

명세서

발명의 명칭: 인증용가상코드를 이용한 사용자 인증 방법 및 이를 위한 시스템

기술분야

- [1] 본 발명은 인증용가상코드를 이용한 비대면 사용자 인증 방법 및 장치에 관한 것이다.

배경기술

- [2] OTP(One Time Password)는 무작위로 생성되는 난수의 일회용 패스워드를 이용하는 사용자 인증 방식이다. OTP 인증 방식은 보안을 강화하기 위하여 도입한 시스템으로, 로그인할 때마다 일회용 패스워드를 생성하여 사용자 인증을 수행하기 때문에, 동일한 패스워드가 반복해서 사용됨으로 발생하는 보안상의 취약점을 극복할 수 있다.
- [3] 하지만, 기존의 OTP 인증 방식은 인증을 시작 시에 비밀번호를 입력하는 등의 인증 방식으로 로그인하여 사용자가 누구인지를 파악한 후에, 해당 사용자에게 부여된 OTP 함수를 이용하여 OTP를 생성하고, 상기 생성된 OTP를 통해 OTP 인증을 완료하는 방식으로, OTP 인증을 수행할 때마다 로그인을 수행해야 하는 불편함이 있다.
- [4] 따라서, 사용자가 인증을 요청할 때마다 로그인하지 않고도 OTP를 생성하여 사용자 인증을 수행할 수 있는 발명이 필요하다. 또한, 다양한 분야에서 비대면 업무처리의 필요성이 높아짐에 따라, 비대면으로 타인에게 사용자 인증 권한을 부여할 수 있는 발명이 필요하다. 이때, 타인에게 부여된 사용자 인증 권한은 임시적으로 이루어져야 하며, 사용자가 지정한 사람에게만 한정적으로 부여되어야 한다.
- [5] 이에 대해, 선행기술문헌으로는 한국등록특허 10-1316466호(2013.10.01)가 존재한다.

발명의 상세한 설명

기술적 과제

- [6] 본 발명이 해결하고자 하는 과제는 비대면으로 사용자가 타인에게 일시적으로 사용자 인증 권한을 부여할 수 있는 인증용가상코드를 이용한 사용자 인증 방법 및 시스템을 제공하는 것이다.
- [7] 또한, 본 발명이 해결하고자 하는 과제는 사용자가 타인에게 사용자 인증 권한 부여 시 권한 한도를 용도별로 설정하거나, 권한 부여 시간을 설정할 수 있는 인증용가상코드를 이용한 사용자 인증 방법 및 시스템을 제공하는 것이다.
- [8] 또한, 본 발명이 해결하고자 하는 과제는 사용자 인증을 요청할 때마다, 중복 생성되지 않으면서 단위카운트 간격으로 신규 생성되는 인증용가상코드를 제공할 수 있는 인증용가상코드를 이용한 사용자 인증 방법 및 시스템을

제공하는 것이다.

- [9] 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제 해결 수단

- [10] 상술한 과정을 해결하기 위한 본 발명은, 가상코드검증수단이 인증용가상코드를 수신하는 단계-상기 인증용가상코드는, 상기 가상코드검증수단에 등록된 가상코드생성수단에 포함된 인증용가상코드생성함수에 의해 생성됨-, 상기 가상코드검증수단이 상기 인증용가상코드를 기반으로 UID(User Identification) 또는 SID(sub-identification)의 저장위치를 탐색하는 단계, 상기 가상코드검증수단이 상기 탐색된 UID 또는 SID에 매칭되어 저장된 권한 정보를 추출하는 단계, 상기 가상코드검증수단이 상기 인증용가상코드가 수신된 시점을 기반으로 인증용가상코드를 검증하는 단계, 상기 가상코드검증수단이 상기 추출된 권한 정보를 기반으로 사용자 인증을 수행하는 단계를 포함하는 인증용가상코드를 이용한 사용자 인증 방법을 제공한다.
- [11] 또한, 본 발명은 하드웨어인 컴퓨터와 결합되어, 상기 인증용가상코드를 이용한 사용자 인증 방법을 실행시키기 위하여 매체에 저장된, 인증용가상코드를 이용한 사용자 인증 프로그램을 제공한다.
- [12] 또한, 본 발명은 사용자 인증을 위한 가상코드생성장치로서, 상기 가상코드생성장치에 등록된 UID(User Identification) 또는 SID(sub-identification)를 기반으로 하나 이상의 세부코드를 생성하는 세부코드생성부, 인증용가상코드생성함수를 이용하여 상기 하나 이상의 세부코드를 조합한 인증용가상코드를 생성하는 가상코드생성부, 가상코드수신수단을 통해 가상코드검증장치에 대한 사용자 인증을 수행하도록, 상기 생성된 인증용가상코드를 가상코드수신장치로 전송하는 인증용가상코드제공부를 포함하는 사용자 인증을 위한 인증용가상코드생성장치를 제공한다.
- [13] 또한, 본 발명은 사용자 인증을 위한 가상코드검증장치로서, 인증용가상코드를 수신하는 가상코드수신부, 상기 인증용가상코드에서 세부코드를 추출하는 세부코드추출부, 상기 세부코드를 기반으로 UID(User Identification) 또는 SID(sub-identification)의 저장위치를 탐색하는 저장위치탐색부, 상기 탐색된 UID 또는 SID에 매칭되어 저장된 권한 정보를 추출하는 권한정보추출부, 상기 인증용가상코드가 수신된 시점을 기반으로 인증용가상코드를 검증하는 가상코드검증부, 상기 추출된 권한 정보를 기반으로 사용자 인증을 수행하는 사용자인증승인부를 포함하는 사용자 인증을 위한 인증용가상코드검증장치를 제공한다.

발명의 효과

- [14] 상기와 같은 본 발명의 인증용가상코드를 이용한 사용자 인증 방법 및 이를 위한 시스템이 제공하는 효과에 대해 설명하면 다음과 같다.
- [15] 첫째, 일시적으로 사용자 인증을 수행할 수 있는 인증용가상코드를 타인에게 제공함으로써, 타인과 접촉하지 않고 타인이 사용자 인증을 수행할 수 있도록 하는 효과를 제공한다.
- [16] 둘째, 인증용가상코드를 사용할 수 있는 시간을 제한함으로써, 특정 시간에 정확하게 타인에게 인증용가상코드를 전달하지 않고도, 타인이 특정 시간에만 사용자 인증을 수행할 수 있도록 하는 효과를 제공한다.
- [17] 셋째, 인증용가상코드를 통해 타인에게 부여될 수 있는 권한의 종류를 제한함으로써, 사용자가 필요한 권한만 선택적으로 타인에게 부여할 수 있도록 하는 효과를 제공한다.
- [18] 넷째, 단위카운트마다 인증용가상코드를 신규로 생성 시에 중복되는 인증용가상코드가 정해진 전 주기 내에 등장하지 않도록 하거나, 인증용가상코드검증장치에서 사용자 정보를 추출할 수 있는 인증용가상코드가 생성되는 순서를 랜덤하게 함에 따라, 인증용가상코드 유출 시에도 사용자 정보가 유출되지 않도록 하는 효과를 제공한다.
- [19] 다섯째, 인증용가상코드를 생성하는 인증용가상코드생성장치(예를 들어, 사용자 단말)에는 인증용가상코드생성함수가 저장되고, 인증용가상코드를 이용하여 사용자 정보를 추출하고 인증용가상코드가 정상적인 코드인지를 검증하는 인증용가상코드검증장치(예를 들어, 서버 등)에는 인증용가상코드검증을 위한 알고리즘이 구비됨으로써, 인증용가상코드 생성 및 검증을 위한 알고리즘이 유출되는 것을 방지할 수 있다.
- [20] 본 발명의 효과들은 이상에서 언급된 효과로 제한되지 않으며, 언급되지 않은 또 다른 효과들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

- [21] 도 1은 본 발명의 일 실시예에 따른 인증용가상코드를 이용한 사용자 인증 시스템의 구성도이다.
- [22] 도 2는 본 발명의 일 실시예에 따른 인증용가상코드생성장치의 구성도이다.
- [23] 도 3은 본 발명의 일 실시예에 따른 인증용가상코드검증장치의 구성도이다.
- [24] 도 4는 본 발명의 일 실시예에 따른 인증용가상코드를 이용한 사용자 인증 방법의 순서도이다.
- [25] 도 5은 본 발명의 일 실시예에 따른 k각형의 구름이동을 통해 UID 또는 SID의 저장위치를 탐색하는 저장위치탐색알고리즘에 대한 예시도이다.
- [26] 도 6은 본 발명의 일 실시예에 따른 인증용가상코드의 검증을 설명하기 위한 예시도이다.

[27] 도 7은 본 발명의 일 실시예에 따른 세부코드를 기반으로 트랙상을 이동하여 UID 또는 SID의 저장위치를 탐색하는 저장위치탐색알고리즘에 대한 예시도이다.

[28] 도 8 및 9는 본 발명의 일 실시예에 따른 가상코드검증장치의 저장공간을 설명하기 위한 예시도이다.

발명의 실시를 위한 형태

[29] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나, 본 발명은 이하에서 개시되는 실시예들에 제한되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술 분야의 통상의 기술자에게 본 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다.

[30] 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 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다. 명세서 전체에 걸쳐 동일한 도면 부호는 동일한 구성 요소를 지칭하며, "및/또는"은 언급된 구성요소들의 각각 및 하나 이상의 모든 조합을 포함한다. 비록 "제1", "제2" 등이 다양한 구성요소들을 서술하기 위해서 사용되나, 이들 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 구성요소를 다른 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제1 구성요소는 본 발명의 기술적 사상 내에서 제2 구성요소일 수도 있음은 물론이다.

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

[32] 본 명세서에서 '사용자 인증'은 출입, 로그인, 금융거래 등 보안이 요구되는 영역으로 사용자가 통과하거나, 특정 물체의 기능을 실행할 수 있도록 승인하는 절차를 의미한다.

[33] 본 명세서에서 '금융거래'는 금융사와 이루어지는 절차를 의미한다. '금융거래'는 카드결제, 은행계좌로부터의 입출금 등을 포함한다.

[34] 본 명세서에서 '문자'는 코드를 구성하는 구성요소로서, 대문자알파벳, 소문자알파벳, 숫자 및 특수문자 등의 전부 또는 적어도 하나를 포함한다.

- [35] 본 명세서에서 '코드'는 문자가 나열된 문자열을 의미한다.
- [36] 본 명세서에서 '인증용가상코드'는 인증용가상코드생성수단에서 생성되는 코드로서, 인증용가상코드검증수단에서 사용자인증을 수행하는데 이용되는 코드를 의미한다. 즉, '인증용가상코드'는 사용자 정보를 추출하고 검증할 수 있도록 단위카운트마다 임시적으로 부여된 가상의 코드를 의미한다.
- [37] 본 명세서에서 '세부코드'는 인증용가상코드에 포함되는 일부코드를 의미한다.
- [38] 본 명세서에서 '단위카운트'는 특정한 시간간격으로 설정되어, 시간간격이 경과됨에 따라 변경되는 것으로 정의된 단위이다. 예를 들어, 1카운트는 특정한 시간간격(예를 들어, 1.5초)으로 설정되어 사용될 수 있다.
- [39] 본 명세서에서 '인증용가상코드생성함수'는 인증용가상코드를 생성하는데 이용되는 함수를 의미한다.
- [40] 본 명세서에서 '구름이동'은 대상체가 회전하면서 병진운동을 하는 것을 의미한다. 즉, '구름이동'은 회전운동과 병진운동을 함께 수행하면서 이동하는 것으로서, 회전하는 대상체의 각 지점이 이동하는 축 상에 차례대로 접하면서 이동하는 것을 의미한다.
- [41] 본 명세서에서 '접근 권한'은 사용자 인증을 통해 부여되는 권한으로, 사용자에게 특정 물체에 대한 '접근 권한'이 부여될 경우, 사용자는 특정 물체에 포함된 물리적 기능을 사용할 수 있는 상태가 된다. '접근 권한'이 부여됨에 따라 사용할 수 있는 물리적 기능은 물체의 종류에 따라 달라질 수 있다. 접근 권한의 종류에 대하여는 후술한다.
- [42] 본 명세서에서 'UID(user identification)'는 사용자를 식별하기 위해 사용자별로 중복되지 않게 부여되는 고유한 코드 형태의 값을 의미한다.
- [43] 본 명세서에서 'SID(sub-identification)'는 접근 권한 부여 대상을 식별하기 위해 권한 부여 대상자 별로 중복되지 않게 부여되는 고유한 코드 형태의 값을 의미한다.
- [44] 본 명세서에서 '저장위치'는 사용자에게 의해 UID 또는 SID 등록이 요청된 시점에 해당하는 트랙 상 지점(카운트)을 의미한다.
- [45] 본 명세서에서 '권한 정보'는 UID 또는 SID의 저장위치에 매칭되어 저장되며, 접근 가능 시간, 접근 권한의 종류 등을 정의하는 정보이다.
- [46] 이하, 첨부된 도면을 참조하여 본 발명의 실시예를 상세하게 설명한다.
- [47] 도 1은 본 발명의 일 실시예에 따른 인증용가상코드를 이용한 사용자 인증 시스템의 구성도이다.
- [48] 도 1에 도시된 바와 같이, 사용자 인증 시스템은 가상코드생성수단(10), 가상코드수신수단(20), 사용자인증수단(30) 및 서버(40)를 포함한다.
- [49] 가상코드생성수단(10)은 인증용가상코드를 생성하기 위한 전용프로그램 또는 전용어플리케이션(이하, 전용프로그램(11))이 내장 또는 설치되어 있는 장치를 의미한다. 보다 구체적으로, 가상코드생성수단(10)은 사용자인증수단(30)에 대한 접근 권한을 타인에게 부여하는 사용자의 단말기일 수 있다.

가상코드생성수단(10)은 일시적 및/또는 제한적 접근 권한이 부여된 인증용가상코드를 다른 장치로 전송할 수 있다.

- [50] 일 실시예로, 가상코드생성수단(10)은 후술할 사용자인증수단(30) 또는 서버(40)에 초기 등록될 수 있다. 가상코드생성수단(10)을 초기 등록하는 방법에 대하여는 후술한다.
- [51] 또한, 일 실시예로, 전용프로그램(11)은 UID 또는 SID를 이용하여 사용자 인증을 위한 인증용가상코드를 생성하는 역할을 수행한다. 여기서, UID 또는 SID는 가상코드생성수단(10) 및 서버(40)에 모두 저장된 정보일 수 있으며, 상기 UID 또는 SID의 저장위치에는 권한 정보가 매칭되어 저장될 수 있다.
- [52] 한편, UID 또는 SID는 반드시 가상코드생성수단(10)에 내장된 메모리에 저장될 필요는 없다. 예를 들어, UID 또는 SID는 별도의 무선 통신이 가능한 카드 또는 웨어러블 장치 내에 저장될 수 있으며, 사용자는 UID 또는 SID가 저장된 단말기가 UID 또는 SID를 가상코드생성수단(10)으로 전송하도록 함으로써, 가상코드생성수단(10)이 인증용가상코드를 생성하도록 할 수 있다.
- [53] 한편, 전용프로그램(11)은 인증용가상코드생성함수를 포함하여 UID 또는 SID를 이용하여 인증용가상코드를 생성한다. 예를 들어, 전용프로그램(11)은 UID 또는 SID를 인증용가상코드생성함수의 시드데이터로 이용하여 인증용가상코드를 생성한다. 다만, 이에 한정되지 않고, 전용프로그램(11)은 가상코드생성수단의 고유값 또는 가상코드검증수단의 고유값을 시드데이터로 하여 인증용가상코드를 생성할 수 있다. 본 명세서에서 설명하는 UID 또는 SID는 가상코드생성수단의 고유값 또는 가상코드검증수단의 고유값으로 대체될 수 있다. 일 실시 예에 있어서, 전용프로그램(11)은 차량, 도어락 또는 단말기의 일련번호를 시드데이터로 하여 인증용가상코드를 생성할 수 있다.
- [54] 인증용가상코드가 가상코드검증수단의 고유값을 시드데이터로하여 생성되는 경우, 가상코드생성수단을 가상코드검증수단에 등록하지 않고도, 사용자 인증을 수행하도록 할 수 있다. 이에 대하여는 후술한다.
- [55] 또한, 일 실시예로, 전용프로그램(11)은 가상코드생성수단(10)을 사용자인증수단(30) 또는 서버(40)에 등록하는 역할을 수행한다. 즉, 사용자는 가상코드생성수단(10)(즉, 사용자 단말)에 전용프로그램(11)을 설치하고, 전용프로그램(11)은 사용자인증수단(30) 또는 서버(40)로 UID 또는 SID를 전송하여 등록한다. 다만, 이에 한정되지 않고, 전용프로그램(11)은 공장 출고시 가상코드생성수단(10)에 내장된 프로그램일 수 있다.
- [56] 구체적인 예로, 전용프로그램(11)은 등록 시에 사용자로부터 UID 또는 SID를 입력받거나, 사용자의 전용프로그램(11) 로그인 정보를 기반으로 사용자 정보를 생성한다. 그 후, 전용프로그램(11)은 사용자 정보를 사용자인증수단(30) 또는 서버(40)로 전송한다. 사용자인증수단(30) 또는 서버(40)가 특정카운트에 UID 또는 SID를 등록함에 따라, 전용프로그램(11)은 사용자인증수단(30) 또는 서버(40)로부터 인증용가상코드생성함수 또는 인증용가상코드생성함수를

특정하기 위한 설정데이터를 수신한다. 이를 통해, 전용프로그램(11)은 사용자인증수단(30) 또는 서버(40) 내에 사용자 정보가 등록된 특정카운트 탐색이 가능한 인증용가상코드를 생성하는 인증용가상코드생성함수를 포함할 수 있다.

- [57] 한편, 다른 일 실시 예로, 전용프로그램(11)은 UID를 사용자인증수단(30) 또는 서버(40)에 등록한 후 추가적으로 SID를 사용자인증수단(30) 또는 서버(40)에 등록할 수 있다. 전용프로그램(11)은 추가적으로 입력받은 SID가 기등록된 UID의 저장위치에 매칭되어 저장되거나, UID와는 별도로 저장되도록 할 수 있다. 사용자인증수단(30) 또는 서버(40)가 특정카운트에 SID를 등록함에 따라, 전용프로그램(11)은 사용자인증수단(30) 또는 서버(40)로부터 인증용가상코드생성함수 또는 인증용가상코드생성함수를 특정하기 위한 설정데이터를 수신한다. 여기서, 인증용가상코드생성함수 또는 인증용가상코드생성함수를 특정하기 위한 설정데이터는 UID 등록시 사용자인증수단(30) 또는 서버(40)로부터 수신한 것과 다를 수 있다. 추후, 사용자는 전용프로그램(11)을 통해 UID에 기반하여 인증용가상코드를 생성할 지, SID에 기반하여 인증용가상코드를 생성할 지 선택할 수 있다.
- [58] 일 실시 예에 있어서, 가상코드생성수단(10)은 인증용가상코드 생성요청시 사용자가 선택한 ID의 종류에 따라 서로 다른 인증용가상코드생성함수를 이용하여 인증용가상코드를 생성할 수 있다. 다만, 이에 한정되지 않고, 가상코드생성수단(10)은 인증용가상코드 생성요청시 사용자가 선택한 ID의 종류에 상관없이 동일한 인증용가상코드생성함수를 사용하되 사용자가 선택한 ID를 시드 데이터로 사용할 수 있다. 가상코드수신수단(20)은 가상코드생성수단(10)에서 생성된 인증용가상코드를 수신하여, 가상코드수신수단(20)에 포함된 디스플레이부에 수신된 인증용가상코드를 표시하거나, 가상코드수신수단(20)에 포함된 통신부를 통해 인증용가상코드를 서버로 송신한다.
- [59] 일 실시 예에 있어서, 가상코드생성수단(10)은 인증용가상코드를 포함하는 텍스트 메시지를 가상코드수신수단(20)으로 전달할 수 있다. 가상코드생성수단(10)의 사용자는 가상코드수신수단(20) 사용자에게 접근 권한을 부여하고 싶은 시간대에 가상코드수신수단(20)으로 텍스트 메시지를 송신할 수 있다.
- [60] 다른 일 실시 예에 있어서, 근거리 통신(예를 들어, NFC 통신)을 통해 가상코드수신수단(20)으로 전달할 수 있다. 이 경우, 가상코드생성수단(10)의 사용자는 가상코드수신수단(20)과의 접촉을 통해 인증용가상코드를 전달할 수 있다.
- [61] 가상코드수신수단(20)에 포함된 통신부는 가상코드생성수단(10) 및 서버(40)와 통신하여 인증용가상코드를 송수신하는 역할을 수행한다. 여기서, 통신부의 무선통신 방식으로는 NFC(Near Field Communication)뿐만 아니라,

블루투스(Bluetooth), BLE(Bluetooth Low Energy), 비콘(Beacon), RFID(Radio Frequency Identification), 적외선 통신(Infrared Data Association; IrDA), UWB(Ultra Wideband), ZigBee 등이 이용될 수도 있다.

- [62] 구체적인 예로, 통신부는 IC 칩에 연결되는 NFC(Near Field Communication) 통신부(예를 들어, NFC안테나)일 수 있다. 예를 들어, 가상코드수신수단(20) 사용자는 사용자인증수단(30)에 태깅함으로써, 수신된 인증용가상코드를 사용자인증수단(30)로 송신할 수 있다.
- [63] 다른 예를 들어, 가상코드수신수단(20)은 인증용가상코드를 수신(예를 들어, 텍스트 메시지로 수신)하여 가상코드수신수단(20)에 포함된 디스플레이부에 수신된 인증용가상코드를 표시한다. 가상코드수신수단(20) 사용자는 디스플레이부에 표시된 인증용가상코드를 사용자인증수단(30)에 입력함으로써, 사용자 인증을 수행할 수 있다.
- [64] 사용자인증수단(30)은 가상코드생성수단(10) 사용자가 타인에게 사용자 인증 권한을 부여하는 대상으로서, 인증용가상코드를 전달받은 타인은 인증용가상코드를 이용하여 사용자인증수단(30)에 대한 접근 권한을 얻을 수 있다.
- [65] 예를 들어, 사용자인증수단(30)은 금융거래장치, 모바일 단말기, 차량, 도어락 등일 수 있다. 다만, 이에 한정되지 않고, 사용자인증수단(30)은 사용자 인증을 통해 접근 권한을 부여받을 수 있는 모든 장치를 포함한다.
- [66] 사용자인증수단(30)은 인증용가상코드를 수신하여 사용자 인증을 직접 수행하거나, 인증용가상코드를 서버로 전달하여 서버를 통해 사용자 인증이 수행되도록하는 역할을 한다.
- [67] 일 실시 예에 있어서, 사용자인증수단(30)은 인증용가상코드를 수신하고, 상기 인증용가상코드를 기반으로 UID 또는 SID를 저장한 저장위치를 탐색한다. 상기 저장위치를 탐색하는 방법에 대하여는 후술한다. 이후, 사용자인증수단(30)은 탐색된 UID 또는 SID에 기반하여 사용자 인증을 수행한다.
- [68] 다른 일 실시 예에 있어서, 사용자인증수단(30)은 인증용가상코드를 수신하고, 수신된 인증용가상코드를 서버(40)로 송신한다. 서버(40)는 인증용가상코드를 수신하고, 상기 인증용가상코드를 기반으로 UID 또는 SID를 저장한 저장위치를 탐색한다. 이후, 서버(40)는 탐색된 UID 또는 SID에 기반하여 사용자 인증을 수행하고, 사용자 인증 여부를 사용자인증수단(30)으로 송신한다.
- [69] 한편, 사용자인증수단(30) 자체가 서버(40)일 수 있다. 일 실시예에 있어서, 가상코드생성장치(10) 사용자는 전용프로그램(11)을 통해 가상코드생성장치(10)를 사용자인증수단(30)에 등록하고, 사용자인증수단(30)은 사용자 정보를 사용자인증수단(30)에 포함된 메모리에 저장할 수 있다.
- [70] 별도의 언급이 없는 한, 본 명세서에서는 인증용가상코드에 기반한 사용자 인증이 사용자인증수단(30)에서 이루어질수도, 서버(40)에서 이루어질수 도

있는 것으로 서술한다. 즉, 사용자인증수단(30) 및 서버(40) 중 어느 하나에서 인증용가상코드에 기반한 사용자 인증을 하는 실시 예는 다른 하나에도 적용될 수 있음이 자명하다.

- [71] 사용자인증수단(30)은 통신부를 포함하며, 통신부는 가상코드생성수단(10), 가상코드수신수단(20) 및 서버(40)와 통신하여 인증용가상코드를 송수신하고, 이를 사용자 인증 수행에 활용할 수 있도록 한다. 여기서, 통신부의 무선통신 방식으로는 NFC(Near Field Communication)뿐만 아니라, 블루투스(Bluetooth), BLE(Bluetooth Low Energy), 비콘(Beacon), RFID(Radio Frequency Identification), 적외선 통신(Infrared Data Association; IrDA), UWB(Ultra Wideband), ZigBee 등이 이용될 수도 있다. 다만, 이에 한정되지 않고, 사용자인증수단(30)은 원거리 무선 통신을 위한 통신 모듈을 구비할 수 있다.
- [72] 한편, 사용자인증수단(30)은 사용자 인증을 통해 접근 권한을 부여한다. 접근 권한은 사용자인증수단(30)의 종류에 따라 달라질 수 있다. 일 실시 예에 있어서, 사용자인증수단(30)이 차량인 경우, 접근 권한은 차량 내부 출입 권한일 수 있으며, 차량 내부 출입 권한이 부여될 경우, 차량은 차량의 도어락을 해제하여 사용자가 차량 내부로 진입할 수 있도록 한다.
- [73] 다른 일 실시 예에 있어서, 사용자인증수단(30)이 도어락인 경우, 접근 권한은 건물 내부 출입 권한일 수 있으며, 건물 내부 출입 권한이 부여될 경우, 차량은 차량의 도어락을 해제하여 사용자가 차량 내부로 진입할 수 있도록 한다.
- [74] 다른 일 실시 예에 있어서, 사용자인증수단(30)이 모바일 단말기인 경우, 접근 권한은 모바일 단말기의 사용 권한일 수 있으며, 모바일 단말기의 사용 권한이 부여될 경우, 모바일 단말기는 단말기 잠금 상태를 해제하여 사용자가 모바일 단말기에 내장된 기능을 이용할 수 있는 상태가 된다.
- [75] 한편, 사용자인증수단(30)의 접근 권한은 단계적으로 부여될 수 있다. 일 실시 예에 있어서, 사용자인증수단(30)이 차량인 경우, 차량에 대한 접근 권한은 차량 내부 접근 권한, 차량 시동 권한, 차량 운전 권한을 포함할 수 있다. 차량 시동 권한은 차량의 시동을 걸어 차량 내 구비된 장치들을 이용할 수는 있지만, 차량의 운전을 할 수 없는 권한으로 해당 권한만 부여받은 경우, 차량은 이동하지 않는다. 또한, 차량 운전 권한은 차량 운전을 포함한 차량의 모든 기능을 사용할 수 있는 권한이다. 사용자는 타인에게 상술한 종류의 권한을 선택적으로 부여할 수 있다.
- [76] 다른 일 실시 예에 있어서, 사용자인증수단(30)이 모바일 단말기인 경우, 접근 권한은 모바일 단말기에 구비된 애플리케이션 별로 부여될 수 있다. 예를 들어, 사용자는 모바일 단말기에 구비된 카메라 애플리케이션에 대한 접근 권한만을 타인에게 부여할 수 있다.
- [77] 한편, 가상코드생성수단(10)의 사용자는 사용자인증수단(30)에 대한 접근 권한이 부여되는 시간대를 설정할 수 있다. 일 실시 예에 있어서, 가상코드생성수단(10)의 사용자는 가상코드생성수단(10)을 통해

사용자인증수단(30) 또는 서버(40)를 접근 가능 시간 정보를 송신하고, 사용자인증수단(30) 또는 서버(40)는 접근 가능 시간 정보를 기 저장된 UID 또는 SID와 매칭시켜 저장한다. 이후, 사용자인증수단(30) 또는 서버(40)는 저장된 접근 가능 시간 정보에 기반하여 사용자 인증 여부를 결정한다. 이에 대하여는 후술한다.

- [78] 서버(40)는 인증용가상코드를 수신하여 사용자 인증을 수행하는 역할을 한다. 이를 위해, 사용자는 가상코드생성수단(10)를 통해, UID 또는 SID를 서버(40)에 초기 등록한다.
- [79] 일 실시 예에 있어서, 사용자는 전용프로그램(11)을 통해 UID 또는 SID를 서버(40)로 송신할 수 있다. 이후, 사용자는 전용프로그램(11)을 통해 권한 정보를 서버(40)에 저장된 UID 또는 SID와 매칭시켜 저장시킬 수 있다. 서버(40)는 UID 또는 SID의 저장위치와 매칭시켜 권한 정보를 저장할 수 있다.
- [80] 일 실시 예에 있어서, UID 또는 SID는 가상코드생성수단(10)가 인증용가상코드를 생성함에 있어서, 시드 데이터로 활용될 수 있다. 이를 통해, 본 발명은 사용자가 다수의 타인에게 사용자인증수단(30)에 대한 접근 권한을 부여할 수 있도록 한다. 이에 대하여는 후술한다.
- [81] 서버(40)는 가상코드생성수단(10)에서 생성된 인증용가상코드를 기반으로, 서버(40) 내에 UID 또는 SID가 저장된 위치를 탐색하고, 인증용가상코드를 수신한 시점과, 인증용가상코드생성수단(20)에서 인증용가상코드가 생성된 시점을 기반으로 인증용가상코드를 검증한다. 인증용가상코드를 검증하여 사용자 인증을 수행하는 방식에 대해서는 상세히 후술한다.
- [82] 도 2는 본 발명의 일 실시예에 따른 가상코드생성장치의 구성도이다.
- [83] 도 2에 도시된 바와 같이, 가상코드생성장치(100)는 세부코드생성부(110), 가상코드생성부(120) 및 가상코드제공부(130)를 포함한다.
- [84] 가상코드생성장치(100)는, 일 실시예로, 사용자 인증을 위한 인증용가상코드를 생성하는 프로그램(즉, 애플리케이션)이 설치된 사용자 단말일 수 있다. 가상코드생성장치(100)는 상술한 가상코드생성수단(10)이 될 수 있다.
- [85] 세부코드생성부(110)는 사용자 정보를 기반으로 하나 이상의 세부코드를 생성하는 역할을 수행한다.
- [86] 인증용가상코드생성함수는 하나 이상의 세부코드생성함수를 포함한다. 예를 들어, 인증용가상코드가 복수의 세부코드를 포함하는 경우, 인증용가상코드생성함수는 복수의 세부코드생성함수를 이용하여 복수의 세부코드를 생성하고, 복수의 세부코드를 결합하는 세부코드결합함수를 이용하여 인증용가상코드를 생성한다.
- [87] 이때, 인증용가상코드는 가상코드생성장치(100), 즉, 사용자 단말 내부에 내장 또는 설치된 전용프로그램(11)에 의해 단위카운트마다 생성되는 것으로서, 모바일 OTP(mobile one time password, mOTP)를 의미한다.
- [88] 일 실시예로, 가상코드생성장치(100)는 가상코드생성장치(100)에 저장된

사용자 정보 중 적어도 일부를 인증용가상코드생성함수의 시드데이터 중 하나로 이용할 수 있다. 구체적인 예로, 세부코드생성부(110)는 하나의 세부코드생성함수를 이용하여 UID 또는 SID를 각 세부코드생성함수의 시드데이터로 이용하여 각각의 세부코드를 생성한다. 이때, 세부코드생성부(110)는 사용자로부터 사용자 인증이 요청된 시점 또는 카운트 값도 이용하여 각각의 세부코드를 생성할 수 있다.

- [89] 일 실시예로, 세부코드생성부(110)는 세부코드생성함수로 제1함수와 제2함수를 포함하여, 제1코드 및 제2코드를 생성할 수 있다. 이때, 인증용가상코드생성장치(100)는 보안성을 높이기 위해 제1코드를 생성하는 제1함수와 제2코드를 생성하는 제2함수를 세부코드생성함수로 포함할 뿐, 제1코드와 제2코드의 상관관계에 대한 데이터는 포함하지 않을 수 있다.
- [90] 가상코드생성부(120)는 인증용가상코드생성함수를 이용하여 하나 이상의 세부코드를 조합하여 인증용가상코드로 생성하는 역할을 수행한다. 일 실시예로, 인증용가상코드는 복수의 세부코드를 특정한 규칙에 따라 결합하여 생성된다. 인증용가상코드생성함수는 복수의 세부코드를 조합하는 규칙(즉, 세부코드결합함수)을 포함한다. 즉, 가상코드생성부(120)는 하나 이상의 세부코드를 인증용가상코드생성함수에 포함된 세부코드결합함수를 이용하여 조합할 수 있다.
- [91] 복수의 세부코드를 결합하여 하나의 인증용가상코드를 생성하는 방식으로는 다양한 방식이 적용될 수 있다. 세부코드결합함수의 일 예로, 인증용가상코드생성부(120)는 N자리의 제1코드와 N자리의 제2코드를 번갈아 배치하는 방식으로 인증용가상코드를 생성할 수 있다. 또한, 다른 일 예로, 세부코드결합함수는 제1코드 뒤에 제2코드를 결합하는 함수일 수 있다. 인증용가상코드에 포함되는 세부코드가 늘어남에 따라 세부코드결합함수도 다양하게 생성될 수 있다.
- [92] 또한, 일 실시예로, 인증용가상코드가 제1코드 및 제2코드의 특정한 규칙에 따른 조합으로 생성되는 경우, 제1코드와 제2코드는 사용자 정보가 저장된 저장위치탐색알고리즘 내의 UID 또는 SID의 저장위치를 탐색하기 위한 각각의 역할을 수행할 수 있다. 예를 들어, 제1코드는 저장위치탐색의 시작지점을 설정하고, 제2코드는 특정한 탐색방식에 따라 상기 시작지점으로부터 상기 UID 또는 SID의 저장위치로의 탐색경로를 설정한다. 즉, 가상코드생성장치(100)에서 단위카운트마다 정상적으로 생성된 인증용가상코드가 제공되면, 가상코드검증장치(100)는 제1코드에 대응하는 탐색시작지점으로부터 제2코드에 상응하는 탐색경로에 따라 이동한 지점을 사용자 정보가 저장된 지점(즉, UID 또는 SID 저장위치)으로 판단한다. 인증용가상코드를 구성하는 제1코드와 제2코드를 기반으로 UID 또는 SID의 저장위치를 탐색하는 구체적인 방식은 후술한다.
- [93] 세부코드생성부(110)가 세부코드를 생성하는 방식의 일 실시예로,

세부코드생성부(110)는 단위카운트마다 새로운 세부코드를 생성하고, 이에 따라 가상코드생성장치(100)는 단위카운트마다 새로운 인증용가상코드를 생성한다. 단위카운트마다 신규로 생성되는 인증용가상코드는 중복되어 생성되지 않는다. 구체적으로, 세부코드생성부(110)는, 단위카운트마다 신규생성되는 인증용가상코드가 특정한 사용자 또는 특정한 가상코드생성장치(100)에게 미리 정해진 기간 동안 중복생성되지 않을 뿐만 아니라, 특정한 그룹에 속한 사용자간에도 중복생성되지 않도록 설정될 수 있다.

[94] 인증용가상코드의 중복생성을 방지하는 구체적인 일 실시예로, M개 문자로 N자리의 제1코드 또는 제2코드를 생성하는 경우, 인증용가상코드생성함수에 포함되는 세부코드생성함수는 MN개의 코드를 제1코드 또는 제2코드로 생성할 수 있고, 각각의 코드를 세부코드생성함수가 구동되는 초기시점으로부터 각 카운트마다 매칭한다. 예를 들어, 단위카운트를 1초로 설정하는 경우, 세부코드생성함수가 최초 구동된 시점에서부터 매 초에 상이한 MN개의 코드를 매칭한다. 그리고, 특정한 세부코드생성함수를 이용하는 주기 또는 가상코드생성장치(100)의 사용주기(예를 들어, 인증용가상코드를 생성하는 애플리케이션이 설치된 사용자 단말의 유효기간)를 MN 카운트에 해당하는 시간길이(예를 들어, 1카운트가 1초인 경우, MN 초)보다 짧은 시간길이를 설정하면 제1코드 또는 제2코드는 사용주기 동안에 동일한 코드가 중복 생성되지 않는다. 즉, 시간이 흐름에 따라 카운트가 증가할 때, 사용자가 특정시점에 가상코드생성장치(100)에 인증용가상코드생성요청을 하는 경우, 가상코드생성장치(100)는 특정시점에 대응되는 카운트에 매칭된 코드값을 제1코드 또는 제2코드로 생성할 수 있다.

[95] 구체적으로, 알파벳 대문자와 0부터 9까지의 숫자를 코드에 포함 가능한 문자로 사용(즉, 36개의 문자를 사용)하고, 제1코드와 제2코드에 각각 6자리를 할당하는 경우, 가상코드생성장치(100)는 제1코드 및 제2코드로 366개의 코드를 제공할 수 있다. 이때, 가상코드생성장치(100)는 각각의 코드를 각 카운트마다 매칭시켜서, 각 카운트마다 변경된 제1코드 및 제2코드를 제공할 수 있다.

[96] 인증용가상코드의 중복생성을 방지하는 구체적인 다른 일 실시예로, 가상코드생성장치(100)의 사용주기가 경과되면, 제1코드 또는 제2코드를 생성하는 함수(즉, 제1함수 또는 제2함수)를 변경하거나 제1코드와 제2코드의 매칭관계를 변경하여 이전 사용주기와 상이한 인증용가상코드가 생성되도록 한다. 인증용가상코드가 제1함수에 의해 생성되는 제1코드와 제2함수에 의해 생성되는 제2코드가 결합되는 경우, 제1코드생성함수 또는 제2코드생성함수가 변경되면, 가상코드생성장치(100)는 제1코드 또는 제2코드가 등장하는 순서가 이전 사용주기와 달라짐에 따라 이전 주기와 상이한 인증용가상코드를 생성하는 인증용가상코드생성함수를 신규 사용주기에 적용할 수 있다. 또한, 가상코드생성장치(100)는 이전 사용주기에서 사용된 인증용가상코드와 동일한 코드가 신규 사용주기 내 각 카운트의 인증용가상코드로 등장하지 않도록(즉,

제1함수에 따라 생성되는 제1코드와 제2함수에 따라 생성되는 제2코드의 매칭관계가 신규 사용주기의 모든 카운트에서 이전 사용주기 내에 포함된 매칭관계 중에 포함되지 않도록) 제1함수와 제2함수를 선택할 수 있다. 즉, MN 개의 코드를 1회씩 적용할 수 있는 사용주기를 경과한 후 인증용가상코드생성함수 조절 또는 갱신을 통해 이전 사용주기와 겹치는 인증용가상코드가 생성되지 않는 신규 사용주기의 인증용가상코드생성함수를 적용할 수 있다.

- [97] 또한, 인증용가상코드의 중복생성을 방지하는 구체적인 또 다른 일 실시예로, 전체주기에서 사용자에게 무관하게 중복된 인증용가상코드가 발생되지 않도록, 제1코드는 제1함수가 구동되는 초기시점으로부터 각 카운트마다 매칭된 코드 중에서 인증용가상코드 생성요청이 된 시점(또는 카운트)에 대응되는 코드값으로 설정하고, 제2코드는 동일시점에 항상 상이하게 존재하는 값(예를 들어, UID 또는 SID)을 반영하여 생성되는 코드값으로 설정하고, 인증용가상코드를 상기 제1코드와 제2코드가 결합된 코드값으로 이용할 수 있다. 제1코드는 각 카운트마다 상이한 코드값이 되고 제2코드는 동일시점에 UID 또는 SID마다 상이한 코드값을 가지게 되어서, 제1코드와 제2코드가 결합된 인증용가상코드는 모든 시점에 상이한 코드값이 출력되게 된다.
- [98] 또한, 다른 일 실시예로, 상기 인증용가상코드생성함수(또는 세부코드생성함수)는, M개의 문자를 오름차순으로 나열하는 다수의 나열규칙 중 어느 하나가 적용된다. 즉, 가상코드생성장치(100)는 인증용가상코드생성함수 내에 포함되는 세부코드생성함수에 M개 문자를 오름차순으로 나열하는 규칙을 다양하게 적용하여 할 수 있다. 예를 들어, 알파벳 대문자를 오름차순으로 나열하는 나열규칙은, 일반적인 순서인 A, B, C,..., Z 순서가 될 수 있고, A, C, B,..., Z 순서가 될 수도 있다. 인증용가상코드생성함수에서 나열규칙이 달라짐에 따라 인증용가상코드생성함수가 구동되는 초기시점부터 각 카운트에 차례대로 코드가 매칭되는 순서가 달라지게 된다.
- [99] 한편, 가상코드생성장치(100)는 인증용가상코드 생성요청이 있는 경우, 사용자로부터 권한 정보를 입력받을 수 있다. 입력받은 권한 정보는 두 가지 다른 방식으로 활용될 수 있다.
- [100] 첫 번째로, 가상코드생성장치(100)는 인증용가상코드 생성요청이 있는 경우, 사용자로부터 권한 정보를 입력받은 후 실시간으로 가상코드검증장치(200)로 전송할 수 있다. 가상코드검증장치(200)는 수신한 권한 정보를 해당 UID 또는 SID에 매칭시켜 저장한다.
- [101] 두 번째, 가상코드생성장치(100)는 사용자로부터 입력받은 권한 정보를 인증용가상코드가 포함되도록 할 수 있다. 후술할 가상코드검증장치(200)는 사전에 특정 권한에 대응하는 권한 코드를 저장하고, 인증용가상코드에 특정 권한 코드가 포함되는 경우, 해당 권한 코드에 대응하는 권한을 부여할 수 있다.

이를 위해, 인증용가상코드는 권한 코드 영역을 포함할 수 있다. 권한 정보가 포함된 인증용가상코드에 대하여는 후술한다.

- [102] 다른 일 실시 예에 있어서, 가상코드생성장치(100)가 사용자로부터 권한 정보를 입력받지 못한 경우, 가상코드생성장치(100)는 상기 권한 코드 영역에 특정 코드(예를 들어, NULL)를 포함하는 인증용가상코드를 생성할 수 있다. 가상코드검증장치(200)는 상기 권한 정보를 정의하는 영역에 특정 코드가 포함된 경우, 인증용가상코드에서 UID 또는 SID를 추출하고, 추출된 UID 또는 SID에 매칭되어 저장된 권한 정보에 기반하여 권한을 부여할 수 있다.
- [103] 다른 일 실시 예에 있어서, 가상코드생성장치(100)는 사용자로부터 인증용가상코드생성요청이 있는 경우, 가상코드검증장치(200)와의 통신 가능여부를 판단한다. 가상코드검증장치(200)와의 통신이 어려운 경우, 사용자로부터 권한 정보를 입력받고, 입력받은 권한 정보가 포함된 인증용가상코드를 생성할 수 있다. 이를 통해, 본 발명은 가상코드생성장치(100)와 가상코드검증장치(200)간의 통신이 어려운 경우에도 제한된 접근 권한을 부여할 수 있게 된다.
- [104] 가상코드제공부(130)는 생성된 인증용가상코드를 가상코드수신수단(20)으로 제공하여 사용자 인증을 진행하는 역할을 수행한다.
- [105] 도 3은 본 발명의 일 실시예에 따른 가상코드검증장치의 구성도이다.
- [106] 가상코드검증장치(200)는 상술한 사용자인증수단(30) 또는 서버(40)일 수 있다.
- [107] 도 3에 도시된 바와 같이, 가상코드검증장치(200)는 가상코드수신부(210), 세부코드추출부(220), 저장위치탐색부(230), 권한정보추출부(240), 가상코드검증부(250) 및 사용자인증승인부(360)를 포함한다.
- [108] 여기서, 가상코드검증장치(200)는 인증용가상코드를 기반으로 UID 또는 SID를 추출하고, 인증용가상코드를 기반으로 수신된 인증용가상코드가 정상적인 코드인지를 판단하여 사용자 인증을 수행한다.
- [109] 사용자인증요청수신부(210)는 가상코드제공부(130)로부터 제공된 인증용가상코드를 기반으로 사용자 인증을 요청받는 역할을 수행한다.
- [110] 일 실시예로, 사용자인증요청수신부(210)는 전용프로그램(11)에 의해 생성된 인증용가상코드를 가상코드수신수단(20)로부터 제공받아 사용자인증을 요청받는다.
- [111] 세부코드추출부(220)는 인증용가상코드에 포함된 하나 이상의 세부코드를 추출하는 역할을 수행한다.
- [112] 일 실시예로, 세부코드추출부(220)는 인증용가상코드생성함수에 포함된 세부코드결합함수를 포함한다. 따라서, 인증용가상코드가 복수의 세부코드를 포함하는 경우, 세부코드추출부(220)는 세부코드결합함수를 적용하여 인증용가상코드에서 복수의 세부코드를 추출할 수 있다. 예를 들어, 가상코드생성장치(100)에서 두 개의 세부코드(즉, 제1코드 및 제2코드)가 결합된 인증용가상코드를 생성하는 경우, 세부코드추출부(220)는 인증용가상코드의

문자배열에서 세부코드결합함수를 적용하여 제1코드 및 제2코드를 분리해낼 수 있다.

- [113] 저장위치탐색부(230)는 추출된 하나 이상의 세부코드를 기반으로 저장위치탐색알고리즘 내에 UID 또는 SID의 저장위치를 탐색하는 역할을 수행한다. 여기서, 저장위치탐색알고리즘은 가상코드생성장치(100)에서 인증용가상코드를 생성할 때 이용했던 인증용가상코드생성함수에 매칭되는 것이다. 저장위치탐색부(230)에서 각각의 세부코드를 기반으로 UID 또는 SID의 저장위치를 탐색하는 방식으로는 다양한 방식이 적용될 수 있다. 저장위치탐색부(230)가 복수의 세부코드를 기반으로 저장위치를 탐색하기 위해 세부코드 간에는 상관관계를 포함할 수 있다.
- [114] 여기서, 저장위치는 사용자에 의해 가상코드생성수단(10)의 등록이 요청된 시점에 해당하는 트랙 상의 지점(카운트)을 의미한다. 즉, 가상코드검증장치(200) 내에서 해당 가상코드생성수단(10)에 대한 트랙이 구동되고, 특정 시점에 특정 사용자에 의해 특정 UID 또는 SID의 등록이 요청되면, 해당 시점에 대응되는 카운트(즉, 트랙의 최종 구동시로부터 등록시점까지 경과된 카운트)에 해당 UID 또는 SID가 등록되게 된다. 그리고 해당 UID 또는 SID의 저장위치에는 권한 정보가 매칭되어 저장된다.
- [115] 인증용가상코드가 제1코드 및 제2코드로 구성되는 경우, 세부코드 간에 상관관계를 가지는 일 실시예로, 저장위치탐색부(230)는 제1코드에 대응하는 탐색시작지점을 결정하고, 상기 탐색시작지점으로부터 제2코드에 상응하는 탐색경로에 따라 이동된 지점을 UID 또는 SID의 저장위치로 찾을 수 있다. 즉, 상기 세부코드는, 저장위치탐색의 시작지점을 설정하는 제1코드 및 특정한 탐색방식에 따라, 상기 시작지점으로부터 상기 UID 또는 SID의 저장위치로의 탐색경로를 설정하는 제2코드를 포함할 수 있다.
- [116] 또한, 다른 일 실시예로, 가상코드생성장치(100)가 단위카운트마다 신규 인증용가상코드를 제공함에 따라, 가상코드검증장치(200)는 각 카운트마다 변경되는 제1코드 및 제2코드를 기반으로 탐색시작지점과 탐색경로를 설정하여 UID 또는 SID의 저장위치를 탐색할 수 있다.
- [117] 또한, 다른 일 실시예로, 저장위치탐색부(230)는 상관관계를 가지는 복수의 세부코드를 이용하여 UID 또는 SID의 저장위치를 찾기 위해, 저장위치탐색알고리즘을 포함할 수 있다. 저장위치탐색알고리즘은 인증용가상코드에 포함되는 각각의 세부코드 적용 시에 저장위치 탐색이 가능하도록 하는 알고리즘으로서, 가상코드생성장치(100)에서 인증용가상코드를 생성할 때 이용했던 인증용가상코드생성함수에 매칭되는 것이다.
- [118] 예를 들어, 인증용가상코드가 저장위치의 탐색시작지점을 결정하는 제1코드 및 상기 탐색시작지점으로부터의 저장위치 방향을 제시하는 제2코드를 포함하는 경우, 저장위치탐색알고리즘은 제1코드에 대응되는 지점에서

제2코드에 대응되는 방향을 지시할 때, 해당 위치에 UID 또는 SID의 등록 시점이 매칭되는 저장위치가 배치되도록 조절하는 알고리즘이다.

- [119] 권한정보추출부(240)는 저장위치탐색부(230)에 의해 탐색된 UID 또는 SID의 저장위치에 매칭되어 저장된 권한정보를 추출한다. 즉, 가상코드검증장치(200)는 저장위치탐색알고리즘 내의 각각의 UID 또는 SID의 저장위치에 매칭되어 저장된 권한 정보를 추출할 수 있다. 사용자인증승인부(360)는 상기 추출된 권한 정보를 사용자 인증 여부를 결정하는데 활용한다. 이에 대하여는 후술한다.
- [120] 저장위치탐색알고리즘을 이용함에 따라, 가상코드검증장치(200)는 인증용가상코드에 포함된 제1코드와 제2코드가 변경되어도 UID 또는 SID 저장위치를 탐색할 수 있다. 저장위치탐색알고리즘은 다양한 방식이 적용될 수 있으며, 구체적인 예시는 후술한다. 다만, 저장위치탐색알고리즘은 후술되는 예시에 한정되지 않는다.
- [121] 예를 들어, 도 5를 참조하면, 저장위치탐색알고리즘이 제1코드에 해당하는 MN개의 코드가 나열된 트랙을 따라 구름이동하는 k각형(k는 MN)이며, k각형의 꼭지점이 제1코드 트랙 상에 코드가 배치되는 지점에 대응되면서 이동하는 경우, k각형의 각 꼭지점이 UID 또는 SID의 저장위치와 매칭되고, 제1코드 트랙(즉, 제1트랙)과 k각형이 대응되는 지점이 제1코드에 대응하는 저장위치 탐색시작지점이 될 수 있다. 이때, 저장위치탐색부(230)는 세부코드추출부(220)에서 추출된 제1코드에 대응되는 지점에 k각형의 꼭지점이 접하도록 k각형을 구름이동을 적용할 수 있다. 이를 통해, 저장위치탐색부(230)는 k각형이 접한 제1트랙 상의 위치에서 제2코드에 상응하는 각도(예를 들어, k각형의 꼭지점을 향하도록 180도를 MN개로 분할한 특정한 각도)로 지시함에 따라, 인증용가상코드에 대응하는 UID 또는 SID가 저장된 저장위치인 k각형의 꼭지점을 탐색할 수 있다.
- [122] 구체적으로, 도 5에서와 같이, 가상코드검증장치(200)는 제1코드에 대응하는 지점으로 k각형을 구름이동(즉, k각형의 각 꼭지점과 트랙 상의 각 지점이 차례대로 접하도록 하면서 이동)시킨다. 그 후, 가상코드검증장치(200)는 제2코드에 상응하는 각도 방향을 지시하여 저장위치에 상응하는 꼭지점을 탐색한다.
- [123] 저장위치탐색부(230)에 의해 저장위치 탐색알고리즘 내에서 인증용가상코드 내의 제1코드 및 제2코드를 이용하여 UID 또는 SID의 저장위치가 탐색된 후에, 권한정보추출부(240)에 의해 해당 위치에 매칭되어 저장된 권한 정보를 추출한다.
- [124] 이외의 다양한 저장위치탐색알고리즘에 대한 상세한 설명은 후술한다.
- [125] 가상코드검증부(250)는 가상코드수신부(210)가 인증용가상코드를 수신한 시점과 인증용가상코드가 인증용가상코드생성수단(즉, 사용자 단말)에서 인증용가상코드생성함수를 이용하여 생성된 시점을 비교하여,

인증용가상코드를 검증하는 역할을 수행한다.

- [126] 일 실시예로, 도 6을 참조하면, 가상코드검증부(250)는 인증용가상코드가 수신된 시점과 사용자 단말에 내장 또는 설치된 전용프로그램(11)에서 인증용가상코드생성함수를 이용하여 인증용가상코드가 생성된 시점을 비교하여, 생성 시점이 수신 시점으로부터 기 설정된 오차 범위 내에 포함된 경우 수신된 상기 인증용가상코드가 정상 코드인 것으로 판단할 수 있다.
- [127] 또한, 인증용가상코드를 검증하는 방식에 대한 다른 일 실시예로, 제1코드 및 제2코드는 가상코드생성수단(10)에 의해 UID 또는 SID가 등록된 시점 또는 사용자 인증이 요청된 시점으로부터 랜덤으로 생성되는 OTP코드만큼 추가된 기준 카운트에 대한 코드일 수 있다.
- [128] 구체적인 실시예로, 인증용가상코드생성장치(100)가 가상보안코드를 외부로 출력하지 않고 제1코드 및 제2코드에 반영하여 생성한다.
인증용가상코드생성수단(예를 들어, 인증용가상코드생성 전용프로그램)은 UID 또는 SID(즉, 고유값)를 기반으로 가상보안코드값(예를 들어, OTP코드)를 생성하고, UID 또는 SID 등록시점에 가상보안코드값을 더한 카운트의 제1코드를 생성하고, 가상보안코드값에 대응되는 카운트의 제2코드를 생성(즉, 가상보안코드 자체를 제2코드로 생성)한다. 즉, 제1코드 및 제2코드는 가상코드생성장치(100)에 의해 UID 또는 SID가 가상코드검증장치(200)에 등록된 A시점으로부터 가상보안코드값만큼 이동(shifting)된 카운트를 기반으로 생성된다. 상기 A시점으로부터 이동(Shifting)된 카운트는 상기 생성된 가상보안코드 값에 따라 현재시점에 대응하는 카운트보다 이전 카운트가 될 수도 있고, 이후 카운트가 될 수도 있다. 가상코드검증장치(200)는 수신된 제1코드와 제2코드를 저장위치탐색알고리즘에 적용하여 UID 또는 SID 저장위치(또는 등록위치)를 탐색할 수 있다. 이를 통해, 타인이 인증용가상코드를 구성하는 제1코드 및 제2코드가 제공되는 순서를 확인할 수 없게 되어, 보안성이 향상될 수 있다.
- [129] 또한, 다른 일 실시예로, 가상코드검증장치(200)는 가상보안코드를 기반으로 생성된 제2코드에서 가상보안코드를 추출한 후, 가상보안코드생성함수(즉, OTP함수)를 인증용가상코드를 수신한 카운트로부터 특정범위 내의 카운트를 입력하여 산출된 OTP번호 중에 가상보안코드와 일치하는 값이 있는지 여부를 확인한다. 가상코드검증장치(200)는 제2코드에 제2함수의 역함수를 적용하여 제2코드 생성에 이용된 가상보안코드값(즉, OTP함수값)을 획득하고, 가상보안코드값과 동일한 값을 산출하는 카운트를 찾아낸다. 인증용가상코드의 전송시간이나 딜레이에 의해 인증용가상코드생성수단에서 가상보안코드가 생성된 시점과 인증용가상코드검증수단이 가상보안코드를 수신한 시점의 차이가 존재함에 따라 인증용가상코드검증수단이 인증용가상코드를 수신한 카운트와 가상보안코드에 해당하는 OTP번호를 생성한 카운트가 일치하지 않을 수도 있으므로, 가상코드검증장치(200)는 인증용가상코드를 수신한

카운트로부터 오차범위를 허용한다. 이를 통해, 가상코드검증장치(200)는
 현시점에 생성된 인증용가상코드가 아닌 이전에 생성된 인증용가상코드로
 사용자 인증을 수행하려는 것을 막을 수 있어서, 보안성이 향상될 수 있다. 또한,
 사용자는, 인증용가상코드 입력 시에 특정한 자릿수의 가상보안코드를
 입력하지 않아도 가상코드검증장치(200)가 자체적으로 가상보안코드를
 탐색하여 사용자를 검증할 수 있다.

- [130] 또한, 다른 일 실시예로, 도 7을 참조하면, 가상코드검증장치(200)는 사용자
 인증이 요청된 시점(B시점)에 UID 또는 SID를 더한 카운트에 대응하는
 제1코드를 생성하고, UID 또는 SID 등록시점(A시점)과
 사용자인증요청시점(B시점) 간의 카운트 차이와 가상보안코드값을 더한
 카운트에 대응하는 제2코드를 생성한다. 즉, 인증용가상코드생성
 전용프로그램이 제1코드와 제2코드를 생성하는 수식은 다음과 같다.
- [131] 제1코드 = $f_1(\text{B시점 카운트} + \text{가상보안코드})$
- [132] 제2코드 = $f_2(\text{B시점 카운트} - \text{A시점 카운트} + \text{가상보안코드})$
- [133] (A시점: UID 또는 SID 등록시점, B시점: 사용자인증요청시점의 카운트,
 가상보안코드: OTP번호)
- [134] 가상코드검증장치(200)는 수신된 인증용가상코드 내의 제1코드 및 제2코드를
 기반으로 UID 또는 SID가 저장된 위치를 탐색하고, 이를 기반으로
 사용자인증요청 수신시점으로부터 특정카운트 범위 내의 가상보안코드(즉,
 OTP번호)를 생성한다.
- [135] 그 후, 가상코드검증장치(200)는 제1코드 및 제2코드를 기반으로 사용자
 정보가 저장된 지점을 탐색함에 따라 UID 또는 SID 등록시점(A시점)을
 파악한다. 서버는 UID 등록시점(A시점)으로부터 사용자인증요청 수신시점을
 기준으로 특정카운트범위 내의 각각의 카운트까지의 카운트 개수 및
 가상보안코드(즉, OTP번호)의 합에 해당하는 계산값을 각각 산출하고, 상기
 각각의 계산값 중에 제2코드에 대응하는 카운트수(즉, 제2코드에 제2함수의
 역함수를 적용한 값)와 같은 카운트가 존재하는지 확인한다. 이를 통해, 서버는
 인증용가상코드가 정상적으로 제공된 것인지 확인할 수 있다.
- [136] 한편, 인증용가상코드는 권한 정보를 포함할 수 있다. 일 실시 예에 있어서,
 인증용가상코드는 제1코드, 제2코드 및 시간 정보를 포함할 수 있다. 여기서,
 상기 시간 정보는 인증용가상코드의 사용가능 시간을 정의하는 데이터 및 접근
 가능시간을 정의하는 데이터 중 적어도 하나를 포함할 수 있다. 즉,
 인증용가상코드는 사용자 인증이 가능한 시점 및 시간 범위 중 적어도 하나와
 관련된 데이터를 포함할 수 있다.
- [137] 다른 일 실시 예에 있어서, 상기 가상코드검증장치(200)가 차량인 경우,
 인증용가상코드는 차량 내부 접근 권한, 차량 시동 권한, 차량 운전 권한 중
 적어도 하나와 관련된 권한 정보를 포함할 수 있다.
- [138] 상기 권한 정보는 인증용가상코드내 별도로 할당된 영역에 포함될 수 있다.

가상코드검증장치(200)는 상기 할당된 영역에서 상기 권한 정보를 추출하고, 상기 추출된 권한 정보에 대응하는 권한을 부여할 수 있다.

- [139] 한편, 제1코드 및 제2코드에 포함된 가상보안코드는 인증용가상코드 생성 시점이 아닌 인증용가상코드 사용 가능 시점에 대응하는 카운트로 형성될 수 있다. 구체적으로, 인증용가상코드생성 전용프로그램이 제1코드와 제2코드를 생성하는 수식은 다음과 같다.
- [140] 제1코드 = “UID 또는 SID” + OTP(사용자가 권한 설정한 인증용가상코드 사용가능 시점을 기반으로 한 가상보안코드)
- [141] 제2코드 = OTP(사용자가 권한 설정한 인증용가상코드 사용가능 시점을 기반으로 한 가상보안코드)
- [142] 사용자로부터 인증용가상코드 생성 요청이 입력되는 경우, 가상코드생성장치(100)는 사용자로부터 인증용가상코드 사용 가능 시간을 입력받거나, 사용자로부터 선택되는 UID 또는 SID에 매칭되어 저장된 접근 가능시간 정보에 기반하여 가상보안코드를 형성하고, 이를 기반으로 제1코드 및 제2코드를 형성한다.
- [143] 가상코드검증장치(200)는 수신된 인증용가상코드 내의 제1코드 및 제2코드를 기반으로 UID 또는 SID가 저장된 위치를 탐색하고, 이를 기반으로 사용자인증요청 수신시점으로부터 특정카운트 범위 내의 가상보안코드(즉, OTP번호)를 생성하고, 상기 생성된 가상보안코드 중 인증용가상코드에서 추출된 가상보안코드와 동일한 코드가 있는지 여부를 판단한다. 가상코드검증장치(200)는 상기 생성된 가상보안코드 중 인증용가상코드에서 추출된 가상보안코드와 동일한 코드가 있는 경우, 사용자 인증을 수행한다.
- [144] 한편, 인증용가상코드는 인증용가상코드 생성시점과 관련된 시간정보를 포함할 수 있다. 일 실시 예에 있어서, 인증용가상코드는 제1 내지 제3코드를 포함할 수 있다. 구체적으로, 인증용가상코드생성 전용프로그램이 제1 내지 제3코드를 생성하는 수식은 다음과 같다.
- [145] 제1코드 = 생성시점코드(Time-Stamp) + OTP(사용자가 권한 설정한 인증용가상코드 사용가능 시점을 기반으로 한 가상보안코드)
- [146] 제2코드 = 제1코드 - “UID 또는 SID”
- [147] 제3코드 = 생성시점코드(Time-Stamp)
- [148] 사용자로부터 인증용가상코드 생성요청이 입력되는 경우, 가상코드생성장치(100)는 사용자로부터 인증용가상코드 사용 가능 시간을 입력받거나, 사용자로부터 선택되는 UID 또는 SID에 매칭되어 저장된 접근 가능시간 정보에 기반하여 가상보안코드를 생성하고, 상기 생성된 가상보안코드와 인증용가상코드 생성시점 데이터를 기반으로 제1 및 제3코드를 생성한다. 한편, 가상코드생성장치(100)는 생성된 제1코드 및 사용자로부터 선택되는 UID 또는 SID를 기반으로 제2코드를 형성한다.
- [149] 가상코드검증장치(200)는 수신된 인증용가상코드 내의 제1코드 및 제2코드를

기반으로 UID 또는 SID가 저장된 위치를 탐색하고, 이를 기반으로 사용자인증요청 수신시점으로부터 특정카운트 범위 내의 가상보안코드(즉, OTP번호)를 생성하고, 상기 생성된 가상보안코드 중 인증용가상코드에서 추출된 가상보안코드와 동일한 코드가 있는지 여부를 판단한다. 또한, 가상코드검증장치(200)는 상기 가상보안코드로부터 인증용가상코드 사용 가능 시간 데이터를 산출하고, 상기 산출된 시간 데이터와 제3코드에 포함된 생성시점 데이터 간의 차이를 산출한다. 가상코드검증장치(200)는 상기 차이 값이 기 설정된 범위 내인 경우에만 사용자 인증을 수행한다. 상기 범위는 사용자에 의해 설정될 수 있다.

- [150] 이를 통해, 본 발명은 인증용가상코드 생성 시점과 인증용가상코드 사용 가능 시점 간에 차이가 있는 경우에도, 해당 인증용가상코드가 정상적으로 생성된 코드인지 판단할 수 있도록 한다.
- [151] 한편, 가상코드생성장치(100)는 가상코드생성장치(100)를 가상코드검증장치(200)에 등록하지 않더라도, 사용자 인증을 할 수 있는 인증용가상코드를 생성할 수 있다.
- [152] 일 실시 예에 있어서, 가상코드생성장치(100)는 가상코드검증장치(200)의 고유값을 시드데이터로하여 제1 및 제2코드를 생성할 수 있다. 이 경우, 가상코드생성장치(100)는 사용자로부터 권한 정보를 입력 받은 후, 상기 입력된 권한 정보를 인증용가상코드에 포함시킬 수 있다. 가상코드검증장치(200)는 제1 및 제2코드로부터 고유값을 추출하고, 상기 추출된 고유값이 가상코드검증장치(200)의 고유값과 일치하는지 판단한다. 상기 추출된 고유값이 가상코드검증장치(200)의 고유값과 일치하는 경우, 가상코드검증장치(200)는 인증용가상코드로부터 권한 정보를 추출한 후, 권한 정보에 대응하는 접근 권한을 부여한다. 이를 통해, 본 발명은 사용자가 가상코드생성장치(100)를 가상코드검증장치(200)에 등록하지 않은 경우에도 타인에게 사용자 인증을 수행할 수 있도록 한다.
- [153] 사용자인증승인부(260)는 가상코드검증부(250)에 의해 인증용가상코드의 검증이 완료되면 사용자 인증을 승인하는 역할을 수행한다.
- [154] 일 실시예로, 출입 시의 사용자 인증의 경우, 저장위치탐색부(230)에 의해 UID 또는 SID가 탐색되고, 가상코드검증부(250)에 의해 인증용가상코드가 정상적으로 생성된 것인지 검증이 완료되면, 사용자인증승인부(360)는 권한정보추출부(240)에 의해 추출된 권한 정보에 기반하여 사용자 인증 여부를 결정한다.
- [155] 구체적으로, 사용자인증승인부(360)는 권한 정보에 포함된 접근 가능 시간 정보와 사용자 인증이 요청된 시점을 비교하여 사용자 인증여부를 결정한다.
- [156] 일 실시 예에 있어서, 사용자는 UID 또는 SID를 가상코드검증장치(200)에 등록할 시에 또는 UID 또는 SID를 가상코드검증장치(200)에 등록한 후에 전용프로그램(11)을 통해 접근 가능 시간을 등록할 수 있다. 전용프로그램(11)은

사용자로부터 입력받은 접근 가능 시간을 UID 또는 SID에 매칭시켜 저장한다. 사용자는 전용프로그램(11)을 통해 UID 또는 SID에 매칭된 접근 가능 시간을 변경하거나, 삭제할 수 있다.

- [157] 일 실시 예에 있어서, 사용자인증승인부(360)는 사용자 인증 요청이 이루어진 시점이 UID 또는 SID에 매칭되어 저장된 접근 가능 시간 범위 내에 있는 경우, 사용자 인증을 수행한다. 구체적인 예를 들어, 사용자가 접근 가능 시간을 오전 9시에서 10시로 설정한 경우, 사용자인증승인부(360)는 오전 9시에서 10시 사이에 이루어진 사용자 인증 요청에 대하여만 사용자 인증을 수행한다.
- [158] 한편, 상기 접근 가능 시간은 UID 및 SID 마다 다르게 설정될 수 있으며, 가상코드인증장치(200)는 UID 및 SID 각각과 이에 대응하는 접근 가능 시간 정보를 매칭시켜 저장할 수 있다. 이를 통해, 본 발명은 하나의 장치에 다수의 사람에게 접근 권한을 부여해야 하는 경우, 권한 부여 대상마다 접근 가능한 시간을 설정할 수 있게 된다.
- [159] 다른 일 실시 예에 있어서, 사용자는 UID 또는 SID를 가상코드검증장치(200)에 등록할 시에 또는 UID 또는 SID를 가상코드검증장치(200)에 등록한 후에 전용프로그램(11)을 통해 접근 권한의 종류를 등록할 수 있다. 전용프로그램(11)은 사용자로부터 입력받은 접근 권한의 종류를 UID 또는 SID에 매칭시켜 저장한다. 사용자는 전용프로그램(11)을 통해 UID 또는 SID에 매칭된 접근 권한의 종류를 변경하거나, 삭제할 수 있다.
- [160] 일 실시 예에 있어서, 사용자인증승인부(260)는 권한 정보에 포함된 접근 권한의 종류에 대응하는 사용자 인증을 수행한다. 가상코드검증장치(200)가 차량인 경우, 사용자인증승인부(260)는 권한 정보에 기반하여 차량 내부 접근 권한, 차량 시동 권한, 차량 운전 권한 중 어느 하나를 부여할 수 있다. 차량 내부 접근 권한이 부여되는 경우, 차량은 차량의 도어락을 해제하고 차량의 다른 기능은 실행되지 않도록 한다. 또한, 차량 시동 권한이 부여되는 경우, 차량은 차량의 도어락을 해제하고, 차량 내부로 들어온 사용자가 시동을 걸 경우 시동이 걸릴 수 있도록 하며, 차량의 시동이 걸린 상태에서 차량이 이동할 수 없도록 한다. 또한, 차량 운전 권한이 부여되는 경우, 차량은 사용자가 차량의 모든 기능을 이용할 수 있도록 한다.
- [161] 다른 일 실시 예에 있어서, 가상코드검증장치(200)가 모바일 단말기인 경우, 사용자는 UID 또는 SID를 가상코드검증장치(200)에 등록할 시에 또는 UID 또는 SID를 가상코드검증장치(200)에 등록한 후에 전용프로그램(11)을 통해 모바일 단말기에서 실행 가능한 애플리케이션을 등록할 수 있다. 이후, 모바일 단말기는 사용자 인증 시 등록된 애플리케이션만 실행될 수 있도록 한다.
- [162] 도 4는 본 발명의 일 실시예에 따른 인증용가상코드를 이용한 사용자 인증 방법의 순서도이다.
- [163] 도 4를 참조하면, 본 발명의 일 실시예에 따른 인증용가상코드를 이용한 사용자 인증 방법은, 가상코드인증장치가 인증용가상코드를 수신하는 단계(S100;

인증용가상코드수신단계), 상기 가상코드인증장치가 상기 인증용가상코드를 기반으로 UID 또는 SID를 탐색하는 단계(S200; 저장위치탐색단계), 가상코드인증장치가 탐색된 상기 UID 또는 SID 저장위치에 매칭되어 저장된 권한 정보를 추출하는 단계(S300), 상기 가상코드인증장치가 상기 인증용가상코드가 수신된 시점을 기반으로 인증용가상코드를 검증하는 단계(S400), 및 가상코드인증장치가 상기 권한 정보에 기반하여 사용자 인증을 승인하는 단계(S500)를 포함한다. 이하, 각 단계에 대한 상세한 설명을 기재한다. 다만, 가상코드생성장치(100)(즉, 전용프로그램이 포함된 사용자 단말) 및 가상코드검증장치(200)(사용자인증수단(30) 또는 서버(40))에 대한 설명 과정에서 상술된 내용에 대한 구체적인 개시는 생략한다.

- [164] 단계 S100에서, 가상코드인증장치(200)는 인증용가상코드를 수신하여 사용자 인증을 요청받는다. 여기서, 인증용가상코드는 UID 또는 SID를 기반으로 인증용가상코드생성용 프로그램에 포함된 인증용가상코드생성함수에 의해 생성되는 것이다.
- [165] 일 실시예에 따라, 인증용가상코드는 가상코드생성장치(100) 내에 포함된 UID 또는 SID를 기반으로 하여 생성될 수 있다.
- [166] 가상코드생성장치(100)는 전용프로그램(11) 내에 포함된 인증용가상코드생성함수를 이용하여 UID 또는 SID를 기반으로 인증용가상코드를 생성하고, 상기 생성된 인증용가상코드를 가상코드검증장치(200)에 제공하게 된다.
- [167] 일 실시예로, 가상코드생성장치(100)는 전용프로그램(11)을 이용하여, UID 또는 SID를 각각의 세부코드생성함수의 시드데이터로 이용하여 각각의 세부코드를 생성할 수 있다.
- [168] 각각의 세부코드생성함수를 이용하여 복수의 세부코드를 생성하면, 가상코드생성장치(100)은 인증용가상코드생성함수에 포함되어 있는 세부코드결합함수를 이용하여 복수의 세부코드가 결합된 인증용가상코드를 생성할 수 있다. 예를 들어, 가상코드생성장치(100)은 전용프로그램(11)을 이용하여, UID 또는 SID를 시드데이터로 이용하여 인증용가상코드를 생성하게 된다.
- [169] 이외에도, 인증용가상코드는 다양한 방식으로 생성될 수 있다. 즉, 인증용가상코드는 다양한 인증용가상코드생성함수에 의해 생성될 수 있다. 다양한 방식으로 인증용가상코드를 생성하는 것에 대한 상세한 설명은 도 5를 참조하여 상술한 설명과 중복되므로 구체적인 개시는 생략한다.
- [170] 이후, 단계 S200에서, 가상코드검증장치(200)가 인증용가상코드를 기반으로 저장위치탐색알고리즘 내에 UID 또는 SID의 저장위치를 탐색한다. 여기서, 저장위치탐색알고리즘은 가상코드생성장치(100)(즉, 사용자 단말)에 내장 또는 설치된 전용프로그램(11) 내에 포함된 인증용가상코드생성함수에 매칭되는 것으로서, 인증용가상코드 내의 적어도 하나의 세부코드를 기반으로 UID 또는

SID의 저장위치를 탐색할 수 있게 한다.

- [171] 가상코드검증장치(200)는 가상코드생성장치(100)을 통해 UID 또는 SID의 등록을 요청받으면, 해당 UID 또는 SID에 대한 저장위치탐색알고리즘 내에 등록 요청된 시점에 해당하는 특정 지점(카운트)에 UID 또는 SID를 등록하고, 해당 지점에 관한 정보를 매칭시켜 저장한다.
- [172] 일 실시 예에 있어서, 각각의 ID에는 별도의 권한 정보가 매칭되어 저장될 수 있다. 사용자는 UID 또는 SID 등록 시 권한 정보를 함께 등록하거나, UID 또는 SID만 먼저 등록한 후 필요에 따라 권한 정보를 업데이트할 수 있다.
- [173] 다른 일 실시 예에 있어서, UID에는 별도의 권한 정보가 매칭되어 저장되지 않을 수 있고, 적어도 하나의 SID는 UID의 저장위치에 매칭되어 저장되며, 적어도 하나의 SID 각각에는 권한 정보가 매칭되어 저장될 수 있다. 가상코드검증장치(200)는 특정 ID에 매칭되어 저장된 권한 정보가 없는 경우, 인증용가상코드가 유효한 것으로 검증되기만 하면 사용자 인증을 수행할 수 있다.
- [174] 사용자는 인증용가상코드 생성시 가상코드 생성의 시드 데이터가 되는 ID를 선택할 수 있다. 사용자는 UID에 기반하여 인증용가상코드를 생성함으로써 사용자인증수단(30)에 대한 무조건적인 접근 권한을 부여받거나, 타인에게 부여할 수 있다. 다만, 상기 인증용가상코드는 일정 시간이 지날 경우 사용할 수 없게 된다.
- [175] 또한, 사용자는 SID에 기반하여 인증용가상코드를 생성함으로써, 제한적인 접근 권한을 타인에게 부여할 수 있다. 예를 들어, 사용자는 SID에 매칭되어 저장되는 접근 가능 시간을 등록하고, 해당 SID에 기반하여 인증용가상코드를 생성함으로써, 타인에게 사용자인증수단(30)에 대한 접근 가능 시간을 제한할 수 있다. 상기 인증용가상코드는 접근 가능 시간 이후 사용할 수 없게 된다.
- [176] 다른 예를 들어, 사용자는 SID에 매칭되어 저장되는 접근 권한의 종류를 등록하고, 해당 SID에 기반하여 인증용가상코드를 생성함으로써, 타인에게 사용자인증수단(30)에 대한 접근 권한의 종류를 제한할 수 있다.
- [177] UID 또는 SID가 가상코드검증장치(200)에 등록된 후, 가상코드검증장치(200)는 가상코드생성장치(100)을 통해 인증용가상코드를 수신하고, 사용자 인증을 요청받으면, 상기 수신된 인증용가상코드를 기반으로 저장위치탐색알고리즘 내에 저장된 UID 또는 SID를 탐색하여 사용자를 확인할 수 있게 된다.
- [178] 일 실시예에 따라, 인증용가상코드가 제1코드와 제2코드의 결합으로 생성된 경우, 서버(30)는 제1코드와 제2코드를 이용하여 저장위치탐색알고리즘 내에서 UID 또는 SID 저장위치를 탐색하게 된다. 예를 들어, 제1코드는 저장위치탐색알고리즘 내에서 UID 또는 SID의 저장위치탐색의 시작지점을 설정하는 코드이고, 제2코드는 특정한 탐색방식에 따라 시작지점으로부터 UID 또는 SID 저장위치로의 탐색경로를 설정하는 코드일 수 있다.

- [179] 도 5에 도시된 바와 같이, 가상코드검증장치(200)는 제1코드에 대응하는 위치를 시작지점으로 설정하고, 제2코드에 적용된 탐색방식에 따라 제2코드를 기반으로 k각형의 배치상태에서의 UID 또는 SID 저장위치에 매칭된 지점(즉, k각형의 특정한 꼭지점)을 탐색한다. 저장위치는 k각형의 각각의 꼭지점에 매칭된다. 제1코드 트랙(즉, 제1트랙)과 k각형이 대응되는 지점이 제1코드에 대응하는 저장위치 탐색시작지점이 된다. 가상코드검증장치(200)는 탐색시작지점에서 제2코드를 기반으로 UID 또는 SID 저장위치의 매칭지점을 탐색한다.
- [180] 제2코드를 기반으로 k각형에서 저장위치를 탐색하는 방식으로는 다양한 방식이 적용될 수 있다. 일 예로, 가상코드검증장치(200)는 k각형이 접한 제1트랙 상의 위치에서 제2코드에 상응하는 각도(예를 들어, k각형의 꼭지점을 향하도록 180도를 MN개로 분할한 특정한 각도)로 지시함에 따라, 인증용가상코드를 기반으로 UID 또는 SID가 저장된 저장위치인 k각형의 꼭지점을 탐색할 수 있다.
- [181] 또한, 다른 예로, k각형이 제1트랙 상의 제1코드에 대응하는 지점에 접한 상태에서, 가상코드검증장치(200)는 k각형의 중심과 제1트랙 상의 접점을 기준으로, 전체 중심각(즉, 360도)을 MN개로 분할하고, 각각의 각도를 MN개의 제2코드에 매칭한다. 이때, k각형의 중심과 제1트랙 상의 접점을 이은 선으로부터 특정개수의 단위각도(즉, 360도/MN)를 이동한 선의 방향은 k각형의 특정한 꼭지점이 된다. 따라서, 특정한 각도에 대응하는 제2코드가 수신되면, 가상코드검증장치(200)는 해당 각도 방향에 위치한 꼭지점을 탐색할 수 있다.
- [182] 또한, 다른 예로, 제2코드의 특정 자리를 각도산출 방향을 결정하는 것으로 사용할 수 있다. 즉, N개(N은 자연수)의 문자를 이용하여 제2코드를 생성하는 경우, 1개의 자리(Digit)로 각도 측정방향을 결정할 수 있다. 예를 들어, 가상코드검증장치(200)는 k각형의 중심과 제1트랙 상의 접점을 기준으로, 전체 중심각(즉, 360도)을 분할하여 각각의 각도에 제2코드를 매칭하는 경우, k각형의 중심과 제1트랙 상의 접점을 이은 선으로부터 좌측 방향으로 측정되는 각도인지 우측 방향으로 측정되는 각도인지를 1개의 자리(Digit)의 값으로 결정할 수 있다.
- [183] 일 예로, 저장위치탐색알고리즘은, k각형 상의 각 꼭지점에 각도 측정방향에 따라 다른 2개의 제2코드가 하나의 꼭지점에 배정할 수 있다. 즉, 하나의 꼭지점에 내각으로 도달 시와 외각으로 도달 시에 다른 제2코드와 매칭되고, 다른 UID 또는 SID의 저장위치가 연결될 수 있다. 다른 일 예로, 저장위치탐색알고리즘은, N개(N은 자연수)의 문자를 이용하여 제2코드를 생성하는 경우에 N-1개로 전체각도(예를 들어, 중심각을 기준으로 분할하는 경우 360도)의 반에 대해 매칭하고 1개 자리를 이용하여 각 꼭지점에 도달하기 위한 각도 적용방향을 결정할 수 있다.
- [184] 제2코드를 기반으로 k각형에서 저장위치를 탐색하는 방식은 이에 한정되지 아니하고, 제2코드에 상응하는 k각형 상의 지점과 제1트랙 상의 접점 사이를 특정한 비율로 나누는 지점을 저장위치로 탐색하는 방식 등의 다양한 방식이

적용될 수 있다.

- [185] 다른 일 실시예에 따라, 인증용가상코드가 단위카운트마다 변경되는 제1코드 및 제2코드를 포함하는 경우, 제1코드는 가상코드검증장치(200)에서 UID 또는 SID 등록을 시작한 최초시점으로부터 경과된 단위카운트를 기반으로 생성되고, 제2코드는 각 사용자가 가상코드생성장치(10)에 설치된 전용프로그램(11)을 통해 UID 또는 SID를 등록한 시점으로부터 경과된 단위카운트를 기반으로 생성되는 것이다. 이때, 단위카운트는 특정한 시간간격으로 설정되어 시간간격이 경과됨에 따라 변경되는 것이다.
- [186] 도 7에 도시된 바와 같이, 저장위치탐색알고리즘은 인증용가상코드를 구성하는 복수의 세부코드를 기반으로 트랙상을 이동하여 UID 또는 SID의 저장위치에 매칭된 지점으로 이동하는 것이다.
- [187] 구체적으로, 인증용가상코드가 서비스를 구동함에 따라 저장위치탐색알고리즘이 시작된 초기시점으로부터 경과된 단위카운트를 기반으로 제1코드와, 각 사용자의 UID 또는 SID가 등록된 시점으로부터 경과된 단위카운트를 기반으로 생성된 제2코드를 포함하는 경우, 도 7에서와 같이, 가상코드검증장치(200)는 제1코드에 대응되는 코드값이 매칭된 트랙상의 카운트를 탐색시작지점으로 설정하고, 제2코드에 상응하는 카운트값만큼 상기 탐색시작지점으로부터 트랙을 따라서 회귀하여 가상코드검증장치(200)에 UID 또는 SID를 등록한 시점의 트랙상의 지점(즉, UID 또는 SID 저장위치)을 탐색한다. 예를 들어, 가상코드검증장치(200)가 제1코드용 트랙에서 인증용가상코드 내의 제1코드가 부여된 지점(또는 카운트)를 탐색하여 탐색시작지점을 설정하고, 탐색시작지점으로부터 역방향으로 제2코드용 트랙을 배치하여 인증용가상코드 내의 제2코드가 부여된 지점(또는 카운트)를 탐색하여 제1코드용 트랙 상에서 UID 또는 SID가 등록된 지점(또는 카운트)를 추출한다. 또한, 예를 들어, 가상코드검증장치(200)가 인증용가상코드 내의 제1코드를 기반으로 탐색시작지점을 설정하고, 인증용가상코드 내의 제2코드에 제2함수의 역함수를 적용함에 따라 산출된 카운트값만큼 회귀하여 UID 또는 SID 등록시점에 대응되는 지점을 탐색한다.
- [188] 이후, 단계 S300에서, 가상코드검증장치(200)는 탐색된 상기 UID 또는 SID 저장위치에 매칭되어 저장된 권한 정보를 추출한다.
- [189] 구체적으로, 가상코드검증장치(200)는 탐색된 UID 또는 SID의 저장위치에 매칭되어 저장된 권한 정보를 추출한다. 즉, 가상코드검증장치(200)는 저장위치탐색알고리즘 내의 각각의 UID 또는 SID 저장위치에 관한 정보를 저장하고 있으므로, 가상코드검증장치(200)는 저장위치탐색알고리즘 내에서 특정 UID 또는 SID의 저장위치에 매칭되어 저장된 권한 정보를 추출할 수 있다.
- [190] 한편, UID 또는 SID 등록 시, 사용자의 설정방식에 따라, UID 또는 SID의 저장위치에 어떠한 권한 정보도 매칭되지 않을 수 있다. 예를 들어, 사용자는 전용프로그램(11)을 통해, UID 또는 SID를 등록한 후 어떠한 권한 정보도

등록하지 않을 수 있다. 또한, 도 9와 같이, 가상코드생성장치(100) 및 가상코드수신장치(200)는 UID 저장위치에 권한 정보를 매칭시켜 저장하지 않고, SID는 UID 저장위치에 매칭되어 저장되며, 각각의 SID 저장위치에는 권한 정보가 매칭되어 저장될 수 있다.

- [191] 이후, 단계 S400에서, 가상코드수신장치(200)가 상기 인증용가상코드가 수신된 시점을 기반으로 인증용가상코드를 검증한다. 구체적으로, 가상코드수신장치(200)는 수신된 상기 인증용가상코드의 수신 시점과 상기 인증용가상코드생성용 프로그램에서 인증용가상코드생성함수를 이용하여 생성된 상기 인증용가상코드의 생성 시점을 비교하여, 도 6에 도시된 바와 같이, 상기 생성 시점이 상기 수신 시점으로부터 오차 범위 내에 포함된 경우 수신된 상기 인증용가상코드가 정상 코드인 것으로 판단할 수 있다.
- [192] 일 실시예로, 출입 요청시 사용자 인증을 수행하는 경우, 가상코드수신장치(200)는 저장위치탐색알고리즘 내에서 인증용가상코드의 수신 시점과 생성 시점을 비교함으로써, 출입요청시 사용자 인증을 요청한 사용자가 권한 부여자의 UID 또는 SID를 이용해 현재 시점에 사용자 인증을 요청했는지의 여부를 확인할 수 있다.
- [193] 구체적인 실시 예로, 사용자가 가상코드생성장치(100)를 이용하여 인증용가상코드 생성을 요청하면, 전용프로그램(11)은 인증용가상코드생성함수를 이용하여 요청 시점(즉, 생성 시점)에 해당하는 카운트 값을 기반으로 인증용가상코드(구체적으로, 제2코드)를 생성한다. 일 실시예로, 복수의 세부코드 중 하나의 세부코드(예를 들어, 제2코드)는 생성 시점을 시드 데이터로 하는 OTP 함수를 이용하여 생성될 수 있다. 즉, 제2코드 내에 OTP 코드가 포함되어 생성될 수 있다.
- [194] 이후, 생성된 인증용가상코드는 가상코드검증장치(200)로 제공되며, 가상코드검증장치(200)는 인증용가상코드생성함수 또는 인증용가상코드생성함수에 매칭되는 저장위치탐색알고리즘을 이용하여 복수의 세부코드를 추출한다. 그리고, 복수의 세부코드 중 하나의 세부코드(예를 들어, 제2코드)를 통해 OTP 코드를 추출하고, OTP 코드를 통해 인증용가상코드가 생성된 시점을 추출하게 된다.
- [195] 이후, 트랙 상에서 가상코드검증장치(200)가 인증용가상코드를 수신한 시점과 가상코드생성장치(100)에서 인증용가상코드가 생성된 시점을 비교하여, 인증용가상코드가 현재 시점에 생성된 코드인지를 검증할 수 있게 된다. 즉, 가상코드검증장치(200)가 인증용가상코드를 수신한 시점으로부터 기 설정된 카운트 값을 포함하는 범위 내에 인증용가상코드의 생성 시점이 포함되면, 해당 인증용가상코드는 현재 시점에 생성된 코드인 것으로 검증되는 것이다.
- [196] 한편, UID 또는 SID 저장위치에 매칭되어 저장된 권한 정보가 접근 가능 시간 정보를 포함하는 경우, 가상코드검증부(250)는 상기 접근 가능 시간 정보에 근거하여 인증용가상코드의 정상 여부를 판단할 수 있다. 구체적으로,

가상코드검증부(250)는 인증용가상코드의 수신 시점이 상기 접근 가능 시간 정보가 정의하는 시간대에 있는 경우, 수신된 인증용가상코드가 정상인 것으로 판단할 수 있다. 이 경우, 인증용가상코드가 상기 접근 가능 시간 정보가 정의하는 시간대 이전에 생성되었다라도 상기 인증용가상코드는 상기 접근 가능 시간 정보가 정의하는 시간대에서만 유효하게 사용될 수 있다.

- [197] 단계 S500에서, 가상코드수신장치(200)는 인증용가상코드가 정상적인 코드인 것으로 판단되면, UID 또는 SID 저장위치에 매칭되어 저장된 권한 정보를 기반으로 사용자 인증을 수행한다.
- [198] 일 실시 예에 있어서, UID 또는 SID 저장위치에 접근 가능 시간 정보가 매칭되어 저장된 경우, 가상코드수신장치(200)는 수신된 인증용가상코드의 수신 시점과 접근 가능 시간 정보에 대응하는 시간대를 비교하여 사용자 인증을 수행한다. 구체적으로, 가상코드수신장치(200)는 상기 수신 시점이 접근 가능 시간 정보에 대응하는 시간대에 있는 경우에만 사용자 인증을 수행한다.
- [199] 한편, 가상코드수신장치(200)는 인증용가상코드에서 추출된 ID가 UID인 경우, 인증용가상코드가 정상적인 코드인 것으로 판단되면, UID의 저장위치에 매칭되어 저장된 권한 정보에 관계없이 사용자 인증을 수행할 수 있다. 가상코드수신장치(200)는 아이디 생성 규칙, ID의 저장위치에 매칭되어 저장된 다른 ID가 있는지 여부에 기반하여 인증용가상코드로부터 추출된 ID가 UID인지 여부를 판단할 수 있다.
- [200] 한편, 가상코드수신장치(200)는 인증용가상코드에서 추출된 ID의 저장위치에 매칭되어 저장된 권한 정보가 없는 경우, 인증용가상코드가 정상적인 코드인 것으로 판단되면, 사용자 인증을 수행할 수 있다.
- [201] 또한, 가상코드수신장치(200)는 사용자 인증을 통해 접근 권한을 부여한다. 가상코드수신장치(200)가 차량인 경우, 접근 권한은 차량 내부 출입 권한일 수 있으며, 차량 내부 출입 권한이 부여될 경우, 차량은 차량의 도어락을 해제하여 사용자가 차량 내부로 진입할 수 있도록 한다.
- [202] 다른 일 실시 예에 있어서, 가상코드수신장치(200)가 도어락인 경우, 접근 권한은 건물 내부 출입 권한일 수 있으며, 건물 내부 출입 권한이 부여될 경우, 차량은 차량의 도어락을 해제하여 사용자가 차량 내부로 진입할 수 있도록 한다.
- [203] 다른 일 실시 예에 있어서, 가상코드수신장치(200)가 모바일 단말기인 경우, 접근 권한은 모바일 단말기의 사용 권한일 수 있으며, 모바일 단말기의 사용 권한이 부여될 경우, 모바일 단말기는 단말기 잠금 상태를 해제하여 사용자가 모바일 단말기에 내장된 기능을 이용할 수 있는 상태가 된다.
- [204] 한편, 가상코드수신장치(200)는 접근 권한을 단계적으로 부여할 수 있다. 일 실시 예에 있어서, 가상코드수신장치(200)가 차량인 경우, 차량에 대한 접근 권한은 차량 내부 접근 권한, 차량 시동 권한, 차량 운전 권한을 포함할 수 있다. 차량 시동 권한은 차량의 시동을 걸어 차량 내 구비된 장치들을 이용할 수는 있지만, 차량의 운전을 할 수 없는 권한으로 해당 권한만 부여받은 경우, 차량은

이동하지 않는다. 또한, 차량 운전 권한은 차량 운전을 포함한 차량의 모든 기능을 사용할 수 있는 권한이다. 사용자는 타인에게 상술한 종류의 권한을 선택적으로 부여할 수 있다.

- [205] 다른 일 실시 예에 있어서, 가상코드수신장치(200)가 모바일 단말기인 경우, 접근 권한은 모바일 단말기에 구비된 애플리케이션 별로 부여될 수 있다. 예를 들어, 사용자는 모바일 단말기에 구비된 카메라 애플리케이션에 대한 접근 권한만 타인에게 부여할 수 있다.
- [206] 이상에서 전술한 본 발명의 일 실시예에 따른 인증용가상코드를 이용한 사용자 인증 방법은, 하드웨어인 컴퓨터와 결합되어 실행되기 위해 프로그램(또는 어플리케이션)으로 구현되어 매체에 저장될 수 있다.
- [207] 상기 전술한 프로그램은, 상기 컴퓨터가 프로그램을 읽어 들여 프로그램으로 구현된 상기 방법들을 실행시키기 위하여, 상기 컴퓨터의 프로세서(CPU)가 상기 컴퓨터의 장치 인터페이스를 통해 읽힐 수 있는 C, C++, JAVA, Ruby, 기계어 등의 컴퓨터 언어로 코드화된 코드(Code)를 포함할 수 있다. 이러한 코드는 상기 방법들을 실행하는 필요한 기능들을 정의한 함수 등과 관련된 기능적인 코드(Functional Code)를 포함할 수 있고, 상기 기능들을 상기 컴퓨터의 프로세서가 소정의 절차대로 실행시키는데 필요한 실행 절차 관련 제어 코드를 포함할 수 있다. 또한, 이러한 코드는 상기 기능들을 상기 컴퓨터의 프로세서가 실행시키는데 필요한 추가 정보나 미디어가 상기 컴퓨터의 내부 또는 외부 메모리의 어느 위치(주소 번지)에서 참조되어야 하는지에 대한 메모리 참조관련 코드를 더 포함할 수 있다. 또한, 상기 컴퓨터의 프로세서가 상기 기능들을 실행시키기 위하여 원격(Remote)에 있는 어떠한 다른 컴퓨터나 서버 등과 통신이 필요한 경우, 코드는 상기 컴퓨터의 통신 모듈을 이용하여 원격에 있는 어떠한 다른 컴퓨터나 서버 등과 어떻게 통신해야 하는지, 통신 시 어떠한 정보나 미디어를 송수신해야 하는지 등에 대한 통신 관련 코드를 더 포함할 수 있다.
- [208] 상기 저장되는 매체는, 레지스터, 캐쉬, 메모리 등과 같이 짧은 순간 동안 데이터를 저장하는 매체가 아니라 반영구적으로 데이터를 저장하며, 기기에 의해 판독(reading)이 가능한 매체를 의미한다. 구체적으로는, 상기 저장되는 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있지만, 이에 제한되지 않는다. 즉, 상기 프로그램은 상기 컴퓨터가 접속할 수 있는 다양한 서버 상의 다양한 기록매체 또는 사용자의 상기 컴퓨터상의 다양한 기록매체에 저장될 수 있다. 또한, 상기 매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장될 수 있다.
- [209] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수

있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.

청구범위

- [청구항 1] 가상코드검증수단이 인증용가상코드를 수신하는 단계-상기 인증용가상코드는, 상기 가상코드검증수단에 등록된 가상코드생성수단에 포함된 인증용가상코드생성함수에 의해 생성됨-; 상기 가상코드검증수단이 상기 인증용가상코드를 기반으로 UID(User Identification) 또는 SID(sub-identification)의 저장위치를 탐색하는 단계; 상기 가상코드검증수단이 상기 탐색된 UID 또는 SID에 매칭되어 저장된 권한 정보를 추출하는 단계; 상기 가상코드검증수단이 상기 인증용가상코드가 수신된 시점을 기반으로 인증용가상코드를 검증하는 단계; 및 상기 가상코드검증수단이 상기 추출된 권한 정보를 기반으로 사용자 인증을 수행하는 단계를 포함하는, 인증용가상코드를 이용한 사용자 인증 방법.
- [청구항 2] 제1 항에 있어서, 상기 수신 단계는, 상기 가상코드생성수단이 인증용가상코드를 생성하는 단계; 상기 가상코드생성수단이 상기 생성된 인증용가상코드를 가상코드수신수단으로 송신하는 단계; 및 상기 가상코드검증수단이 상기 가상코드수신수단으로부터 상기 인증용가상코드를 수신하는 단계;를 포함하는 것인, 인증용가상코드를 이용한 사용자 인증 방법.
- [청구항 3] 제2 항에 있어서, 상기 인증용가상코드를 수신하기 이전에, 상기 가상코드생성수단이 UID 또는 SID에 매칭되는 접근 가능 시간 정보를 상기 가상코드검증수단으로 송신하는단계; 및 상기 가상코드검증수단이 상기 수신된 접근 가능 시간 정보를 상기 UID 또는 SID에 매칭시켜 저장하는 단계;를 더 포함하는, 인증용가상코드를 이용한 사용자 인증방법.
- [청구항 4] 제3 항에 있어서, 상기 수행 단계는, 상기 가상코드검증수단이 상기 UID 또는 SID의 저장위치에 매칭되어 저장된 접근 가능 시간 정보를 추출하는 단계;를 포함하고, 상기 가상코드검증수단은, 상기 인증용가상코드가 상기 추출된 접근 가능 시간 정보에 대응하는 시간 범위에 수신된 경우에만 사용자 인증을 수행하는, 인증용가상코드를 이용한 사용자 인증방법.
- [청구항 5] 제1 항에 있어서, 상기 검증 단계는, 상기 가상코드검증수단이 상기 인증용가상코드의 생성 시점이 상기 인증용가상코드의 수신 시점으로부터 오차 범위 내에 포함된 경우에,

- 상기 인증용가상코드가 정상 코드인 것으로 판단하는 단계;를 포함하는, 인증용가상코드를 이용한 사용자 인증 방법.
- [청구항 6] 제5 항에 있어서, 상기 검증 단계는, 상기 UID 또는 SID의 저장위치에 접근 가능 시간 정보가 매칭되어 저장된 상태이고, 상기 수신 시점이 상기 접근 가능 시간 정보에 대응하는 시간대에 속한 경우에, 상기 가상코드검증수단이 상기 인증용가상코드가 정상 코드인 것으로 판단하는 단계;를 포함하는, 인증용가상코드를 이용한 사용자 인증 방법.
- [청구항 7] 제1 항에 있어서, 상기 수행 단계는, 상기 가상코드검증수단이 상기 인증용가상코드에서 UID를 추출하는 단계; 및 상기 인증용가상코드가 검증된 인증용가상코드인 경우, 상기 추출된 UID의 저장위치에 매칭되어 저장된 권한 정보에 관계없이 사용자 인증을 수행하는 단계;를 포함하는, 인증용가상코드를 이용한 사용자 인증 방법.
- [청구항 8] 제2 항에 있어서, 상기 인증용가상코드를 수신하기 이전에, 상기 가상코드생성수단이 UID 또는 SID에 매칭되는 접근 권한의 종류를 상기 가상코드검증수단으로 송신하는 단계; 및 상기 가상코드검증수단이 상기 수신된 접근 권한의 종류를 상기 UID 또는 SID에 매칭시켜 저장하는 단계;를 더 포함하는, 인증용가상코드를 이용한 사용자 인증 방법.
- [청구항 9] 제8 항에 있어서, 상기 수행 단계는, 상기 가상코드검증수단이 상기 UID 또는 SID의 저장위치에 매칭되어 저장된 접근 권한의 종류를 추출하는 단계를 포함하고, 상기 가상코드검증수단은 상기 인증용가상코드가 상기 접근 권한의 종류에 대응하는 사용자 인증을 수행하는, 인증용가상코드를 이용한 사용자 인증 방법.
- [청구항 10] 하드웨어인 컴퓨터와 결합되어, 제1항 내지 제9항 중 어느 한 항의 방법을 실행시키기 위하여 매체에 저장된, 인증용가상코드를 이용한 사용자 인증 프로그램.
- [청구항 11] 사용자 인증을 위한 가상코드생성장치로서, 상기 가상코드생성장치에 등록된 UID(User Identification) 또는 SID(sub-identification)를 기반으로 하나 이상의 세부코드를 생성하는 세부코드생성부; 인증용가상코드생성함수를 이용하여 상기 하나 이상의 세부코드를 조합한 인증용가상코드를 생성하는 가상코드생성부; 및 가상코드수신수단을 통해 가상코드검증장치에 대한 사용자 인증을

수행하도록, 상기 생성된 인증용가상코드를 가상코드수신장치로 전송하는 인증용가상코드제공부;를 포함하는, 사용자 인증을 위한 인증용가상코드생성장치.

- [청구항 12] 사용자 인증을 위한 가상코드검증장치로서,
 인증용가상코드를 수신하는 가상코드수신부;
 상기 인증용가상코드에서 세부코드를 추출하는 세부코드추출부;
 상기 세부코드를 기반으로 기반으로 UID(User Identification) 또는 SID(sub-identification)의 저장위치를 탐색하는 저장위치탐색부;
 상기 탐색된 UID 또는 SID에 매칭되어 저장된 권한 정보를 추출하는 권한정보추출부;
 상기 인증용가상코드가 수신된 시점을 기반으로 인증용가상코드를 검증하는 가상코드검증부; 및
 상기 추출된 권한 정보를 기반으로 사용자 인증을 수행하는 사용자인증승인부를 포함하는, 사용자 인증을 위한 인증용가상코드검증장치.
- [청구항 13] 제12 항에 있어서,
 상기 인증용가상코드검증장치는, 차량 또는 도어락을 포함하는, 사용자 인증을 위한 인증용가상코드검증장치.
- [청구항 14] 제13 항에 있어서,
 상기 인증용가상코드검증장치가 차량인 경우, 상기 가상코드생성장치로부터 상기 UID 또는 SID와 UID 또는 SID에 매칭되는 접근 권한의 종류를 수신하고, 상기 접근 권한의 종류를 상기 UID 또는 SID에 매칭시켜 저장하고,
 상기 접근 권한의 종류는, 차량 내부 접근 권한, 차량 시동 권한 및 차량 운전 권한을 포함하는, 사용자 인증을 위한 인증용가상코드검증장치.
- [청구항 15] 제14 항에 있어서, 상기 사용자인증승인부는,
 상기 UID 또는 SID의 저장위치에 매칭되어 저장된 접근 권한의 종류를 추출하고,
 상기 추출된 접근 권한의 종류에 따라 상기 차량 내부 접근 권한, 상기 차량 시동 권한 및 상기 차량 운전 권한 중 어느 하나를 부여하여 사용자 인증을 수행하는, 사용자 인증을 위한 인증용가상코드검증장치.