단과 관련된 정보가 하나의 서버에 보관되어 관리되는 경우, 해당 서버에 대한 공격, 해킹으로 복수의 사용자의 인증 수단이 외부로 노출될 수 있는 문제가 발생될 수 있다.

[0008] 따라서, 더욱 안전하고 보안성이 강화된 금융 서비스 환경을 제공하여 비대면 금융 업무의 활성화 및 안정한 비대면 금융 업무가 수행되는 것을 지원할 수 있는 사용자 인증 방법이 요구되고 있는 실정이다.

발명의 내용

해결하려는 과제

[0010] 본 발명의 목적은, 사용자의 입력 패턴 정보를 기초로 사용자 인증을 진행함으로써, 사용자가 더욱 안전하게 비대면 금융 업무를 수행할 수 있도록 하는 입력 패턴 정보를 이용한 사용자 인증 방법 및 장치를 제공하는 것이다.

[0011] 또한, 본 발명의 목적은, 대상자의 프라이버시, 개인 정보를 보호하면서 인증 모델에 대한 개별 학습을 진행할 수 있는 입력 패턴 정보를 이용한 사용자 인증 방법 및 장치를 제공하는 것이다.

[0012] 또한, 본 발명의 목적은, 분류 모델을 통해 데이터 분류 이전에 데이터의 공간 변환을 먼저 수행함으로써, 효율적인 분류 모델의 학습과 높은 분류 성능을 제공할 수 있는 인증 모델을 포함하는 입력 패턴 정보를 이용한 사용자 인증 방법 및 장치를 제공하는 것이다.

[0013] 또한, 본 발명의 목적은, 수집된 데이터에 대한 정규화 과정을 통해 향상된 분류 성능과 정합성을 가지도록 인증 모델을 구축하는 입력 패턴 정보를 이용한 사용자 인증 방법 및 장치를 제공하는 것이다.

[0014] 본 발명의 목적들은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 본 발명의 다른 목적 및 장점들은 하기의 설명에 의해서 이해될 수 있고, 본 발명의 실시예에 의해 보다 분명하게 이해될 것이다. 또한, 본 발명의 목적 및 장점들은 특허 청구 범위에 나타낸 수단 및 그 조합에 의해 실현될 수 있음을 쉽게 알 수 있을 것이다.

과제의 해결 수단

[0016] 상기 기술적 과제를 달성하기 위한 본 발명의 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법은 사용자 장치 또는 금융 서버에서 수행되는 사용자 인증 방법으로, 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계, 상기 입력 데이터를 데이터 공간 변환 모델에 입력하여 상기 입력 데이터의 데이터 공간을 변환하는 단계 및 상기 데이터 공간이 변환된 입력 데이터를 분류 모델을 통해 분석하여 상기 대상자에 대한 사용자 인증 결과를 출력하는 단계를 포함한다.

[0017] 또한, 상기 입력 패턴 정보는 입력 인터페이스 상에서 인증 정보가 입력되는 공간 정보 및 상기 입력 인터페이

스 상에서 상기 인증 정보가 입력되는 시간과 관련된 시간 정보를 포함할 수 있다.

[0018] 또한, 상기 입력 데이터를 구성하는 단계는 상기 공간 정보 및 상기 시간 정보를 이용하여 시간 정규화 정보를 계산하는 단계 및 상기 공간 정보, 상기 시간 정보 및 상기 시간 정규화 정보 중 적어도 하나를 이용하여 상기 입력 데이터를 구성하는 단계를 포함할 수 있다.

[0019] 또한, 상기 데이터 공간 변환 모델은 사용자 데이터가 잠재 공간에서 특정 분포를 따르도록 미리 학습된 모델일 수 있다.

[0020] 또한, 상기 데이터 공간 변환 모델은 상기 사용자 데이터가 상기 잠재 공간 상에서 정규 분포를 구성하도록 학습된 노말라이징 플로우(Normalizing Flow)로 구성되며, 상기 데이터 공간을 변환하는 단계에서, 상기 입력 데이터는 상기 데이터 공간 변환 모델의 상기 학습된 노말라이징 플로우에 의해 상기 잠재 공간의 특정 위치로 투영될 수 있다.

[0021] 또한, 상기 데이터 공간 변환 모델은 상기 사용자 데이터에서 추출된 피처를 잠재 공간으로 투영하고, 상기 투영된 피처를 기초로 상기 사용자 데이터와 동일 또는 유사한 데이터를 재구성하도록 학습된 오토 인코더로 구성되며, 상기 데이터 공간을 변환하는 단계에서 상기 입력 데이터는 상기 학습된 오토 인코더에 의해 피처가 추출되고, 상기 피처는 상기 잠재 공간의 특정 위치로 투영될 수 있다.

[0022] 또한, 상기 분류 모델은 상기 데이터 공간이 변환된 입력 데이터에 기초하여 상기 대상자가 미리 등록된 사용자와 일치하는지 여부를 판단하도록 학습된 기계 학습 모델 기반의 분류 모델일 수 있다.

[0023] 또한, 상기 데이터 공간 변환 모델에 입력되는 상기 입력 데이터, 및 상기 입력 데이터에 대응하여 상기 데이터 공간 변환 모델에서 출력되는 출력 데이터를 제1 학습 데이터로 저장하는 단계 및 상기 분류 모델에 입력되는 상기 변환된 입력 데이터, 및 상기 변환된 입력 데이터에 대응하여 상기 분류 모델에서 출력되는 출력 데이터를 제2 학습 데이터로 저장하는 단계를 더 포함할 수 있다.

[0024] 또한, 상기 데이터 공간 변환 모델과 상기 분류 모델을 포함하는 인증 모델이 학습 가능한 상태인지 여부를 판단하는 단계 및 상기 인증 모델이 학습 가능한 상태인 경우, 상기 제1 학습 데이터로 상기 데이터 공간 변환 모델을 학습시키고, 상기 제2 학습 데이터로 상기 분류 모델을 학습시키는 단계를 더 포함할 수 있다.

[0025] 또한, 상기 데이터 공간 변환 모델에 대한 학습이 완료된 제1 학습 데이터와 상기 분류 모델에 대한 학습이 완료된 제2 학습 데이터를 삭제하는 단계를 더 포함할 수 있다.

[0026] 또한, 상기 입력 패턴 정보를 이용한 사용자 인증 방법은, 상기 데이터 공간 변환 모델 및 상기 분류 모델을 메모리 또는 스토리지에 저장하여 이용하는 상기 사용자 장치에서 수행될 수 있다.

[0027] 또한, 상기 대상자의 사용자 인증이 완료되는 경우, 상기 대상자에게 상기 금융 서버로부터 제공되는 금융 서비스 환경을 제공하는 단계를 더 포함할 수 있다.

[0028] 상기 기술적 과제를 달성하기 위한 본 발명의 실시예에 따른 장치는 프로세서, 상기 프로세서에 의해 실행되는 컴퓨터 프로그램을 로드하는 메모리 및 상기 컴퓨터 프로그램을 저장하는 스토리지를 포함하되, 상기 컴퓨터 프로그램은 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계, 상기 입력 데이터를 데이터 공간 변환 모델에 입력하여 상기 입력 데이터의 데이터 공간을 변환하는 단계 및 상기 데이터 공간이 변환된 입력 데이터를 분류 모델을 통해 분석하여 상기 대상자에 대한 사용자 인증 결과를 출력하는 단계를 포함할 수 있다.

[0029] 상기 기술적 과제를 달성하기 위한 본 발명의 실시예에 따른 기록매체는 상기 방법을 실행할 수 있는 프로그램을 기록한 컴퓨터로 읽을 수 있다.

발명의 효과

[0031] 본 발명의 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법 및 장치는, 사용자의 입력 패턴 정보를 통해 사용자 인증을 진행하여, 사용자가 더욱 안전하게 비대면 금융 업무를 수행하는 것을 지원할 수 있다.

[0032] 또한, 본 발명은, 사용자 장치에서 학습에 사용된 학습 데이터를 학습이 완료된 이후 삭제하도록 구성(즉, 온-디바이스(on-device)에서 구동)하여, 대상자의 프라이버시 및 개인 정보를 보호하면서 인증 모델에 대한 개별 학습을 진행할 수 있다.

[0033] 또한, 본 발명은, 분류 모델을 통해 데이터 분류 이전에 데이터의 공간 변환을 먼저 수행함으로써, 효율적인 분류 모델의 학습과 높은 분류 성능을 제공할 수 있다.

[0034] 또한, 본 발명은, 수집된 데이터에 대한 정규화 과정을 통해 향상된 분류 성능과 정합성을 가진 인증 모델을 구축할 수 있다.

[0035] 상술한 내용과 더불어 본 발명의 구체적인 효과는 이하 발명을 실시하기 위한 구체적인 사항을 설명하면서 함께 기술한다.

도면의 간단한 설명

[0037] 도 1은 본 발명의 몇몇 실시예에 따른 사용자 장치를 설명하기 위한 개념도이다.

도 2는 본 발명의 몇몇 실시예에 따른 사용자 장치와 금융 서버와의 관계를 설명하기 위한 개념도이다.

도 3은 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법의 순서도이다.

도 4는 입력 패턴 정보를 설명하기 위한 예시도이다.

도 5는 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계의 세부 단계를 도시한다.

도 6은 공간 정보 및 시간 정보를 통해 시간 정규화 정보를 생성하는 과정을 설명하기 위한 예시도이다.

도 7은 본 발명의 몇몇 실시예에 따른 인증 모델의 구조를 예시적으로 도시한다.

도 8은 노말라이징 플로우로 구성된 데이터 공간 변환 모델을 학습하는 과정을 설명하기 위한 예시도이다.

도 9는 노말라이징 플로우에서 입력 데이터에 대응하는 변수(x)와 잠재 공간을 나타내는 변수(z) 사이의 공간 변환 개념을 설명하기 위한 예시도이다.

도 10은 학습된 데이터 공간 변환 모델(노말라이징 플로우)를 통해 사용자가 구분되는 과정을 설명하기 위한 예시도이다.

도 11은 오토 인코더로 구성된 데이터 공간 변환 모델을 설명하기 위한 예시도이다.

도 12는 데이터 공간 변환이 수행되기 이전 상태에서 분류 모델을 통해 데이터를 분류하는 과정을 예시적으로 도시한다.

도 13은 데이터 공간 변환이 수행된 상태에서 분류기를 통해 데이터를 분류하는 과정을 예시적으로 도시한다.

도 14는 입력 데이터에 따라 인증 모델의 성능을 비교, 분석한 결과를 나타낸다.

도 15는 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법의 인증 모델을 학습하는 세부 단계의 순서도이다.

도 16은 추론 프로세스와 인증 프로세스와의 관계를 설명하기 위한 예시도이다.

도 17은 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법을 수행하는 시스템의 하드웨어 구현을 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0038] 본 명세서 및 특허청구범위에서 사용된 용어나 단어는 일반적이거나 사전적인 의미로 한정하여 해석되어서는 아니된다. 발명자가 그 자신의 발명을 최선의 방법으로 설명하기 위해 용어나 단어의 개념을 정의할 수 있다는 원칙에 따라, 본 발명의 기술적 사상과 부합하는 의미와 개념으로 해석되어야 한다. 또한, 본 명세서에 기재된 실시예와 도면에 도시된 구성은 본 발명이 실현되는 하나의 실시예에 불과하고, 본 발명의 기술적 사상을 전부 대변하는 것이 아니므로, 본 출원시점에 있어서 이들을 대체할 수 있는 다양한 균등물과 변형 및 응용 가능한 예들이 있을 수 있음을 이해하여야 한다.

[0039] 본 명세서 및 특허청구범위에서 사용된 제1, 제2, A, B 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성

요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. '및/또는' 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

[0040] 본 명세서 및 특허청구범위에서 사용된 용어는 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함한다. 본 출원에서 "포함하다" 또는 "가지다" 등의 용어는 명세서상에 기재된 특징, 숫자, 단계, 동작, 구성요소, 부품 또는 이들을 조합한 것들의 존재 또는 부가 가능성을 미리 배제하지 않는 것으로 이해되어야 한다.

[0041] 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해서 일반적으로 이해되는 것과 동일한 의미를 가지고 있다.

[0042] 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 출원에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.

[0043] 또한, 본 발명의 각 실시예에 포함된 각 구성, 과정, 공정 또는 방법 등은 기술적으로 상호 간 모순되지 않는 범위 내에서 공유될 수 있다.

[0044] 이하에서, 도 1 내지 도 17을 참조하여 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법 및 장치에 대해 설명하도록 한다.

[0046] 도 1은 본 발명의 몇몇 실시예에 따른 사용자 장치를 설명하기 위한 개념도이다. 도 2는 본 발명의 몇몇 실시예에 따른 사용자 장치와 금융 서버와의 관계를 설명하기 위한 개념도이다.

[0047] 도 1을 참조하면, 사용자 장치(100)는 금융 서버(200)가 제공하는 금융 서비스 환경을 대상자(P)에게 제공하도록 구성될 수 있다.

[0048] 사용자 장치(100)는 유무선 통신 환경에서 금융 어플리케이션을 동작 시킬 수 있는 통신 단말기를 의미한다. 실시예에서, 사용자 장치(100)는 사용자의 휴대용 단말기일 수 있다. 즉, 사용자 장치(100)는 휴대용 단말기의 일종인 스마트폰(smart phone)일 수 있으나, 금융 서버(200)의 금융 서비스 환경을 제공할 수 있는 금융 어플리케이션을 탑재할 수 있으며, 사용자의 입력을 수신하고, 금융 서비스를 사용자에게 출력할 수 있는 장치에 제한없이 적용될 수 있다.

[0049] 예를 들어, 사용자 단말기(200)는 퍼스널 컴퓨터(PC), 노트북, 태블릿, 휴대폰, 스마트폰, 웨어러블 디바이스(예를 들어, 워치형 단말기) 등의 다양한 형태의 전자 장치를 포함할 수 있다.

[0050] 사용자 장치(100)와 금융 서버(200)는 통신망을 통해 데이터를 교환할 수 있다. 통신망은 사용자 장치(100)가 금융 서버(100)에 접속한 후 데이터를 송수신할 수 있도록 접속 경로를 제공할 수 있다. 통신망은 예컨대 LANs(Local Area Networks), WANs(Wide Area Networks), MANs(Metropolitan Area Networks), ISDNs(Integrated Service Digital Networks) 등의 유선 네트워크나, 무선 LANs, CDMA, 블루투스, 위성 통신 등의 무선 네트워크를 망라할 수 있으나, 본 발명의 범위가 이에 한정되는 것은 아니다.

[0051] 대상자(P)는 이러한 사용자 장치(100)를 이용하여 금융 서버(200)에서 제공하는 금융 서비스 환경을 이용하려는 객체일 수 있다. 구체적으로, 금융 서버(200)가 제공하는 금융 서비스 환경은 복수의 사용자 계정을 포함할 수 있으며, 대상자(P)는 복수의 사용자 계정 중 하나의 사용자 계정과 관련된 금융 서비스를 이용하려는 객체일 수 있다. 즉, 대상자(P)는 사용자 계정의 사용자일 수 있으나, 이에 한정되는 것은 아니며, 사용자 계정을 무단으로 이용하려는 침입자일 수 있다.

[0052] 사용자 장치(100)는 이러한 대상자(P)에게 사용자 인증을 요청할 수 있다. 사용자 장치(100)는 대상자(P)가 사용자 인증을 진행하고 사용자 인증이 정상적으로 수행되는 경우, 대상자(P)에게 특정 사용자 계정과 관련된 금융 서비스를 제공할 수 있다. 실시예에서, 사용자 장치(100)는 인증 정보를 요청하는 사용자 인터페이스를 출력하고, 대상자(P)의 입력을 수신하도록 구성된 입출력 장치(미도시)를 포함할 수 있다. 여기서, 입출력 장치는 패드, 키패드, 키보드, 마우스, 터치패드, 터치스크린 및 디스플레이 장치 중 적어도 하나일 수 있으나, 이에 한정되는 것은 아니다.

[0053] 여기서, 사용자가 사용자 장치(100)의 입출력 장치를 통해 인증 정보를 입력하는 과정에서, 사용자의 개인화된

입력 특성이 나타날 수 있다. 예를 들어, 입출력 장치가 터치 스크린인 경우, 터치 스크린을 터치하는 위치, 터치하는 시간 등이 사용자별로 상이하게 나타날 수 있다. 본 명세서에서, 사용자가 입출력 장치를 통해 인증 정보 또는 특정 정보를 입력할 때 나타나는 개인화된 입력 특성을 '입력 패턴 정보'라 정의한다.

[0054] 사용자 장치(100)는 대상자(P)가 사용자 인증을 위한 절차를 수행하는 과정에서 대상자의 입력 패턴 정보를 수집할 수 있다. 구체적으로, 사용자 장치(100)는 대상자(P)가 사용자 인증을 위해 인증 정보를 입력하는 과정에서 대상자의 입력 패턴 정보와 대상자가 입력한 인증 정보를 각각 수집할 수 있다.

[0055] 본 발명에서, 대상자(P)에 대한 사용자 인증은 이러한 입력 패턴 정보에 기반하여 수행될 수 있다. 몇몇 실시예에서, 입출력 장치를 통해 수집되는 인증 정보와 입력 패턴 정보 중 적어도 하나에 기초하여 사용자 인증이 수행될 수 있다. 몇몇 실시예에서, 입출력 장치를 통해 수집되는 인증 정보와 특정 사용자 계정의 인증 정보와 일치 여부를 먼저 판단하고, 인증 정보가 일치된 대상자(P)의 입력 패턴 정보를 더 분석하여 사용자 인증을 수행할 수 있다. 즉, 종래의 인증 방법, 인증 시스템은 수집된 인증 정보와 미리 저장된 인증 정보 사이의 일치 여부만으로 사용자 인증을 수행한 것에 비해, 사용자 인증의 보안성 및 안전성이 더욱 강화될 수 있다.

[0056] 몇몇 실시예에서, 사용자 장치(100)는 대상자의 입력 패턴 정보에 기반하여 대상자의 사용자 인증을 수행하기 위한 인증 모델을 포함할 수 있으며, 인증 모델을 이용하여 대상자에 대한 사용자 인증을 수행하게 된다.

[0057] 도 2를 참조하면, 사용자 장치(100)는 인증 모델을 포함하는 온-디바이스(On-device) 방식으로 구성될 수 있다. 인증 모델은 금융 서버(200)가 아닌 사용자 장치(100)에 포함될 수 있다. 사용자 장치(100)에서 수집된 정보를 중앙 서버(금융 서버(200) 또는 별도의 분석 서버)로 전송하여 분석하고, 다시 분석된 결과를 전송받는 종래의 분석 방식이 아닌 기기 자체적으로 정보를 수집하고 연산하도록 구성될 수 있다. 즉, 단말 기기 내부에서 정보를 처리하기 때문에 저지연을 통한 빠른 작업이 가능할 뿐만 아니라, 복수의 사용자들의 인증 정보가 한 번에 유출되거나, 해킹되는 등의 보안 문제도 해결할 수 있게 된다.

[0058] 사용자 장치(100)는 포함된 인증 모델을 이용하여 대상자(P)의 사용자 인증이 정상적으로 수행되는 경우, 인증 완료를 금융 서버(200)에 전달할 수 있다. 금융 서버(200)는 사용자 장치(100)에서 제공된 인증 완료에 대응하여, 특정 사용자와 관계된 금융 서비스 환경을 사용자 장치(100)에 제공할 수 있다. 사용자 장치(100)는 제공된 금융 서비스 환경을 입출력 장치를 통해 출력하여, 대상자(P)에게 금융 서비스를 제공할 수 있다.

[0059] 또한, 몇몇 실시예에 따른 사용자 장치(100)는 포함된 인증 모델에 대한 학습을 더 수행하도록 구성될 수 있다. 사용자 장치(100)는 사용자 인증을 위해 수집된 대상자(P)의 입력 패턴 정보를 수집할 수 있으며, 수집된 입력 패턴 정보와 사용자 인증 결과를 이용하여 인증 모델에 대한 학습을 수행하여, 인증 모델의 식별력 및 정확성을 더욱 강화시킬 수 있으며, 학습을 완료한 이후 수집된 학습 데이터는 폐기하여 대상자의 프라이버시 보호 및 보안성을 더욱 높일 수 있다.

[0060] 정리하면, 본 발명의 몇몇 실시예에 따른 사용자 장치(100)는 온-디바이스 기반의 장치로, 인증 모델을 통해 대상자의 입력 패턴 정보를 분석하여 대상자의 사용자 인증을 수행할 수 있다.

[0061] 다만, 본 발명의 실시예가 이에 한정되는 것은 아니며, 몇몇 실시예에서 인증 모델은 금융 서버(200)에 포함될 수 있으며, 금융 서버(200)에서 사용자 장치(100)로부터 제공된 인증 정보 및 입력 패턴 정보에 대한 사용자 인증이 수행될 수도 있다. 그러나 본 명세서에서는, 온-디바이스 기반의 사용자 인증 방법에 대해 설명하는 바, 이하에서는 사용자 장치(100)에서 사용자 인증 방법을 수행하는 실시예들을 위주로 설명한다.

[0062] 금융 서버(200)는 대상자에 대한 사용자 인증이 정상적으로 수행되는 경우, 인증 완료와 함께 특정 사용자와 관계된 금융 서비스 환경을 사용자 장치(100)에 제공할 수 있다.

[0064] 이하에서는 도 3 내지 도 14를 참조하여, 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법에 대해 자세히 설명하도록 한다. 실시예에 따른 방법은 사용자 장치(100) 또는 금융 서버(200)에서 수행될 수 있다.

[0065] 도 3은 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법의 순서도이다. 도 4는 입력 패턴 정보를 설명하기 위한 예시도이다. 도 5는 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계의 세부 단계를 도시한다. 도 6은 공간 정보 및 시간 정보를 통해 시간 정규화 정보를 생성하는 과정을 설명하기 위한 예시도이다. 도 7은 본 발명의 몇몇 실시예에 따른 인증 모델의 구조를 예시적으로 도시한다. 도 8은 노말라이징 플로우로 구성된 데이터 공간 변환 모델을 학습하는 과정을 설명하기 위한 예시도이다. 도 9는

노말라이징 플로우에서 입력 데이터에 대응하는 변수(x)와 잠재 공간을 나타내는 변수(z) 사이의 공간 변환 개념을 설명하기 위한 예시도이다. 도 10은 학습된 데이터 공간 변환 모델(노말라이징 플로우)를 통해 사용자가 구분되는 과정을 설명하기 위한 예시도이다. 도 11은 오토 인코더로 구성된 데이터 공간 변환 모델을 설명하기 위한 예시도이다. 도 12는 데이터 공간 변환이 수행되기 이전 상태에서 분류 모델을 통해 데이터를 분류하는 과정을 예시적으로 도시한다. 도 13은 데이터 공간 변환이 수행된 상태에서 분류기를 통해 데이터를 분류하는 과정을 예시적으로 도시한다. 도 14는 입력 데이터에 따라 인증 모델의 성능을 비교, 분석한 결과를 나타낸다.

[0067] 도 3을 참조하면, 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법은 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계(S110), 입력 데이터를 데이터 공간 변환 모델에 입력하여 입력 데이터의 데이터 공간을 변환하는 단계(S120), 데이터 공간이 변환된 입력 데이터를 분류 모델을 통해 분석하여 상기 대상자에 대한 사용자 인증 결과를 출력하는 단계(S130)를 포함한다.

[0068] 먼저, 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성한다(S110).

[0069] 대상자(P)는 이용하려는 사용자 계정에 대한 사용자 인증을 위해 인증 정보를 입력할 수 있다. 대상자(P)는 사용자 계정에 대한 인증을 위해 사용자 장치(100)를 이용 중인 사용자일 수 있다. 대상자(P)가 인증 정보를 입력하는 과정에서 대상자의 입력 패턴 정보가 수집될 수 있다. 여기서, 인증 정보는 비밀번호, 패턴, 인증서 정보 또는 지문 등의 생체 정보일 수 있다. 대상자(P)는 이러한 인증 정보를 입력하는 과정에서 개인화된 입력 특성이 나타낼 수 있으며, 단계(S110)에서, 이러한 개인화된 입력 특성이 입력 패턴 정보로 수집될 수 있다.

[0070] 입력 패턴 정보는 입력 인터페이스 상에서 인증 정보가 입력되는 공간 정보를 포함할 수 있다. 실시예에서, 입력 인터페이스는 인증 정보를 입력하기 위한 입력 아이콘을 제공할 수 있다. 예를 들어, 입력 아이콘은 입력 인터페이스에서 일정 공간을 가지도록 구성될 수 있으며, 입력 아이콘의 공간은 X-Y 평면 좌표로 정의될 수 있다. 여기에서, 본 발명에서 이용하는 좌표축은 X-Y 좌표로 한정되는 것은 아니나, 이하에서는 설명의 편의를 위해 X-Y 평면 좌표축을 이용하는 것을 예로 들어 설명하도록 한다.

[0071] 대상자는 입력 아이콘의 공간 좌표와 상호 작용(터치 또는 클릭)하여 인증 정보를 입력할 수 있으며, 사용자가 상호 작용한 공간 좌표(X-Y)가 입력 패턴 정보의 공간 정보로 수집되게 된다.

[0072] 몇몇 실시예에서, 인증 정보는 복수의 숫자로 구성된 비밀번호일 수 있으며, 입력 인터페이스는 도 4의 <a>와 같이 숫자를 입력할 수 있는 0에서 9에 대응하는 숫자 아이콘을 대상자에게 제공할 수 있다.

[0073] 대상자는 비밀번호에 대응되도록 숫자 아이콘에서 복수의 숫자를 선택하여 순서대로 입력할 수 있다. 입력 인터페이스에서 각각의 숫자 아이콘은 미리 설정된 공간에 위치할 수 있으며, 각 공간에 대한 X-Y 평면 좌표가 설정될 수 있다. 대상자는 입력 인터페이스에서 각 숫자 아이콘의 공간 좌표를 터치 또는 클릭하는 상호 작용을 할 수 있으며, 해당 숫자가 입력될 수 있다. 여기서, 복수의 사용자들이 숫자 6을 인증 정보로 입력하더라도, 각 사용자가 숫자 6 아이콘에서 상호 작용(터치 또는 클릭)한 X-Y 평면 좌표는 상이할 수 있다. 따라서, 이러한 공간 정보는 각 사용자들의 개인화된 입력 특성을 나타내는 정보로 활용될 수 있다. 예를 들어, 인증 정보가 6개의 숫자로 구성된 비밀번호인 경우, 6개의 숫자 아이콘과의 상호 작용에 기초하여 도 4의 <b>와 같은 6개의 X, Y 평면 좌표가 공간 정보로 수집될 수 있다.

[0074] 또한, 입력 패턴 정보는 입력 인터페이스 상에서 인증 정보가 입력되는 시간과 관련된 시간 정보를 포함할 수 있다. 사용자에 따라 입력 인터페이스를 통해 인증 정보를 입력하는 시간이 상이할 수 있다. 따라서, 이러한 시간 정보는 각 사용자들의 개인화된 입력 특성을 나타내는 정보로 활용될 수 있다. 여기서, 시간 정보는 인증 정보가 입력되는 전체 시간을 의미할 수 있으나, 본 발명의 실시예가 이에 한정되는 것은 아니다.

[0075] 몇몇 실시예에서, 인증 정보는 입력 인터페이스의 복수의 입력 아이콘과 관계되도록 구성될 수 있다. 복수의 입력 아이콘은 인증 정보에 따라 순서대로 대상자와 상호 작용하게 되며, 각각의 아이콘에 대한 상호 작용이 수행되는 시간이 수집될 수 있다. 실시예에서, 도 4의 <c>와 같이, 시간 정보는 선행 아이콘의 상호 작용 시간과 후행 아이콘의 상호 작용 시간 사이의 차이를 의미할 수 있다. 예를 들어, 인증 정보가 6개의 숫자로 구성된 비밀번호인 경우 6개의 숫자 아이콘과의 상호 작용에 기초하여 X, Y 평면 좌표가 공간 정보로 수집될 수 있으며, 각 평면 좌표의 수집 시각 사이의 시간 차이가 시간 정보로 수집될 수 있다.

[0076] 단계(S110)에서, 상술한 바와 같이 수집된 입력 패턴 정보를 입력 데이터로 구성할 수 있다.

[0077] 예를 들어, 대상자가 6개의 숫자로 구성된 비밀번호를 입력하는 과정에 따라 수집된 공간 정보(X1, X2, …, X6

및 Y1, Y2, …, Y6))와 시간 정보(T1, T2, …, T5)가 대상자에 대응한 입력 데이터로 도 4의 <d>와 같이 구성될 수 있다.

[0078] 몇몇 실시예에서, 단계(S110)는 수집된 입력 패턴 정보를 변형하여 추가적인 입력 데이터를 구성할 수 있다. 이러한 입력 데이터는 후술하는 단계(S120) 및 단계(S130)에서 인공지능 기반의 인증 모델에 입력되는 데이터에 해당한다. 실시예에서, 단계(S120) 및 단계(S130)에서 사용되는 인증 모델은 단계(S110)에서 구성되는 입력 데이터에 기반하여 미리 학습된 상태일 수 있다.

[0079] 도 5를 참조하면, 단계(S110)는, 공간 정보 및 시간 정보를 이용하여 시간 정규화 정보를 계산하는 단계(S112) 및 공간 정보, 시간 정보 및 시간 정규화 정보 중 적어도 하나를 이용하여 입력 데이터를 구성하는 단계(S114)를 포함할 수 있다.

[0080] 단계(S112)에서, 공간 정보와 시간 정보를 이용하여 시간 정규화 정보가 계산될 수 있다. 이러한, 시간 정규화 정보는 인공지능 기반의 인증 모델에 사전 지식(prior knowledge)를 더해줄 수 있으며, 매개 변수(parameters)에 대한 사전 분포가 더욱 구체적으로 지정되도록 하여 학습 가능한 함수의 집합에 제약을 두는 역할을 제공할 수 있다. 이에 따라, 인증 모델이 과적합(overfitting)되는 것을 방지하고, 더욱 정확한 예측이 수행되는 것을 가능하게 한다.

[0081] 단계(S112)에서, 시간 정규화 정보는 연속하는 공간 정보가 수집된 시간을 연속하는 공간 정보 사이의 거리로 나누어 계산될 수 있다. 예시적으로, 제1 시간(T1)에 대응하는 제1 시간 정규화 정보(T1 norm)은 도 6의 <a>에 도시된 바와 같이, 제1 시간(T1)을 제2 공간 정보(X2, Y2)와 제1 공간 정보(X1, Y1) 사이의 거리로 나누어서 계산될 수 있다. 각각의 시간에 대응하는 시간 정규화 정보(T norm)가 단계(S112)에서 계산될 수 있다.

[0082] 단계(S114)에서, 공간 정보, 시간 정보 및 시간 정규화 정보 중 적어도 하나를 이용하여 입력 데이터가 구성된다.

[0083] 단계(S114)는 예측 모델에 입력할 입력 데이터를 구성하고, 구성된 입력 데이터에 대한 전처리를 수행하는 단계일 수 있다. 실시예에서, 입력 데이터는 공간 정보, 시간 정보 및 시간 정규화 정보 중 적어도 하나를 이용하여 구성될 수 있다. 몇몇 실시예에서, 입력 데이터는 수집된 공간 정보 및 시간 정보와 계산된 시간 정규화 정보를 모두 포함하도록 구성될 수 있으나, 본 발명의 실시예가 이에 한정되는 것은 아니다. 도 6의 <b>에 도시된 예시와 같이, 입력 데이터는 시간 정보 및 시간 정규화 정보를 포함하도록 구성될 수도 있다.

[0085] 다시, 도 3을 참조하면, 구성된 입력 데이터를 통해 사용자 인증을 수행하는 단계(S120, S130)가 수행되게 된다.

[0086] 본 발명의 실시예에서, 인증 모델은 특정 사용자와 관련된 사용자 데이터에 기초하여 미리 학습된 상태일 수 있다. 여기서, 사용자 데이터는 대상자가 이용하려는 특정 사용자 계정에 대응되는 사용자가 종래 입력한 입력 데이터를 의미할 수 있다. 종래 사용자 계정의 사용자는 인증 정보를 입력하는 과정에서 복수의 입력 데이터가 수집될 수 있으며, 이러한 입력 데이터를 기초로 인증 모델이 미리 구축, 학습된 상태일 수 있다. 실시예에서, 인증 모델은 사용자 계정에 따라 개별적으로 미리 구축, 학습된 상태일 수 있다.

[0087] 도 7을 참조하면, 인증 모델(AM)은 데이터 공간 변환 모델(DTM)과 분류 모델(CM)을 포함할 수 있다. 인증 모델(AM)에서, 데이터 공간 변환 모델(DTM)과 분류 모델(CM)은 순차적으로 동작할 수 있다. 데이터 공간 변환 모델(DTM)을 통해 특정 분포를 가지도록 먼저 데이터를 공간 변환한 이후, 공간 변환된 데이터에 대한 분류가 분류 모델(CM)을 이용하여 수행될 수 있다. 이하에서, 데이터 공간 변환 모델(DTM) 및 분류 모델(CM)을 각각을 학습하는 과정과 학습된 모델들을 이용하여 대상자의 입력 데이터가 분석되는 단계들을 함께 설명하도록 한다.

[0089] 먼저, 이전 단계(S110)에서 구성된 입력 데이터는 데이터 공간 변환 모델(DTM)에 입력되어 입력 데이터의 데이터 공간이 변환된다(S120).

[0090] 여기서, 데이터 공간의 변환은 잠재 공간(latent space)로의 투영을 의미할 수 있다. 데이터 공간 변환 모델은 잠재 공간에서 동일 또는 유사한 특징을 가진 입력 데이터가 인접하게 위치되어 군집을 형성하도록 입력 데이터의 공간을 변환할 수 있다. 즉, 데이터 공간 변환 모델(DTM)을 통해 입력 데이터는 동일 또는 유사한 특징을 가진 데이터들이 투영된 공간으로 이동될 수 있다.

[0091] 단계(S120)에서, 데이터 공간 변환 모델(DTM)은 사용자 데이터를 기초로 미리 학습된 상태일 수 있다. 즉, 데이터 공간 변환 모델(DTM)은 특정 사용자와 관련된 사용자 데이터가 변형된 잠재 공간에서 특정 범위 내의 위치로 공간 이동되도록 학습된 모델에 해당한다. 여기에서, 데이터 공간 변환 모델(DTM)은 사용자 데이터가 잠재 공간에서 특정 분포를 따르도록 미리 학습된 모델일 수 있다. 몇몇 실시예에서, 이러한 데이터 공간 변환 모델(DTM)은 생성 모델(Generative model)에 기반하여 구성될 수 있다.

[0092] 구체적으로, 몇몇 실시예에 따른 데이터 공간 변환 모델(DTM)은 노말라이징 플로우(Normalizing Flow)로 구성될 수 있다. 노말라이징 플로우는 학습을 통해 입력 데이터를 역변환이 존재하는 여러 변환을 거쳐 정규 분포(gaussian distribution)를 따르는 잠재 벡터값을 갖도록 함으로써 공간 변환을 구현할 수 있다. 즉, 단계(S120)에서, 대상자의 입력 데이터는 학습된 노말라이징 플로우에 의해 상기 잠재 공간의 특정 위치로 투영될 수 있다.

[0093] 도 8을 참조하면, 학습에 사용된 사용자 데이터가 정규 분포를 이루도록 노말라이징 플로우에 대한 학습이 수행되게 된다. 예시적으로 도시된 사용자 데이터의 공간 정보 및 2차원 산점도에서, 사용자 데이터는 서로 공간적으로 분산된 상태인 것을 알 수 있다. 노말라이징 플로우는 이러한 사용자 데이터가 잠재 공간 내에서 정규 분포를 구성하도록 학습될 수 있다.

[0094] 도 9는 노말라이징 플로우에서 입력 변수(X)와 잠재 공간을 나타내는 변수(Z) 사이의 공간 변환 개념을 설명한다. 여기서, 학습 과정에서 입력 변수(X)는 사용자 데이터를 의미한다. 도 9를 참조하면, 입력 변수(X)는 최종적인 잠재 공간(Latent Space, Z_k)에 적어도 하나의 정규화 함수(f)를 통해 변환될 수 있다. 여기서, 최종적인 잠재 공간은 정규 분포가 형성된 공간을 의미할 수 있다. 도 9에 도시된 바와 같이, 잠재 공간은 순차적으로 이동되는 복수의 계층으로 구성될 수 있으며, 잠재 공간 사이의 데이터 변환은 대응되는 정규화 함수를 통해 수행될 수 있다. 즉, 노말라이징 플로우는 이러한 정규화 함수들의 시퀀스를 포함하는 것으로 이해될 수 있으며, 노말라이징 플로우에 대한 학습은 입력되는 데이터가 정규 분포를 구성하도록 변환되는 확률을 높이도록 정규화 함수들을 구성하는 과정일 수 있다. 또한, 이러한 정규화 함수(f)는 가역적인 특성을 가지는 함수로 역함수(f^{-1})로의 변환이 가능한 함수일 수 있으며, 잠재 공간에 배치된 데이터를 기준으로 입력 변수를 재구축하는 과정은 역함수를 통해 수행될 수 있다.

[0095] 도 9에 도시된 과정을 최적화하기 위한 본 발명의 실시예에 따른 노말라이징 플로우의 목적 함수(objective function)은 하기 수학식 1과 같이 표현될 수 있다.

[0097] [수학식 1]

[0098]
$$\log p_x(x) = \log p_z(z_k) + \sum_{i=1}^{k} \log \left| \det \frac{\partial f_i(x)}{\partial z_{i-1}} \right|$$

[0100] 여기서, P_x는 입력 데이터(x)의 확률 밀도 함수, P_z는 잠재 공간에 투영된 데이터(z)의 확률 밀도 함수로서, z_k에서 정규 분포를 구성하며, k는 노말라이징 플로우의 계층 수를 나타내며 1 이상의 자연수, f는 정규화 함수를 의미한다.

[0102] 상술한 목적 함수를 최적화하는 과정을 통해 노말라이징 플로우에 대한 학습이 진행될 수 있다. 학습된 노말라이징 플로우는 학습에 사용된 사용자 데이터와 학습에 사용되지 않은 사용자 데이터가 아닌 타인의 데이터 사이에 특정한 거리를 형성하도록 유도할 수 있다.

[0103] 도 10을 참조하면, 평가용 사용자 데이터와 평가용 침입자 데이터는 서로 분산된 공간에 분포되어 있으나, 학습된 노말라이징 플로우를 통해 변환된 잠재 공간 상에서 정규 분포를 이루도록 이동되는 것을 알 수 있다. 또한, 학습된 노말라이징 플로우를 통해 평가용 사용자 데이터와 평가용 침입자 데이터는 잠재 공간 상에서 일정 거리가 확보되도록 위치하게 되는 것을 알 수 있다.

[0105] 또한, 본 발명의 몇몇 실시예에 따른 데이터 공간 변환 모델(DTM)은 오토 인코더로 구현될 수 있다. 즉, 단계(S120)에서, 대상자의 입력 데이터가 학습된 오토 인코더에 인가된 경우, 오토 인코더로부터 피쳐가 추출될 수 있으며, 추출된 피쳐는 잠재 공간의 특정 위치로 투영될 수 있다.

[0106] 도 11을 참조하면, 데이터 공간 변환 모델(DTM)은 오토 인코더(AE)로 구성되어, 인코더(En) 및 디코더(De)를 포함할 수 있다.

[0107] 인코더(En)는 입력 데이터(X)을 특징, 피쳐를 추출할 수 있으며, 추출된 데이터를 잠재 공간(Latent space, z)으로 이동시킬 수 있다. 실시예에서, 인코더(En)는 추출된 입력 데이터(X)의 특징, 피쳐가 잠재 공간 내에서 동일 또는 유사한 위치로 투영되도록 학습될 수 있다. 디코더(De)는 잠재 공간에 투영된 특징, 피쳐를 기초로 입력 데이터와 동일 또는 유사한 데이터를 재구성하도록 학습될 수 있으며, 재구축된 출력 데이터(X')를 출력 데이터로 출력할 수 있다. 또한, 몇몇 실시예에서, 디코더(De)는 동일 또는 유사한 재구축된 출력 데이터(X')가 동일 또는 유사한 공간에 위치하도록 출력할 수 있다. 실시예에서, 오토 인코더(AE)는 입력 데이터(X)와 재구축된 데이터(X') 사이의 차이가 최소화되도록 인코더(En)와 디코더(De)에 대한 학습이 각각 진행될 수 있다.

[0108] 사용자 데이터로 학습이 충분히 수행된 오토 인코더(AE)는 사용자 데이터의 특징과 사용자가 아닌 침입자 데이터의 특징을 서로 다른 잠재 공간에 투영되도록 추출하고, 추출된 특징에 기초하여 서로 다른 데이터로 구분되도록 각각 데이터를 재구축하여 출력 데이터로 출력할 수 있다. 실시예에서, 오토 인코더(AE)의 디코더(De)는 사용자 데이터에 기반하여 재구축된 출력 데이터와 침입자 데이터에 기반하여 재구축된 출력 데이터가 데이터 공간 상의 위치가 상이하도록 출력할 수도 있다.

[0109] 몇몇 실시예에서, 데이터 공간 변환 모델(DTM)은 상술한 바와 같이 학습된 오토 인코더(AE)를 부분적 또는 전체적으로 활용하도록 구성될 수 있다. 즉, 데이터 공간 변환 모델(DTM)은 학습된 오토 인코더(AE)에서 인코더(En)를 부분적으로 활용하여 잠재 공간으로 이동된 피쳐 값을 후술하는 분류 모델(CM)이 이용하도록 구성될 수 있다. 즉, 잠재 공간에서 분류된 피쳐 값을 입력 받아 분류 모델(CM)은 피쳐 값을 분류하고, 이에 따른 사용자 인증 결과를 출력할 수 있다. 다만, 이에 한정되는 것은 아니며, 데이터 공간 변환 모델(DTM)은 학습된 오토 인코더(AE)를 전체적으로 이용하도록 구성되어, 디코더(De)에서 출력되는 출력 데이터를 후술하는 분류 모델(CM)이 이용하도록 할 수 있다. 즉, 디코터(De)가 데이터 공간에 출력한 출력 데이터를 입력 받아 분류 모델(CM)은 출력 데이터를 분류하고, 이에 따른 사용자 인증 결과를 출력할 수 있다.

[0111] 다음으로, 데이터 공간이 변환된 입력 데이터를 분류 모델을 통해 분석하여 대상자에 대한 사용자 인증 결과를 출력한다(S130).

[0112] 단계(S130)에서, 분류 모델(CM)은 데이터 공간이 변환된 입력 데이터를 분석하여 대상자에 대한 사용자 인증 결과를 출력한다. 분류 모델(CM)은 투영된 입력 데이터를 분석하여 대상자가 사용자 계정에 따른 사용자인지 또는 상기 사용자가 아닌 제3 자(침입자)인지 여부를 분류할 수 있다. 즉, 분류 모델(CM)에서 출력되는 사용자 인증 결과는 대상자가 상기 사용자인지, 사용자가 아닌지 여부를 분류한 결과일 수 있다.

[0113] 실시예에서, 분류 모델(CM)은 데이터 공간이 변환된 입력 데이터, 즉, 잠재 공간으로 투영된 입력 데이터가 사용자에 해당하는 지 여부를 판단하도록 학습된 기계 학습 모델 기반의 분류 모델일 수 있다. 몇몇 실시예에서, 분류 모델(CM)은, 선형 회귀, 로지스틱 회귀, 결정 트리들, 원 클래스 서포트 벡터 기계(OC-SVM), 나이브 베이즈, K-최근접 이웃(KNN), K 평균 클러스터링, 아이솔레이션 포레스트, 로컬 아웃라이어 팩터(LOF), 랜덤 포레스트(random forest), 차원수 감소 알고리즘들, 구배 부스팅 알고리즘, 신경망들(예컨대, 콘볼루션, 재귀, 퍼셉트론(perceptron)들, 장단기 메모리(LSTM), 홉필드(Hopfield), 볼츠만(Boltzmann), 심층 신뢰, 디콘볼루션, 생성적 대립, 액체 상태 기계 등), 및/또는 다른 유형들의 기계 학습 모델을 사용하여 구현될 수 있다.

[0114] 여기서, 분류 모델(CM)은 데이터 공간 변환 모델(DTM)에 의해 잠재 공간으로 투영된 입력 데이터를 분석할 수 있다. 즉, 입력 데이터는 데이터 공간 변환 모델(DTM)을 통해 잠재 공간의 특정 위치로 이동된 상태로, 분류 모델(CM)에 의한 분류가 더욱 용이해진 상태일 수 있다. 즉, 분류 모델(CM)을 단독으로 사용하여 입력 데이터를 분류하는 것에 비해 데이터 공간 변환 모델(DTM)과 분류 모델(CM)을 함께 구현함에 따라 전체적인 모델의 학습 효과와 분류 성능이 향상되는 효과를 제공할 수 있다.

[0115] 도 12는 데이터 공간 변환이 수행되기 이전 상태에서 데이터를 분류 모델을 통해 분류하는 과정을 예시적으로 도시하며, 도 13은 데이터 공간 변환이 수행된 상태에서 데이터를 분류 모델을 통해 분류하는 과정을 예시적으

로 도시한다. 도 12 및 도 13에서, <a>는 주변 이웃의 데이터를 확인하여 신규 데이터의 범주를 결정하는 K-최근접 이웃(KNN) 분류 모델, <b>는 로컬 영역에서 탐지된 이상치를 통해 신규 데이터의 범주를 결정하는 로컬 아웃라이어 팩터(LOF) 분류 모델, <c>는 데이터를 스플릿하여 모든 관측치를 고립함에 따라 데이터의 범주를 결정하는 아이솔레이션 포레스트 분류 모델, <d>는 주어진 데이터를 잘 설명할 수 있는 최적의 서포트 벡터(support vector)를 계산하고 이를 통해 데이터를 분류하는 원 클래스 서포트 벡터 기계(OC-SVM) 분류 모델을 의미하며, 이러한 분류 모델을 통해 제1 데이터(★)와 제2 데이터(●)를 분류하는 과정을 예시적으로 도시한다.

[0116] 도 12 및 도 13의 각 예시에서, 제1 데이터(★)와 제2 데이터(●)는 상이한 종류의 데이터를 의미하며, 분류 모델은 제1 데이터(★)와 제2 데이터(●)를 분류하도록 학습되어야 한다.

[0117] 도 12를 참조하면, 데이터 공간 변환이 수행되기 이전에는 제1 데이터(★)와 제2 데이터(●)가 공간적으로 혼재되어 있는 것을 알 수 있다. 따라서, 제1 데이터(★)와 제2 데이터(●)를 구분하기 위해서는 구체적이고 세부적인 상태를 분류할 수 있는 분류 모델의 구축이 필요하며, 더욱 많은 데이터와 학습이 요구되는 문제점이 있었다.

[0118] 도 13을 참조하면, 데이터 공간 변환 모델(DTM)을 통해 데이터에 대한 변환 작업을 진행한 경우, 제1 데이터(★)와 제2 데이터(●) 사이에 공간적인 분리가 이루어진 것을 알 수 있다. 이러한, 제1 데이터(★)와 제2 데이터(●) 사이의 공간 분리를 통해, 학습 모델을 학습하기 위한 기준이 더욱 명확해질 수 있으며, 분류 모델에 대한 효율적인 학습이 진행되는 것이 지원될 수 있다. 또한, 효율적인 학습에 따라 더욱 정확한 분류 성능을 나타내는 분류 모델의 구축이 가능해진다.

[0119] 단계(S130)에서, 상술한 바와 같이 구축된 분류 모델을 통해 잠재 공간으로 투영된 데이터에 대한 분류가 수행되며, 대상자에 대한 사용자 인증 결과가 출력되게 된다.

[0120] 몇몇 실시예에 따른 사용자 인증 방법은 대상자의 인증 정보를 더 수집하는 단계를 포함한다. 단계(S130)는, 수집된 대상자의 인증 정보 및 인증 모델에서 출력된 사용자 인증 결과에 기초하여 사용자 인증을 수행하는 것을 포함할 수 있다. 예시적인 실시예에서, 단계(S130)는 사용자 계정의 인증 정보와 수집된 대상자의 인증 정보의 일치 여부를 먼저 판단하고, 인증 정보가 일치된 대상자의 사용자 인증 결과에 따라 사용자 인증을 수행할 수 있다.

[0122] 다시 도 3을 참조하면, 단계(S130)에서, 대상자의 사용자 인증이 완료되는 경우 대상자에게 금융 서버로부터 제공되는 금융 서비스 환경을 제공한다(S140).

[0123] 단계(S140)에서, 이전 단계(S130)에서 사용자 인증이 완료된 대상자에게 사용자 계정에 대응되는 금융 서비스 환경이 제공되게 된다.

[0125] 도 14는 다양하게 구성된 입력 데이터에 따른 인증 모델의 정확도를 측정한 결과를 나타낸다. 각각의 실시예에서, 인증 모델은 노말라이징 플로우(NF)로 구성된 데이터 공간 변환 모델과 KNN으로 구성된 분류 모델로 구성되었다.

[0126] 실시예 1은 입력 데이터로 공간 정보를 사용하여 인증 모델을 구축하고 정확도를 측정하였다. 실시예 2는 입력 데이터로 시간 정보를 사용하여 인증 모델을 구축하고 정확도를 측정하였다. 실시예 3은 입력 데이터로 시간 정규화 정보를 사용하여 인증 모델을 구축하고 정확도를 측정하였다. 실시예 4는 입력 데이터로 공간 정보와 시간 정보를 함께 사용하여 인증 모델을 구축하고 정확도를 측정하였다. 실시예 5는 입력 데이터로 공간 정보와 시간 정규화 정보를 함께 사용하여 인증 모델을 구축하고 정확도를 측정하였다. 실시예 6은 입력 데이터로 시간 정보와 시간 정규화 정보를 함께 사용하여 인증 모델을 구축하고 정확도를 측정하였다. 실시예 7은 입력 데이터로, 공간 정보, 시간 정보 및 시간 정규화 정보를 함께 사용하여 인증 모델을 구축하고 정확도를 측정하였다.

[0127] 각 실시예에 대한 정확도 측정은 통합 오류율(integrated error) 및 동일 오류율(equal error rate)을 각각 측정하였다. 도 14를 참조하면, 공간 정보를 활용하는 실시예 1에 비해, 시간 정보를 활용하는 실시예 2가 더욱 개선된 정확성을 나타내는 것을 알 수 있다. 또한, 단일 정보를 활용하는 실시예들에 비해, 정규화된 정보인 시간 정규화 정보를 함께 고려한 실시예 5, 6 및 7의 경우, 유의미한 정확도 개선이 나타난 것을 알 수 있다. 특히, 공간 정보, 시간 정보 및 시간 정규화 정보를 모두 입력 데이터로 구성하여 인증 모델을 구현한 실시예 7이

가장 높은 정확성을 제공하는 것을 알 수 있다.

[0129] 여기서, 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법은 인증 모델을 학습하는 과정을 더 포함할 수 있다. 이하에서는, 도 15 및 도 16을 참조하여 사용자 장치에서 인증 모델의 학습이 수행되는 과정을 예시적으로 설명한다.

[0130] 도 15는 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법의 인증 모델을 학습하는 세부 단계의 순서도이다. 도 16은 추론 프로세스와 인증 프로세스와의 관계를 설명하기 위한 예시도이다.

[0131] 도 15 및 도 16을 참조하면, 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법은 학습 데이터를 저장하는 단계(S210), 인증 모델이 학습 가능한 상태인지를 판단하는 단계(S220), 인증 모델의 학습이 가능한 경우 학습 데이터로 인증 모델을 학습하는 단계(S230) 및 학습 데이터를 삭제하는 단계(S240)를 포함한다.

[0132] 실시예에서, 단계들(S210 내지 S240)는 인증 모델을 포함하는 장치에서 수행될 수 있다. 몇몇 실시예에서, 단계들(S210 내지 S240)은 인증 모델을 포함하는 사용자 장치(100)에서 수행될 수 있으나, 본 발명의 실시예가 이에 한정되는 것은 아니다. 다른 실시예에서, 인증 모델은 금융 서버(200)에 포함될 수 있으며, 단계들(S210 내지 S240)은 금융 서버(200)에서 수행될 수 있다.

[0133] 먼저, 학습 데이터가 수집 및 저장된다(S210).

[0134] 학습 데이터는 대상자의 입력 데이터에 대한 추론, 판단을 하는 단계(S120, S130)에서 수집되어 저장될 수 있다. 즉, 도 16에 도시된 바와 같이, 대상자의 입력 데이터를 데이터 공간 변환 모델에 순차적으로 입력하고, 데이터 공간 변환 모델에서 출력되는 결과를 분류 모델에 입력하여 대상자에 대한 사용자 인증을 수행하는 과정에서 수집되는 데이터를 학습 데이터로 저장할 수 있다.

[0135] 구체적으로, 단계(S210)는, 대상자의 입력 데이터 및 입력 데이터에 대응하여 데이터 공간 변환 모델에서 출력되는 출력 데이터를 제1 학습 데이터로 저장하는 단계를 포함할 수 있다. 즉, 학습 데이터는 입력 데이터와 데이터 공간 변환 모델에서 출력되는 출력 데이터로 구성되는 제1 학습 데이터를 포함할 수 있다. 추론 프로세스에 따른 단계(S120)에서, 데이터 공간 변환 모델은 입력 데이터에 따라 출력 데이터를 출력할 수 있다. 이러한 데이터 공간 변환 모델에 입력되는 입력 데이터와 데이터 공간 변환 모델이 출력하는 출력 데이터가 제1 학습 데이터로 수집되게 된다.

[0136] 여기서, 데이터 공간 변환 모델의 출력 데이터는 데이터 공간이 변환된 입력 데이터(이하, 공간 변환 데이터)와 입력 데이터에 따라 데이터 공간 변환 모델이 예측한 값과 실제 값 사이의 차이인 제1 손실 값을 포함할 수 있다. 실시예에서, 데이터 공간 변환 모델이 노말라이징 플로우로 구성되는 경우, 제1 손실 값은 수학식 1에 따른 입력 데이터(x)의 목적 함수에 대한 Negative Log-Likelihood(NLL)로 구성될 수 있다. 또한, 데이터 공간 변환이 오토 인코더로 구성되는 경우, 제1 손실 값은 입력 데이터(x)와 재구축 데이터(x') 사이의 차이에 해당할 수 있다. 추론 프로세스가 진행되는 동안, 입력 데이터, 공간 변환 데이터 및 제1 손실 값이 수집되어 제1 학습 데이터로 저장될 수 있다.

[0137] 또한, 실시예에서, 단계(S210)는, 데이터 공간 변환 모델에서 출력되는 공간 변환 데이터와 공간 변환 데이터를 분류 모델에 입력하여 출력되는 출력 데이터를 제2 학습 데이터로 저장하는 단계를 포함할 수 있다. 추론 프로세스에 따른 단계(S130)에서, 분류 모델은 입력되는 공간 변환 데이터에 따라 출력 데이터를 출력할 수 있다. 이러한 분류 모델에 입력되는 입력 데이터와 분류 모델에서 출력되는 출력 데이터가 제2 학습 데이터로 수집되게 된다.

[0138] 분류 모델에서 출력되는 출력 데이터는 공간 변환 데이터를 분석한 결과인 사용자 인증 결과와 공간 변환 데이터에 따라 분류 모델이 예측한 값과 실제 값 사이의 차이인 제2 손실 값을 포함할 수 있다. 추론 프로세스가 진행되는 동안, 공간 변환 데이터, 사용자 인증 결과 및 제2 손실 값이 수집되어 제2 학습 데이터로 저장될 수 있다.

[0139] 다음으로, 인증 모델이 학습 가능한 상태인지 여부를 판단한다(S220).

[0140] 단계(S220)에서, 저장된 학습 데이터가 충분한지 여부가 판단될 수 있다. 또한, 인증 모델에 대한 학습을 수행하기에 해당 장치의 전력이 충분한 지 여부가 판단될 수 있다. 저장된 제1 학습 데이터 및 제2 학습 데이터 각

각이 미리 설정된 개수 이상인 경우, 학습 데이터의 개수가 충분한 것으로 판단될 수 있다. 또한, 사용자 장치(100)가 충전 상태이거나, 배터리가 일정 수치 이상인 경우, 인증 모델에 대한 학습을 수행하기에 전력이 충분한 것으로 판단될 수 있다. 예시적으로, 사용자 장치(100)의 배터리 잔량이 70% 이상으로 측정되는 경우, 인증 모델에 대한 학습을 수행하기에 전력이 충분한 상태로 판단될 수 있다.

[0141] 단계(S220)에서, 저장된 학습 데이터의 수가 충분하지 않은 것으로 판단되는 경우, 이전 단계(S210)로 돌아가서 학습 데이터를 더 수집할 수 있다. 또한, 단계(S220)에서, 사용자 장치(100)의 전력이 충분하지 않은 것으로 판단되는 경우, 장치의 전력이 충분한 상태로 변경될 때까지 인증 모델의 학습을 대기할 수 있다. 특히, 사용자 장치(100)에 인증 모델이 포함되는 온-디바이스 방식인 경우, 장치의 전력이 충분한 지 여부는 인증 모델 학습이 전력 부족으로 학습 중간에 중단되는 것이 방지될 수 있으며, 학습에 따른 전력 소모로 다른 장치, 구성의 동작에 영향이 발생되는 것이 방지될 수 있다.

[0142] 몇몇 실시예에서, 단계(S220)는 대기 상태에서 미리 설정된 주기에 따라 실행되어 장치의 전력 상태를 확인할 수 있다. 또한, 단계(S220)는 대기 상태에서 사용자 장치(100)의 전력 상태를 변경하는 것을 요청하는 알람을 사용자에게 표시하는 것을 포함할 수 있다.

[0143] 단계(S220)에서, 저장된 학습 데이터가 충분하고, 전력이 충분한 상태인 경우, 다음 단계(S230)로 진행하게 된다.

[0144] 단계(S230)에서, 제1 학습 데이터로 데이터 공간 변환 모델이 학습되고, 제2 학습 데이터로 분류 모델이 학습될 수 있다.

[0145] 즉, 추론 프로세스를 통해 수집된 정보에 기초하여 사용자 장치(100)에 포함된 인증 모델(예컨대, 데이터 공간 변환 모델, 분류 모델)에 대한 추가적인 학습이 더 수행될 수 있다. 이에 따라, 사용자의 입력 패턴 특성이 더욱 반영되거나, 침입자로 분류된 대상자를 더욱 배제할 수 있는 인증 모델이 구현되게 된다.

[0146] 이어서, 인증 모델에 대한 학습이 완료된 이후, 학습에 사용된 제1 학습 데이터, 제2 학습 데이터는 삭제된다(S240). 기 저장된 제1 학습 데이터 및 제2 학습 데이터는 폐기될 수 있으며, 대상자의 개인 정보가 외부로 노출되는 것이 사전에 방지될 수 있다. 특히, 사용자 장치(100)에서 온-디바이스 방식으로 학습을 수행하더라도 학습에 이용된 정보가 사용자 장치(100)에 잔존하지 않게 되어, 사용자 장치(100)가 분실 또는 도난 되더라도 대상자/사용자의 개인 정보가 외부로 유출되거나 노출되는 것이 방지될 수 있다.

[0148] 도 17은 본 발명의 몇몇 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법을 수행하는 장치의 하드웨어 구현을 설명하기 위한 도면이다.

[0149] 도 17을 참조하면, 본 발명의 몇몇 실시예들에 따른 입력 패턴 정보를 이용한 사용자 인증 방법을 수행하는 장치는 전자 장치(1000)로 구현될 수 있다. 여기서, 전자 장치(1000)는 사용자 장치(100)일 수 있으나, 이에 한정되는 것은 아니며, 금융 서버(200)에 해당할 수도 있다.

[0150] 전자 장치(1000)는 프로세서(1010), 입출력 장치(1020, I/O), 메모리(1030, memory), 인터페이스(1040), 스토리지(1050, storage) 및 버스(1060, bus)를 포함할 수 있다. 프로세서(1010), 입출력 장치(1020), 메모리(1030), 인터페이스(1040), 및/또는 스토리지(1050)는 버스(1060)를 통하여 서로 결합될 수 있다. 버스(1060)는 데이터들이 이동되는 통로(path)에 해당한다.

[0151] 구체적으로, 프로세서(1010)는 CPU(Central Processing Unit), MPU(Micro Processor Unit), MCU(Micro Controller Unit), GPU(Graphic Processing Unit), 마이크로프로세서, 디지털 신호 프로세스, 마이크로컨트롤러, 어플리케이션 프로세서(AP, application processor) 및 이들과 유사한 기능을 수행할 수 있는 논리 소자들 중에서 적어도 하나를 포함할 수 있다.

[0152] 입출력 장치(1020)는 키패드(keypad), 키보드, 터치스크린 및 디스플레이 장치 중 적어도 하나를 포함할 수 있다.

[0153] 메모리(1030)는 데이터 및/또는 프로그램 등을 로드(load)할 수 있다. 이때, 메모리(1030)는 프로세서(1010)의 동작을 향상시키기 위한 동작 메모리로서, 고속의 디램 및/또는 에스램 등을 포함할 수 있다. 메모리(1030)는 DDR SDRAM(Double Data Rate Static DRAM), SDR SDRAM(Single Data Rate SDRAM)과 같은 하나 이상의 휘발성 메모리 장치 및/또는 EEPROM(Electrical Erasable Programmable ROM), 플래시 메모리(flash memory)과 같은 하나

이상의 비휘발성 메모리 장치를 포함할 수 있다.

[0154] 인터페이스(1040)는 통신 네트워크로 데이터를 전송하거나 통신 네트워크로부터 데이터를 수신하는 기능을 수행할 수 있다. 인터페이스(1040)는 유선 또는 무선 형태일 수 있다. 예컨대, 인터페이스(1040)는 안테나 또는 유무선 트랜시버 등을 포함할 수 있다.

[0155] 스토리지(1050)는 데이터 및/또는 프로그램 등을 저장 및 보관할 수 있다. 스토리지(1050)는 반도체 드라이브(SSD, Solid State Drive), 하드 드라이브(hard drive), 플래시 메모리(flash memory)와 같은 하나 이상의 비휘발성 메모리 장치를 포함할 수 있다. 본 발명에서 스토리지(1050)는 전술한 사용자 인증 방법을 수행하기 위한 인스트럭션(instruction)으로 구성된 컴퓨터 프로그램을 저장할 수 있다.

[0156] 실시예에서, 컴퓨터 프로그램은, 대상자의 입력 패턴 정보를 수집하여 입력 데이터를 구성하는 단계, 상기 입력 데이터를 데이터 공간 변환 모델에 입력하여 상기 입력 데이터의 데이터 공간을 변환하는 단계 및 상기 데이터 공간이 변환된 입력 데이터를 분류 모델을 통해 분석하여 상기 대상자에 대한 사용자 인증 결과를 출력하는 단계를 포함할 수 있다.

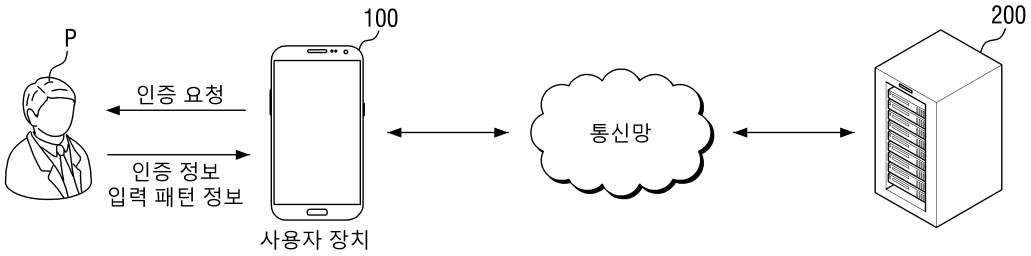
[0158] 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법은 컴퓨터에 의해 실행 가능한 명령어 및 데이터를 저장하는, 컴퓨터로 판독 가능한 매체의 형태로도 구현될 수 있다. 이때, 명령어 및 데이터는 프로그램 코드의 형태로 저장될 수 있으며, 프로세서에 의해 실행되었을 때, 소정의 프로그램 모듈을 생성하여 소정의 동작을 수행할 수 있다. 또한, 컴퓨터로 판독 가능한 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터로 판독 가능한 매체는 컴퓨터 기록 매체일 수 있는데, 컴퓨터 기록 매체는 컴퓨터 판독 가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함할 수 있다. 예를 들어, 컴퓨터 기록 매체는 HDD 및 SSD 등과 같은 마그네틱 저장 매체, CD, DVD 및 블루레이 디스크 등과 같은 광학적 기록 매체, 또는 네트워크를 통해 접근 가능한 서버에 포함되는 메모리일 수 있다.

[0159] 또한 실시예에 따른 입력 패턴 정보를 이용한 사용자 인증 방법은 컴퓨터에 의해 실행 가능한 명령어를 포함하는 컴퓨터 프로그램(또는 컴퓨터 프로그램 제품)으로 구현될 수도 있다. 컴퓨터 프로그램은 프로세서에 의해 처리되는 프로그래밍 가능한 기계 명령어를 포함하고, 고레벨 프로그래밍 언어(High-level Programming Language), 객체 지향 프로그래밍 언어(Object-oriented Programming Language), 어셈블리 언어 또는 기계 언어 등으로 구현될 수 있다. 또한 컴퓨터 프로그램은 유형의 컴퓨터 판독가능 기록매체(예를 들어, 메모리, 하드 디스크, 자기/광학 매체 또는 SSD(Solid-State Drive) 등)에 기록될 수 있다.

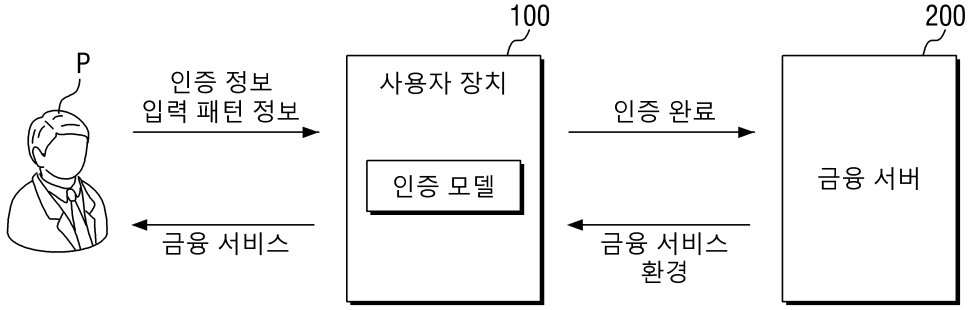
[0161] 이상의 설명은 본 실시예의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 실시예가 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 실시예의 본질적인 특성에서 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능할 것이다. 따라서, 본 실시예들은 본 실시예의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예에 의하여 본 실시예의 기술 사상의 범위가 한정되는 것은 아니다. 본 실시예의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 실시예의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

도면

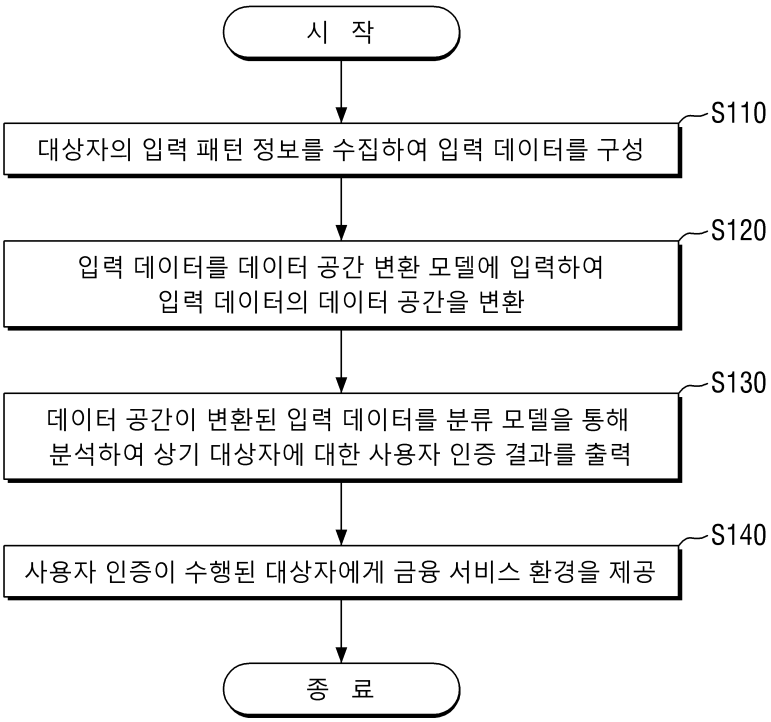
도면1



도면2



도면3

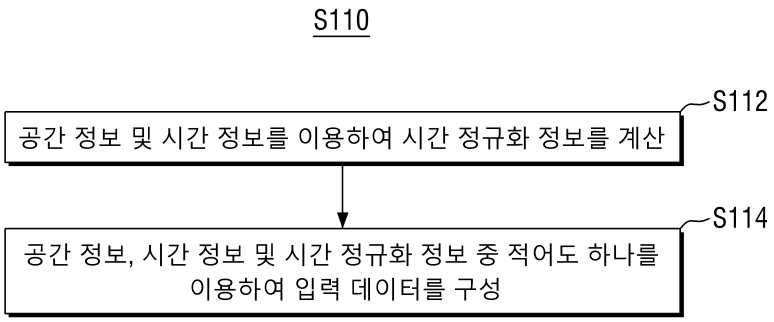


도면4

< d >

사용자	X1	X2	X3	X4	X5	X6	Y1	Y2	Y3	Y4	Y5	Y6	T1	T2	T3	T4	T5
User A	0.52	0.90	0.51	0.82	0.21	0.18	0.16	0.73	0.64	0.40	0.59	0.35	393	667	917	1498	1751

도면5



도면6

$$* \text{제1 시간 정규화 정보 (T1 norm)} = \frac{T1}{\text{거리}[(x2\ , y2\ ), (x1\ , y1)]}$$

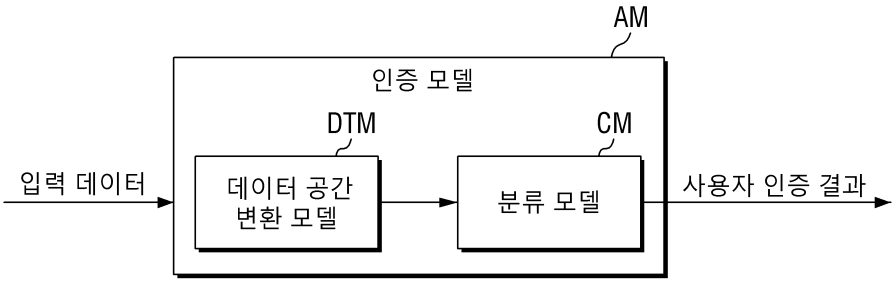
$$= \frac{393}{\sqrt{(0.90 - 0.52)^2 + (0.73 - 0.16)^2}}$$

< a >

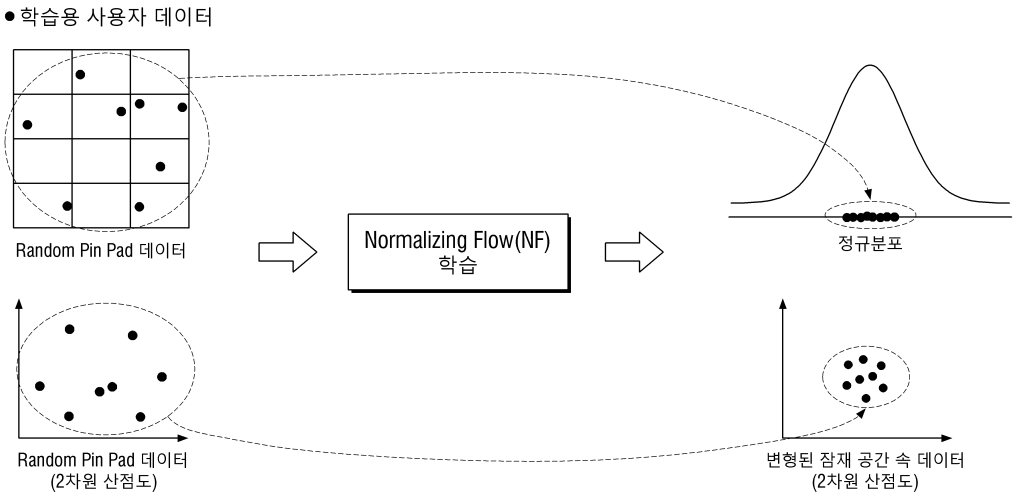
사용자	T1	T2	T3	T4	T5	T1 norm	T2 norm	T3 norm	T4 norm	T5 norm
대상자	393					573.68				

< b >

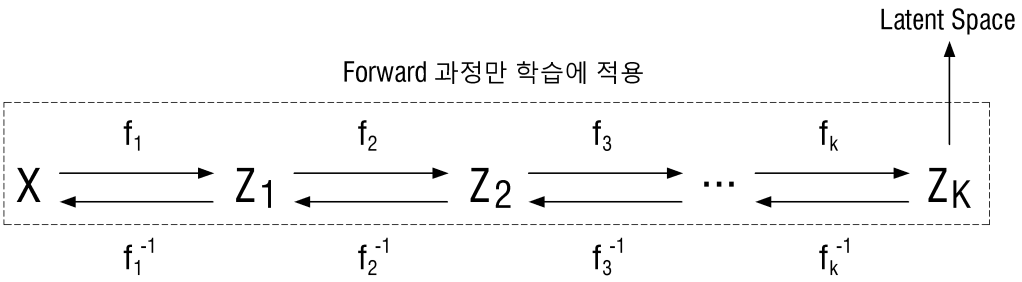
도면7



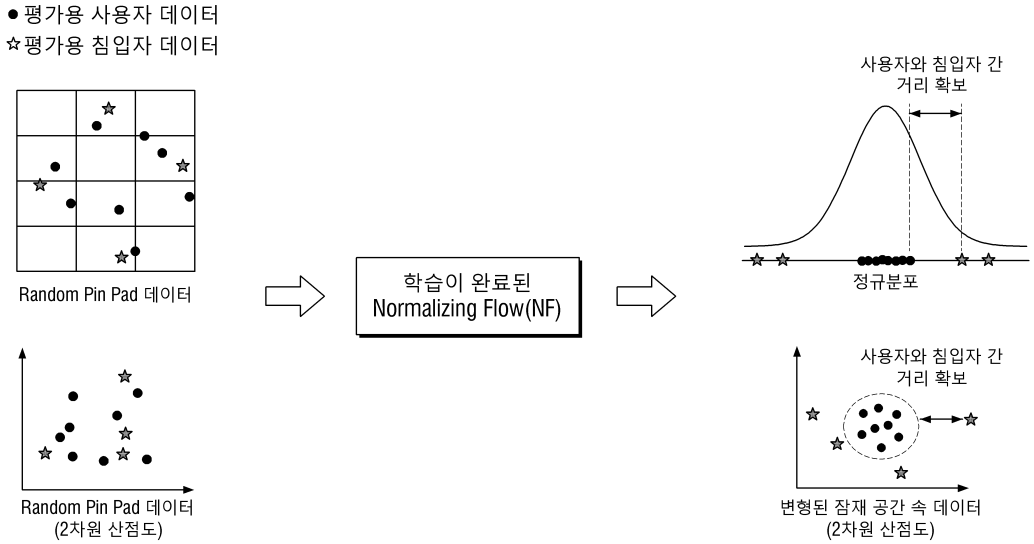
도면8


● 학습용 사용자 데이터
Random Pin Pad 데이터
Normalizing Flow(NF)
학습
정규분포
Random Pin Pad 데이터
(2차원 산점도)
변형된 잠재 공간 속 데이터
(2차원 산점도)

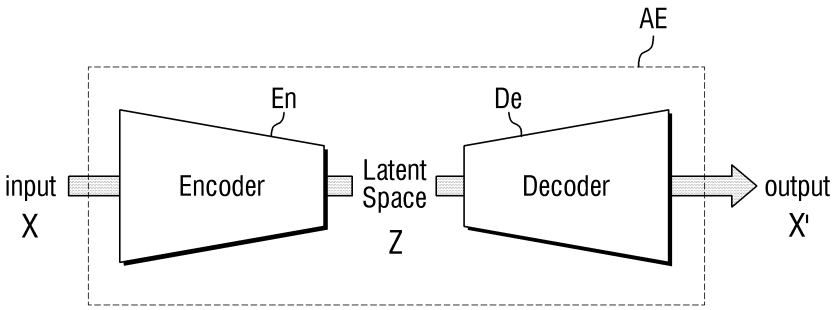
도면9


Latent Space
Forward 과정만 학습에 적용
X
Z1
Z2
ZK
f1
f2
f3
fk
f1-1
f2-1
f3-1
fk-1

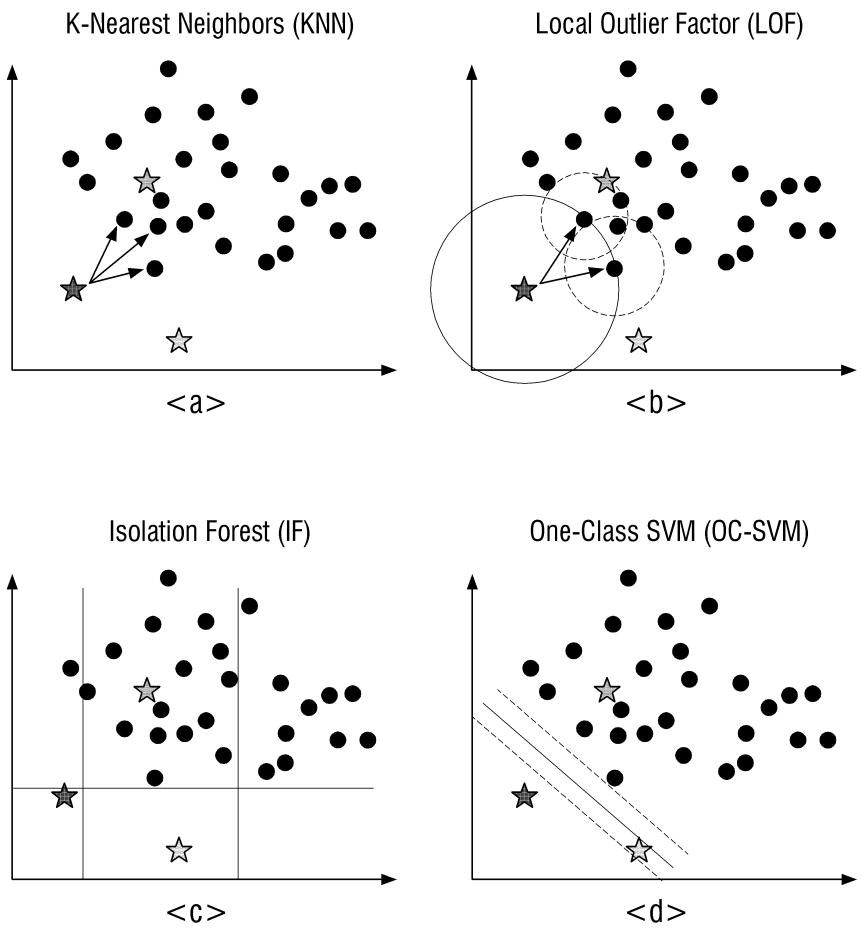
도면10


●평가용 사용자 데이터
☆평가용 침입자 데이터
Random Pin Pad 데이터
학습이 완료된
Normalizing Flow(NF)
사용자와 침입자 간
거리 확보
정규분포
Random Pin Pad 데이터
(2차원 산점도)
사용자와 침입자 간
거리 확보
변형된 잠재 공간 속 데이터
(2차원 산점도)

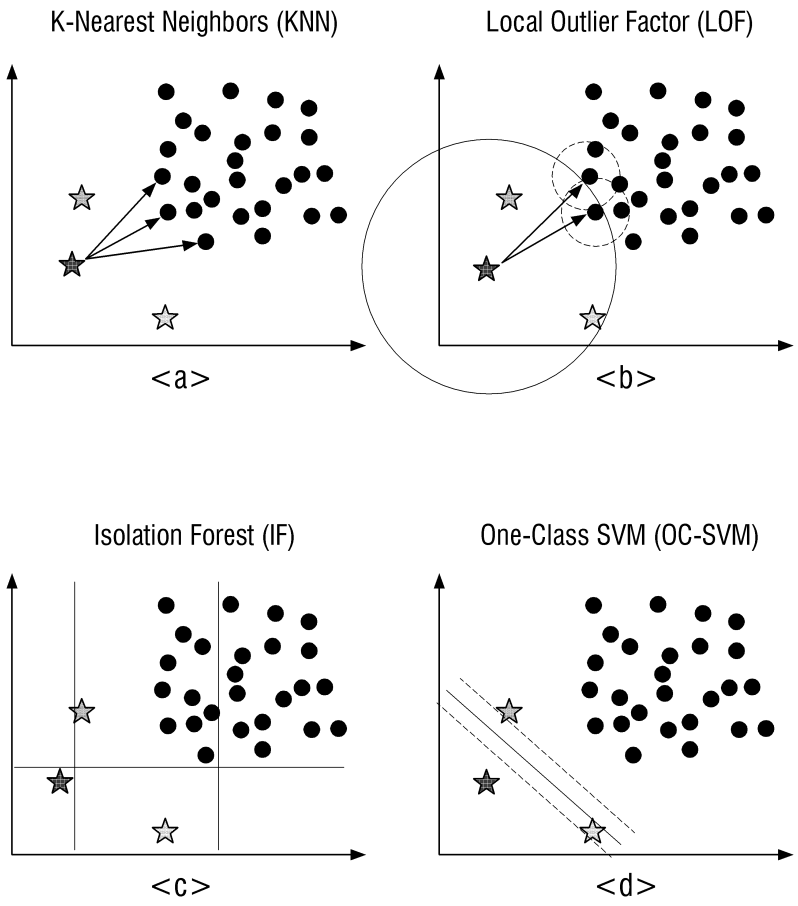
도면11


AE
En
De
input
X
Encoder
Latent
Space
Z
Decoder
output
X'

도면12


K-Nearest Neighbors (KNN)
Local Outlier Factor (LOF)
<a>
<b>
Isolation Forest (IF)
One-Class SVM (OC-SVM)
<c>
<d>

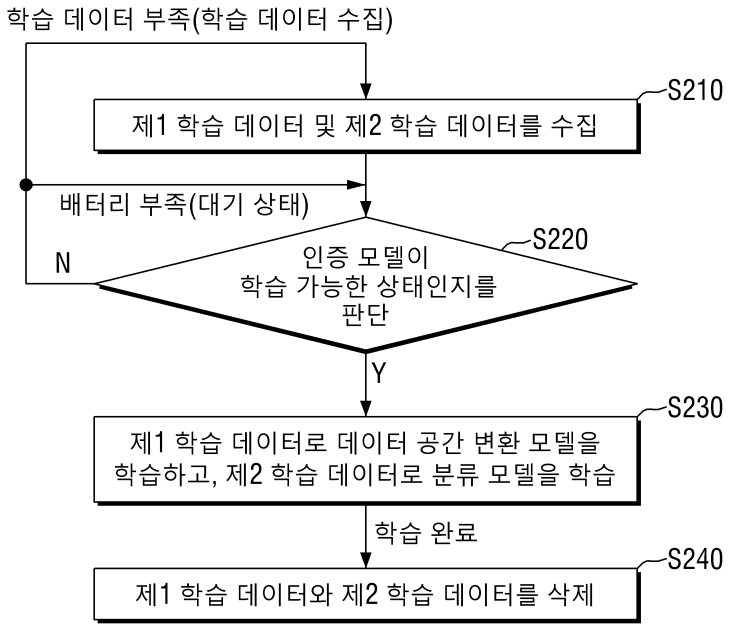
도면13


K-Nearest Neighbors (KNN)
Local Outlier Factor (LOF)
<a>
<b>
Isolation Forest (IF)
One-Class SVM (OC-SVM)
<c>
<d>

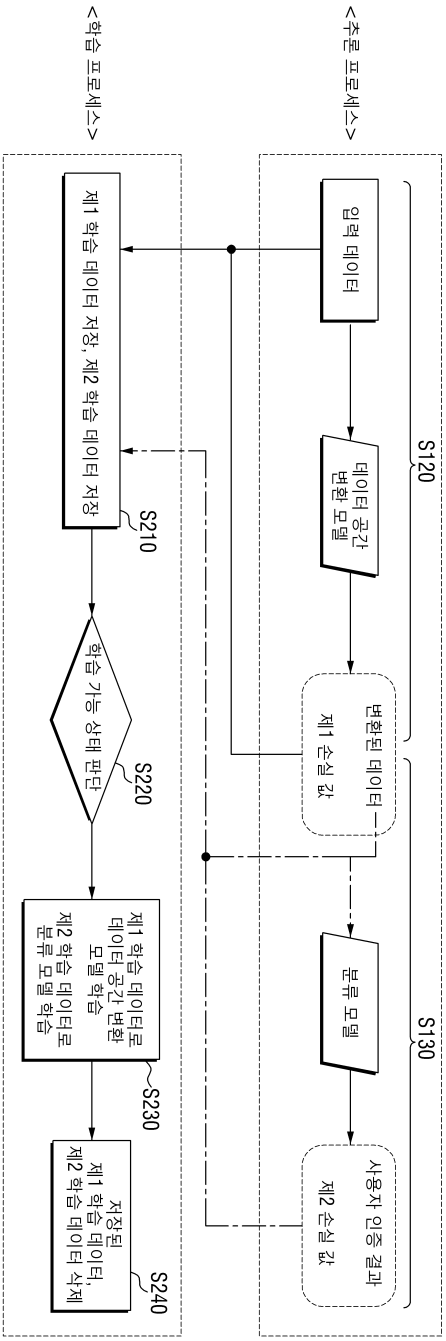
도면14

측정 기법	인증 모델	NF + KNN	NF + KNN	NF + KNN	NF + KNN	NF + KNN	NF + KNN	NF + KNN
	입력 데이터	공간 정보 (실시예 1)	시간 정보 (실시예 2)	시간 정규화 정보 (실시예 3)	공간 정보, 시간 정보 (실시예 4)	공간 정보, 시간 정규화 정보 (실시예 5)	시간 정보, 시간 정규화 정보 (실시예 6)	공간 정보, 시간 정보, 시간 정규화 정보 (실시예 7)
Integrated Error	Average	0.2941	0.2641	0.2413	0.2237	0.1898	0.1832	0.1617
	Std	0.1274	0.1612	0.0972	0.1415	0.0881	0.1054	0.0967
	Max	0.7033	0.8031	0.6712	0.6610	0.4812	0.5627	0.5274
	Min	0.0000	0.0044	0.0315	0.0017	0.0027	0.0020	0.0013
Equal Error Rate	Average	0.3456	0.3100	0.3045	0.2812	0.2672	0.2492	0.2320
	Std	0.1163	0.1427	0.0913	0.1369	0.0886	0.1061	0.0975
	Max	0.6586	0.7536	0.6256	0.6510	0.5862	0.5965	0.5124
	Min	0.0000	0.0096	0.0551	0.0042	0.0096	0.0045	0.0026

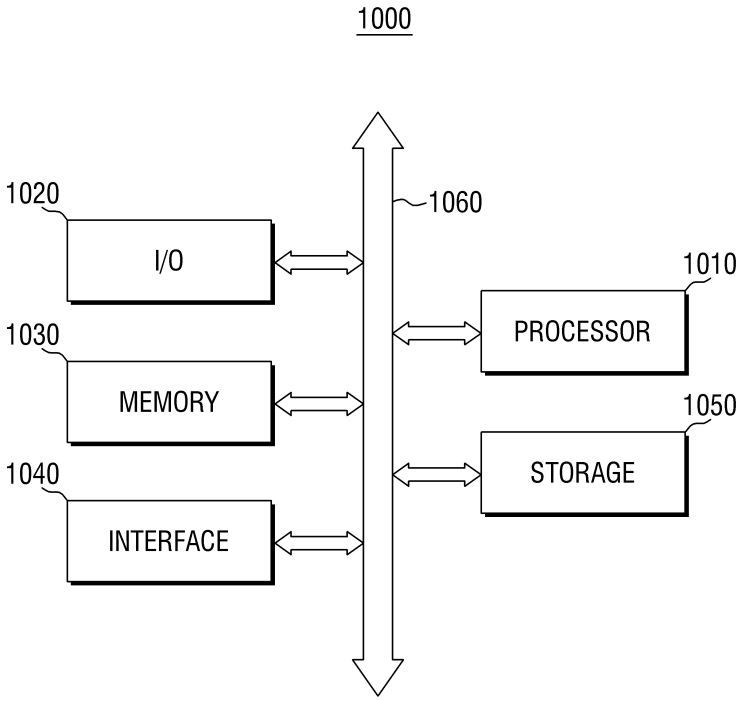
도면15


학습 데이터 부족(학습 데이터 수집)
S210
제1 학습 데이터 및 제2 학습 데이터를 수집
배터리 부족(대기 상태)
S220
N
인증 모델이
학습 가능한 상태인지를
판단
Y
S230
제1 학습 데이터로 데이터 공간 변환 모델을
학습하고, 제2 학습 데이터로 분류 모델을 학습
학습 완료
S240
제1 학습 데이터와 제2 학습 데이터를 삭제

도면16


<추론 프로세스>
<학습 프로세스>
입력 데이터
데이터 공간 변환 모델
변환된 데이터
제1 손실 값
분류 모델
사용자 인증 결과
제2 손실 값
S120
S130
제1 학습 데이터 저장, 제2 학습 데이터 저장
S210
학습 가능 상태 판단
S220
제1 학습 데이터로 데이터 공간 변환 모델 학습
제2 학습 데이터로 분류 모델 학습
S230
저장된 제1 학습 데이터, 제2 학습 데이터 삭제
S240

도면17


1000
1020
I/O
1030
MEMORY
1040
INTERFACE
1060
1010
PROCESSOR
1050
STORAGE