



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년03월13일
(11) 등록번호 10-1838400
(24) 등록일자 2018년03월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/36 (2013.01) G06F 21/46 (2013.01)
G06F 3/041 (2006.01)
(52) CPC특허분류
G06F 21/36 (2013.01)
G06F 21/46 (2013.01)
(21) 출원번호 10-2016-0149548
(22) 출원일자 2016년11월10일
심사청구일자 2016년11월10일
(56) 선행기술조사문헌
KR1020150067814 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대현
서울특별시 서초구 서초중앙로 200, 17동 901호(서초동, 삼풍아파트)
(74) 대리인
양성보

전체 청구항 수 : 총 7 항

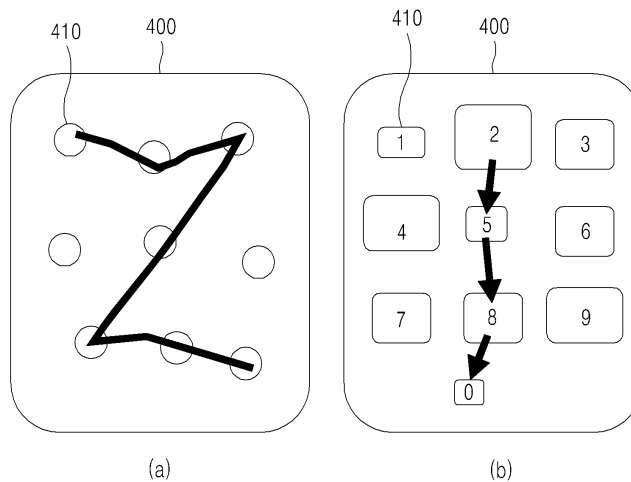
심사관 : 문남두

(54) 발명의 명칭 비정형화된 레이아웃으로부터 패턴 정보를 인식하는 사용자 인증 방법 및 장치

(57) 요약

사용자 인증 방법 및 장치가 개시된다. 일 실시예에 따른 사용자 인증 방법은, 일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면을 표시하는 단계; 사용자로부터 상기 인증 화면을 통하여 입력된 입력 정보를 수신하는 단계; 상기 입력 정보에 기초하여 상기 입력 정보로부터 패턴 정보를 추출하는 단계; 및 상기 패턴 정보와 기 저장된 인증 정보와의 비교에 기반하여 사용자를 인증하는 단계를 포함할 수 있다.

대표도 - 도4



(52) CPC특허분류
G06F 3/0416 (2013.01)

명세서

청구범위

청구항 1

사용자 인증 방법에 있어서,

일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면을 표시하는 단계;

사용자로부터 상기 인증 화면을 통하여 입력된 입력 정보를 수신하는 단계;

상기 입력 정보에 기초하여 상기 입력 정보로부터 패턴 정보를 추출하는 단계; 및

상기 패턴 정보와 기 저장된 인증 정보와의 비교에 기반하여 사용자를 인증하는 단계

를 포함하고,

상기 사용자로부터 상기 인증 화면을 통하여 입력된 입력 정보를 수신하는 단계는,

상기 인증 화면을 구성하는 상기 사용자로부터의 입력 정보가 감지되는 복수의 입력 인터페이스들 중, 소기의 입력 인터페이스에 대한 사용자의 터치 입력을 감지하는 단계

를 포함하고,

상기 소기의 입력 인터페이스는 상기 인증 화면에서 사용자가 인식 가능하도록 표시되어 있지 않은 것

을 포함하는 사용자 인증 방법.

청구항 2

제1항에 있어서,

상기 사용자로부터 입력되는 입력 정보에 기초하여 상기 사용자의 인증을 위한 인증 정보를 등록하는 단계

를 더 포함하고,

상기 인증 정보를 등록하는 단계는,

2회 이상 상기 사용자로부터 입력 정보를 수신하는 단계;

상기 2회 이상 수신된 입력 정보에 기반하여 상기 사용자와 연관된 패턴 정보를 생성하는 단계; 및 상기 생성된 패턴 정보를 상기 사용자의 인증을 위한 인증 정보로서 등록하는 단계

를 포함하는 사용자 인증 방법.

청구항 3

제1항에 있어서,

상기 일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면은,

표시 형태가 변경되어 표시된, 사용자의 입력 정보가 감지되는 적어도 하나의 입력 인터페이스를 포함하고,

상기 표시 형태는 상기 인증 화면 내의 상기 입력 인터페이스의 위치, 색상, 크기, 모양 및 표시 여부 중 적어도 하나이고,

상기 입력 인터페이스는 문자, 숫자 및 도형 중 적어도 하나를 포함하는 사용자 인증 방법.

청구항 4

제1항에 있어서,

상기 패턴 정보는,

상기 사용자의 인증을 위해 패스워드 또는 패스워드 패턴의 인식과는 구분되는 것으로서, 상기 인증 화면에 표시된 사용자의 입력 정보가 감지되는 입력 인터페이스에 대한 상기 사용자의 입력과 연관된 리듬 정보, 상기 입력과 연관된 시간 정보, 상기 입력과 연관된 상기 인증 화면 내의 위치 정보 및 상기 인증 화면에 표시된 입력 인터페이스들 중 2 이상의 입력 인터페이스들에 대한 입력 시간 간격 정보를 포함하는 사용자 인증 방법.

청구항 5

제1항에 있어서,

상기 입력 정보에 기초하여 상기 사용자의 패턴 정보를 추출하는 단계는,

상기 입력 정보가 상기 사용자의 인증을 위한 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는지 여부를 판단하는 단계; 및

상기 입력 정보가 상기 패스워드 정보 또는 패스워드 패턴 정보를 포함할 경우, 상기 입력 정보로부터 상기 사용자의 패턴 정보를 추출하는 단계

를 포함하는 사용자 인증 방법.

청구항 6

삭제

청구항 7

삭제

청구항 8

사용자 인증 방법에 있어서,

일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면을 표시하는 단계;

사용자로부터 상기 인증 화면을 통하여 입력된 입력 정보를 수신하는 단계;

상기 입력 정보에 기초하여 상기 입력 정보로부터 패턴 정보를 추출하는 단계; 및

상기 패턴 정보와 기 저장된 인증 정보와의 비교에 기반하여 사용자를 인증하는 단계

를 포함하고,

상기 인증 화면은,

상기 사용자의 인증을 위한 상기 사용자의 인증 정보의 등록 시, 상기 사용자로부터의 입력 정보가 감지되는 소정의 입력 인터페이스에 대한 상기 사용자의 입력에 따라, 표시 형태가 변경된 상기 소정의 입력 인터페이스를 포함하고,

상기 소정의 인터페이스는 상기 사용자의 인증을 위한 상기 사용자의 입력 정보의 등록 시의 상기 사용자의 입력의 횟수에 따라 투명도가 변경된 표시 형태를 갖는 것을 특징으로 하는 사용자 인증 방법.

청구항 9

사용자 인증 장치에 있어서,

일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면을 표시하는 표시부;

사용자로부터 상기 인증 화면을 통하여 입력된 입력 정보를 수신하는 수신부;

상기 입력 정보에 기초하여 상기 입력 정보로부터 패턴 정보를 추출하는 추출부; 및

상기 패턴 정보와 기 저장된 인증 정보와의 비교에 기반하여 사용자를 인증하는 인증부

를 포함하고,

상기 수신부는,

상기 인증 화면을 구성하는 상기 사용자로부터의 입력 정보가 감지되는 복수의 입력 인터페이스들 중, 소기의 입력 인터페이스에 대한 사용자의 터치 입력을 감지하는 것

을 포함하고,

상기 소기의 입력 인터페이스는 상기 인증 화면에서 사용자가 인식 가능하도록 표시되어 있지 않은 것

을 포함하는 사용자 인증 장치.

발명의 설명

기술 분야

[0001] 아래의 설명은 사용자 인증 기술에 관한 것으로, 정형화 또는 비정형화된 레이아웃을 통하여 입력되는 사용자에게 대한 패턴 정보를 인식함으로써 사용자 인증을 수행하는 방법 및 장치에 관한 것이다.

배경 기술

[0002] 사용자 인증은 특정 시스템(컴퓨터, 웹 서버, 스마트 폰 등)에 접근을 시도하는 사용자가 접근 권한이 있는지를 확인하여 접근을 허용하는 일련의 절차로서, 최근에는 바이오 인식이나 하드웨어 토큰 기반의 방법도 점차 보급되고 있다. 가장 일반적으로는 패스워드, 개인식별번호(Personal Identification Number: 이하 PIN) 등 지식 기반의 인증이 가장 널리 쓰이고 있다. 지식 기반의 인증은 사용자와 시스템 간에 미리 공유되어 있는 비밀 정보를 기반으로 하며 사용자가 비밀 정보인 패스워드 또는 PIN을 직접 키패드나 터치패드 등을 통해 입력하는 방법이다. 하지만 이러한 방법은 공격자가 사용자의 입력 장면을 옆에서 관찰할 경우 비밀 정보가 그대로 노출되는 단점이 존재한다.

[0003] 또 다른 예로서, 신체적 특징 기반의 생물측정학(biometrics)적 인증은 사용자의 신체적 특성 예를 들면 사용자의 지문, 홍채 등을 분석하는 것으로, 생성한 사용자 특성 정보를 미리 저장해 두고, 로그인하고자 하는 사용자의 사용자 특성 정보를 획득하여 비교함으로써 수행한다. 상기 방법은 사용자 특성 정보를 분석하는 기기의 정확도에 따라 사용자 인증의 정확도가 결정되기 때문에 분석 장치의 정확도를 증가시키기 위한 비용이 증가한다는 문제점이 존재한다. 또한 분석 과정 및 비교 과정이 비교적 복잡하여 구현 비용 자체도 높은 편이다.

[0004] 또 다른 예로서, 행동 기반의 생물측정학적 인증은 사용자의 행동 패턴 특히 타이핑 패턴을 분석함으로써 생성된 사용자 특성 정보를 이용하는 것으로 사용자의 타이핑 패턴을 저장해 두고, 로그인시에 입력된 사용자의 타이핑 패턴이 미리 저장된 진정한 사용자의 타이핑 패턴과 동일한지를 비교함으로써 사용자 인증을 수행한다. 이러한 방법에 의하면, 타이핑 패턴은 사용자의 의식적 행동의 결과이기 때문에 사용자의 노력에 따라 패턴의 품질을 증가시킬 수 있고, 구현 비용이 적게 들고, 구현 절차가 간단하다는 이점이 있다.

발명의 내용

해결하려는 과제

[0005] 비정형화된 레이아웃으로 형성된 인증 화면을 통해 입력된 사용자의 입력 정보에 기초하여 사용자 고유의 패턴 정보를 추출하고, 추출된 패턴 정보와 기 저장된 인증 정보를 매칭함으로써 사용자 인증을 수행하는 방법 및 장치를 제공할 수 있다.

[0006] 정형화된 레이아웃으로 형성된 인증 화면을 통해 사용자로부터 보이지 않는 특정 위치를 포함하는 소기의 입력 인터페이스를 입력시키도록 함으로써 사용자 인증을 수행하는 방법 및 장치를 제공할 수 있다.

과제의 해결 수단

[0007] 사용자 인증 방법은, 일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면을 표시하는 단계; 사용자로부터 상

기 인증 화면을 통하여 입력된 입력 정보를 수신하는 단계; 상기 입력 정보에 기초하여 상기 입력 정보로부터 패턴 정보를 추출하는 단계; 및 상기 패턴 정보와 기 저장된 인증 정보와의 비교에 기반하여 사용자를 인증하는 단계를 포함할 수 있다.

[0008] 상기 사용자로부터 입력되는 입력 정보에 기초하여 상기 사용자의 인증을 위한 인증 정보를 등록하는 단계를 더 포함하고, 상기 인증 정보를 등록하는 단계는, 2회 이상 상기 사용자로부터 입력 정보를 수신하는 단계; 상기 2회 이상 수신된 입력 정보에 기반하여 상기 사용자와 연관된 패턴 정보를 생성하는 단계; 및 상기 생성된 패턴 정보를 상기 사용자의 인증을 위한 인증 정보로서 등록하는 단계를 포함할 수 있다.

[0009] 상기 일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면은, 표시 형태가 변경되어 표시된, 사용자의 입력 정보가 감지되는 적어도 하나의 입력 인터페이스를 포함하고, 상기 표시 형태는 상기 인증 화면 내의 상기 입력 인터페이스의 위치, 색상, 크기, 모양 및 표시 여부 중 적어도 하나이고, 상기 입력 인터페이스는 문자, 숫자 및 도형 중 적어도 하나를 포함할 수 있다.

[0010] 상기 패턴 정보는, 상기 사용자의 인증을 위해 패스워드 또는 패스워드 패턴의 인식과는 구분되는 것으로서, 상기 인증 화면에 표시된 사용자의 입력 정보가 감지되는 입력 인터페이스에 대한 상기 사용자의 입력과 연관된 리듬 정보, 상기 입력과 연관된 시간 정보, 상기 입력과 연관된 상기 인증 화면 내의 위치 정보 및 상기 인증 화면에 표시된 입력 인터페이스들 중 2 이상의 입력 인터페이스들에 대한 입력 시간 간격 정보를 포함할 수 있다.

[0011] 상기 입력 정보에 기초하여 상기 사용자의 패턴 정보를 추출하는 단계는, 상기 입력 정보가 상기 사용자의 인증을 위한 소기의 패스워드 정보 또는 소기의 패스워드 패턴 정보를 포함하는지 여부를 판단하는 단계; 및 상기 입력 정보가 상기 패스워드 정보 또는 패스워드 패턴 정보를 포함할 경우, 상기 입력 정보로부터 상기 사용자의 패턴 정보를 추출하는 단계를 포함할 수 있다.

[0012] 상기 사용자로부터 상기 인증 화면을 통하여 입력된 입력 정보를 수신하는 단계는, 상기 인증 화면을 구성하는 상기 사용자로부터의 입력 정보가 감지되는 복수의 입력 인터페이스들 중, 소기의 입력 인터페이스에 대한 사용자의 터치 입력을 감지하는 단계를 포함하고, 상기 소기의 입력 인터페이스는 상기 인증 화면에서 사용자가 인식 가능하도록 표시되어 있지 않을 수 있다.

[0013] 상기 인증 화면은, 상기 사용자의 인증을 위한 상기 사용자의 인증 정보의 등록 시, 상기 사용자로부터의 입력 정보가 감지되는 소정의 입력 인터페이스에 대한 상기 사용자의 입력에 따라, 표시 형태가 변경된 상기 소정의 입력 인터페이스를 포함할 수 있다.

[0014] 상기 소정의 인터페이스는 상기 사용자의 인증을 위한 상기 사용자의 입력 정보의 등록 시의 상기 사용자의 입력의 횟수에 따라 투명도가 변경된 표시 형태를 가질 수 있다.

[0015] 사용자 인증 장치는, 일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면을 표시하는 표시부; 사용자로부터 상기 인증 화면을 통하여 입력된 입력 정보를 수신하는 수신부; 상기 입력 정보에 기초하여 상기 입력 정보로부터 패턴 정보를 추출하는 추출부; 및 상기 패턴 정보와 기 저장된 인증 정보와의 비교에 기반하여 사용자를 인증하는 식별부를 포함할 수 있다.

발명의 효과

[0016] 일 실시예에 따른 사용자 인증 장치는 비정형화된 레이아웃으로 형성된 인증 화면을 통하여 입력된 사용자 고유의 패턴 정보를 더욱 증폭시켜 획득할 수 있게 된다. 이에 따라 사용자 인증 장치는 상기 사용자 고유의 패턴 정보를 통하여 사용자 인증을 수행함으로써 보안을 보다 강화할 수 있다. 또한, 사용자 인증 장치는 패스워드 정보뿐만 아니라 패턴 정보를 기반으로 사용자 인증을 수행하기 때문에 보안성을 유지할 수 있게 된다.

[0017] 일 실시예에 따른 인증 장치는 사용자 인증 정보를 등록하는 과정에서 패턴 정보를 트레이닝하여 저장하고 있기 때문에 패턴 정보를 통한 사용자 인증을 수행함에 있어 인식률 및 정확도를 향상시킬 수 있다.

[0018] 일 실시예에 따른 사용자 인증 장치는 인증 화면에 소기의 입력 인터페이스를 포함하는 복수의 인터페이스들을 제공함으로써 패스워드가 노출되더라도 보안을 유지할 수 있다. 이에 따라, 사용자 인증 장치는 사용자만이 알고 있는 특정 위치를 포함한 패스워드를 입력하도록 제공함으로써 해킹의 위험을 줄일 수 있다.

도면의 간단한 설명

- [0019] 도 1은 사용자 인증 과정을 설명하기 위한 도면이다.
- 도 2는 일 실시예에 따른 사용자 인증 장치의 구성을 설명하기 위한 블록도이다.
- 도 3은 일 실시예에 따른 사용자 인증 장치의 데이터베이스에 저장된 정보를 설명하기 위한 도면이다.
- 도 4 및 도 5는 일 실시예에 따른 사용자 인증 장치의 사용자 인증 과정을 설명하기 위한 예이다.
- 도 6은 일 실시예에 따른 사용자 인증 장치의 사용자 인증 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

- [0020] 이하, 실시예를 첨부한 도면을 참조하여 상세히 설명한다.
- [0021] 도 1은 사용자 인증 과정을 설명하기 위한 도면이다.
- [0022] 인증 화면(100)은 컴퓨터 장치로 구현되는 고정형 단말이거나 이동형 단말을 통하여 표시될 수 있다. 예를 들면, 스마트폰(smart phone), 휴대폰, 네비게이션, 컴퓨터, 노트북, 디지털방송용 단말, PDA(Personal Digital Assistants), PMP(Portable Multimedia Player), 태블릿 PC 등의 디스플레이 창을 통하여 인증 화면(100)이 표시될 수 있다. 이와 같이 인증 화면(100)이 표시된 스마트 기기를 통하여 사용자로부터 입력 정보가 수신됨에 따라 사용자 인증을 수행할 수 있다.
- [0023] 인증 화면(100)은 단말에서 입출력 장치로서의 기능을 수행하며, 단말 내부에 명령을 전달하거나 다른 단말 또는 서버로 메시지를 전달하는 등의 일을 수행할 때 디스플레이할 수 있다.
- [0024] 인증 화면(100)의 입력 인터페이스는 문자, 숫자 또는 패턴 중 적어도 하나로 구성될 수 있다. 예를 들면, 도 1(a)를 참고하면, 인증 화면(100)에 출력된 입력 인터페이스가 문자 또는 숫자일 경우, 입력하고자 하는 문자 또는 숫자를 인증 화면(100)에서 터치 또는 드래그함으로써 입력할 수 있다. 더욱 상세하게는, 입력 인터페이스가 일정하게 배열된 구성된 레이아웃을 포함하는 인증 화면이 표시될 수 있다. 이때, 인증 화면(100)의 레이아웃은 입력 인터페이스들의 배열, 크기 및 위치가 일정하게 배열되어 있을 수 있다. 예를 들면, 사용자는 인증 화면(100)에서 '2', '5', '8', '0'을 입력하고자 한다면, '2'를 선택한 후 연속적으로 '5', '8', '0'을 드래그한 후, 인증 화면(100)에 터치를 종료함으로써 입력하고자 하는 숫자를 입력하게 된다. 또는 사용자는 '2'를 선택한 후 연속적으로 '5', '8', '0'를 선택함으로써 숫자를 입력하게 된다.
- [0025] 또한, 도 1(b)를 참고하면, 인증 화면(100)에 출력된 입력 인터페이스가 패턴으로 구성될 경우, 입력하고자 하는 패턴을 터치&드래그를 통하여 연속적으로 패턴을 드래그함으로써 입력할 수 있다. 또는 입력하고자 하는 패턴에 대하여 제스처를 취함으로써 입력할 수도 있다. 마찬가지로, 사용자는 인증 화면(100)에 출력된 패턴들을 통하여 사용자가 'Z' 형태의 패턴을 입력할 수 있다.
- [0026] 하지만 도 1과 같이 정형화된 레이아웃으로 형성된 인증 화면을 통하여 사용자 인증을 수행할 경우, 사용자가 입력한 입력 정보가 그대로 노출되기 때문에 보안에 취약하다는 문제점이 존재한다. 이에 따라 아래의 설명에서는 비정형적인 레이아웃으로 형성된 인증 화면을 통하여 사용자의 비해결 특성을 증폭시켜 사용자 고유의 패턴 정보를 인식함으로써 사용자 인증을 수행하는 방법에 대하여 설명하기로 한다.
- [0027] 도 2는 일 실시예에 따른 사용자 인증 장치의 구성을 설명하기 위한 블록도이다.
- [0028] 사용자 인증 장치(200)는 사용자의 패턴 정보에 기초하여 사용자 인증을 수행하기 위한 것으로, 표시부(210), 수신부(220), 추출부(230), 인증부(240), 등록부(250) 및 설정부(260)를 포함할 수 있다. 사용자 인증 장치(200)는 비정형적 또는 정형적인 레이아웃(Layout)으로 구성된 인증 화면을 통하여 사용자의 패턴 정보를 인식함으로써 사용자 인증을 수행할 수 있다.
- [0029] 표시부(210)는 일정하지 않은 레이아웃(Layout)으로 형성된 인증 화면을 표시할 수 있다. 예를 들면, 인증 화면은 표시 형태가 변경되어 표시된, 사용자의 입력 정보가 감지되는 적어도 하나의 입력 인터페이스를 포함하고, 표시 형태는 상기 인증 화면 내의 입력 인터페이스의 위치, 색상, 크기, 모양 및 표시 여부 중 적어도

하나이고, 입력 인터페이스가 문자, 숫자 및 도형 중 적어도 하나를 포함할 수 있다. 또는, 예를 들면, 인증 화면은 인증 화면에 구성된 복수의 입력 인터페이스들 중 사용자 인증을 위한 사용자의 입력 정보 등록 시 사용자의 입력 횟수에 따라 투명도가 변경된 표시 형태를 가질 수 있다.

[0030] 수신부(220)는 사용자로부터 상기 인증 화면을 통하여 입력된 입력 정보를 수신할 수 있다. 수신부(220)는 사용자로부터 인증 화면을 통하여 패스워드 정보 및 패스워드 패턴 정보를 입력 정보로서 수신할 수 있다. 수신부(220)는 인증 화면을 구성하는 사용자로부터의 입력 정보가 감지되는 복수의 입력 인터페이스들 중, 소기의 입력 인터페이스에 대한 사용자의 터치 입력을 감지할 수 있다.

[0031] 추출부(230)는 입력 정보에 기초하여 입력 정보로부터 패턴 정보를 추출할 수 있다. 추출부(230)는 사용자로부터 입력된 입력 정보가 패스워드 정보 또는 패스워드 패턴 정보를 포함하는지 여부를 판단할 수 있다. 추출부(230)는 입력 정보가 패스워드 정보 또는 패스워드 패턴 정보를 포함할 경우, 입력 정보로부터 사용자의 패턴 정보를 추출할 수 있다. 추출부(230)는 인증 화면에 표시된 사용자의 입력 정보가 감지되는 입력 인터페이스에 대한 사용자의 입력과 연관된 리듬 정보, 입력과 연관된 시간 정보, 입력과 연관된 인증 화면 내의 위치 정보 및 인증 화면에 표시된 입력 인터페이스들 중 2 이상의 입력 인터페이스들에 대한 입력 시간 간격 정보를 패턴 정보로서 추출할 수 있다.

[0032] 인증부(240)는 패턴 정보와 기 저장된 인증 정보와의 비교에 기반하여 사용자를 인증할 수 있다.

[0033] 등록부(250)는 사용자로부터 입력되는 입력 정보에 기초하여 사용자의 인증을 위한 인증 정보를 등록할 수 있다. 등록부(250)는 2회 이상 상기 사용자로부터 입력 정보를 수신하고, 2회 이상 수신된 입력 정보에 기반하여 사용자와 연관된 패턴 정보를 생성할 수 있고, 생성된 패턴 정보를 상기 사용자의 인증을 위한 인증 정보로서 등록할 수 있다. 데이터베이스(241)는 패스워드 및 패스워드에 대한 패턴 정보를 저장할 수 있다.

[0034] 도 3을 참고하면, 데이터베이스(241)는 패스워드에 대한 패턴 정보를 저장하고 있을 수 있다. 예를 들면, 사용자가 숫자를 통하여 패스워드를 입력하고자 한다면, 사용자 인증 장치는 기 설정된 자리(예를 들면, 4자리 이상 8자리 이하)의 숫자를 입력하도록 제공할 수 있다. 사용자는 패스워드로 설정하기 위한 번호를 입력함에 따라 사용자 인증 장치는 사용자로부터 번호가 입력되는 패턴 정보, 예를 들면, 인증 화면에 표시된 사용자의 입력 정보가 감지되는 입력 인터페이스에 대한 사용자의 입력과 연관된 리듬 정보, 입력과 연관된 시간 정보, 입력과 연관된 상기 인증 화면 내의 위치 정보 및 인증 화면에 표시된 입력 인터페이스들 중 2 이상의 입력 인터페이스들에 대한 입력 시간 간격 정보를 저장할 수 있다. 예를 들면, 도 3을 참고하면, 제1 패턴 정보(310)에 대하여 a 값(320)이 획득될 수 있다. 사용자 인증 장치는 사용자로부터 입력된 패턴 정보를 기 설정된 횟수 이상 트레이닝하고, 트레이닝된 패턴 정보를 저장함으로써 사용자 고유의 특성 정보로서 이용되도록 제공할 수 있다. 또는 사용자 인증 장치는 사용자로부터 입력된 패턴 정보를 연산(예를 들면, 평균)하여 저장할 수 있다. 또한, 사용자 인증 장치는 사용자로부터 입력된 패턴 정보에 대한 값에 대한 평균을 도출하고, 도출된 평균값의 기 설정된 범위를 설정하여 추후에 사용자가 입력한 패턴 정보의 값이 기 설정된 범위에 존재할 경우, 일치함을 판단할 수 있도록 제공할 수도 있다.

[0035] 설정부(260)는 인증 화면을 구성하는 복수의 입력 인터페이스들에 대하여 소기의 입력 인터페이스에 대한 사용자의 터치 입력을 감지하도록 설정할 수 있다. 설정부(260)는 기 설정된 특정 위치를 포함하는 입력 정보가 인증 화면에 입력됨에 따라 사용자 인증이 수행되도록 제공할 수 있다. 예를 들면, 사용자 인증을 수행하기 위한 인증 정보를 데이터베이스(241)에 저장할 수 있다. 사용자는 사용자 인증을 수행하기 위한 패스워드 정보, 소정의 위치에 대한 위치 정보를 포함하는 패턴 정보를 입력할 수 있다.

[0036] 도 4 및 도 5는 일 실시예에 따른 사용자 인증 장치의 사용자 인증 과정을 설명하기 위한 예이다.

[0037] 사용자 인증 장치는 일정하지 않은 레이아웃으로 형성된 인증 화면(400)을 통하여 사용자 인증을 수행할 수 있고, 일정한 레이아웃으로 형성된 인증 화면(500)을 통하여 사용자 인증을 수행할 수 있다. 이때, 사용자 인증 장치는 사용자에게 각기 다른 인증 화면을 표시할 수 있다.

[0038] 인증 화면은 표시 형태가 변경되어 표시된, 사용자의 입력 정보가 감지되는 적어도 하나의 입력 인터페이스를 포함할 수 있다. 이때, 표시 형태는 인증 화면 내의 입력 인터페이스의 위치, 색상, 크기, 모양 및 표시 여부 중 적어도 하나이고, 입력 인터페이스는 문자, 숫자 및 도형 중 적어도 하나를 포함할 수 있다. 이때, 입력 인터페이스는 사용자 인터페이스일 수 있다.

[0039] 도 4를 참고하면, 사용자 인증 장치는 인증 화면(400)을 표시할 수 있다. 인증 화면은 표시 형태가 변경되어 표시되고, 사용자의 입력 정보가 감지되는 적어도 하나의 입력 인터페이스를 포함할 수 있다. 이때, 입력 인터페이스

이스는 사용자 인터페이스일 수 있다. 사용자 인장 장치는 인증 화면에 구성된 입력 인터페이스의 위치, 폰트 색깔, 크기 등을 비정형적으로 형성함으로써 일정하지 않은 레이아웃을 형성할 수 있다. 이때, 인증 화면의 입력 인터페이스가 문자, 숫자 또는 도형 중 적어도 하나로 구성될 수 있다.

[0040] 예를 들면, 도 4(a, b)를 참고하면, 인증 화면(400)에서 입력 인터페이스들의 위치, 크기, 배열이 균일하지 않음을 확인할 수 있다. 사용자 인증 장치는 도 4와 같이 일정하지 않은 레이아웃으로 구성된 인증 화면을 통하여 입력되는 사용자의 패턴 정보를 획득함으로써 사용자 고유의 특징을 보다 정확하게 추출할 수 있게 된다.

[0041] 사용자 인증 장치는 사용자 인증을 수행하기 전에, 사용자로부터 사용자가 인증 정보를 등록하도록 등록 과정을 제공할 수 있다. 예를 들면, 사용자는 사용자 인증을 위한 패스워드로 '2', '5', '8', '0'을 입력하되, '2', '5', '8', '0'을 입력하는 패턴 정보를 함께 입력할 수 있다. 사용자로부터 입력된 패턴 정보, 예를 들면, 2->5->8->0이 입력되는 시간 간격 정보, 사용자가 2를 입력한 후, 5를 입력하기 까지는 0.5초가 소요되고, 5를 입력한 후, 8을 입력하기 까지는 0.1초가 소요되고, 8을 입력한 후, 0을 입력하기 까지는 0.3초가 입력됨을 판단하여 패턴 정보로서 저장할 수 있다. 상기 설명한 패턴 정보에 한정되지 아니하며, 다양한 패턴 정보가 획득될 수 있다. 이때, 사용자로부터 입력되는 패턴 정보는 사용자가 패턴 정보를 입력할 때마다 동일하지 않으므로, 등록 과정에서 패턴 정보를 트레이닝시킬 수 있다. 사용자 인증 장치는 사용자로부터 입력된 패턴 정보를 기 설정된 횟수 이상 트레이닝하여 사용자의 인증 정보로서 데이터베이스에 저장하게 된다.

[0042] 사용자 인증 장치는 사용자로부터 인증 화면(400)에 표시된 입력 인터페이스(410) 각각을 이용하여 입력된 입력 정보를 수신할 수 있다. 사용자 인증 장치는 입력 정보에 기초하여 사용자의 패턴 정보를 추출할 수 있다. 사용자 인증 장치는 입력 정보가 사용자 식별을 위한 패스워드 정보와 일치하는지 여부를 판단할 수 있다. 사용자 인증 장치는 입력 정보가 패스워드 정보와 일치할 경우, 입력 정보로부터 사용자의 패스워드 패턴 정보를 추출할 수 있다.

[0043] 도 4(b)를 참고하면, 사용자는 인증 화면(400)에서 '2', '5', '8', '0'이라는 패스워드를 입력하고자 한다면, '2'를 선택한 후 연속적으로 '5', '8', '0'을 드래그한 후, 인증 화면(400)에 터치를 종료함으로써 입력하고자 하는 숫자를 입력할 수 있다. 또는 사용자는 '2'를 선택한 후 연속적으로 '5', '8', '0'를 선택함으로써 숫자를 입력하게 된다. 이때, 사용자 인증 장치는 사용자로부터 입력된 패스워드 패턴 정보, 예를 들면, 2->5->8->0이 입력되는 시간 간격 정보, 사용자가 2를 입력한 후, 5를 입력하기 까지는 0.5초가 소요되고, 5를 입력한 후, 8을 입력하기 까지는 0.1초가 소요되고, 8을 입력한 후, 0을 입력하기 까지는 0.3초가 입력됨을 판단하여 패턴 정보를 추출할 수 있다. 또는 사용자가 2->5->8->0을 입력하는데 있어서, 각각의 숫자를 입력하는 위치를 판단하여 패턴 정보를 획득할 수 있다. 사용자 인증 장치는 추출된 패턴 정보와 기 저장된 인증 정보를 매칭함으로써 사용자를 식별할 수 있다.

[0044] 일 실시예에 따른 사용자 인증 장치는 핸드폰과 같은 전자 장치의 패턴 언락(un-lock), 핀(FIN)뿐만 아니라 쿼터 키보드에도 적용될 수 있다.

[0045] 도 5를 참고하면, 사용자 인증 장치는 인증 화면(500)을 표시할 수 있다. 이때, 인증 화면(500)은 일정한 레이아웃 또는 일정하지 않은 레이아웃으로 형성되어 표시될 수 있다. 일정한 레이아웃이란 인증 화면에 구성된 복수의 입력 인터페이스들의 배열, 위치 및 크기 등이 일정하게 형성된 것을 의미할 수 있으며, 일정하지 않은 레이아웃은 인증 화면에 구성된 복수의 입력 인터페이스들의 배열, 위치, 크기, 폰트, 색 등이 일정하지 않은 형태로 형성된 것을 의미할 수 있다.

[0046] 사용자 인증 장치는 인증 화면(500)에 구성된 복수의 인터페이스들(510) 중 패스워드 정보와 구별되는 소기의 입력 인터페이스(520)에 대한 입력 정보를 수신할 수 있다. 이때, 인증 화면에 구성된 복수의 입력 인터페이스들(510) 중 사전에 설정된 특정 위치에 대응하는 입력 인터페이스를 입력하도록 설정될 수 있다. 예를 들면, 사용자가 입력하는 패스워드와 구별되는 특정 위치가 입력되도록 설정될 수 있다.

[0047] 사용자 인증 장치는 사용자 인증을 수행하기 전에, 사용자로부터 입력되는 입력 정보에 기초하여 사용자의 인증을 위한 인증 정보를 등록하도록 등록 과정을 제공할 수 있다. 사용자 인증 장치는 사용자의 인증을 위한 사용자의 인증 정보의 등록 시, 사용자로부터의 입력 정보가 감지되는 소정의 입력 인터페이스에 대한 사용자의 입력에 따라, 표시 형태가 변경된 소정의 입력 인터페이스를 포함할 수 있다.

[0048] 사용자 인증 장치는 인증 화면을 표시할 수 있다. 사용자 인증 장치는 인증 화면(500)을 구성하는 복수의 입력 인터페이스들(510)에 대해 소기의 입력 인터페이스(520)에 대한 사용자의 터치 입력을 감지할 수 있다. 이때, 소기의 입력 인터페이스(520)는 인증 화면에서 사용자가 인식 가능하도록 표시되어 있지 않을 수 있다. 예를

들면, 소기의 입력 인터페이스는 사용자로부터 기 설정된 횟수 이상 입력되어 트레이닝 될 경우, 인증 화면의 소기의 입력 인터페이스(520)가 점차적으로 흐릿해질 수 있다. 다시 말해서, 사용자의 인증을 위한 상기 사용자의 입력 정보의 등록 시의 사용자의 입력의 횟수에 따라 인증 화면에 표시된 소기의 입력 인터페이스의 투명도가 변경된 표시 형태를 가질 수 있다. 예를 들면, 사용자가 소기의 인터페이스를 입력하는 것이 익숙해짐에 따라 소기의 입력 인터페이스(520)의 투명도가 점차 높아져 사용자는 인증 화면에서 소기의 입력 인터페이스(520)를 인지할 수 없게 된다.

[0049] 사용자로부터 소기의 입력 인터페이스에 대한 사용자의 입력을 감지할 수 있다. 사용자 인증 장치는 패스워드 정보, 패스워드 패턴 정보를 인증 정보로서 저장할 수 있다. 예를 들면, 사용자는 패스워드 정보를 입력할 때, 패스워드 정보 및 소기의 입력 인터페이스를 입력할 수 있다. 이때, 사용자 인증 장치는 패스워드 정보 및 소기의 입력 인터페이스의 입력 정보를 포함하는 패스워드 패턴 정보를 저장할 수 있다. 사용자 인증 장치는 2회 이상 사용자로부터 입력 정보를 수신하고, 2회 이상 수신된 입력 정보를 트레이닝하여 사용자와 연관된 패턴 정보를 생성하고, 생성된 패턴 정보를 인증 정보로서 저장할 수 있다.

[0050] 사용자 인증 장치는 인증 정보를 등록 과정에서 소기의 입력 인터페이스를 표시하여 사용자를 트레이닝시킨 후, 사용자 인증 과정에서는 인증 화면(500)의 소기의 입력 인터페이스(520)가 흐릿하거나 투명하게 보일 수 있다. 이와 같이 인증 화면에서 소기의 입력 인터페이스(520)가 흐릿하거나 투명한 것은, 다른 사람이 사용자의 입력 정보를 해킹하더라도 인증 화면에는 소기의 입력 인터페이스가 표시되지 않기 때문에 소기의 입력 인터페이스의 위치에 대하여 입력을 하지 않을 가능성이 높아지므로 보안을 더욱 강화할 수 있다. 이에 따라 사용자 인증 장치는 사용자가 설정한 특정 위치를 숨김으로써 사용자인이 알고 있는 특정 위치를 포함한 패스워드를 입력하도록 제공할 수 있다.

[0051] 사용자 인증 장치는 사용자로부터 인증 화면에 표시된 입력 인터페이스 각각을 이용하여 입력된 입력 정보를 수신할 수 있다. 이때, 입력 정보에는 소기의 입력 인터페이스에 대한 입력 정보도 포함될 수 있다. 예를 들면, 사용자는 인증 화면을 통하여, 패스워드 정보를 입력한 후, 소기의 인터페이스의 위치를 입력함에 따라 패스워드 정보, 소기의 인터페이스의 입력을 포함하는 패스워드 패턴 정보 입력 정보를 입력하게 된다.

[0052] 사용자 인증 장치는 입력 정보에 기초하여 패스워드 정보 또는 패스워드 패턴 정보를 포함하는지 여부를 판단할 수 있다. 사용자 인증 장치는 입력 정보가 패스워드 정보 또는 패스워드 패턴 정보를 포함할 경우, 입력 정보로부터 사용자의 패턴 정보를 추출할 수 있다.

[0053] 도 6은 일 실시예에 따른 사용자 인증 장치의 사용자 인증 방법을 설명하기 위한 흐름도이다.

[0054] 단계(610)에서 사용자 인증 장치는 사용자로부터 입력되는 입력 정보에 기초하여 사용자의 인증을 위한 인증 정보를 등록할 수 있다. 예를 들면, 사용자는 사용자 인증을 수행하기 위한 패스워드 정보 및 패스워드 패턴 정보를 입력할 수 있다.

[0055] 단계(620)에서 사용자 인증 장치는 일정하지 않은 레이아웃으로 형성된 인증 화면을 표시할 수 있다. 예를 들면, 사용자 인증 장치는 표시 형태가 변경되어 표시된, 사용자의 입력 정보가 감지되는 적어도 하나의 입력 인터페이스를 포함하고, 표시 형태는 상기 인증 화면 내의 입력 인터페이스의 위치, 색상, 크기, 모양 및 표시 여부 중 적어도 하나이고, 입력 인터페이스가 문자, 숫자 및 도형 중 적어도 하나를 포함할 수 있다.

[0056] 단계(630)에서 사용자 인증 장치는 사용자로부터 인증 화면을 통하여 입력된 입력 정보를 수신할 수 있다. 이때, 사용자 인증 장치는 사용자로부터 인증 화면을 통하여 패스워드 정보 및 패스워드 패턴 정보를 입력 정보로서 수신할 수 있다. 이때, 패스워드 정보는 사용자 인증을 위한 패스워드(예를 들면, 숫자, 문자, 패턴)에 대한 정보를 의미할 수 있다.

[0057] 단계(640)에서 사용자 인증 장치는 사용자로부터 입력된 입력 정보가 패스워드 정보 또는 패스워드 패턴 정보를 포함하는지 여부를 판단할 수 있다. 이때, 사용자 인증 장치는 패스워드 정보가 일치하지 않을 경우, 단계(620)의 인증 화면을 재표시하여 사용자가 사용자 인증을 위한 입력 정보를 재입력하도록 제공할 수 있다.

[0058] 단계(650)에서 사용자 인증 장치는 입력 정보가 패스워드 정보 또는 패스워드 패턴 정보를 포함할 경우, 입력 정보로부터 사용자의 패턴 정보를 추출할 수 있다. 이때, 사용자 인증 장치는 사용자로부터 입력된 입력 정보에 기초하여 사용자 패턴 정보를 추출할 수 있다.

[0059] 단계(660)에서 사용자 인증 장치는 패턴 정보를 기 저장된 인증 정보와 비교할 수 있다. 예를 들면, 사용자 인증 장치는 추출된 다양한 기준의 패턴 정보에 기초하여 인증 정보와 매칭시킬 수 있다. 사용자 인증 장치는 입

력 정보로부터 추출된 제1 패턴 정보가 데이터베이스에 저장된 제1 인증 정보와 일치하지 않을 경우, 제2 패턴 정보와 제2 인증 정보와 재매칭시킬 수 있다. 또는 사용자 인증 장치는 추출된 다양한 기준의 패턴 정보 중 사용자로부터 설정된 기준에 따른 패턴 정보에 기초하여 데이터베이스에 저장된 인증 정보를 추출함으로써 비교할 수 있다.

[0060] 단계(670)에서 사용자 인증 장치는 패턴 정보와 기 저장된 인증 정보와의 비교에 기반하여 사용자를 인증할 수 있다.

[0061] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0062] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 영구적으로, 또는 일시적으로 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

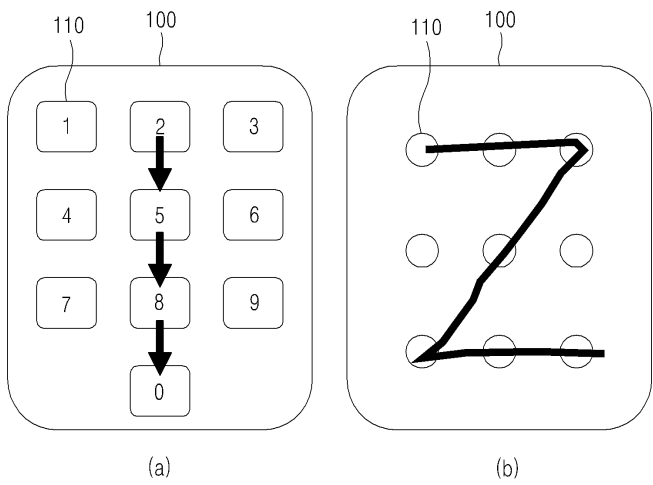
[0063] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다.

[0064] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

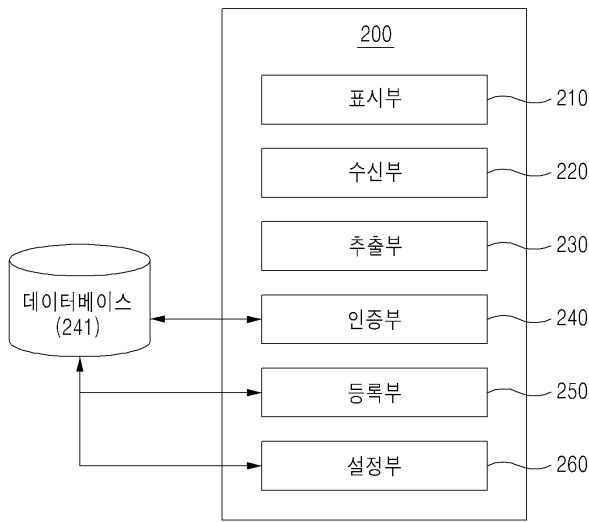
[0065] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

도면1



도면2



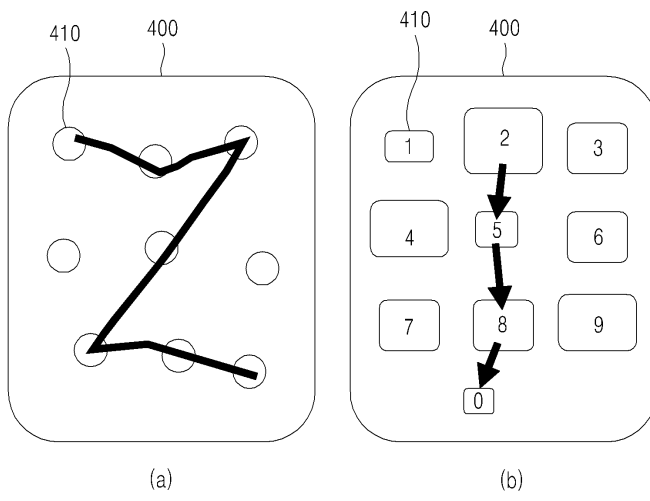
도면3

241				
제1 패턴 정보	제2 패턴 정보	제3 패턴 정보	제4 패턴 정보	...
a값	b값	c값	d값	e값

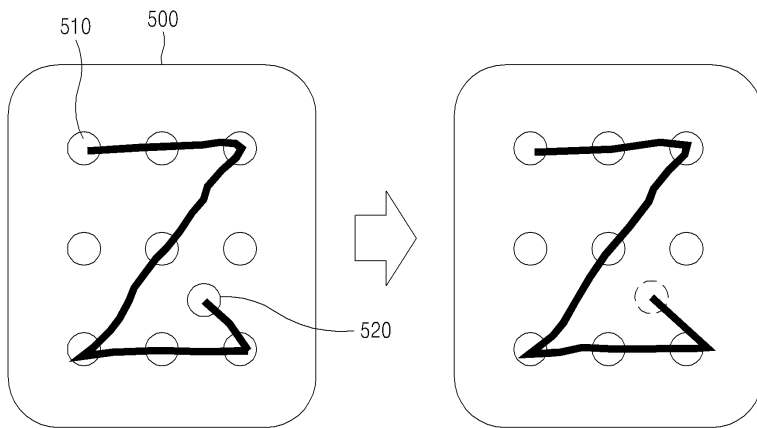
310

320

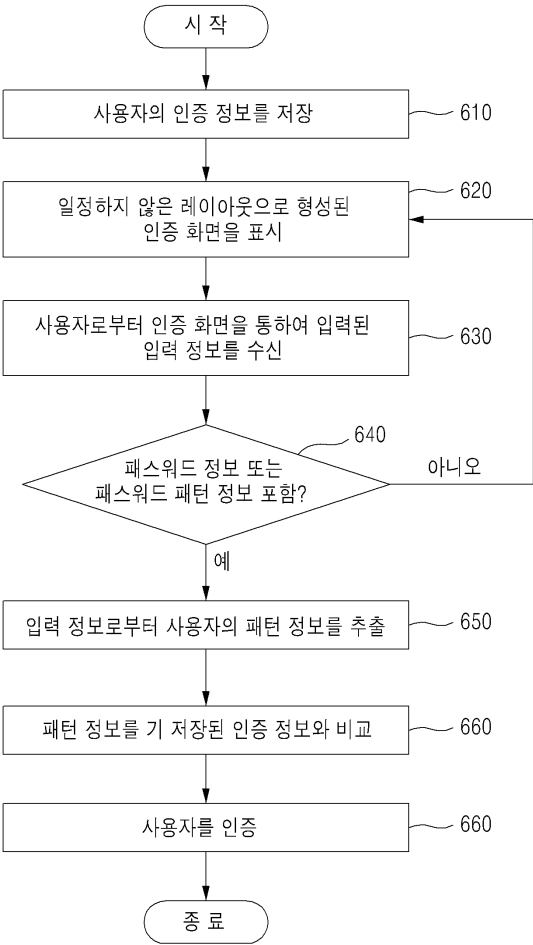
도면4



도면5



도면6



도면7

