

명세서

발명의 명칭: 가변 키패드와 생체 인식을 이용한 본인 인증 방법 및 시스템

기술분야

- [1] 본 발명은 본인 인증 방법 및 시스템에 관한 것으로서, 더욱 상세하게는 단말에서 가변 키패드를 통해 비밀번호 입력 순서에 따른 비밀번호 위치 정보 및 생체정보를 입력 받아 이를 서버로 전송하고, 서버에서 본인 인증을 수행하는 본인 인증 방법 및 시스템에 관한 것이다.

배경기술

- [2] 현대 사회에서는 스마트폰을 이용한 전자결제 시 비밀번호를 필수적으로 입력해야 한다. 기존 휴대폰과는 달리 스마트폰은 누구나 애플리케이션을 개발할 수 있다는 특성 때문에 일반 PC와 마찬가지로 해킹에 취약하다.
- [3] 특히, 고정 키패드를 통해 비밀번호가 입력될 때 사용자의 비밀번호 터치 좌표가 노출될 경우 비밀번호 자체가 그대로 유출될 수 있으므로 사용자의 각별한 주의가 필요하다.
- [4] 그래서, 이를 보완한 것이 가변 키패드를 사용한 인증 방법이다. 가변 키패드 방식은 사용자가 접속할 때마다 키패드의 입력버튼 위치가 변경되므로, 제3자가 스마트폰의 키패드의 입력 버튼 위치를 절취하더라도 비밀번호가 누출될 가능성이 낮다.
- [5] 사용자가 비밀번호 자체를 알지 못하면 본인 인증을 수행할 수 없다.
- [6] 그런데, 가변 키패드를 사용한 인증 방법은, 인증 요청 시 단말에서 서버로 비밀번호 자체가 전송되므로, 전송 도중에 해커가 침입하여 비밀번호를 해킹하면 해커가 비밀번호 자체를 알아낼 수 있으므로 개인 정보가 유출될 우려가 있고 보안성이 취약한 문제점이 있었다.
- [7] 또한, 비밀번호 자체를 알고 있는 제3자가 본인임을 사칭하고 본인 인증 수행 시 이를 막을 수 없는 문제점이 있었다.

발명의 상세한 설명

기술적 과제

- [8] 본 발명은 상기한 문제점을 해결하기 위한 것으로서, 휴대단말에서 본인 인증 서버로 비밀번호 위치 정보를 전송하여 비밀번호 유출을 방지하고, 보안성을 향상시키는 본인 인증 방법 및 시스템을 제공하는 것을 목적으로 한다.
- [9] 나아가, 생체정보를 인증 수단에 추가하여 보안성을 더욱 높은 본인 인증 방법 및 시스템을 제공하는 것을 목적으로 한다.

과제 해결 수단

- [10] 본 발명의 일면에 따른, 비밀번호 및 생체정보 혼합 본인 인증 서버는 암호키와 생체인증키를 포함하는 가변 키패드를 생성하되, 상기 암호키 각각의 위치와

상기 생체인증키의 위치가 매 생성시마다 가변되도록 생성하는 가변 키패드 생성부; 휴대단말 이용 사용자들의 비밀번호 및 생체정보를 저장하는 인증정보 저장부; 및 생성된 상기 가변 키패드를 원격의 휴대단말로 제공하고, 상기 휴대단말로부터 사용자가 입력한 순서에 따른 상기 암호키의 위치 정보 및 생체정보를 수신하여 이를 토대로 본인 인증을 수행하는 인증 수행부를 포함한다.

- [11] 본 발명의 다른 면에 따른, 본인 인증 휴대단말은 암호키 각각의 위치와 상기 생체인증키의 위치가 매 생성시마다 가변되도록 생성되는 가변 키패드를 표시하는 표시부; 및 본인 인증 서버로부터 상기 가변 키패드를 제공받고, 상기 가변 키패드를 통하여 획득한 암호키 위치 정보, 암호키 입력 순서 및 생체정보를 상기 본인 인증 서버로 전달하는 제어부를 포함한다.

- [12] 본 발명의 또 다른 면에 따른, 본인 인증 서버의 비밀번호 및 생체정보 혼합 본인 인증 방법은 암호키와 생체인증키를 포함하는 가변 키패드를 생성하되, 상기 암호키 각각의 위치와 상기 생체인증키의 위치가 매 생성시마다 가변되도록 생성하는 단계; 생성된 상기 가변 키패드를 휴대단말로 전송하는 단계; 상기 휴대단말로부터 사용자가 입력한 순서에 따른 상기 암호키의 위치 및 생체정보를 수신하는 단계; 및 수신한 상기 암호키의 위치 정보 및 생체정보를 토대로 본인 인증을 수행하는 단계를 포함한다.

발명의 효과

- [13] 본 발명에 따르면, 가변 키패드를 통한 입력된 비밀번호 자체를 본인 인증 서버로 전송하는 것이 아니라, 사용자가 입력한 순서에 따른 비밀번호의 위치 정보를 전송한다. 따라서, 단말에서 서버로 전송하는 중간에 해커가 전송되는 비밀 정보의 위치 정보를 절취하여도 비밀번호를 알 수 없으므로 보안성을 향상시킬 수 있다.
- [14] 또한, 비밀번호와 생체 정보를 통해 본인 인증을 수행하므로, 단순히 비밀번호 4자리만 입력하고 비밀번호의 위치를 가변하는 종래의 발명에 비하여 더욱 보안성을 향상시킬 수 있다.
- [15] 이어, 생체 정보가 홍채 정보일 경우, 홍채는 개인마다 개별적 특성을 지니므로 도난이나 위조를 방지할 수 있고, 홍채는 지문보다 많은 식별 특성을 지니고 지문보다 복잡하고 정교하므로 비밀번호와 결합하여 더욱 보안성을 향상시킬 수 있다.

도면의 간단한 설명

- [16] 도 1은 본 발명의 실시 예에 따른 비밀번호 및 생체정보 혼합 본인 인증 시스템을 도시한 구성도.
- [17] 도 2는 본 발명의 실시 예에 따른 비밀번호 및 생체정보 혼합 본인 인증 방법의 순서도.
- [18] 도 3a는 본 발명의 실시 예에 따라 암호키와 생체인증키를 포함하는 가변

키패드에서 암호키 각각의 위치와 생체인증키의 위치가 생성시마다 가변되도록 생성하는 것을 도시한 것으로, 제1회 생성시를 도시한 도면.

- [19] 도 3b는 본 발명의 실시 예에 따라 암호키와 생체인증키를 포함하는 가변 키패드에서 암호키 각각의 위치와 생체인증키의 위치가 생성시마다 가변되도록 생성하는 것을 도시한 것으로, 제2회 생성시를 도시한 도면.
- [20] 도 4a는 본 발명의 실시 예에 따라, 가변 키패드를 xy평면에 도시한 도면.
- [21] 도 4b는 본 발명의 실시 예에 따라, 가변 키패드의 위치정보를 xy평면에 도시한 도면.
- [22] 도 5는 본 발명의 실시 예에 따라, 비밀번호의 위치정보 및 생체정보를 휴대단말에서 본인 인증 서버로 전송하는 것을 도시한 도면.
- [23] 도 6은 본 발명의 실시 예에 따라, 암호키의 위치로부터 비밀번호를 추출하여 본인 인증을 수행하는 것을 도시한 순서도.
- [24] 도 7은 본 발명의 실시 예에 따라, 사용자의 홍채를 촬영하고 촬영된 홍채 이미지를 본인 인증 서버로 전송하는 것을 도시한 도면.
- [25] 도 8은 본 발명의 실시 예에 따른 인증서버 및 단말에 저장된 가변 키패드에 상응하는 식별자를 도시한 도면.
- [26] 도 9는 본 발명의 실시 예에 따라, 임시 대칭키, 사용자의 공개키, 사용자의 개인키로 암호화, 복호화를 수행하는 것을 도시한 순서도.
- [27] 도 10은 본 발명의 실시 예에 따른 생체정보에 기반한 본인 인증 방법을 나타내는 순서도.

발명의 실시를 위한 최선의 형태

- [28] 본 발명의 기술한 목적 및 그 이외의 목적과 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다.
- [29] 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 이하의 실시예들은 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 목적, 구성 및 효과를 용이하게 알려주기 위해 제공되는 것일 뿐으로서, 본 발명의 권리범위는 청구항의 기재에 의해 정의된다.
- [30] 한편, 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성소자, 단계, 동작 및/또는 소자가 하나 이상의 다른 구성소자, 단계, 동작 및/또는 소자의 존재 또는 추가됨을 배제하지 않는다.
- [31] 이하, 첨부된 도면을 참조하여 본 발명의 실시 예를 상세히 설명하기로 한다.
- [32] 도 1은 본 발명의 일 실시 예에 따른 비밀번호 및 생체정보 혼합 본인 인증

시스템을 도시한 구성도이다.

- [33] 도 1에 도시한 바와 같이, 비밀번호 및 생체정보 혼합 본인 인증 서버(200)는 가변 키패드 생성부(210), 인증 수행부(220) 및 인증 정보 저장부(230)를 포함한다.
- [34] 가변 키패드 생성부(210)는 암호키와 생체인증키를 포함하는 가변 키패드를 생성하되, 암호키 각각의 위치와 생체인증키의 위치가 매 생성시마다 가변되도록 생성한다.
- [35] 인증 수행부(220)는 생성된 가변 키패드의 정보(즉, 각 키 버튼의 배치정보)를 원격의 휴대단말(100)로 제공한다.
- [36] 다른 실시 예로서, 사전에 복수의 가변 키패드를 생성하고 각 가변 키패드마다 식별자를 부여하여 이를 휴대단말과 공유한 후, 매 인증시마다 가변 키패드의 식별자만을 가변 키패드 정보로서 전송하는 방법을 취할 수도 있다.
- [37] 인증 수행부(220)는 휴대단말(100)로부터 사용자가 입력한 순서에 따른 암호키의 위치 정보 및 생체정보를 수신하여 이를 토대로 본인 인증을 수행한다.
- [38] 예컨대, 인증수행부(220)는 휴대단말 (예컨대, 스마트폰)로부터 사용자가 입력한 순서에 따른 암호키의 위치 정보(도 4(a)를 참조시 키패드에서의 4, 3, 1, 2 -> (0.5, 2.5), (3.5, 3.5), (1.5, 3.5), (2.5, 3.5)), 및 생체정보를 수신하여 이를 토대로 본인 인증을 수행한다.
- [39] 인증 수행부(220)는 가변 키패드 생성시마다 비밀번호에 대응하는 각 암호키의 위치 정보 및 입력순서를 저장하고, 휴대단말(100)로부터 사용자가 입력한 순서에 따른 암호키의 위치 정보 및 생체정보를 수신하면, 이를 기저장된 암호키의 위치 정보, 입력순서 및 사용자의 생체정보와 비교하여 인증을 수행한다.
- [40] 예컨대, 비밀번호가 4, 3, 1, 2이면, 이에 대응하는 비밀번호(암호키)의 위치 정보는 도 4(a)를 참조하면, (0.5, 2.5), (3.5, 3.5), (1.5, 3.5), (2.5, 3.5)가 되고, 입력순서도 위의 순서와 동일하게 된다.
- [41] 이 때, 추가적인 실시예로, 인증 수행부(220)는 도 4(a)에 도시된 바와 같이 생체인증키의 영역(1.5, 2.5)에 인식된 생체정보(예: 지문정보)를 그 위치 정보와 함께 수신하여 이를 토대로 본인 인증을 수행하는 것 역시 가능하다.
- [42]
- [43] 인증 수행부(220)는 가변 키패드 생성시마다 위의 사항을 인증 정보 저장부(230)에 저장하고, 위의 사항을 휴대단말(100)에 제공한다.
- [44] 인증 수행부(220)는 휴대단말(100)로부터 사용자가 입력한 순서에 따른 비밀번호의 위치 정보는 (0.5, 2.5), (3.5, 3.5), (1.5, 3.5), (2.5, 3.5)가 된다. 그리고, 비밀번호의 위치정보, 입력순서, 지문 정보를 휴대단말(100)로부터 수신하면, 이를 인증 정보 저장부(230)에 저장된 비밀번호의 위치 정보 (0.5, 2.5), (3.5, 3.5), (1.5, 3.5), (2.5, 3.5), 입력순서 및 사용자의 지문 정보를 포함하는 인증정보와 비교하여 인증을 수행한다.

- [45] 본 발명은 생체 정보를 지문, 홍채, 음성, 혈관 (정맥) 등을 이용할 수 있다.
- [46] 생체 정보가 지문인 경우, 인증 수행부(220)는 단말장치(100)로부터 수신한 지문 이미지의 특징점의 위치와 인증 정보 저장부(230)에 저장된 지문의 특징점의 위치를 비교하여 통계를 내고 이를 통해 점수를 산출하며, 산출한 점수가 기설정된 임계값 (예컨대, 80%) 이상이면 동일 지문으로 판단한다.
- [47] 지문인식기술은 지문에 빛을 쏘서 반사되는 지문의 굴곡을 인식하여 판독하는 기술이다. 이 기술은 스캐너의 표면에 손가락을 올려놓기만 하면, 빠른 스캔이 이루어지기 때문에 상당히 많은 곳에서 활용되고 있다.
- [48] 지문인식기술은 사람마다 다양한 지문 유형을 파악하고 지문의 갈라진 점, 이어진 점, 끝점을 스캔하여 각 지문의 특징을 좌표로 얻어 기존 데이터와 대조하여, 신분을 확인하는 기술이다.
- [49] 지문인식을 위한 입력 장치로서는 프리즘이나 홀로그램 등을 이용하는 광학방식과 손가락의 열, 압력, 전기장이나 초음파 등을 감지하는 비광학방식이 있다.
- [50] 지문인식기술은 다른 생체인식기술에 비해 지문을 저장하고 식별하는 센서와 반도체칩의 가격이 저렴한 데다 기술 발달이 상대적으로 빠르고 응용분야의 폭이 넓다.
- [51] 지문인식의 장점은 0.5% 이내의 에러율이라는 비교적 높은 인식률과 1초 이내에 이루어지는 빠른 검증속도에 있다. 지문인식의 장점은 수용성, 편의성, 신뢰성에 있다.
- [52] 그리고, 사용자들은 지문인식을 사용할 때 다른 여러 생체인식기술과 비교하여 부담감을 적게 나타낸다. 또한 지문인식 장비는 매우 적은 공간을 차지한다
- [53] 생체 정보가 음성인 경우, 인증 수행부(220)는 단말장치(100)로부터 수신한 음성에서 특성을 추출하여 기준 패턴을 생성하고, 생성된 기준 패턴과 인증정보 저장부(230)에 저장된 기준 패턴을 비교하여 유사도를 측정하고, 측정한 유사도가 기설정된 임계값 이상 (예컨대, 80%)이면 동일 음성으로 판단한다.
- [54] 음성인식기술은 사람마다 가지고 있는 고유한 목소리의 패턴을 통해 정보를 인식한다. 음성인식기술은 잡음을 제거하고 각 사람마다 갖고 있는 고유한 음역대역을 파악하여 이를 토대로 신원을 확인한다.
- [55] 따라서, 음성인식기술을 초기에 활용하려면, 주변 소음이 최대한 없는 상태에서 녹음을 하는 것이 필수적으로 요구된다.
- [56] 생체 정보가 정맥인식기술인 경우, 인증수행부(220)는 손등 위의 혈관을 스캔하여 변형이 적은 혈관의 위치를 특정 좌표로 얻어 인식한다. 정맥인식기술은 국내에서 개발된 기술로 적외선을 손가락에 쏘았을 때, 적혈구만 적외선이 통과하지 못해 혈관만 어둡게 카메라에 찍히는 것을 이용, 그 결과를 판독하는 원리이다.
- [57] 적외선을 활용하기 때문에 인체에 무해하다는 큰 장점이 있다. 고속도로처럼 복잡하게 얹혀있는 정맥 분기점의 각도와 개수를 일일이 파악하여 빠르게

판독하는, 기술이라 할 수 있다.

- [58] 이외에 생체정보는 개인의 특성과 관련되는 얼굴인식(face), 장문인식(palmprint), 손모양(hand geomatry), 열상(thermal image), 필체(signature), 혈관(vein), 타이핑(typing keystroke dynamics), 망막(retina)를 포함한다.
- [59] 인증 정보 저장부(230)는 휴대단말 이용 사용자들의 비밀번호 및 생체정보를 저장한다.
- [60] 또한, 인증 정보 저장부(230)는 가변 키패드 생성부(210)가 생성한 가변 키패드들의 암호키(비밀번호), 암호키의 위치 정보 및 생체정보를 포함하는 인증정보를 저장한다.
- [61] 본인 인증 휴대단말(100)은 가변 키패드(110), 표시부(120), 제어부(130) 및 카메라부(140)를 포함한다.
- [62] 여기서, 휴대단말(100)은 스마트폰, 핸드폰, 태블릿 PC, 노트북, 이동형 신용카드 결제 단말기, 은행 ATM, 약국, 관공서 등에 설치된 키오스크 등을 포함한다.
- [63] 가변 키패드(110)는 사용자로부터 암호키 각각의 위치와 생체인증키의 위치가 매 생성시마다 가변되도록 생성된다. 즉, 원래는 본인 인증 서버(200)의 가변 키패드 생성부(210)가 가변 키패드를 생성하고, 휴대단말(100)의 가변 키패드(110)는 본인 인증 서버(200)에서 생성된 가변 키패드 정보를 기초로 사용자에게 가변 키패드를 보여주는 역할을 수행한다.
- [64] 표시부(120)는 암호키 각각의 위치와 생체인증키의 위치가 매 생성시마다 가변되도록 생성되는 가변 키패드(110)의 정보를 표시한다.
- [65] 제어부(130)는 본인 인증 서버(200)로부터 가변 키패드의 정보를 제공받고, 획득한 암호키 위치 정보, 암호키 입력 순서 및 생체정보를 본인 인증 서버(200)로 전송한다.
- [66] 카메라부(140)는 사용자의 전방을 촬영한다. 여기서 카메라부(140)는 홍채 인식 시스템이 장착되어 있고, 복잡한 홍채의 무늬를 '웨이블릿(wavelet) 변환'이라는 수학적 기법을 사용하여 일련의 디지털 부호로 변화할 수 있게 하는 기능을 포함할 수 있다.
- [67]
- [68] 도 2는 본 발명의 일 실시 예에 따른 비밀번호 및 생체정보 혼합 본인 인증 방법의 순서도이다.
- [69] 도 2에 도시한 바와 같이, 먼저, 암호키와 생체인증키를 포함하는 가변 키패드를 생성하되, 암호키 각각의 위치와 생체인증키의 위치가 매 생성시마다 가변되도록 생성한다(S110).
- [70] 다음으로, 생성된 가변 키패드를 휴대단말로 전송한다(S120).
- [71] 이어, 휴대단말(100)로부터 사용자가 입력한 순서에 따른 암호키의 위치 정보 및 생체정보를 수신한다(S130).
- [72] 끝으로, 수신한 입력 순서에 따른 암호키의 위치 정보 및 생체정보를 토대로

본인 인증을 수행한다(S140).

- [73] 본 발명의 실시 예에 따르면, 본인 인증을 수행시, 암호키 일부의 위치 정보를 토대로 본인 인증을 수행한다.
- [74] 예컨대, 비밀번호가 4312인 경우, 사용자가 네 자리의 비밀번호를 모두 입력하는 것이 아니고, 앞에서 두 자리 43, 뒤에서 두 자리 12, 네 자리 중 첫번째, 세번째의 비밀번호의 일부를 입력하는 것이다.
- [75] 앞에서 두 자리 43을 입력하는 경우, 비밀번호 위치는 도 4를 참조하면, (0.5, 2.5), (3.5, 3.5)가 된다.
- [76] 따라서, 본인 인증을 수행시 비밀번호의 위치 (0.5, 2.5), (3.5, 3.5), 입력순서, 생체정보(지문 정보, 홍채 정보 등)를 토대로 본인 인증을 수행한다.
- [77] 암호키 일부의 위치 정보를 토대로 본인 인증을 수행시에는 인증을 수행하는 데이터량이 암호키 전체의 위치 정보 입력에 비하여 상대적으로 적어 연산 속도를 향상시킬 수 있고, 입력해야 할 암호키의 수가 전체 입력에 비하여 상대적으로 적어 사용자 편의성을 향상시킬 수 있다.
- [78] 도 3A는 본 발명의 일 실시 예에 따라 암호키와 생체인증키를 포함하는 가변 키패드에서 암호키 각각의 위치와 생체인증키의 위치가 생성시마다 가변되도록 생성하는 것을 도시한 것으로 제1회 생성시를 도시한 도면이고, 도 3(b)는 제2회 생성시를 도시한 도면이다.
- [79] 도 3A, 도 3B에 도시한 바와 같이, 생성시마다 가변 키패드에서 암호키 각각의 위치와 생체인증키(Bio)의 위치가 생성시마다 가변된다.
- [80]
- [81] 도 4A는 본 발명의 일 실시 예에 따라, 가변 키패드를 xy평면에 도시한 도면이고, 도 4B는 가변 키패드의 위치정보를 xy평면에 도시한 도면이다.
- [82] 도 4A에 도시한 바와 같이, 사용자가 휴대단말(100)에서 비밀번호 (예컨대, 4312)와 생체정보 입력버튼(Bio)을 누른다.
- [83] 예컨대, 비밀번호의 위치 정보는 XY 평면에서 좌표값으로 설정될 수 있다. 또한, XY 평면에서 픽셀의 위치 좌표값으로 설정될 수 있다. 이는 예시에 불과하며, 비밀번호의 위치 정보는 다른 형식으로 얼마든지 변환이 가능하다.
- [84] 비밀번호 4312에 대응하는 위치 정보는 (0.5, 2.5), (3.5, 3.5), (1.5, 3.5), (2.5, 3.5)가 되고, 4->3->1->2처럼 비밀번호 입력순서와 같이 위치 정보의 순서도 큰 의미가 있다.
- [85] 사용자가 생체정보 입력버튼(Bio)을 누르면, 입력버튼을 누를 때 바로 그 위치에서 지문 입력 스캔 센서가 작동해서, 지문 입력 스캔 센서가 사용자의 지문 이미지를 획득한다.
- [86] 다른 실시 예에 따르면, 생체정보 입력버튼(Bio)을 누르면 지문 입력 창이 따로 팝업창 형태로 나타난다. 지문 입력 창은 그 크기가 가로 x 세로, 2.5 cm x 2.5 cm 가 되어, 충분히 크기에 해당되므로 검지뿐만 아니라, 다른 손가락의 지문을 획득할 수 있다.

- [87] 지문 입력 창은 터치 스크린 입력 형식으로 사용자가 손가락의 지문을 터치하고 소정 시간 (예컨대 1초)이 경과하면, 자동으로 지문 입력 스캔 센서가 작동하여 지문 입력 창은 사용자의 지문 이미지를 획득한다.
- [88]
- [89] 도 5는 비밀번호의 위치정보 및 생체정보를 휴대단말에서 본인 인증 서버로 전송하는 것을 도시한 도면이다.
- [90] 도 5에 도시한 바와 같이, 휴대단말(100)은 비밀번호의 위치 정보, 입력순서 및 생체정보(예컨대, (0.5, 2.5), (3.5, 3.5), (1.5, 3.5), (2.5, 3.5), 위치정보의 입력순서, 지문 정보)를 본인 인증 서버(200)로 전송한다.
- [91]
- [92] 도 6은 본 발명의 일 실시 예에 따라, 암호키의 위치로부터 비밀번호를 추출하여 본인 인증을 수행하는 것을 도시한 순서도이다.
- [93] 즉, 이 경우는 비밀번호는 본인 인증 서버(200)에 기저장되어 있음을 기초로, 단말장치(100)로부터 비밀번호의 위치 정보를 수신하여, 수신한 비밀번호의 위치 정보와 입력순서로부터 비밀번호를 추출하고, 추출된 비밀번호와 인증 저장부(230)에 저장된 비밀번호를 비교하여 본인 인증을 수행하는 것이다.
- [94] 도 6에 도시한 바와 같이, 인증 수행부(220)는 휴대단말(100)로부터 회원이 입력한 순서에 따른 암호키의 위치(예컨대, (0.5, 2.5), (3.5, 3.5), (1.5, 3.5), (2.5, 3.5), 위치정보의 입력순서)를 전송받아 회원이 입력한 비밀번호 (예컨대, 4312)를 추출한다(S142).
- [95] 인증 수행부(220)는 추출된 비밀번호(예컨대, 4312)와 수신된 생체정보(예컨대, 지문 정보, 홍채 정보)를 인증 정보 저장부(230)에 저장된 비밀번호 (예컨대, 4312) 및 생체정보 (예컨대, 지문 정보, 홍채 정보)와 비교하여 인증을 수행한다(S144).
- [96]
- [97] 도 7은 본 발명의 일 실시 예에 따라, 사용자의 홍채를 촬영하고 촬영된 홍채 이미지를 본인 인증 서버(200)로 전송하는 것을 도시한 도면이다.
- [98] 도 7에 도시한 바와 같이, 생체정보가 홍채 정보일 경우에는, 가변 키패드(110)가 사용자로부터 홍채 입력 지시 버튼 입력을 획득한다.
- [99] 제어부(130)는 카메라부(140)가 전방 사용자의 홍채를 촬영하도록 제어한다.
- [100] 카메라부(140)는 제어부(130)의 지시에 따라 전방 사용자의 홍채를 촬영한다. 카메라부(140)는 생체 확인 모듈을 포함하고 있고, 생체 확인 모듈은 홍채 촬영시 살아있는 사람의 홍채인지를 확인하는 기능을 수행하며 빛에 따라 동공이 확대, 축소되는지를 검토한다. 따라서, 사망한 사람의 안구를 이용해 홍채 인식을 하는 것은 원칙적으로 불가능하므로 보안성을 더욱 향상시킬 수 있다.
- [101] 제어부(130)는 촬영된 홍채 이미지를 본인 인증 서버(200)로 전송한다.
- [102] 다음으로, 본인 인증 서버(200)에서 휴대단말(100)로부터 수신된 홍채 이미지를 기초로 본인 인증 하는 과정을 살펴본다.

- [103] 본인 인증 서버(200)의 인증 수행부(220)는 단말장치(100)로부터 수신한 홍채 이미지에서 식별 특징을 추출한다.
- [104] 본인 인증 서버(200)는 추출한 식별 특징과 인증 정보 저장부(230)에 저장된 식별 특징을 비교하여 유사도를 측정하고, 측정한 유사도가 기설정된 임계값(예컨대 80%) 이상이면 동일 홍채로 판단한다.
- [105] 사람의 홍채는 생후 18개월 이후 완성된 뒤, 평생 변하지 않는 특성을 가지고 있다. 또한 세상에는 다양한 사람들이 살고 있지만, 절대 홍채 모양이 같은 사람은 없다.
- [106] 이러한 홍채의 고유한 특성으로 생체인식기술이 더욱 높은 보안성을 갖게 된다. 홍채인식기술은 눈을 스캔했을 때, 검정색의 동공을 중심으로 홍채와 공막의 영역을 나눈 후 홍채의 무늬를 스캔한다.
- [107] 홍채는 대략 266개의 측정 가능한 식별특징을 지니고 있어 40개 정도의 식별특징을 갖고 있는 지문보다 훨씬 복잡하고 정교하다.
- [108] 도 8의 좌측은 본 발명의 일 실시 예에 따라, 가변 키패드에 상응하는 식별자를 통해 1차 인증을 수행하는 것을 도시한 것으로 인증 서버에 저장된 가변 키패드에 상응하는 식별자를 도시한 도면이고, 도 8의 우측은 단말에 저장된 가변 키패드에 상응하는 식별자를 도시한 도면이다.
- [109] 도 8에 도시한 바와 같이, 인증 수행부(220)는 복수의 가변 키패드를 생성하고, 이에 대응되는 식별자(index)를 생성한다. 즉 본인 인증 서버(200)에서 가변 키패드를 생성시, 가변 키패드 1, 2, 3에 대응하는 식별자(index 1, 2, 3)를 생성하고, 가변 키패드 1, 2, 3과 식별자(index 1, 2, 3)를 사전에 휴대단말(100)에 제공한다.
- [110] 구체적으로, 인증 수행부(220)는 가변 키패드 생성시마다 생성된 가변 키패드에 상응하는 식별자를 인증 정보 저장부(230)에 저장한다.
- [111] 예컨대, 가변 키패드가 No. 1이면 이에 상응하는 식별자 index 1이 되고 이를 인증 정보 저장부(230)에 저장하고, 휴대단말과 사전에 공유한다.
- [112] 인증 수행부(220)는 인증 요청을 받으면 저장된 식별자 중 하나를 선택하여 이를 휴대단말(100)에게 제공한다. 휴대단말(100)은 수신된 식별자를 토대로 사전에 제공받은 가변 키패드 중에서 이번 인증에 이용될 가변 키패드를 선택하여 화면에 표출한다.
- [113] 인증 수행부(220)는 휴대단말(100)로부터 수신한 암호키의 위치 정보, 입력순서, 생체인증키의 위치 정보 및 회원의 생체정보와 인증정보 저장부(230)에 저장된 암호키의 위치 정보, 입력순서, 생체인증키의 위치 정보 및 회원의 생체정보를 비교하여 제2차 인증을 수행한다.
- [114] 본 실시 예는 인증시에 가변 키패드 배치 구조가 서버에서 휴대단말로 전송되지 않고 식별자만이 전송되므로 보안성이 보다 향상될 수 있다.
- [115] 본 발명에 따르면, 가변 키패드를 통한 입력된 비밀번호 자체를 본인 인증 서버로 전송하는 것이 아니라, 사용자가 입력한 순서에 따른 비밀번호의 위치

정보를 전송한다. 따라서, 단말에서 서버로 전송하는 중간에 해커가 전송되는 비밀 정보의 위치 정보를 절취하여도 비밀번호를 알 수 없으므로 보안성을 향상시킬 수 있다.

[116] 또한, 비밀번호와 생체 정보를 통해 본인 인증을 수행하므로, 단순히 비밀번호 4자리만 입력하고 비밀번호의 위치를 가변하는 종래의 발명에 비하여 더욱 보안성을 향상시킬 수 있다.

[117] 계속하여, 휴대단말은 비밀정보의 일부만 보안 인증 서버로 전송하여 데이터 전송량을 줄일 수 있고, 사용과 편의성을 증대할 수 있다.

[118]

[119] 도 9는 본 발명의 일 실시 예에 따라, 임시 대칭키, 사용자의 공개키, 사용자의 개인키로 암호화, 복호화를 수행하는 것을 도시한 순서도이다.

[120] 도 9에 도시된 바와 같이, 인증 수행부(220)는 임시 대칭키를 생성하고(210) 이를 휴대 단말(100)로 전송한다(S220).

[121] 휴대 단말(100)은 인증 수행부(220)로부터 수신한 임시 대칭키로 메시지를 암호화하여 암호문을 생성한다(S230).

[122] 이후, 휴대 단말(100)은 사용자 A의 공개키로 임시 대칭키를 암호화하여 E-KEY를 생성하고(S240), 이를 인증 수행부(220)로 전송한다(S250).

[123] 인증 수행부(220)는 휴대 단말(100)로부터 수신한 암호문 E-KEY를 사용자 A의 개인키로 복호화하여 임시 대칭키 복원을 수행하고(S260), 암호문을 임시 대칭키로 복호화하여 메시지를 복원한다(S270).

[124] 이어서, 인증 수행부(220)는 복원한 메시지로부터 암호키의 위치, 암호키 입력 순서 및 생체 정보를 추출하고(S280), 이를 기저장된 인증 정보와 비교하여 본인인증을 수행한다(S290).

[125]

[126] 본 발명의 다른 실시 예에 따르면, 생체 정보만으로 본인 인증을 실행할 수 있다.

[127] 도 10은 본 발명의 실시 예에 따른 생체정보에 기반한 본인 인증 방법을 나타내는 순서도이다.

[128] 도 10을 참조하면, 생체인증키를 포함하는 가변 키패드를 생성하되, 생체인증키의 위치가 매 생성시마다 가변되도록 생성한다(S310). 이 때, 구체적으로, 가변 키패드 생성부(210)는 홍채 입력버튼, 지문 입력버튼의 위치가 매 생성시마다 가변되도록 생성한다.

[129] 이어서, 생성된 가변 키패드는 휴대단말로 전송되고, 휴대단말(100)로부터 회원이 입력한 적어도 하나의 생체정보를 수신한다(S320).

[130] 예컨대, 회원이 휴대단말(100)의 가변 키패드를 통해 홍채 입력버튼, 지문 입력버튼을 누르면, 휴대단말(100)로부터 홍채 입력버튼의 위치, 지문입력버튼의 위치, 홍채정보, 지문 정보를 수신한다.

[131] 이어서, 수신한 적어도 하나의 생체인증키의 위치 및 적어도 하나의

생체정보를 토대로 회원 인증을 수행한다(S330).

- [132] 예컨대, 인증 수행부는 홍채 입력버튼의 위치 정보(1.5, 2.5), 지문 입력버튼의 위치 정보(1.5, 1.5), 홍채정보, 지문정보와 인증 정보 저장부(230)에 저장된 홍채 입력버튼의 위치 정보, 지문 입력버튼의 위치 정보, 홍채 정보, 지문 정보를 비교하여 동일성 판단으로 본인 인증을 수행한다.
- [133] 생체정보를 이용하게 되면, 사용자의 입장에서서는 비밀번호를 외울 필요가 없어 사용자 편의성이 향상되고, 비밀번호가 유출될 염려가 없어 보안성이 향상되며, 온라인에서 타인에 의해 도용될 가능성을 원천적으로 차단시킬 수 있다.
- [134] 또한, 전자상거래에서 판매자의 입장에서 생체정보는 고객이 이를 이용하여 사기나 기망을 하기 어렵고, 비용이 절감되며, 계좌 등이 비밀로 유지된다.
- [135] 그리고, 공공의 측면에서 사기행위를 보다 쉽게 적발할 수 있고 타인 정보의 오용과 남용의 위험을 감소시킬 수 있다.
- [136]
- [137] 이상의 설명은 본 발명의 기술적 사상을 예시적으로 설명한 것에 불과한 것으로서, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면, 본 발명의 본질적 특성을 벗어나지 않는 범위에서 다양한 수정 및 변형이 가능하다. 따라서, 본 발명에 표현된 실시 예들은 본 발명의 기술적 사상을 한정하는 것이 아니라, 설명하기 위한 것이고, 이러한 실시 예에 의하여 본 발명의 권리범위가 한정되는 것은 아니다. 본 발명의 보호범위는 아래의 특허청구범위에 의하여 해석되어야 하고, 그와 동등하거나, 균등한 범위 내에 있는 모든 기술적 사상은 본 발명의 권리범위에 포함되는 것으로 해석되어야 할 것이다.

청구범위

- [청구항 1] 암호키와 생체인증키를 포함하는 가변 키패드를 생성하되, 상기 암호키 각각의 위치와 상기 생체인증키의 위치가 매 생성시마다 가변되도록 생성하는 가변 키패드 생성부;
휴대단말 이용 사용자들의 인증정보를 저장하는 인증정보 저장부;
및
생성된 상기 가변 키패드의 정보를 원격의 휴대단말로 제공하고, 상기 휴대단말로부터 수신한 사용자 입력 순서에 따른 상기 암호키의 위치 정보 및 생체정보를 상기 인증정보 저장부에 저장된 인증정보와 비교하여 본인 인증을 수행하는 인증 수행부를 포함하는 비밀번호 및 생체정보 혼합 본인 인증 서버.
- [청구항 2] 제1항에 있어서, 상기 인증 수행부는
상기 휴대단말로부터 사용자가 입력한 순서에 따른 상기 암호키의 위치 정보로부터 상기 사용자가 입력한 비밀번호를 추출한 후, 추출된 상기 비밀번호와 수신된 상기 생체정보를 상기 인증정보 저장부에 저장된 상기 인증정보와 비교하여 인증을 수행하는 것인 비밀번호 및 생체정보 혼합 본인 인증 서버.
- [청구항 3] 제1항에 있어서, 상기 인증 수행부는
상기 가변 키패드 생성시마다 상기 비밀번호에 대응하는 각 암호키의 위치 정보 및 입력순서를 저장하고, 상기 휴대단말로부터 사용자가 입력한 순서에 따른 상기 암호키의 위치 정보 및 생체정보를 수신하면, 이를 기저장된 암호키의 위치 정보, 입력순서 및 사용자의 생체정보와 비교하여 인증을 수행하는 것인 비밀번호 및 생체정보 혼합 본인 인증 서버.
- [청구항 4] 제1항에 있어서, 상기 인증 수행부는
상기 가변 키패드 생성시마다 생성된 상기 가변 키패드에 상응하는 식별자를 저장하고, 저장된 상기 식별자를 상기 휴대단말에게 제공하며, 상기 휴대단말로부터 식별자를 수신하면, 이를 기저장된 식별자와 비교하여 제1차 인증을 수행하고, 제1차 인증 수행결과가 성공이면, 상기 휴대단말로부터 수신한 암호키의 위치 정보, 입력순서 및 사용자의 생체정보와 상기 인증정보 저장부에 저장된 암호키의 위치 정보, 입력순서 및 사용자의 생체정보를 비교하여 제2차 인증을 수행하는 것인 비밀번호 및 생체정보 혼합 본인 인증 서버.
- [청구항 5] 제1항에 있어서, 상기 인증 수행부는
상기 가변 키패드 생성시마다 임시 대칭키를 생성하고, 생성된 임시 대칭키를 휴대단말에게 제공하고,

상기 임시 대칭키로 암호키의 위치 정보, 암호키 입력순서, 생체정보를 포함한 메시지를 암호화하고 사용자의 공개키로 상기 임시 대칭키를 암호화하는 상기 휴대단말로부터 암호화된 상기 메시지 및 암호화된 상기 임시 대칭키를 수신하면, 상기 사용자의 개인키로 암호화된 상기 임시 대칭키를 복호화하고, 복호화된 상기 임시 대칭키로 상기 메시지를 복호화하고, 복호화된 상기 메시지에서 암호키의 위치 정보, 암호키 입력 순서, 생체정보를 추출하고 이를 기저장된 암호키의 위치 정보, 암호키 입력 순서, 생체정보와 비교하여 본인 인증을 수행하는 것

인 비밀번호 및 생체정보 혼합 본인 인증 서버.

[청구항 6]

암호키 각각의 위치와 생체인증키의 위치가 매 생성시마다 가변되도록 생성되는 가변 키패드 정보를 표시하는 표시부; 및 본인 인증 서버로부터 상기 가변 키패드의 정보를 제공받고, 상기 가변 키패드를 통하여 획득한 암호키 위치 정보, 암호키 입력 순서 및 생체정보를 상기 본인 인증 서버로 전달하는 제어부를 포함하는 본인 인증 휴대단말.

[청구항 7]

제6항에 있어서, 전방을 촬영하는 카메라부를 더 포함하고, 상기 생체정보가 홍채 정보일 경우, 상기 가변 키패드가 사용자로부터 홍채 입력 지시 버튼 입력을 획득하면, 상기 제어부는 상기 카메라부가 전방 사용자의 홍채를 촬영하도록 제어하고, 촬영된 홍채 이미지를 상기 본인 인증 서버로 전송하는 것

인 본인 인증 휴대단말.

[청구항 8]

본인 인증 서버가 암호키와 생체인증키를 포함하는 가변 키패드를 생성하되, 상기 암호키 각각의 위치와 상기 생체인증키의 위치가 매 생성시마다 가변되도록 생성하는 단계; 생성된 상기 가변 키패드를 휴대단말로 전송하는 단계; 상기 휴대단말로부터 사용자가 입력한 순서에 따른 상기 암호키의 위치 정보 및 생체정보를 수신하는 단계; 및 수신한 상기 암호키의 위치 정보 및 상기 생체정보를 토대로 본인 인증을 수행하는 단계를 포함하는 본인 인증 서버의 비밀번호 및 생체정보 혼합 본인 인증 방법.

[청구항 9]

제8항에 있어서, 상기 본인 인증을 수행하는 단계는 상기 암호키 일부의 위치 정보를 토대로 본인 인증을 수행하는 것인 본인 인증 서버의 비밀번호 및 생체정보 혼합 본인 인증 방법.

- [청구항 10] 제8항에 있어서, 상기 본인 인증을 수행하는 단계는
상기 휴대단말로부터 사용자가 입력한 순서에 따른 상기 암호키의
위치 정보로부터 상기 사용자가 입력한 비밀번호를 추출한 후,
추출된 상기 비밀번호와 수신된 상기 생체정보를 인증 정보
저장부에 저장된 비밀번호 및 생체정보와 비교하여 본인 인증을
수행하는 것
- [청구항 11] 인 본인 인증 서버의 비밀번호 및 생체정보 혼합 본인 인증 방법.
본인 인증 서버가, 생체인증키를 포함하는 가변 키패드를
생성하되, 상기 생체인증키의 위치가 매 생성시마다 가변되도록
생성하는 단계;
생성된 상기 가변 키패드를 휴대단말로 전송하는 단계;
상기 휴대단말로부터 사용자가 입력한 적어도 하나의
생체인증키의 위치 정보 및 적어도 하나의 생체정보를 수신하는
단계; 및
수신한 상기 적어도 하나의 생체인증키의 위치 정보 및 상기
적어도 하나의 생체정보를 토대로 회원 인증을 수행하는 단계
를 포함하는 생체정보에 기반한 본인 인증 방법.