(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년06월08일
(11) 등록번호 10-2406363
(24) 등록일자 2022년06월02일

(51) 국제특허분류(Int. Cl.)
G06N 3/08 (2006.01) *G06F 21/84* (2013.01)
G06N 3/04 (2006.01)
(52) CPC특허분류
G06N 3/082 (2013.01)
G06F 21/84 (2013.01)
(21) 출원번호 10-2021-0016948
(22) 출원일자 2021년02월05일
심사청구일자 2021년02월05일
(65) 공개번호 10-2022-0068876
(43) 공개일자 2022년05월26일
(30) 우선권주장
1020200155318 2020년11월19일 대한민국(KR)
(56) 선행기술조사문헌
KR1020190129672 A*
Sungyup Nam et al., Recurrent GANs Password Cracker For IoT Password Security Enhancement, In Proceedings of the International Workshop on Information Security Applications, 1-19pages (2020. 5. 31.)*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
연세대학교 산학협력단
서울특별시 서대문구 연세로 50 (신촌동, 연세대학교)
(72) 발명자
권태경
서울특별시 강남구 선릉로 221, 410동 1602호(도곡동, 도곡렉슬아파트)
박래현
서울특별시 도봉구 도당로31길 20, 302호(방학동, 세광빌라)
(74) 대리인
특허법인우인

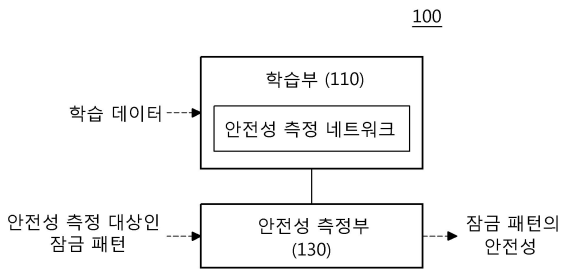
전체 청구항 수 : 총 8 항 심사관 : 양대경

(54) 발명의 명칭 **딥러닝 기반 잠금 패턴 안전성 측정 장치 및 방법**

(57) 요 약

본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 장치 및 방법은, 잠금 패턴의 수치적 특징뿐만 아니라 인간의 시각적 인식을 반영하는 잠금 패턴의 시각적 특징을 이용하여 잠금 패턴의 안전성을 측정함으로써, 숄더 서핑 공격(shoulder-surfing attack)에 대한 잠금 패턴의 안전성을 보다 정확하게 측정할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
G06N 3/04 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711120086
과제번호	2020-0-01602-001
부처명	과학기술정보통신부
과제관리(전문)기관명	정보통신기획평가원
연구사업명	정보통신방송혁신인재양성
연구과제명	지능형 사이버 위협 대응 기술 개발 및 인력양성
기 여 율	1/1
과제수행기관명	숭실대학교 산학협력단
연구기간	2020.07.01 ~ 2025.12.31

명 세 서

청구범위

청구항 1

합성곱 신경망(Convolutional neural network, CNN)으로 이루어지며, 학습 데이터 세트를 구성하는 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 안전성 측정 네트워크를 학습하는 학습부; 및

안전성 측정 대상인 잠금 패턴을 상기 안전성 측정 네트워크에 입력하고, 상기 안전성 측정 네트워크의 출력을 기반으로 안전성 측정 대상인 잠금 패턴의 안전성을 측정하는 안전성 측정부;

를 포함하며,

상기 학습부는, 잠금 패턴의 수치적 특징을 추출하고, 상기 안전성 측정 네트워크의 합성곱 레이어(convolution layer)를 이용하여 잠금 패턴의 시각적 특징을 추출하는 특징 추출 모듈; 및 상기 안전성 측정 네트워크의 완전 연결 레이어(fully connected layer)를 이용하여 상기 특징 추출 모듈을 통해 추출된 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 선형 회귀 분석 모듈;을 포함하고,

상기 합성곱 레이어의 가중치 및 상기 완전 연결 레이어의 가중치는, 상기 학습 데이터 세트를 이용한 학습 과정에서, 상기 학습 데이터 세트에 대응되는 그라운드 트루스(ground-truth) 레이블을 이용하여 조정되며,

상기 학습 데이터 세트는, 조합 가능한 모든 잠금 패턴 각각에서 추출된 수치적 특징을 기반으로 조합 가능한 모든 잠금 패턴을 미리 설정된 유사 판단 기준에 따라 군집화(clustering)하고, 각 군집 마다 중심점(centroid)에 대응하는 잠금 패턴을 획득하며, 군집 각각에서 획득한 잠금 패턴으로 구성되는,

딥러닝 기반 잠금 패턴 안전성 측정 장치.

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

제1항에서,

상기 그라운드 트루스 레이블은,

실제 사용자를 대상으로 하는 설문을 통해, 상기 학습 데이터 세트를 구성하는 잠금 패턴 각각에 대해 획득되는,

딥러닝 기반 잠금 패턴 안전성 측정 장치.

청구항 6

제5항에서,

상기 설문은,

하나의 잠금 패턴에 대해, 답변 가능한 복잡도의 범위가 서로 동일한 복수개의 질문 항목으로 이루어지며,

하나의 잠금 패턴에 대한 상기 그라운드 트루스 레이블은,

상기 복수개의 질문 항목 각각에 대해 사용자가 답변한 복잡도를 기반으로 획득되는,

딥러닝 기반 잠금 패턴 안전성 측정 장치.

청구항 7

제6항에서,

하나의 잠금 패턴에 대한 상기 그라운드 트루스 레이블은,

수학식 $C=\sqrt{\sum_{i=1}^{N} S_i^2}$ 을 통해 획득되고, 상기 C는 상기 그라운드 트루스 레이블을 나타내며, 상기 N은 상기 질문 항목의 개수를 나타내고, 상기 S는 상기 질문 항목에 대해 사용자가 답변한 복잡도를 나타내는,

딥러닝 기반 잠금 패턴 안전성 측정 장치.

청구항 8

제1항에서,

상기 잠금 패턴은,

이미지 형태로 이루어지는,

딥러닝 기반 잠금 패턴 안전성 측정 장치.

청구항 9

제1항에서,

상기 수치적 특징은,

방향(direction), 교차점(crosspoints), 선의 겹침(overlaps), 각도(angles), 회전(turns), 마코프(markov) 확률, 반복된 하위 패턴(subpatterns) 중 적어도 하나인,

딥러닝 기반 잠금 패턴 안전성 측정 장치.

청구항 10

합성곱 신경망(Convolutional neural network, CNN)으로 이루어지며, 학습 데이터 세트를 구성하는 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 안전성 측정 네트워크를 학습하는 단계; 및

안전성 측정 대상인 잠금 패턴을 상기 안전성 측정 네트워크에 입력하고, 상기 안전성 측정 네트워크의 출력을 기반으로 안전성 측정 대상인 잠금 패턴의 안전성을 측정하는 단계;

를 포함하며,

상기 학습 단계는, 잠금 패턴의 수치적 특징을 추출하고, 상기 안전성 측정 네트워크의 합성곱 레이어(convolution layer)를 이용하여 잠금 패턴의 시각적 특징을 추출하는 단계; 및 상기 안전성 측정 네트워크의 완전 연결 레이어(fully connected layer)를 이용하여 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 단계;를 포함하고,

상기 합성곱 레이어의 가중치 및 상기 완전 연결 레이어의 가중치는, 상기 학습 데이터 세트를 이용한 학습 과정에서, 상기 학습 데이터 세트에 대응되는 그라운드 트루스(ground-truth) 레이블을 이용하여 조정되며,

상기 학습 데이터 세트는, 조합 가능한 모든 잠금 패턴 각각에서 추출된 수치적 특징을 기반으로 조합 가능한 모든 잠금 패턴을 미리 설정된 유사 판단 기준에 따라 군집화(clustering)하고, 각 군집 마다 중심점(centroid)에 대응하는 잠금 패턴을 획득하며, 군집 각각에서 획득한 잠금 패턴으로 구성되는,

딥러닝 기반 잠금 패턴 안전성 측정 방법.

청구항 11

삭제

청구항 12

삭제

청구항 13

제10항에 기재된 딥러닝 기반 잠금 패턴 안전성 측정 방법을 컴퓨터에서 실행시키기 위하여 컴퓨터로 읽을 수 있는 기록 매체에 저장된 컴퓨터 프로그램.

발명의 설명

기 술 분 야

[0001] 본 발명은 딥러닝 기반 잠금 패턴 안전성 측정 장치 및 방법에 관한 것으로서, 더욱 상세하게는 잠금 패턴의 안전성을 측정하는, 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 스마트폰 잠금 패턴의 안전성을 측정하기 위해 다양한 방법이 제시되고 있다. 하지만, 기존의 측정 방법의 기준들은 모두 경험적으로(heuristic) 수립되었기 때문에 잠금 패턴의 안전성에 영향을 주는 일부 특징들을 반영하지 못하는 문제가 있다.

[0003] 숄더 서핑 공격(shoulder-surfing attack)은 잠금 패턴을 보고 외우는 과정을 거치므로 이러한 공격에 대한 안전성에 영향을 주는 특징들은 인간의 시각적 인식과 관련이 있으나, 기존의 측정 기준은 잠금 패턴에서 직접 추출 가능한 수치적 특징들만 활용하고 있고, 잠재적으로 표현되는 인간의 시각적 인식과 관련된 특징을 반영하지 않고 있다.

[0004] 또한, 기존의 측정 방법은 특징들의 가중치를 인간의 관점과는 다르게 설정하고, 결과적으로 인간의 기준에서 더 복잡하고 어려운 패턴을 더 단순하고 쉬운 패턴으로 측정하는 비일관성의 오류가 발생되는 문제가 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 이루고자 하는 목적은, 잠금 패턴의 수치적 특징뿐만 아니라 인간의 시각적 인식을 반영하는 잠금 패턴의 시각적 특징을 이용하여 잠금 패턴의 안전성을 측정하는, 딥러닝 기반 잠금 패턴 안전성 측정 장치 및 방법을 제공하는 데 있다.

[0006] 본 발명의 명시되지 않은 또 다른 목적들은 하기의 상세한 설명 및 그 효과로부터 용이하게 추론할 수 있는 범위 내에서 추가적으로 고려될 수 있다.

과제의 해결 수단

[0007] 상기의 목적을 달성하기 위한 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 장치는, 합성곱 신경망(Convolutional neural network, CNN)으로 이루어지며, 학습 데이터 세트를 구성하는 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 안전성 측정 네트워크를 학습하는 학습부; 및 안전성 측정 대상인 잠금 패턴을 상기 안전성 측정 네트워크에 입력하고, 상기 안전성 측정 네트워크의 출력을 기반으로 안전성 측정 대상인 잠금 패턴의 안전성을 측정하는 안전성 측정부;를 포함한다.

[0008] 여기서, 상기 학습부는, 잠금 패턴의 수치적 특징을 추출하고, 상기 안전성 측정 네트워크의 합성곱 레이어(convolution layer)를 이용하여 잠금 패턴의 시각적 특징을 추출하는 특징 추출 모듈; 및 상기 안전성 측정 네트워크의 완전 연결 레이어(fully connected layer)를 이용하여 상기 특징 추출 모듈을 통해 추출된 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 선형 회귀 분석 모듈;을 포함할 수 있다.

[0009] 여기서, 상기 합성곱 레이어의 가중치 및 상기 완전 연결 레이어의 가중치는, 상기 학습 데이터 세트를 이용한 학습 과정에서, 상기 학습 데이터 세트에 대응되는 그라운드 트루스(ground-truth) 레이블을 이용하여 조정될 수 있다.

[0010] 여기서, 상기 학습 데이터 세트는, 조합 가능한 모든 잠금 패턴 각각에서 추출된 수치적 특징을 기반으로 조합 가능한 모든 잠금 패턴을 미리 설정된 유사 판단 기준에 따라 군집화(clustering)하고, 각 군집 마다 중심점(centroid)에 대응하는 잠금 패턴을 획득하며, 군집 각각에서 획득한 잠금 패턴으로 구성될 수 있다.

[0011] 여기서, 상기 그라운드 트루스 레이블은, 실제 사용자를 대상으로 하는 설문을 통해, 상기 학습 데이터 세트를 구성하는 잠금 패턴 각각에 대해 획득될 수 있다.

[0012] 여기서, 상기 설문은, 하나의 잠금 패턴에 대해, 답변 가능한 복잡도의 범위가 서로 동일한 복수개의 질문 항목으로 이루어지며, 하나의 잠금 패턴에 대한 상기 그라운드 트루스 레이블은, 상기 복수개의 질문 항목 각각에 대해 사용자가 답변한 복잡도를 기반으로 획득될 수 있다.

[0013] 여기서, 하나의 잠금 패턴에 대한 상기 그라운드 트루스 레이블은, 수학식 $C=\sqrt{\sum_{i=1}^{N} S_i^2}$ 을 통해 획득되고, 상기 C는 상기 그라운드 트루스 레이블을 나타내며, 상기 N은 상기 질문 항목의 개수를 나타내고, 상기 S는 상기 질문 항목에 대해 사용자가 답변한 복잡도를 나타낼 수 있다.

[0014] 여기서, 상기 잠금 패턴은, 이미지 형태로 이루어질 수 있다.

[0015] 여기서, 상기 수치적 특징은, 방향(direction), 교차점(crosspoints), 선의 겹침(overlaps), 각도(angles), 회전(turns), 마코프(markov) 확률, 반복된 하위 패턴(subpatterns) 중 적어도 하나일 수 있다.

[0017] 상기의 목적을 달성하기 위한 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 방법은, 합성곱 신경망(Convolutional neural network, CNN)으로 이루어지며, 학습 데이터 세트를 구성하는 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 안전성 측정 네트워크를 학습하는 단계; 및 안전성 측정 대상인 잠금 패턴을 상기 안전성 측정 네트워크에 입력하고, 상기 안전성 측정 네트워크의 출력을 기반으로 안전성 측정 대상인 잠금 패턴의 안전성을 측정하는 단계;를 포함한다.

[0018] 여기서, 상기 학습 단계는, 잠금 패턴의 수치적 특징을 추출하고, 상기 안전성 측정 네트워크의 합성곱 레이어(convolution layer)를 이용하여 잠금 패턴의 시각적 특징을 추출하는 단계; 및 상기 안전성 측정 네트워크의 완전 연결 레이어(fully connected layer)를 이용하여 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 단계;를 포함할 수 있다.

[0019] 여기서, 상기 합성곱 레이어의 가중치 및 상기 완전 연결 레이어의 가중치는, 상기 학습 데이터 세트를 이용한 학습 과정에서, 상기 학습 데이터 세트에 대응되는 그라운드 트루스(ground-truth) 레이블을 이용하여 조정될 수 있다.

[0021] 상기의 기술적 과제를 달성하기 위한 본 발명의 바람직한 실시예에 따른 컴퓨터 프로그램은 컴퓨터로 읽을 수 있는 기록 매체에 저장되어 상기한 딥러닝 기반 잠금 패턴 안전성 측정 방법 중 어느 하나를 컴퓨터에서 실행시킨다.

발명의 효과

[0022] 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 장치 및 방법에 의하면, 잠금 패턴의 수치적 특징뿐만 아니라 인간의 시각적 인식을 반영하는 잠금 패턴의 시각적 특징을 이용하여 잠금 패턴의 안전성을 측정함으로써, 숄더 서핑 공격(shoulder-surfing attack)에 대한 잠금 패턴의 안전성을 보다 정확하게 측정할 수 있다.

[0023] 본 발명의 효과들은 이상에서 언급한 효과들로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0024] 도 1은 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 장치를 설명하기 위한 블록도이다.

도 2는 도 1에 도시한 학습부의 세부 구성을 설명하기 위한 블록도이다.

도 3은 본 발명의 바람직한 실시예에 따른 안전성 측정 네트워크의 학습 과정을 설명하기 위한 도면이다.

도 4는 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 방법을 설명하기 위한 흐름도이다.

도 5는 도 4에 도시한 안전성 측정 네트워크 학습 단계의 세부 단계를 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0025] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명한다. 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 게시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 게시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0026] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0027] 본 명세서에서 "제1", "제2" 등의 용어는 하나의 구성요소를 다른 구성요소로부터 구별하기 위한 것으로, 이들 용어들에 의해 권리범위가 한정되어서는 아니 된다. 예를 들어, 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다.

[0028] 본 명세서에서 각 단계들에 있어 식별부호(예를 들어, a, b, c 등)는 설명의 편의를 위하여 사용되는 것으로 식별부호는 각 단계들의 순서를 설명하는 것이 아니며, 각 단계들은 문맥상 명백하게 특정 순서를 기재하지 않는 이상 명기된 순서와 다르게 일어날 수 있다. 즉, 각 단계들은 명기된 순서와 동일하게 일어날 수도 있고 실질적으로 동시에 수행될 수도 있으며 반대의 순서대로 수행될 수도 있다.

[0029] 본 명세서에서, "가진다", "가질 수 있다", "포함한다" 또는 "포함할 수 있다"등의 표현은 해당 특징(예: 수치, 기능, 동작, 또는 부품 등의 구성요소)의 존재를 가리키며, 추가적인 특징의 존재를 배제하지 않는다.

[0030] 또한, 본 명세서에 기재된 '~부'라는 용어는 소프트웨어 또는 FPGA(field-programmable gate array) 또는 ASIC과 같은 하드웨어 구성요소를 의미하며, '~부'는 어떤 역할들을 수행한다. 그렇지만 '~부'는 소프트웨어 또는 하드웨어에 한정되는 의미는 아니다. '~부'는 어드레싱할 수 있는 저장 매체에 있도록 구성될 수도 있고 하나 또는 그 이상의 프로세서들을 재생시키도록 구성될 수도 있다. 따라서, 일 예로서 '~부'는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터 구조들 및 변수들을 포함한다. 구성요소들과 '~부'들 안에서 제공되는 기능은 더 작은 수의 구성요소들 및 '~부'들로 결합되거나 추가적인 구성요소들과 '~부'들로 더 분리될 수 있다.

[0032] 이하에서 첨부한 도면을 참조하여 본 발명에 따른 딥러닝 기반 잠금 패턴 안전성 측정 장치 및 방법의 바람직한 실시예에 대해 상세하게 설명한다.

[0034] 먼저, 도 1을 참조하여 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 장치에 대하여 설명한다.

[0035] 도 1은 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 장치를 설명하기 위한 블록도이다.

[0036] 도 1을 참조하면, 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 장치(이하 '잠금 패턴 안전성 측정 장치'라 한다)(100)는 잠금 패턴의 수치적 특징뿐만 아니라 인간의 시각적 인식을 반영하는 잠금 패턴의 시각적 특징을 이용하여 잠금 패턴의 안전성을 측정한다.

[0037] 여기서, 잠금 패턴은 스마트폰, 태블릿 등의 전자 디바이스의 보안을 위해 사용자에 의해 설정되는 패턴으로, 서로 이격되어 있는 복수개의 점 중에서 일부의 점이나 전부의 점을 잇는 선으로 이루어질 수 있다.

[0038] 그리고, 수치적 특징은 잠금 패턴의 형태로부터 획득되는 특징으로서, 방향(direction), 교차점(crosspoints), 선의 겹침(overlaps), 각도(angles), 회전(turns), 마코프(markov) 확률, 반복된 하위 패턴(subpatterns) 중 적어도 하나일 수 있다. 시각적 특징은 인간이 잠금 패턴을 시각적으로 인식하는 정도로부터 획득되는 잠재적 특징을 말한다.

[0039] 이때, 잠금 패턴 안전성 측정 장치(100)에 입력되는 잠금 패턴은 이미지 형태로 이루어질 수 있다.

[0041] 이를 위해, 잠금 패턴 안전성 측정 장치(100)는 학습부(110) 및 안전성 측정부(130)를 포함할 수 있다.

[0042] 학습부(110)는 학습 데이터 세트를 기반으로 안전성 측정 네트워크를 학습한다.

[0043] 여기서, 안전성 측정 네트워크는 합성곱 신경망(Convolutional neural network, CNN)으로 이루어지며, 학습 데이터 세트를 구성하는 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득한다.

[0045] 안전성 측정부(130)는 학습부(110)를 통해 학습된 안전성 측정 네트워크를 이용하여 안전성 측정 대상인 잠금 패턴의 안전성을 측정한다.

[0046] 즉, 안전성 측정부(130)는 안전성 측정 대상인 잠금 패턴을 안전성 측정 네트워크에 입력하고, 안전성 측정 네트워크의 출력을 기반으로 안전성 측정 대상인 잠금 패턴의 안전성을 측정한다.

[0047] 여기서, 안전성은 안전성 측정 네트워크의 출력인 복잡도를 미리 설정된 기준에 따라 분류하여 획득한 안전성 등급일 수 있다. 예컨대, 안전성 등급은 상/중/하 중 하나이거나, 별점 형태로 이루어지거나, 점수 형태로 이루어질 수 있다.

[0050] 그러면, 도 2 및 도 3을 참조하여 본 발명의 바람직한 실시예에 따른 안전성 측정 네트워크의 학습 과정에 대하여 보다 자세하게 설명한다.

[0051] 도 2는 도 1에 도시한 학습부의 세부 구성을 설명하기 위한 블록도이고, 도 3은 본 발명의 바람직한 실시예에 따른 안전성 측정 네트워크의 학습 과정을 설명하기 위한 도면이다.

[0052] 도 2를 참조하면, 학습부(110)는 특징 추출 모듈(111) 및 선형 회귀 분석 모듈(113)을 포함할 수 있다.

[0053] 즉, 학습부(110)는 도 3에 도시된 바와 같이, 안전성 측정 네트워크의 합성곱 레이어를 통해 잠금 패턴의 시각적 특징(즉, 잠재적 특징)을 추출하는 특징 추출(feature extraction) 단계를 수행한 다음, 이를 잠금 패턴의 수치적 특징과 결합하여 회귀 분석을 통해 잠금 패턴의 복잡도를 측정하는 선형 회귀 분석(linear regression) 단계를 수행할 수 있다.

[0055] 특징 추출 모듈(111)은 잠금 패턴의 수치적 특징을 추출하고, 안전성 측정 네트워크의 합성곱 레이어(convolution layer)를 이용하여 잠금 패턴의 시각적 특징을 추출할 수 있다.

[0056] 즉, 특징 추출 모듈(111)은 잠금 패턴의 수치적 특징과 잠금 패턴에 잠재된 시각적 특징을 추출할 수 있다. 잠재된 시각적 특징은 인간의 시각적인 인식을 반영하지만, 이를 명확하게 설명할 수 없다는 특징을 가지고 있으며, 따라서 인간의 관점에서 이러한 특징을 추출하기 위해 합성곱 레이어(convolution layer)를 활용한다. 합성곱 레이어는 잠금 패턴 이미지를 입력 레이어로부터 입력받아 최종적으로 연속된 1차원 데이터들을 시각적 특징으로서 출력한다.

[0057] 이때, 잠금 패턴의 수치적 특징은 조합 가능한 모든 잠금 패턴 각각에 대하여 미리 수치적 특징을 추출하여 저장되어 있을 수 있다. 예컨대, 잠금 패턴이 일정한 간격을 두고 위치하는 9개의 점 상의 패턴인 경우, 조합 가능한 모든 389,112개의 잠금 패턴 각각에 대한 수치적 특징은 사전에 측정되어 저장되어 있을 수 있다.

[0059] 선형 회귀 분석 모듈(113)은 안전성 측정 네트워크의 완전 연결 레이어(fully connected layer)를 이용하여 특징 추출 모듈(111)을 통해 추출된 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득할 수 있다.

[0060] 즉, 선형 회귀 분석 모듈(113)은 회귀 분석 결과를 나타내는 하나의 뉴런만 생성하는 완전 연결 레이어(fully connected layer)를 포함한다. 완전 연결 레이어는 잠금 패턴의 수치적 특징을 또 다른 입력 레이어로부터 입력받고, 동시에 합성곱 레이어에서 추출된 1차원 데이터 배열을 입력받는다.

[0061] 그리고, 선형 회귀 분석 모듈(113)은 앞서 추출한 수치적 특징과 시각적 특징의 각 성분을 완전 연결 레이어의 뉴런과 가중치로서 연결함으로써 잠금 패턴의 최종 복잡도를 산출할 수 있다. 완전 연결 레이어의 단일 뉴런은

입력받은 데이터들과 각각에 대한 가중치로 연결되고, 별도의 활성화 함수를 거치지 않고 최종 복잡도를 산출한다.

[0062] 예컨대, 잠금 패턴의 복잡도는 수학식 $C=\sum_{i=1}^{N} w_i f_i + b$ 을 통해 획득될 수 있다. C는 복잡도를 나타내고, N은 특징의 개수를 나타내며, f_i는 i번째 특징을 나타내고, w_i는 i번째 특징에 대한 가중치를 나타내고, b는 뉴런의 편향을 나타낸다.

[0064] 여기서, 합성곱 레이어의 가중치 및 완전 연결 레이어의 가중치는 학습 데이터 세트를 이용한 학습 과정에서, 학습 데이터 세트에 대응되는 그라운드 트루스(ground-truth) 레이블을 이용하여 조정될 수 있다. 가중치 조정은 학습 데이터 세트를 구성하는 잠금 패턴의 그라운드 트루스 레이블에 대한 손실 함수(loss function)를 활용할 수 있다. 즉, 각 특징에 대한 가중치를 실제 사용자 설문을 통한 그라운드 트루스 레이블을 기반으로 학습하기 때문에 다양한 특징들의 숄더 서핑 공격에 대한 연관성을 복잡도에 충분히 반영할 수 있다.

[0065] 이때, 학습 데이터 세트는 조합 가능한 모든 잠금 패턴 각각에서 추출된 수치적 특징을 기반으로 조합 가능한 모든 잠금 패턴을 미리 설정된 유사 판단 기준에 따라 군집화(clustering)하고, 각 군집 마다 수치적 특징 벡터의 중심점(centroid)에 대응하는 잠금 패턴을 획득하며, 군집 각각에서 획득한 잠금 패턴으로 구성될 수 있다. 예컨대, 잠금 패턴이 일정한 간격을 두고 위치하는 9개의 점 상의 패턴인 경우, 조합 가능한 모든 389,112개의 잠금 패턴 각각에 대해 그라운드 트루스 레이블을 수집하는 것은 어려움이 있다. 따라서, 389,112개의 잠금 패턴을 대표하는 일부 잠금 패턴을 선정하고, 선정된 잠금 패턴에 대해서만 그라운드 트루스 레이블을 수집할 수 있다.

[0066] 그리고, 그라운드 트루스 레이블은 실제 사용자를 대상으로 하는 설문을 통해, 학습 데이터 세트를 구성하는 잠금 패턴 각각에 대해 획득될 수 있다. 학습 데이터를 구성하는 잠금 패턴의 그라운드 트루스 레이블은 실제 사용자의 인식을 대표해야 하기 때문에 실제 사용자를 대상으로 해당 잠금 패턴의 복잡도에 대한 그라운드 트루스 레이블을 수집하여야 한다.

[0067] 여기서, 설문은 하나의 잠금 패턴에 대해, 답변 가능한 복잡도의 범위가 서로 동일한 복수개의 질문 항목으로 이루어질 수 있다. 하나의 잠금 패턴에 대한 그라운드 트루스 레이블은 복수개의 질문 항목 각각에 대해 사용자가 답변한 복잡도를 기반으로 획득될 수 있다. 예컨대, 하나의 잠금 패턴에 대한 그라운드 트루스 레이블은 수학식 $C=\sqrt{\sum_{i=1}^{N} S_i^2}$ 을 통해 획득될 수 있다. C는 그라운드 트루스 레이블을 나타내고, N은 질문 항목의 개수를 나타내며, S는 질문 항목에 대해 사용자가 답변한 복잡도를 나타낸다. 예컨대, 설문은 다수의 잠금 패턴을 제시하고 각각의 복잡도 순위를 결정하는 방식, 하나의 잠금 패턴을 제시하여 절대적인 복잡도를 질문하는 방식 등과 같이 다양한 방식으로 이루어질 수 있다.

[0070] 그러면, 도 4 및 도 5를 참조하여 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 방법에 대하여 설명한다.

[0071] 도 4는 본 발명의 바람직한 실시예에 따른 딥러닝 기반 잠금 패턴 안전성 측정 방법을 설명하기 위한 흐름도이다.

[0072] 도 4를 참조하면, 잠금 패턴 안전성 측정 장치(100)는 합성곱 신경망으로 이루어지며, 학습 데이터 세트를 구성하는 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 안전성 측정 네트워크를 학습한다(S110).

[0074] 이후, 잠금 패턴 안전성 측정 장치(100)는 안전성 측정 대상인 잠금 패턴을 안전성 측정 네트워크에 입력하고, 안전성 측정 네트워크의 출력을 기반으로 안전성 측정 대상인 잠금 패턴의 안전성을 측정한다(S130).

[0077] 도 5는 도 4에 도시한 안전성 측정 네트워크 학습 단계의 세부 단계를 설명하기 위한 흐름도이다.

[0078] 도 5를 참조하면, 잠금 패턴 안전성 측정 장치(100)는 잠금 패턴의 수치적 특징을 추출하고, 안전성 측정 네트워크의 합성곱 레이어를 이용하여 잠금 패턴의 시각적 특징을 추출할 수 있다(S111).

[0079] 이때, 잠금 패턴의 수치적 특징은 조합 가능한 모든 잠금 패턴 각각에 대하여 미리 수치적 특징을 추출하여 저장되어 있을 수 있다.

[0081] 그런 다음, 잠금 패턴 안전성 측정 장치(100)는 안전성 측정 네트워크의 완전 연결 레이어를 이용하여 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득할 수 있다(S113).

[0083] 여기서, 합성곱 레이어의 가중치 및 완전 연결 레이어의 가중치는 학습 데이터 세트를 이용한 학습 과정에서, 학습 데이터 세트에 대응되는 그라운드 트루스(ground-truth) 레이블을 이용하여 조정될 수 있다.

[0084] 이때, 학습 데이터 세트는 조합 가능한 모든 잠금 패턴 각각에서 추출된 수치적 특징을 기반으로 조합 가능한 모든 잠금 패턴을 미리 설정된 유사 판단 기준에 따라 군집화(clustering)하고, 각 군집 마다 수치적 특징 벡터의 중심점(centroid)에 대응하는 잠금 패턴을 획득하며, 군집 각각에서 획득한 잠금 패턴으로 구성될 수 있다.

[0085] 그리고, 그라운드 트루스 레이블은 실제 사용자를 대상으로 하는 설문을 통해, 학습 데이터 세트를 구성하는 잠금 패턴 각각에 대해 획득될 수 있다.

[0086] 여기서, 설문은 하나의 잠금 패턴에 대해, 답변 가능한 복잡도의 범위가 서로 동일한 복수개의 질문 항목으로 이루어질 수 있다. 하나의 잠금 패턴에 대한 그라운드 트루스 레이블은 복수개의 질문 항목 각각에 대해 사용자가 답변한 복잡도를 기반으로 획득될 수 있다. 예컨대, 하나의 잠금 패턴에 대한 그라운드 트루스 레이블은 수학식 $C=\sqrt{\sum_{i=1}^{N} S_i^2}$ 을 통해 획득될 수 있다. C는 그라운드 트루스 레이블을 나타내고, N은 질문 항목의 개수를 나타내며, S는 질문 항목에 대해 사용자가 답변한 복잡도를 나타낸다.

[0089] 정리하면, 본 발명에 따른 잠금 패턴 안전성 측정 장치(100)는 수치적 특징뿐만 아니라 인간의 시각적 인식을 반영하는 잠재적 특징도 활용하고, 활용된 특징의 가중치를 정확하게 설정하기 위해 신뢰할 수 있는 레이블을 수집하여, 잠금 패턴의 안정성을 측정할 수 있다.

[0090] 예컨대, 안드로이드 패턴 락(android pattern lock)은 안드로이드 사용자들로부터 널리 쓰이고 있는 인증 방법 중의 하나이다. 사용자는 패턴의 모양과 길이를 자유롭게 설정할 수 있지만, 단순한 모양과 짧은 길이의 패턴은 공격에 취약한 단점이 있다. 특히, 숄더 서핑 공격은 사용자의 근처에 있는 사람이라면 특별한 배경 지식이 없이도 공격자가 될 수 있으므로 인증 환경에 더 만연하다고 할 수 있다. 사용자는 편의성을 위해 단순한 모양의 패턴을 고르는 경향이 있으므로 이러한 공격으로부터 안전한 패턴을 선택하기 위한 유도 장치가 필요하다. 하지만, 현재까지의 기술은 이러한 목적을 달성하지 못하므로 정확한 안전성을 측정하기 위한 기술의 개발이 필요하다. 한편, 딥러닝(deep learning) 알고리즘은 복잡한 문제를 처리할 수 있으며 꾸준한 개발을 통해 다양한 분야에서 인간의 식별 능력과 비슷한 수준의 높은 성능을 나타내고 있다. 그 중에서도 합성곱 신경망(CNN)은 시각적인 데이터를 처리하는데 특화되어 있고, 합성곱 신경망이 인간과 비슷한 수준의 이미지 인식 능력을 가지고 있기 때문에 시각적인 데이터로 표현되는 패턴도 동일한 성능으로 인식할 것이며, 합성곱 신경망을 통해 기존의 활용된 수치적인 특징을 넘어 인간의 인식과 관련된 잠재적인 특징을 추출할 수 있고, 네트워크의 학습을 통해 이에 대한 가중치 또한 적절하게 설정할 수 있다. 안드로이드 잠금 패턴 또한 시각적인 데이터와 관련이 있기 때문에 해당 기술과 접목될 수 있다. 이와 같은 점에 착안하여, 본 발명에 따른 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 안전성 측정 네트워크를 도출하였다. 이때, 안전성 측정 네트워크의 안정적인 성능을 확보하기 위해 신뢰할 수 있는 레이블을 기반으로 하는 학습이 진행되어야 하며, 이를 위해 본 발명은 실제 사용자 설문을 통해 잠금 패턴에 대한 실제 사용자들의 인식에 대한 그라운드 트루스 레이블을 수집하고 이를 이용하여 안전성 측정 네트워크의 학습을 진행한다.

[0092] 즉, 본 발명은 딥러닝을 기반으로 다양한 특징을 활용하고 적절한 가중치를 설정하는 점에서 종래 기술과 차별성이 있다. 기존의 안드로이드 패턴 락의 안전성 측정 방식은 경험에 의거했기 때문에 활용된 특징이 부족했으며, 안전성에 주는 영향력 또한 잘못 고려되는 문제가 있다. 이에 반면, 본 발명은 딥러닝, 특히 합성곱 신경망을 활용함으로써 기존의 수치적 특징뿐만 아니라 인간의 인식을 반영하는 잠재적인 시각적 특징을 추출할 수 있고, 이러한 특징이 숄더 서핑 공격에 대한 안전성에 주는 가중치를 학습을 통해 적절하게 설정할 수 있다.

[0093] 그리고, 본 발명은 실제 사용자 설문을 통한 잠금 패턴에 대한 그라운드 트루스 레이블을 수집하는 점에서 종래 기술과 차별성이 있다. 측정 네트워크의 구조가 효과적이어도 학습이 철저하게 이루어지지 않으면 정확한 복잡도 측정이 불가능한 문제가 있다. 본 발명은 전체 잠금 패턴의 복잡도를 대표하는 설문 잠금 패턴을 선정하고, 실제 사용자들이 해당 잠금 패턴에 대해 답변한 그라운드 트루스 복잡도를 활용함으로써, 딥러닝 모델이 실제 사용자의 측정 기준을 반영하도록 할 수 있다.

[0094] 또한, 본 발명은 잠금 패턴을 사용하는 사용자에게 높은 안전성을 제공할 수 있다. 본 발명을 통해 잠금 패턴

의 안전성이 정확하게 측정된다면, 잠금 패턴은 지문, 얼굴 등을 템플릿으로서 저장하여야 하는 생체 인식보다 부담이 적은 인증 방법으로서, 널리 쓰일 가능성을 가지고 있다.

[0095] 아울러, 본 발명은 잠금 해제뿐만 아니라 인증이 필요한 다양한 분야에 사용될 수 있다. 잠금 패턴이 사용되는 단계가 스마트폰 등과 같은 전자 디바이스의 잠금 해제가 대부분이지만, 전자 결제나 본인 인증과 같은 스마트폰 환경에서의 인증이 필요한 다양한 서비스에서도 적용이 가능해짐으로써, 해당 서비스의 사용을 촉진하는 계기를 마련할 수 있다.

[0098] 이상에서 설명한 본 발명의 실시예를 구성하는 모든 구성요소들이 하나로 결합하거나 결합하여 동작하는 것으로 기재되어 있다고 해서, 본 발명이 반드시 이러한 실시예에 한정되는 것은 아니다. 즉, 본 발명의 목적 범위 안에서라면, 그 모든 구성요소들이 하나 이상으로 선택적으로 결합하여 동작할 수도 있다. 또한, 그 모든 구성요소들이 각각 하나의 독립적인 하드웨어로 구현될 수 있지만, 각 구성요소들의 그 일부 또는 전부가 선택적으로 조합되어 하나 또는 복수개의 하드웨어에서 조합된 일부 또는 전부의 기능을 수행하는 프로그램 모듈을 갖는 컴퓨터 프로그램으로서 구현될 수도 있다. 또한, 이와 같은 컴퓨터 프로그램은 USB 메모리, CD 디스크, 플래쉬 메모리 등과 같은 컴퓨터가 읽을 수 있는 기록 매체(Computer Readable Media)에 저장되어 컴퓨터에 의하여 읽혀지고 실행됨으로써, 본 발명의 실시예를 구현할 수 있다. 컴퓨터 프로그램의 기록 매체로서는 자기기록매체, 광기록매체 등이 포함될 수 있다.

[0099] 이상의 설명은 본 발명의 기술 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 본 발명의 본질적인 특성에서 벗어나지 않는 범위 내에서 다양한 수정, 변경 및 치환이 가능할 것이다. 따라서, 본 발명에 개시된 실시예 및 첨부된 도면들은 본 발명의 기술 사상을 한정하기 위한 것이 아니라 설명하기 위한 것이고, 이러한 실시예 및 첨부된 도면에 의하여 본 발명의 기술 사상의 범위가 한정되는 것은 아니다. 본 발명의 보호 범위는 아래의 청구범위에 의하여 해석되어야 하며, 그와 동등한 범위 내에 있는 모든 기술 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

부호의 설명

[0100] 100 : 잠금 패턴 안전성 측정 장치,

110 : 학습부,

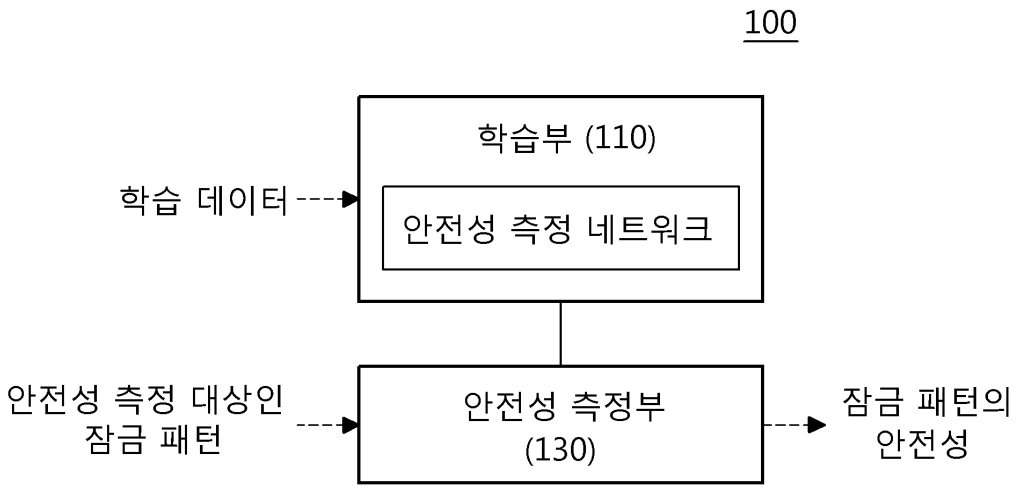
111 : 특징 추출 모듈,

113 : 선형 회귀 분석 모듈,

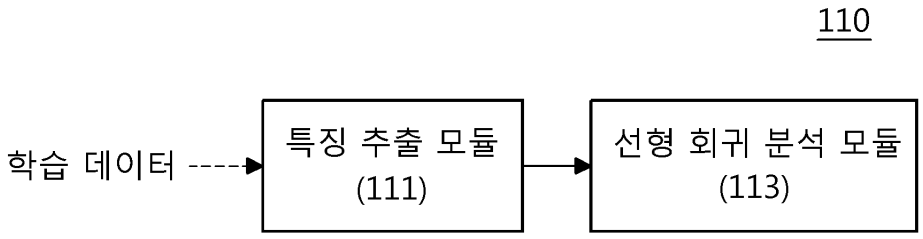
130 : 안전성 측정부

도면

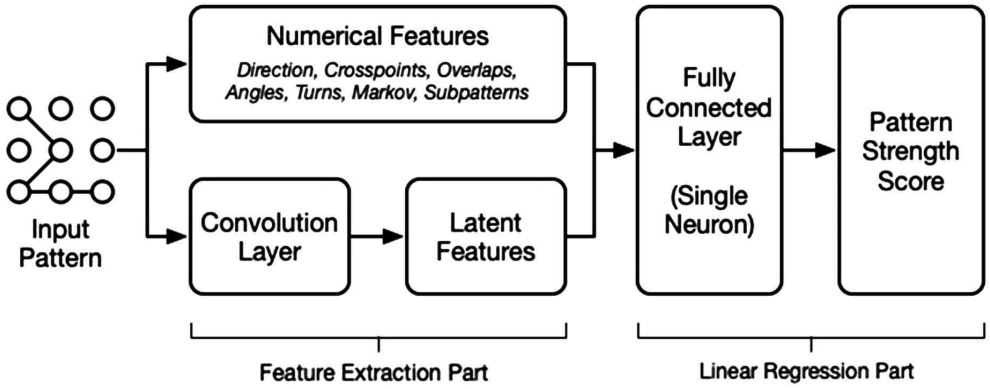
도면1



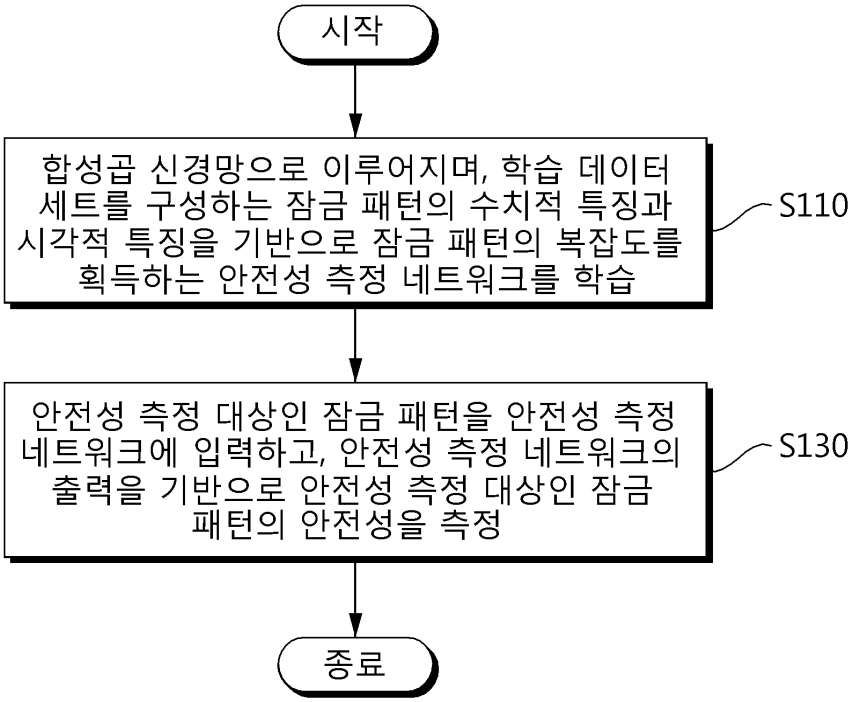
도면2


110
학습 데이터
특징 추출 모듈
(111)
선형 회귀 분석 모듈
(113)

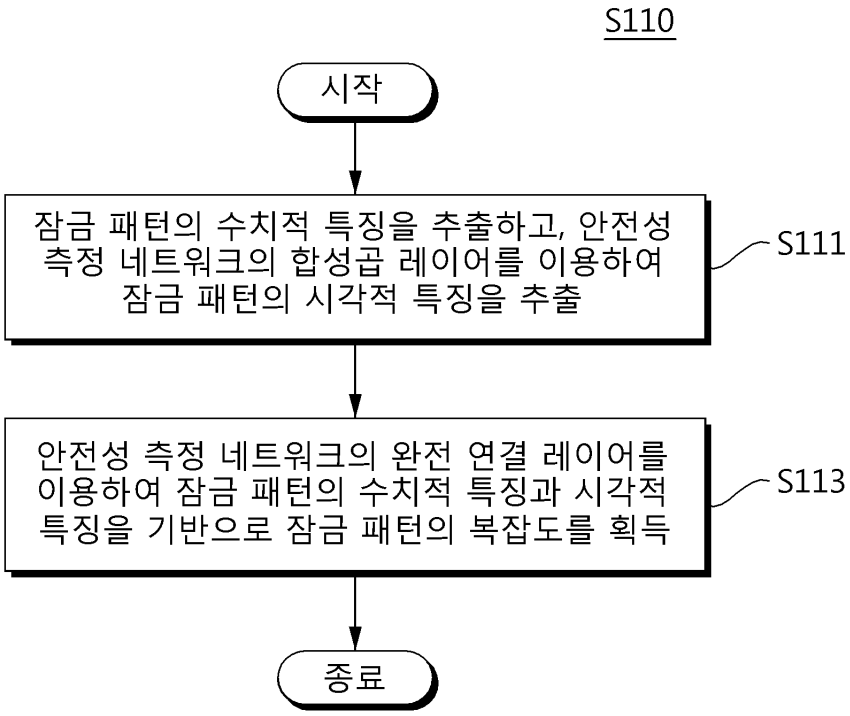
도면3


Numerical Features
Direction, Crosspoints, Overlaps, Angles, Turns, Markov, Subpatterns
Input Pattern
Convolution Layer
Latent Features
Fully Connected Layer
(Single Neuron)
Pattern Strength Score
Feature Extraction Part
Linear Regression Part

도면4


시작
합성곱 신경망으로 이루어지며, 학습 데이터 세트를 구성하는 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득하는 안전성 측정 네트워크를 학습
S110
안전성 측정 대상인 잠금 패턴을 안전성 측정 네트워크에 입력하고, 안전성 측정 네트워크의 출력을 기반으로 안전성 측정 대상인 잠금 패턴의 안전성을 측정
S130
종료

도면5


S110
시작
잠금 패턴의 수치적 특징을 추출하고, 안전성 측정 네트워크의 합성곱 레이어를 이용하여 잠금 패턴의 시각적 특징을 추출
S111
안전성 측정 네트워크의 완전 연결 레이어를 이용하여 잠금 패턴의 수치적 특징과 시각적 특징을 기반으로 잠금 패턴의 복잡도를 획득
S113
종료