(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년07월06일
(11) 등록번호 10-1636068
(24) 등록일자 2016년06월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *H04L 9/08* (2006.01)
(52) CPC특허분류
H04L 9/3228 (2013.01)
H04L 9/0869 (2013.01)
(21) 출원번호 10-2015-0137066(분할)
(22) 출원일자 2015년09월25일
심사청구일자 2015년09월25일
(65) 공개번호 10-2015-0118566
(43) 공개일자 2015년10월22일
(62) 원출원 특허 10-2009-0063255
원출원일자 2009년07월10일
심사청구일자 2014년07월10일
(56) 선행기술조사문헌
KR1020080075956 A*
KR1020090051147 A*
KR1020070084801 A
KR100715651 B1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 비즈모델라인
서울특별시 마포구 와우산로 77, 6층 (서교동, 대창빌딩)
(72) 발명자
김재형
서울특별시 강남구 압구정로 313, 42동 302호 (압구정동, 한양아파트)
권봉기
경기도 안양시 동안구 시민대로 287 1214호 (관양동,동양그라테아)

전체 청구항 수 : 총 4 항 심사관 : 양종필

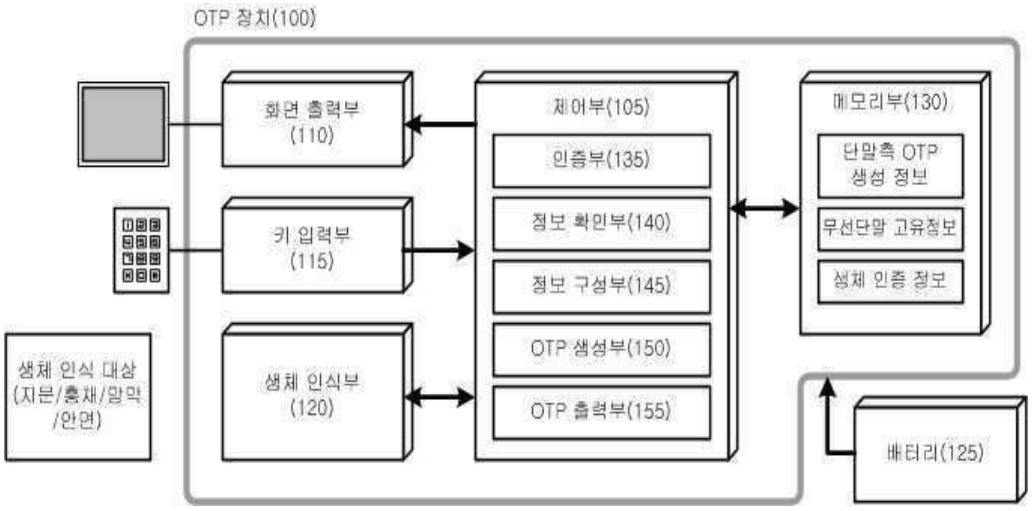
(54) 발명의 명칭 **생체 인식을 이용한 오티피 운영 방법**

(57) 요 약

본 발명의 생체 인식을 이용한 오티피 운영 방법에 따르면, OTP(One Time Password)를 생성하는 장치에서 실행되는 방법에 있어서, 사용자의 생체를 인증하기 위한 생체 인증 정보를 상기 장치의 지정된 저장영역에 암호화 저장하고 OTP를 생성하기 위한 고정 씨드 값을 상기 장치의 지정된 저장영역에 암호화 저장하고, 상기 장치에 구비

(뒷면에 계속)

대 표 도 - 도1



된 생체 인식부를 통해 인식된 생체 인식 정보를 확인하고, 상기 생체 인증 정보를 통해 상기 생체 인식 정보에 대응하는 사용자의 생체를 인증하는 절차를 수행하고, 상기 사용자의 생체가 인증된 경우 상기 장치의 지정된 저장영역에 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 구성하며, 상기 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 상기 장치에 구비된 코드생성알고리즘에 대입하여 OTP를 동적 생성한다.

(52) CPC특허분류
H04L 9/3231 (2013.01)

명 세 서

청구범위

청구항 1

OTP(One Time Password)를 생성하는 장치에서 실행되는 방법에 있어서,

사용자의 생체를 인증하기 위한 생체 인증 정보를 상기 장치의 지정된 저장영역에 암호화 저장하고 OTP를 생성하기 위한 고정 씨드 값을 상기 장치의 지정된 저장영역에 암호화 저장하는 제1 단계;

상기 장치에 구비된 생체 인식부를 통해 인식된 생체 인식 정보를 확인하는 제2 단계;

상기 생체 인증 정보를 통해 상기 생체 인식 정보에 대응하는 사용자의 생체를 인증하는 절차를 수행하는 제3 단계;

상기 사용자의 생체가 인증된 경우 상기 장치의 지정된 저장영역에 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 구성하는 제4 단계;

상기 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 상기 장치에 구비된 코드생성알고리즘에 대입하여 OTP를 동적 생성하는 제5 단계;를 포함하는 생체 인식을 이용한 오티피 운영 방법.

청구항 2

제 1항에 있어서, 상기 제4 단계는,

상기 사용자의 생체가 인증된 경우 상기 사용자의 생체 인증에 성공한 생체 인식 정보를 상기 코드 생성알고리즘에 대입할 씨드 값 구조로 가공하는 단계를 포함하여 이루어지는 것을 특징으로 하는 생체 인식을 이용한 오티피 운영 방법.

청구항 3

제 1항에 있어서,

상기 OTP를 동적 생성한 경우, 상기 장치의 근거리 통신수단을 통해 상기 생성된 OTP를 근거리의 단말 또는 장치로 출력하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 생체 인식을 이용한 오티피 운영 방법.

청구항 4

제 1항에 있어서, 상기 사용자의 생체는,

사용자의 지문, 홍채, 망막, 안면 중 적어도 하나를 포함하여 이루어지는 것을 특징으로 하는 생체 인식을 이용한 오티피 운영 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은, OTP(One Time Password)를 생성하는 장치에서 실행되는 방법에 있어서, 사용자의 생체를 인증하기 위한 생체 인증 정보를 상기 장치의 지정된 저장영역에 암호화 저장하고 OTP를 생성하기 위한 고정 씨드 값을 상기 장치의 지정된 저장영역에 암호화 저장하고, 상기 장치에 구비된 생체 인식부를 통해 인식된 생체 인식 정

보를 확인하고, 상기 생체 인증 정보를 통해 상기 생체 인식 정보에 대응하는 사용자의 생체를 인증하는 절차를 수행하고, 상기 사용자의 생체가 인증된 경우 상기 장치의 지정된 저장영역에 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 구성하며, 상기 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 상기 장치에 구비된 코드생성알고리즘에 대입하여 OTP를 동적 생성하는 생체 인식을 이용한 오티피 운영 방법에 관한 것이다.

배 경 기 술

[0003] 정보통신 기술의 발전으로 통신망을 이용한 비대면 거래가 활성화되면서, 비대면 거래 제공자는 통신망을 통해 연결된 사용자가 유효한 거래자인지 인증하여 만약에 발생할 수도 있는 거래사고에 대비해야 한다.

[0005] 상기와 같은 비대면 거래에서 통신망을 통해 연결된 사용자를 인증하는 가장 보편적인 방식으로는 ID/PW를 이용하여 인증하는 방식이 사용되고 있으나, 상기 ID/PW는 쉽게 노출되는 문제점으로 인해 비대면 거래 인증용으로 사용되기 보다는 거래자를 식별하는 용도로 사용되고 있다.

[0007] 상기 ID/PW를 이용하는 방식보다 더 고도한 비대면 거래 인증 방식으로는, 공인인증서를 이용한 인증 방식이 사용되는데, 상기 공인인증서가 기록되어 있는 매체(예컨대, 컴퓨터)가 해킹되거나, 키보드 해킹 프로그램이 설치된 단말을 통해 비대면 거래를 처리하는 경우, 상기 공인인증서 역시 신뢰할 수 있는 정도의 비대면 거래 인증을 제공하지는 못하는 문제점을 지니고 있다.

[0009] 상기와 같은 공인인증서의 문제점을 해소하기 위한 방법으로 일회용 비밀번호(One Time Password; OTP)가 사용되고 있다. 상기 OTP는 하나 이상의 고정 씨드 값과 비밀번호를 생성하는 시점에 동적으로 결정하는 고정 씨드 값을 비대면 거래 당사자가 교환/공유한 후, 각각의 거래 당사자가 비대면 인증 시점에 확인/결정되는 고정 씨드 값과 동적 씨드 값을 기 설정된 코드 생성 알고리즘(예컨대, 해시 함수)에 대입하여 한번 사용 가능한 OTP를 생성하고, 상기 생성된 OTP를 교환 및 인증하는 것으로, 설령 상기 OTP가 노출되더라도 동일한 OTP를 재사용할 수 없으므로, 다른 인증수단에 비해 해킹에 안전한 인증수단으로 사용되고 있다.

발명의 내용

해결하려는 과제

[0011] 본 발명의 목적은, OTP(One Time Password)를 생성하는 장치에서 실행되는 방법에 있어서, 사용자의 생체를 인증하기 위한 생체 인증 정보를 상기 장치의 지정된 저장영역에 암호화 저장하고 OTP를 생성하기 위한 고정 씨드 값을 상기 장치의 지정된 저장영역에 암호화 저장하는 제1 단계와 상기 장치에 구비된 생체 인식부를 통해 인식된 생체 인식 정보를 확인하는 제2 단계와 상기 생체 인증 정보를 통해 상기 생체 인식 정보에 대응하는 사용자의 생체를 인증하는 절차를 수행하는 제3 단계와 상기 사용자의 생체가 인증된 경우 상기 장치의 지정된 저장영역에 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 구성하는 제4 단계와 상기 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 상기 장치에 구비된 코드생성알고리즘에 대입하여 OTP를 동적 생성하는 제5 단계를 포함하는 생체 인식을 이용한 오티피 운영 방법을 제공함에 있다.

과제의 해결 수단

[0013] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법은, OTP(One Time Password)를 생성하는 장치에서 실행되는 방법에 있어서, 사용자의 생체를 인증하기 위한 생체 인증 정보를 상기 장치의 지정된 저장영역에 암호화 저장하고 OTP를 생성하기 위한 고정 씨드 값을 상기 장치의 지정된 저장영역에 암호화 저장하는 제1 단계와 상기 장치에 구비된 생체 인식부를 통해 인식된 생체 인식 정보를 확인하는 제2 단계와 상기 생체 인증 정보를 통해 상기 생체 인식 정보에 대응하는 사용자의 생체를 인증하는 절차를 수행하는 제3 단계와 상기 사용자의 생체가 인증된 경우 상기 장치의 지정된 저장영역에 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 구성하는 제4 단계와 상기 저장된 고정 씨드 값과 상기 사용자의 생체 인증에 성공한 생체 인식 정보에 대응하는 씨드 값과 상기 사용자의 생체를 인증한 시점의 시간 값을 포함하는 씨드를 상기 장치에 구비된 코드생성알고리즘에 대입하여 OTP를 동적 생성하는 제5 단계를 포함하는 것을 특징으로 한다.

[0014] 삭제

[0015] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 제4 단계는, 상기 사용자의 생체가 인증된 경우 상기 사용자의 생체 인증에 성공한 생체 인식 정보를 상기 코드 생성알고리즘에 대입할 씨드 값 구조로 가공하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0016] 삭제

[0017] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 OTP를 동적 생성한 경우, 상기 장치의 근거리 통신수단을 통해 상기 생성된 OTP를 근거리의 단말 또는 장치로 출력하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0019] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 사용자의 생체는, 사용자의 지문, 홍채, 망막, 안면 중 적어도 하나를 포함하여 이루어지는 것을 특징으로 한다.

[0022] 본 발명에 따른, 생체 인식을 이용한 오티피 운영 방법은, OTP(One Time Password)를 생성하는 장치에서 실행되는 방법에 있어서, 사용자의 생체를 인증하기 위한 생체 인증 정보를 지정된 저장영역에 저장하는 제1 단계와 상기 무선단말에 구비된 생체 인식부를 통해 인식된 생체 인식 정보를 확인하는 제2 단계와 상기 생체 인증 정보를 통해 상기 생체 인식 정보에 대응하는 사용자의 생체를 인증하는 절차를 수행하는 제3 단계와 상기 사용자의 생체가 인증된 경우 상기 인증된 사용자의 생체를 이용하여 OTP 생성을 위한 씨드 중 적어도 하나의 씨드 값을 구성하는 제4 단계 및 상기 OTP 생성을 위한 씨드를 이용하여 OTP를 동적 생성하는 제5 단계를 포함하는 것을 특징으로 한다.

[0024] 본 발명에 따른, 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 제4 단계는, 상기 사용자의 생체를 인증한 생체 인식 정보를 이용하여 OTP 생성을 위한 씨드 중 적어도 하나의 씨드 값을 구성하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0026] 본 발명에 따른, 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 제4 단계는, 상기 인증된 사용자의 생체 인식 정보를 가공하여 OTP 생성을 위한 씨드 중 적어도 하나의 씨드 값을 구성하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0028] 본 발명에 따른, 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 사용자의 생체는, 사용자의 지문, 홍채, 망막, 안면 중 적어도 하나를 포함하여 이루어지는 것을 특징으로 한다.

[0030] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법은, OTP(One Time Password) 장치에서 OTP 생성 시, 사용자의 생체 인식 대상으로부터 사용자의 생체 인식 정보를 인식하는 단계와, 상기 인식된 생체 인식 정보를 씨드 값으로 포함하는 OTP 생성 정보를 구성하는 단계 및 상기 OTP 생성 정보에 포함된 하나 이상의 고정 씨드 값과 동적으로 결정되는 동적 씨드 값을 이용하여 OTP를 생성하여 출력하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0032] 한편, 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법은, 저장매체에 OTP 매체 정보-OTP 장치 고유정보, 고객정보-와 사용자의 생체로부터 획득한 생체 인식 정보 및 서버측 OTP 생성 정보를 연계하여 저장하는 단계와, 사용자의 생체 인식 대상으로부터 인식한 생체 인식 정보를 씨드 값으로 포함하는 OTP 생성 정보를 통해 생성된 OTP를 수신하는 단계와, 상기 OTP를 생성한 OTP 매체 정보를 확인하고, 상기 저장매체로부터 상기 OTP 매체 정보와 연계된 생체 인식 정보와 서버측 OTP 생성 정보를 확인하고, 서버측 OTP 생성 정보에 포함된 씨드 값과 상기 생체 인식 정보에 대응하는 씨드 값을 포함하는 OTP 생성 정보를 구성하는 단계 및 상기 OTP 생성 정보를 통해 OTP’ 를 생성하고, 상기 수신된 OTP와 상기 생성된 OTP’ 를 비교(또는 검증 연산)하여 상기 수신된 OTP 유효성을 인증하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0034] 한편, 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법은, 저장매체에 OTP 매체 정보-OTP 장치 고유정보, 고객정보-와 사용자의 생체로부터 획득한 생체 인식 정보를 씨드 값으로 포함하는 OTP 생성 정보를 연계하여 저

장하는 단계와, 사용자의 생체 인식 대상으로부터 인식한 생체 인식 정보를 씨드 값으로 포함하는 OTP 생성 정보를 통해 생성된 OTP를 수신하는 단계와, 상기 OTP를 생성한 OTP 매체 정보를 확인하고, 상기 저장매체로부터 상기 OTP 매체 정보와 연계된 OTP 생성 정보를 확인하는 단계와, 상기 OTP 생성 정보를 통해 OTP' 를 생성하고, 상기 수신된 OTP와 상기 생성된 OTP' 를 비교(또는 검증 연산)하여 상기 수신된 OTP 유효성을 인증하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

[0036] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법은, OTP 장치의 저장영역에 생체 인증 정보를 저장하는 단계 및 상기 생체 인식 정보가 리딩되면, 상기 생체 인식 정보와 상기 저장영역에 저장된 생체 인증 정보를 비교(또는 검증 연산)하여 OTP 생성 유효성을 확인하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0038] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법은, 상기 생체 인식 정보를 상기 OTP 생성 정보의 씨드 값 데이터 구조로 해시하여 가공하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0040] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 생체 인식 대상은, 사용자의 지문, 홍채, 망막, 안면 중 어느 하나를 포함하고, 상기 생체 인식 정보는, 상기 생체 인식 대상으로부터 인식되는 지문 인식 정보, 홍채 인식 정보, 망막 인식 정보, 안면 인식 정보 중 어느 하나를 포함하여 이루어지는 것을 특징으로 한다.

[0042] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 생체 인식 정보는, 상기 OTP 생성 정보의 고정 씨드 값으로 포함되는 것을 특징으로 한다.

[0044] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 OTP 생성 정보는, 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하는 파라미터를 포함하는 단말측 OTP 생성 정보와 상기 생체 인식 정보를 조합하여 구성되는 것을 특징으로 한다.

[0046] 본 발명에 따른 생체 인식을 이용한 오티피 운영 방법에 있어서, 상기 OTP 생성 정보는, 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하는 파라미터를 포함하는 서버측 OTP 생성 정보와 상기 생체 인식 정보를 조합하여 구성되는 것을 특징으로 한다.

[0048] 한편, 상기 전술한 생체 인식을 이용한 오티피 운영 방법을 실행하는 프로그램을 기록한 것을 특징으로 하는 컴퓨터로 판독 가능한 기록매체를 포함한다.

[0050] 한편, 본 발명에 따른 OTP 장치는, OTP(One Time Password) 장치에서 OTP 생성 시, 사용자의 생체 인식 대상으로부터 사용자의 생체 인식 정보를 인식하는 생체 인식부와, 상기 인식된 생체 인식 정보를 씨드 값으로 포함하는 OTP 생성 정보를 구성하는 정보 구성부 및 상기 OTP 생성 정보에 포함된 하나 이상의 고정 씨드 값과 동적으로 결정되는 동적 씨드 값을 이용하여 OTP를 생성하는 OTP 생성부를 구비하여 이루어지는 것을 특징으로 한다.

[0052] 한편, 본 발명에 따른 생체 인식을 이용한 오티피 운영 시스템은, OTP 매체 정보-OTP 장치 고유정보, 고객정보-와 사용자의 생체로부터 획득한 생체 인식 정보 및 서버측 OTP 생성 정보를 연계하여 저장하는 저장매체와, 사용자의 생체 인식 대상으로부터 인식한 생체 인식 정보를 씨드 값으로 포함하는 OTP 생성 정보를 통해 생성된 OTP를 수신하는 정보 수신수단과, 상기 OTP를 생성한 OTP 매체 정보를 확인하고, 상기 저장매체로부터 상기 OTP 매체 정보와 연계된 생체 인식 정보와 서버측 OTP 생성 정보를 확인하고, 서버측 OTP 생성 정보에 포함된 씨드 값과 상기 생체 인식 정보에 대응하는 씨드 값을 포함하는 OTP 생성 정보를 구성하는 정보 구성수단 및 상기 OTP 생성 정보를 통해 OTP' 를 생성하고, 상기 수신된 OTP와 상기 생성된 OTP' 를 비교(또는 검증 연산)하여 상기 수신된 OTP 유효성을 인증하는 OTP 인증수단을 구비하여 이루어지는 것을 특징으로 한다.

[0054] 한편, 본 발명에 따른 생체 인식을 이용한 오티피 운영 시스템은, OTP 매체 정보-OTP 장치 고유정보, 고객정보-와 사용자의 생체로부터 획득한 생체 인식 정보를 씨드 값으로 포함하는 OTP 생성 정보를 연계하여 저장하는 저장매체와, 사용자의 생체 인식 대상으로부터 인식한 생체 인식 정보를 씨드 값으로 포함하는 OTP 생성 정보를 통해 생성된 OTP를 수신하는 정보 수신수단과, 상기 OTP를 생성한 OTP 매체 정보를 확인하고, 상기 저장매체로부터 상기 OTP 매체 정보와 연계된 OTP 생성 정보를 확인하는 정보 확인수단 및 상기 OTP 생성 정보를 통해 OTP' 를 생성하고, 상기 수신된 OTP와 상기 생성된 OTP' 를 비교(또는 검증 연산)하여 상기 수신된 OTP 유효성을 인증하는 OTP 인증수단을 구비하여 이루어지는 것을 특징으로 한다.

발명의 효과

[0056] 본 발명에 따르면, 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 생체 인식 대상으로부터 사용자

의 생체 정보를 인식하는 생체 인식 기능을 구비한 OTP 장치에서 OTP 생성시, 상기 OTP 장치에서 상기 사용자의 생체로부터 인식되는 생체 인식 정보를 상기 OTP의 씨드 값으로 사용하여 OTP를 생성하고, 상기 OTP를 인증하는 서버에서 상기 OTP 인증시, 기 등록된 사용자의 생체 인식 정보를 확인한 후, 상기 확인된 생체 인식 정보를 상기 동일한 씨드 값으로 사용하여 상기 OTP를 인증하도록 함으로써, 설령 상기 OTP 장치가 도난/탈취되어 제3자에 의해 악의적으로 이용되지 않도록 하는 이점과, OTP에 대한 투-팩터 인증(Two-Factor Authentication) 한계를 해소하는 이점을 지니고 있다.

도면의 간단한 설명

[0058] 도 1은 본 발명의 실시 방법에 따라 생체 인식 정보를 이용하여 OTP를 생성하는 기능을 구비한 OTP 장치 기능 구성을 도시한 도면이다.

도 2는 본 발명의 실시 방법에 따른 OTP 시스템 구성을 도시한 도면이다.

도 3은 본 발명의 실시 방법에 따른 OTP 매체 등록 과정을 도시한 도면이다.

도 4는 본 발명의 일 실시 방법에 따른 OTP 생성 과정을 도시한 도면이다.

도 5는 본 발명의 다른 일 실시 방법에 따른 OTP 생성 과정을 도시한 도면이다.

도 6은 본 발명의 실시 방법에 따른 OTP 인증 과정을 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0059] 이하 첨부된 도면과 설명을 참조하여 본 발명의 바람직한 실시예에 대한 동작 원리를 상세히 설명한다. 다만, 하기에 도시되는 도면과 후술되는 설명은 본 발명의 특징을 효과적으로 설명하기 위한 여러 가지 방법 중에서 바람직한 실시 방법에 대한 것이며, 본 발명이 하기의 도면과 설명만으로 한정되는 것은 아니다. 또한, 하기에서 본 발명을 설명함에 있어 관련된 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서, 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 발명에서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0061] 결과적으로, 본 발명의 기술적 사상은 청구범위에 의해 결정되며, 이하 실시예는 진보적인 본 발명의 기술적 사상을 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 효율적으로 설명하기 위한 일 수단일 뿐이다.

[0063] 도면1은 본 발명의 실시 방법에 따라 생체 인식 정보를 이용하여 OTP를 생성하는 기능을 구비한 OTP 장치(100) 기능 구성을 도시한 도면이다.

[0065] 보다 상세하게 본 도면1은 사용자가 소유하고 있는 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 생체 인식 대상으로부터 사용자의 생체 정보를 인식하는 사용자 생체 인식 기능을 구비한 OTP 장치(100)에서 상기 생체 인식 정보를 이용하여 N(N>=2)자리수의 OTP(One Time Password)를 생성하는 기능 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면1을 참조 및/또는 변형하여 상기 생체 인식 정보를 이용하여 OTP를 생성하는 기능을 구비한 실시 방법을 유추할 수 있을 것이며, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면1에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0067] 도면1을 참조하면, 상기 OTP 장치(100)는, 상기 OTP 장치(100) 내 구성요소를 제어하는 제어부(105)와, LCD(Liquid Crystal Display)에 대응하는 화면 출력부(110)와, 키패드에 대응하는 키 입력부(115)와, 비휘발성 메모리에 대응하는 메모리부(130) 및 전원 공급을 위한 배터리(125)를 구비하여 이루어지는 것을 특징으로 하며, 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 사용자의 생체 인식 대상으로부터 사용자의 지문 정보, 홍채 정보, 망막 정보, 안면 정보 중 어느 하나에 대응하는 생체 정보를 인식하고, 상기 생체 정보에 포함된 사용자의 고유한 생체 패턴을 비교 가능한 데이터 구조로 구성한 생체 인식 정보를 구성하는 생체 인식부(120)를 구비하여 이루어지는 것을 특징으로 한다.

[0069] 여기서, 상기 사용자 매체 정보는 비접촉식 IC카드 또는 접촉식 IC카드에 대응하는 사용자 매체로부터 리딩되는 카드정보(또는 사용자 매체 정보로 설정되어 상기 IC카드의 메모리에 기록된 코드 정보), MS카드에 대응하는 사용자 매체로부터 리딩되는 카드정보(또는 사용자 매체 정보로 설정되어 상기 MS카드의 트랙에 기록된 디지트 정보), RF카드에 대응하는 사용자 매체로부터 리딩되는 카드정보(또는 사용자 매체 정보로 설정되어 상기 RF카드

의 메모리에 기록된 코드 정보), RFID에 대응하는 사용자 매체로부터 리딩되는 RFID정보(또는 사용자 매체 정보로 설정되어 상기 RFID의 메모리에 기록된 코드 정보), USB장치에 대응하는 사용자 매체로부터 리딩되는 USB장치정보(또는 사용자 매체 정보로 설정되어 상기 USB장치의 메모리에 기록된 코드 정보) 중 어느 하나를 포함하여 이루어지는 것이 바람직하다.

[0071] 상기 사용자 매체 정보와 사용자 매체 인증 정보가 비교되어 상기 OTP 생성 유효성을 인증하는 경우, 상기 사용자 매체 인증 정보는 상기 사용자 매체 정보를 그대로 포함하여 이루어지는 것이 바람직하며, 상기 사용자 매체 정보와 사용자 매체 인증 정보가 검증 연산되어 상기 OTP 생성 유효성을 인증하는 경우, 상기 사용자 매체 인증 정보는 상기 사용자 매체 정보와 연산되어 기 설정된 연산 결과를 유도하는 사용자 매체 정보 검증 값을 포함하여 이루어지는 것이 바람직하다.

[0073] 본 발명의 실시 방법에 따르면, 상기 메모리부(130)는, 상기 OTP 장치(100)에서 상기 N(N>=2)자리수의 OTP를 생성하는 단말측 OTP 생성 정보를 암호화하여 저장하는 것이 가능하며, 실시 방법에 따라 상기 단말측 OTP 생성 정보가 생략되어도 무방하다. 단, 상기 단말측 OTP 생성 정보가 상기 메모리부(130)에 저장되는 경우, 상기 단말측 OTP 생성 정보는 암호화하여 상기 메모리부(130)에 저장되는 것이 바람직하다.

[0075] 상기 단말측 OTP 생성 정보는, N(N>=2)자리수의 OTP를 생성하기 위한 고정 씨드(seed) 값 동적 씨드 값을 결정하기 위한 파라미터를 하나 이상 포함하여 이루어지는 것이 바람직하며, 상기 고정 씨드 값과 파라미터에 의해 결정되는 동적 씨드 값은 기 설정된 OTP 생성 알고리즘 및 OTP 생성 방식에 대입되어 N자리수의 OTP를 생성한다.

[0077] 예를들어, 상기 OTP가 시간-동기화 방식으로 생성된다면, 상기 단말측 OTP 생성 정보는 상기 시간-동기화 방식의 OTP 생성 알고리즘에 대입할 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터(예컨대, 상기 시간-동기화 방식 OTP의 동적 씨드 값에 대응하는 동기화 시각을 결정하기 위한 동기화 시각 설정 값)를 포함하여 이루어지는 것이 바람직하다.

[0079] 또는, 상기 OTP가 챌린지-리스폰스 방식으로 생성된다면, 상기 단말측 OTP 생성 정보는 상기 챌린지-리스폰스 방식의 OTP 생성 알고리즘에 대입할 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터(예컨대, 상기 챌린지-리스폰스의 난수를 생성하는 난수 생성 값, 또는 난수를 수신하기 위한 난수 수신 정보)를 포함하여 이루어지는 것이 바람직하다.

[0081] 본 발명의 실시 방법에 따르면, 상기 메모리부(130)는, 상기 OTP 장치(100)에 구비된 사용자 생체 인식 기능을 통해 획득되는 생체 인식 정보를 인증하기 위한 생체 인증 정보를 암호화 저장하는 것이 가능하며, 이 경우 상기 사용자 생체 인식 기능을 통해 상기 생체 인식 정보가 획득되면, 상기 OTP 장치(100)는 생체 인식 정보와 생체 인증 정보를 비교(또는 검증 연산)하여 상기 OTP 장치(100)에서 상기 생체 인식 정보를 이용하여 OTP를 생성하는 것에 대한 유효성을 인증하는고, 상기 유효성 인증 결과를 상기 OTP 장치(100)로 응답하는 것이 바람직하다.

[0083] 여기서, 상기 생체 인식 정보는 사용자의 지문으로부터 인식되는 지문 정보에 포함된 사용자의 고유한 지문 패턴을 비교 가능한 데이터 구조로 구성하는 지문 인식 정보, 사용자의 홍채로부터 인식되는 홍채 정보에 포함된 사용자의 고유한 홍채 패턴을 비교 가능한 데이터 구조로 구성하는 홍채 인식 정보, 사용자의 망막으로부터 인식되는 망막 정보에 포함된 사용자의 고유한 망막 패턴을 비교 가능한 데이터 구조로 구성하는 망막 인식 정보, 사용자의 안면으로부터 인식되는 안면 정보에 포함된 사용자의 고유한 안면 패턴을 비교 가능한 데이터 구조로 구성하는 안면 인식 정보 중 어느 하나를 포함하여 이루어지는 것이 바람직하다.

[0085] 상기 생체 인식 정보와 생체 인증 정보가 비교되어 상기 OTP 생성 유효성을 인증하는 경우, 상기 생체 인증 정보는 상기 생체 인식 정보를 그대로 포함하여 이루어지는 것이 바람직하며, 상기 생체 인식 정보와 생체 인증 정보가 검증 연산되어 상기 OTP 생성 유효성을 인증하는 경우, 상기 생체 인증 정보는 상기 생체 인식 정보와 연산되어 기 설정된 연산 결과를 유도하는 생체 인식 정보 검증 값을 포함하여 이루어지는 것이 바람직하다.

[0087] 상기 생체 인식부(120)는 사용자의 지문으로부터 상기 사용자의 지문 정보에 대응하는 생체 정보를 인식하는 지문 인식모듈, 사용자의 홍채로부터 상기 사용자의 홍채 이미지에 대응하는 생체 정보를 인식하거나, 사용자의 망막으로부터 상기 사용자의 망막 이미지에 대응하는 생체 정보를 인식하거나, 사용자의 안면으로부터 상기 사용자의 안면 이미지에 대응하는 생체 정보를 인식하는 카메라 모듈을 구비하여 이루어지는 것을 특징으로 하며, 당업자의 의도에 따라 상기 생체 인식 대상과 이에 대응하는 생체 인식부(120)는 다양하게 확장 가능하며, 생체 인식 대상과 이에 대응하는 생체 인식 방법에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.

[0089] 여기서, 상기 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 사용자의 생체 인식 대상으로부터 인식된 사용자의 지문 정보, 홍채 정보, 망막 정보, 안면 정보 중 어느 하나에 대응하는 생체 정보는, 각 생체 인식 방식에 대응하는 이미지 데이터 또는 벡터 데이터를 포함하여 이루어지는 것이 바람직하다.

[0091] 예를들어, 전자식 지문 인식 방식으로 인식된 지문 정보는 벡터 데이터를 포함하여 이루어지는 것이 바람직하며, 광학식 지문 인식 방식으로 인식된 지문 정보 및 카메라부를 통해 인식된 홍채 정보, 망막 정보, 안면 정보 등은 이미지 데이터를 포함하여 이루어지는 것이 바람직하다.

[0093] 본 발명의 실시 방법에 따르면, 상기 생체 인식부(120)는 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 사용자의 생체 인식 대상으로부터 인식된 사용자의 지문 정보, 홍채 정보, 망막 정보, 안면 정보 중 어느 하나에 대응하는 생체 정보에 포함된 사용자의 고유한 생체 패턴을 비교(또는 검증 연산) 가능한 데이터 구조를 포함하는 생체 인식 정보로 구성하는 것이 바람직하다.

[0095] 여기서, 상기 생체 인식 정보는, 상기 생체 정보에 포함된 사용자의 생체 패턴을 고유하게 특정하는 패턴 데이터에 대응하는 이미지 데이터, 벡터 데이터, 이미지/벡터 데이터를 하나 이상 포함하거나, 또는 상기 패턴 데이터를 기 설정된 해시함수로 해시한 지문 코드 값을 포함하여 이루어지는 것이 바람직하다.

[0097] 본 발명의 실시 방법에 따라 상기 사용자의 지문으로부터 상기 사용자의 지문 정보를 인식하는 경우, 상기 지문 인식 정보는 상기 사용자의 지문 패턴을 고유하게 특정하는 지문 패턴 데이터에 대응하는 지문 패턴 이미지 데이터, 지문 패턴 벡터 데이터, 지문 패턴 이미지/벡터 데이터를 하나 이상 포함하거나, 또는 상기 지문 패턴 데이터를 기 설정된 해시함수로 해시한 지문 코드 값을 포함하여 이루어지는 것이 바람직하다.

[0099] 또는, 상기 사용자의 홍채로부터 상기 사용자의 홍채 정보를 인식하는 경우, 상기 홍채 인식 정보는 상기 사용자의 홍채 패턴을 고유하게 특정하는 홍채 패턴 데이터에 대응하는 홍채 패턴 이미지 데이터, 홍채 패턴 벡터 데이터, 홍채 패턴 이미지/벡터 데이터를 하나 이상 포함하거나, 또는 상기 홍채 패턴 데이터를 기 설정된 해시함수로 해시한 지문 코드 값을 포함하여 이루어지는 것이 바람직하다.

[0101] 또는, 상기 사용자의 망막으로부터 상기 사용자의 망막 정보를 인식하는 경우, 상기 망막 인식 정보는 상기 사용자의 망막 패턴을 고유하게 특정하는 망막 패턴 데이터에 대응하는 망막 패턴 이미지 데이터, 망막 패턴 벡터 데이터, 망막 패턴 이미지/벡터 데이터를 하나 이상 포함하거나, 또는 상기 망막 패턴 데이터를 기 설정된 해시함수로 해시한 지문 코드 값을 포함하여 이루어지는 것이 바람직하다.

[0103] 또는, 상기 사용자의 안면으로부터 상기 사용자의 안면 정보를 인식하는 경우, 상기 안면 인식 정보는 상기 사용자의 안면 패턴을 고유하게 특정하는 안면 패턴 데이터에 대응하는 안면 패턴 이미지 데이터, 안면 패턴 벡터 데이터, 안면 패턴 이미지/벡터 데이터를 하나 이상 포함하거나, 또는 상기 안면 패턴 데이터를 기 설정된 해시함수로 해시한 지문 코드 값을 포함하여 이루어지는 것이 바람직하다.

[0105] 도면1을 참조하면, 상기 OTP 장치(100)는, 상기 생체 인식부(120)를 통해 상기 생체 인식 정보가 획득되면, 상기 생체 인식 정보와 상기 메모리부(130)에 저장된 생체 인증 정보를 비교(또는 검증 연산)하여 상기 생체 인식 정보를 통해 OTP를 생성하는 유효성을 인증하는 인증부(135)를 구비하여 이루어지는 것을 특징으로 한다.

[0107] 상기 생체 인식부(120)를 통해 상기 생체 인식 정보가 획득되면, 상기 인증부(135)는 상기 생체 인식 정보를 상기 메모리부(130)에 저장된 생체 인증 정보와 비교 가능한 데이터 구조, 또는 상기 생체 인증 정보와 기 설정된 검증 연산을 처리할 수 있는 데이터 구조로 가공한다(단, 상기 생체 인식 정보의 데이터 구조가 상기 생체 인증 정보와 비교(또는 검증 연산) 가능한 데이터 구조를 포함하는 경우 생략 가능).

[0109] 본 발명의 다른 실시 방법에 따르면, 상기 메모리부(130)는 사용자가 등록한 비밀번호(또는 개인식별번호)를 저장하고, 키 입력을 통해 사용자의 비밀번호(또는 개인식별번호)가 입력되면, 상기 인증부(135)는 상기 입력된 비밀번호(또는 개인식별번호)를 인증하여 상기 생체 인식 정보를 통해 OTP를 생성하는 유효성을 인증하거나, 상기 생체 인식 정보를 이용한 인증에 상기 비밀번호(또는 개인식별번호)을 더 포함하는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0111] 도면1을 참조하면, 상기 OTP 장치(100)는, 상기 생체 인식 정보를 N(N>=2)자리수의 OTP를 생성하기 위한 씨드 값으로 포함하는 OTP 생성 정보를 구성하는 정보 구성부(145)와, 상기 구성된 OTP 생성 정보로부터 상기 N자리수의 OTP를 생성하기 위한 하나 이상의 고정 씨드 값과 동적 씨드 값을 확인/결정하고, 상기 확인/결정된 하나 이상의 고정 씨드 값과 동적 씨드 값을 기 설정된 OTP 생성 알고리즘에 대입하여 OTP를 생성하는 OTP 생성부(150)를 구비하여 이루어지는 것을 특징으로 하며, 상기 메모리부(130)에 단말측 OTP 생성 정보가 저장된 경우,

상기 메모리부(130)로부터 단말측 OTP 생성 정보를 확인하는 정보 확인부(140)를 더 구비하는 것을 특징으로 하며, 상기 정보 구성부(145)는 상기 단말측 OTP 생성 정보와 상기 생체 인식 정보를 조합하여 N(N>=2)자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것을 특징으로 한다.

[0113] 상기 인증부(135)에 의해 상기 생체 인식 정보를 통해 OTP를 생성하는 유효성이 인증되면, 상기 정보 구성부(145)는 상기 생체 인식부(120)를 통해 획득된 생체 인식 정보를 확인하고, 상기 생체 인식 정보가 상기 N자리수의 OTP를 생성하기 위한 데이터 구조와 매칭되지 않는 경우, 상기 획득된 생체 인식 정보를 상기 N자리수의 OTP를 생성하기 위한 데이터 구조로 변환하는 것을 특징으로 한다. 만약 상기 생체 인식부(120)를 통해 획득된 생체 인식 정보가 상기 N자리수의 OTP를 생성하기 위한 데이터 구조로 이루어져 있거나, 또는 상기 생체 인식부(120)를 통해 획득된 생체 인식 정보의 데이터 구조를 그대로 생성하여 상기 N자리수의 OTP를 생성할 수 있는 경우, 상기 생체 인식 정보의 데이터 구조를 변환하지 않아도 무방하며, 이에 의해 본 발명이 한정되지 아니한다.

[0115] 본 발명의 실시 방법에 따르면, 상기 생체 인식 정보는 일련의 텍스트/바이너리 데이터를 상기 OTP 생성 정보를 구성하는 씨드 값의 데이터 구조로 해시(Hash)하는 해시 함수를 통해 해시되어 상기 N자리수의 OTP를 생성하기 위한 데이터 구조로 변환되는 것이 바람직하다.

[0117] 상기 정보 구성부(145)는 상기 생체 인식 정보를 상기 N자리수의 OTP를 생성하기 위한 고정 씨드 값으로 포함하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것을 특징으로 한다.

[0119] 본 발명의 실시 방법에 따르면, 상기 정보 구성부(145)는 상기 메모리부(130)에 저장된 OTP 장치(100) 고유정보를 상기 OTP 생성 정보의 고정 씨드 값으로 포함시켜 상기 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0121] 만약 상기 N자리수의 OTP가 시간-동기화 방식의 OTP라면, 상기 정보 구성부(145)는 상기 OTP 장치(100)에 구비된 타이머로부터 확인되는 시간 값(또는 특정 시간 구간에 대한 시간 값)을 결정하고, 상기 결정된 시간 값을 상기 OTP 생성 정보의 동적 씨드 값으로 포함시켜 상기 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0123] 또는, 상기 N자리수의 OTP가 챌린지-동기화 방식의 OTP라면, 상기 정보 구성부(145)는 소정의 난수 값을 생성하여 서버와 전송/교환하거나, 또는 상기 서버에서 생성한 난수 값을 수신/교환한 후, 상기 난수 값을 상기 OTP 생성 정보의 동적 씨드 값으로 포함시켜 상기 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0125] 만약 상기 메모리부(130)에 단말측 OTP 생성 정보가 저장된 경우, 상기 정보 확인부(140)는 상기 메모리부(130)로부터 단말측 OTP 생성 정보를 확인하며, 상기 정보 구성부(145)는 상기 생체 인식 정보를 상기 N자리수의 OTP를 생성하기 위한 고정 씨드 값으로 처리한 후, 상기 확인된 단말측 OTP 생성 정보와 상기 생체 인식 정보를 조합하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0127] 상기 정보 구성부(145)에 의해 상기 생체 인식 정보를 상기 N자리수의 OTP를 생성하기 위한 고정 씨드 값으로 포함하는 OTP 생성 정보가 구성되면, 상기 OTP 생성부(150)는 상기 구성된 OTP 생성 정보에 포함된 하나 이상의 고정 씨드 값을 확인하고, 상기 OTP 생성 정보에 포함된 파라미터를 통해 하나 이상의 동적 씨드 값을 결정하고, 상기 확인/결정된 하나 이상의 고정 씨드 값과 동적 씨드 값을 기 설정된 OTP 생성 알고리즘에 대입하여 N(N>=2)자리수의 OTP를 생성하는 것을 특징으로 한다. 여기서, 상기 OTP에 대한 N의 자리수는 고정될 수도 있고, OTP를 생성할 때마다 동적으로 변경되어도 무방하며, 이에 의해 본 발명이 한정되지 아니한다.

[0129] 도면1을 참조하면, 상기 OTP 장치(100)는, 상기 OTP 생성부(150)를 통해 상기 N자리수의 OTP가 생성되면, 상기 생성된 OTP를 상기 화면 출력부(110)를 통해 출력하는 OTP 출력부(155)를 구비하여 이루어지는 것을 특징으로 하며, 상기 OTP 장치(100)에 근거리 통신수단(도시생략)이 구비된 경우, 상기 OTP 출력부(155)는 상기 근거리 통신수단을 통해 상기 생성된 OTP를 상기 OTP 장치(100)와 근거리에 위치한 단말(또는 장치)로 출력하는 것이 가능하다.

[0131] 상기 OTP가 생성되면, 상기 OTP 출력부(155)는 상기 화면 출력부(110)와 연계하여 상기 생성된 OTP를 상기 OTP 장치(100) 화면 상의 일정 영역에 출력하는 것을 특징으로 한다.

[0133] 본 발명의 일 실시 방법에 따르면, 상기 OTP 출력부(155)는 상기 화면 출력부(110)와 연계하여 상기 OTP 장치(100) 화면 상에 OTP 출력 화면을 출력하고, 상기 OTP 출력 화면에 상기 생성된 OTP를 출력하는 것이 바람직하

다.

[0135] 본 발명의 다른 일 실시 방법에 따르면, 상기 OTP 출력부(155)는 상기 화면 출력부(110)와 연계하여 상기 OTP 장치(100) 화면에 현재 출력된 화면 영역에 OTP 출력 영역을 출력(또는 할당)하고, 상기 OTP 출력 영역에 상기 생성된 OTP를 출력하는 것이 바람직하다.

[0137] 만약 상기 OTP 장치(100)에 근거리 통신수단(예컨대, 블루투스, 적외선통신, RFID통신, RF통신 등, 도시생략)이 구비된 경우, 상기 OTP 출력부(155)는 상기 근거리 통신수단을 통해 상기 생성된 OTP를 상기 OTP 장치(100)와 근거리에 위치한 단말(또는 장치)로 출력하는 것이 가능하다.

[0139] 도면2는 본 발명의 실시 방법에 따른 OTP 시스템 구성을 도시한 도면이다.

[0141] 보다 상세하게 본 도면2는 상기 사용자 생체 인식 기능을 구비한 OTP 장치(200)에서 상기 생체 인식 정보를 이용하여 생성한 N자리수의 OTP를 인증하는 OTP 시스템 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면2를 참조 및/또는 변형하여 상기 OTP 시스템 구성에 대한 다양한 실시 방법(예컨대, 일부 구성부가 생략되거나, 또는 세분화되거나, 또는 합쳐진 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면2에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0143] 도면2를 참조하면, 상기 OTP 시스템은, 상기 도면1에 도시된 기능 구성을 구비한 OTP 장치(200)와, 상기 OTP 장치(200)를 소지한 사용자에게 OTP 인증을 요청하는 OTP 인증요청 서버(210)와, 상기 도면1과 같은 기능 구성을 구비하여 OTP 매체로 등록되는 OTP 장치(200)에 대응하는 OTP 매체 정보와 서버측 OTP 생성 정보를 연계하여 저장매체(240)에 저장한 후, 상기 OTP 장치(200)를 OTP 매체로 사용시, 상기 생체 인식 정보를 이용하여 상기 OTP 장치(200)에서 생성한 N자리수의 OTP를 수신하여 인증하는 OTP 운영 시스템을 포함하여 이루어지는 것을 특징으로 하며, 당업자의 의도에 따라 상기 OTP 장치(200)를 소지한 사용자가 이용하는 사용자 단말(205)과, 상기 OTP 장치(200)에서 생성된 N자리수의 OTP를 인증하는 별도의 OTP 서버(215)를 더 포함하여 이루어진다.

[0145] 본 발명에 따르면, 상기 OTP 운영 시스템은, 상기 OTP 운영 시스템을 구성하는 각각의 수단이 하나의 통합 서버 형태로 구현되거나, 또는 상기 OTP 운영 시스템을 구성하는 각각의 수단(또는 두개 이상 수단의 조합)이 각각의 서버 형태로 구현되는 서버 시스템 형태로 구현되거나, 상기 OTP 운영 시스템을 구성하는 수단 중 일부는 서버 형태로 구현되고 나머지 일부는 상기 OTP 서버(215), OTP 인증요청 서버(210) 중 하나 이상의 서버의 구성요소 형태로 구현되거나, 또는 상기 OTP 운영 시스템을 구성하는 각각의 수단이 상기 OTP 서버(215), OTP 인증요청 서버(210) 중 하나 이상의 서버의 구성요소 형태로 분산되어 구현되는 것이 모두 가능하며, 상기 OTP 운영 시스템이 구현되는 방식과 서버 종류와 구현 위치 및 개수에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.

[0147] 상기 OTP 장치(200)는, 상기 사용자 생체 인식 기능을 구비한 OTP 장치(200) 중 상기 생체 인식 정보를 이용하여 N자리수의 OTP를 생성하는 OTP 매체로 등록된 무선통신 단말장치로서, 키 입력수단을 통한 OTP 생성 요청, 또는 기 설정된 메뉴 선택에 따른 OTP 생성 요청에 의해 기 설정된 OTP 생성 유효성 인증 후, 상기 생체 인식 정보를 포함하는 OTP 생성 정보를 구성하여 N자리수의 OTP를 생성, 출력하는 것을 특징으로 한다.

[0149] 상기 OTP 인증요청 서버(210)는, 상기 OTP 장치(200)에서 생성하는 OTP를 통해 사용자, 지불결제, 금융거래를 인증하도록 요청하는 서버들의 총칭으로서, 상기 OTP 장치(200)에서 생성하는 OTP를 통해 사용자 인증을 처리하는 웹서버, 상기 OTP 장치(200)에서 생성하는 OTP를 통해 지불결제를 인증을 처리하는 쇼핑몰 서버 또는 컨텐츠 제공 서버 또는 홈쇼핑 서버, 상기 OTP 장치(200)에서 생성하는 OTP를 통해 금융거래를 인증하는 뱅킹 서버를 하나 이상 포함하여 이루어지며, 본 발명은 상기 OTP 인증요청 서버(210)의 종류와 OTP 인증요청 방식에 의해 본 발명이 한정되지 아니한다.

[0151] 상기 사용자 단말(205)은, 상기 OTP 장치(200)를 소지한 사용자가 통신망을 통해 상기 OTP 인증요청 서버(210)에 접속하는 통신단말의 총칭으로서, 키 입력수단, 화면 출력수단, 데이터 통신수단을 구비한 모든 종류의 단말장치를 포함하여 이루어지며, 바람직하게는 PC, 노트북을 포함하는 컴퓨터 단말, 무선 통신망에 연결된 무선통신단말(예컨대, OTP 장치(200), 휴대인터넷단말 등), 양방향 통신 기능이 구비된 디지털TV, IP-TV, 홈 네트워크에 연결된 가전단말 등을 포함하여 이루어진다.

[0153] 상기 OTP 서버(215)는, 상기 OTP 장치(200)에서 생성된 N자리수의 OTP를 통신망을 통해 수신하고, 상기 OTP와 매칭되는 OTP' 를 생성하고, 상기 OTP와 OTP' 를 비교(또는 검증 연산)하여 상기 OTP 인증을 처리하는 서버의 총칭으로서, 상기 OTP 서버(215)에서 상기 OTP를 인증하는 기능은 상기 OTP 운영 시스템에 구비되어도

무방하며, 이에 의해 본 발명이 한정되지 아니한다.

[0155] 도면2를 참조하면, 상기 OTP 운영 시스템은, 상기 사용자 생체 인식 기능을 구비한 OTP 장치(200)를 상기 생체 인식 정보를 이용하여 N자리수의 OTP를 생성하는 OTP 매체로 등록하고, 상기 OTP 장치(200)에서 생성한 N자리수의 OTP를 인증하는 OTP' 를 생성하기 위한 서버측 OTP 생성 정보를 구성하여 저장매체(240)에 저장하는 OTP 매체 등록수단(220)을 구비하여 이루어지는 것을 특징으로 하며, 상기 OTP 매체로 등록된 OTP 장치(200)는 상기 서버측 OTP 생성 정보와 매칭되는 단말측 OTP 생성 정보가 구비된다.

[0157] 기 설정된 OTP 등록단말에서 상기 OTP 매체로 등록될 OTP 장치(200) 고유정보와 상기 OTP 장치(200)를 이용하는 고객의 고객정보를 제공하면, 상기 OTP 매체 등록수단(220)은 상기 OTP 장치(200) 고유정보와 고객정보를 포함하는 OTP 매체 정보를 구성하여 저장매체(240)에 저장하는 것을 특징으로 하며, 상기 OTP 등록단말(또는 상기 고객이 이용하는 고객단말)에서 생체 인식 정보를 제공하면, 상기 OTP 매체 등록수단(220)은 상기 생체 인식 정보를 상기 OTP 매체 정보에 더 포함하여 저장매체(240)에 저장한다.

[0159] 여기서, 상기 OTP 등록단말은, 상기 OTP 장치(200)를 OTP 매체로 등록하도록 요청하는 단말장치의 총칭으로서, 상기 사용자가 이용하는 사용자 단말(205), OTP 등록기관(예컨대, 국가기관, OTP 인증요청 서버(210) 운영기관, 카드사, 금융사, 증권사 등)에 구비된 단말(예컨대, 국가기관 단말, OTP 인증요청 서버(210) 운영기관 단말, 카드사 단말, 금융사 단말, 증권사 단말 등)를 하나 이상 포함하여 이루어진다.

[0161] 상기 OTP 매체 정보에 포함된 OTP 장치(200) 고유정보는, 복수의 OTP 장치(200) 중 상기 고객(사용자)에게 제공된 OTP 장치(200)에 부여된 장치 식별정보(또는 고유정보)를 포함하여 이루어지는 것이 바람직하다.

[0163] 상기 고객정보는, 상기 OTP 매체로 사용될 OTP 장치(200)의 명의자(또는 사용자)에 대응하는 주민등록번호를 포함하여 이루어지는 것이 바람직하며, 당업자의 의도에 따라 상기 명의자(또는 사용자)의 성명, 주소, 연락처와 같은 개인정보를 더 포함하는 것이 바람직하다.

[0165] 만약 상기 OTP 장치(200)를 OTP 매체로 이용하여 인증하는 대상에 금융거래가 포함되는 경우, 상기 고객정보는 상기 고객정보에 대응하는 고객의 금융정보(예컨대, 계좌번호, 은행 등)를 더 포함하는 것이 바람직하다.

[0167] 또는 상기 OTP 장치(200)를 OTP 매체로 이용하여 인증하는 대상에 카드거래가 포함되는 경우, 상기 고객정보는 상기 고객정보에 대응하는 고객의 카드정보(예컨대, 카드번호, 카드사 등)를 더 포함하는 것이 바람직하다.

[0169] 본 발명을 실시하는 당업자의 의도 및 상기 OTP 장치(200)를 OTP 매체로 이용하는 분야에 따라 상기 고객정보는 다양한 정보(예컨대, 상기 OTP 장치(200)를 OTP 매체로 이용하여 인증하는 대상이 게임 접속자 인증을 포함하는 경우, 상기 게임에 대한 고객 계정정보 등)를 더 포함하는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0171] 사용자의 생체 인식 대상은 사용자의 지문, 홍채, 망막, 안면 중 어느 하나를 포함하며, 상기 생체 인식 정보는 상기 사용자의 생체 인식 대상으로부터 사용자의 지문 정보, 홍채 정보, 망막 정보, 안면 정보 중 어느 하나에 대응하는 생체 정보 중, 사용자의 지문으로부터 인식되는 지문 정보에 포함된 사용자의 고유한 지문 패턴을 비교 가능한 데이터 구조로 구성한 지문 인식 정보, 사용자의 홍채로부터 인식되는 홍채 정보에 포함된 사용자의 고유한 홍채 패턴을 비교 가능한 데이터 구조로 구성한 홍채 인식 정보, 사용자의 망막으로부터 인식되는 망막 정보에 포함된 사용자의 고유한 망막 패턴을 비교 가능한 데이터 구조로 구성한 망막 인식 정보, 사용자의 안면으로부터 인식되는 안면 정보에 포함된 사용자의 고유한 안면 패턴을 비교 가능한 데이터 구조로 구성한 안면 인식 정보 중 어느 하나를 포함하여 이루어지는 것이 바람직하다.

[0173] 상기 OTP 매체 정보가 수신되면, 상기 OTP 매체 등록수단(220)은, 상기 OTP 매체 정보를 기반으로 OTP 장치(200)에서 상기 생체 인식 정보를 이용하여 생성하는 N자리수의 OTP를 인증하기 위한 서버측 OTP 생성 정보를 생성(또는 할당)한다.

[0175] 여기서, 상기 서버측 OTP 생성 정보는, 상기 OTP 운영 시스템 상에 유지되며, 상기 OTP 장치(200)에서 생성한 N자리수의 OTP와 비교(또는 검증 연산)될 N자리수의 OTP' 를 생성하기 위한 하나 이상의 고정 씨드 값과, 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 바람직하다.

[0177] 상기 OTP 장치(200)에서 상기 생체 인식 정보가 상기 N자리수의 OTP를 생성하는 고정 씨드 값으로 사용되는 경우, 상기 서버측 OTP 생성 정보는 상기 생체 인식 정보를 상기 N자리수의 OTP' 를 생성하는 고정 씨드 값으로 포함하여 이루어지는 것이 바람직하다.

[0179] 본 발명의 실시 방법에 따르면, 상기 서버측 OTP 생성 정보는 상기 OTP 매체 정보에 포함된 OTP 장치(200) 고유정보 및/또는 고객정보를 기반으로 생성되는 고정 씨드 값을 포함하여 이루어지는 것이 바람직하며, 상기 생성된 고정 씨드 값은 상기 OTP 장치(200)로 제공될 단말측 OTP 생성 정보에 포함되는 것이 바람직하다.

[0181] 만약 상기 N자리수의 OTP가 시간-동기화 방식으로 생성되는 경우, 상기 서버측 OTP 생성 정보는 상기 시간-동기화 방식 OTP의 동적 씨드 값에 대응하는 동기화 시각을 결정하기 위한 동기화 시각 설정 정보를 포함하여 이루어지는 것이 바람직하다.

[0183] 또는 상기 N자리수의 OTP가 챌린지-리스폰스 방식으로 생성되는 경우, 상기 서버측 OTP 생성 정보는 상기 챌린지-리스폰스 방식 OTP의 동적 씨드 값에 대응하는 난수를 생성하거나, 또는 상기 난수를 수신하기 위한 난수 생성 값을 포함하여 이루어지는 것이 바람직하다.

[0185] 상기 OTP 매체 등록수단(220)은 상기 OTP 매체 정보와 상기 서버측 OTP 생성 정보를 연계하여 저장매체(240)에 저장함으로써, 상기 OTP 장치(200)를 상기 생체 인식 정보를 이용하여 N자리수의 OTP를 생성하는 OTP 매체로 등록한다.

[0187] 만약 상기 OTP 등록단말로부터 상기 생체 인식 정보가 수신되면, 상기 OTP 매체 등록수단(220)은 상기 생체 인식 정보를 상기 OTP 매체 정보에 더 포함하여 상기 저장매체(240)에 저장하는 것이 바람직하다.

[0189] 또한, 상기 OTP 매체 등록수단(220)은 상기 OTP 장치(200) 상기 생체 인식 정보에 대응하는 생체 인증 정보를 제공하여 상기 OTP 장치(200)에 구비된 메모리부에 기록되도록 처리하는 것이 바람직하다.

[0191] 상기 OTP 장치(200)에서 생체 인식 정보와 생체 인증 정보가 비교되어 상기 OTP 생성 유효성을 인증하는 경우, 상기 생체 인증 정보는 상기 생체 인식 정보를 그대로 포함하여 이루어지는 것이 바람직하며, 상기 생체 인식 정보와 생체 인증 정보가 검증 연산되어 상기 OTP 생성 유효성을 인증하는 경우, 상기 생체 인증 정보는 상기 생체 인식 정보와 연산되어 기 설정된 연산 결과를 유도하는 생체 인식 정보 검증 값을 포함하여 이루어지는 것이 바람직하다.

[0193] 도면2를 참조하면, 상기 OTP 운영 시스템은, 통신망을 통해 상기 OTP 장치(200)에서 상기 생체 인식 정보를 이용하여 생성한 N자리수의 OTP를 수신하고, 상기 OTP를 생성한 OTP 장치(200)에 대응하는 OTP 매체 정보를 확인하는 정보 수신수단(225)과, 상기 수신된 N자리수의 OTP와 비교(또는 검증 연산)될 N자리수의 OTP’ 를 생성하기 위한 OTP 생성 정보를 확인하는 정보 확인수단(235)과, 상기 OTP 생성 정보를 통해 N자리수의 OTP’ 를 생성하고, 상기 N자리수의 OTP와 OTP’ 를 비교(또는 검증 연산)하여 상기 수신된 OTP가 유효한지 인증하는 OTP 인증수단(230)을 구비하여 이루어지는 것을 특징으로 하며, 상기 정보 수신수단(225), 정보 확인수단(235) 및 OTP 인증수단(230)은 별도의 OTP 서버(215)에 구현되는 것이 가능하며, 본 발명은 상기 유추 가능한 모든 실시 방법을 포함하여 이루어짐을 명백하게 밝혀두는 바이다.

[0195] 상기 OTP 장치(200)에서 상기 N자리수의 OTP를 생성하고, 상기 사용자 단말(205)에 표시된 OTP 입력 인터페이스를 통해 상기 OTP가 입력되어 전송되면, 상기 정보 수신수단(225)은, 통신망을 통해 상기 사용자 단말(205)로부터 상기 OTP를 수신하는 것을 특징으로 하며, 이 경우 상기 사용자 단말(205)은 상기 OTP 장치(200) 고유정보 또는 고객정보 중 하나 이상을 포함하는 OTP 매체 정보를 더 전송하며, 상기 정보 수신수단(225)은 상기 사용자 단말(205)로부터 상기 OTP 매체 정보를 수신하는 것이 바람직하다.

[0197] 본 발명의 실시 방법에 따르면, 상기 OTP가 암호화되어 전송되면, 상기 정보 수신수단(225)은 기 설정된 복호화 방식에 따라 상기 OTP를 복호화 처리한다.

[0199] 상기 OTP가 수신되면, 상기 정보 확인수단(235)은 상기 저장매체(240)로부터 상기 OTP 매체 정보와 연계된 서버측 OTP 생성 정보를 확인한다.

[0201] 본 발명의 일 실시 방법에 따라 상기 확인된 서버측 OTP 생성 정보가 상기 OTP 장치(200)에서 N자리수의 OTP를 생성하기 위해 상기 생체 인식 정보를 포함하여 구성한 OTP 생성 정보와 동일한 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하고 있으면, 상기 정보 확인수단(235)은 상기 확인된 서버측 OTP 생성 정보를 N자리수의 OTP’ 를 생성하기 위한 OTP 생성 정보로 확인한다.

[0203] 본 발명의 다른 일 실시 방법에 따라 상기 확인된 서버측 OTP 생성 정보가 상기 생체 인식 정보를 포함하고 있지 않으면, 상기 정보 확인수단(235)은 상기 저장매체(240)로부터 상기 OTP 매체 정보에 포함(또는 연계)된 생체 인식 정보를 확인하고, 상기 서버측 OTP 생성 정보와 상기 생체 인식 정보를 조합하여 N자리수의 OTP’ 를 생성하기 위한 OTP 생성 정보를 구성하며, 상기 생체 인식 정보가 상기 N자리수의 OTP’ 를 생성하기 위한 데이터

구조와 매칭되지 않는 경우, 상기 정보 확인수단(235)은 상기 생체 인식 정보를 상기 N자리수의 OTP' 를 생성하기 위한 데이터 구조로 변환하는 것이 바람직하다.

[0205] 상기 N자리수의 OTP' 를 생성하기 위한 OTP 생성 정보가 확인/구성되면, 상기 OTP 인증수단(230)은 상기 OTP 생성 정보로부터 상기 OTP' 를 생성하기 위한 하나 이상의 고정 씨드 값을 확인하고, 상기 OTP 생성 정보에 포함된 파라미터를 통해 하나 이상의 동적 씨드 값을 결정하고, 상기 확인/결정된 하나 이상의 고정 씨드 값과 동적 씨드 값을 기 설정된 OTP 생성 알고리즘에 대입하여 N자리수의 OTP' 를 생성한다.

[0207] 상기 N자리수의 OTP' 가 생성되면, 상기 OTP 인증수단(230)은 상기 수신된 N자리수의 OTP와 상기 생성된 OTP' 를 비교(또는 검증 연산)하여 상기 OTP 유효성을 인증한다.

[0209] 만약 상기 비교 결과 상기 OTP와 OTP' 가 일치(또는 매칭)되거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되면, 상기 OTP 인증수단(230)은 상기 OTP 유효성이 인증된 것으로 처리하고, 상기 OTP 유효성 인증 결과를 상기 OTP 인증 결과를 필요로 하는 OTP 인증요청 서버(210), 사용자 단말(205), OTP 장치(200) 중 하나 이상의 OTP 인증결과 수신수단으로 제공한다.

[0211] 반면 상기 비교 결과 상기 OTP와 OTP' 가 일치(또는 매칭)되지 않거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되지 않으면, 상기 OTP 인증수단(230)은 상기 OTP 유효성이 인증되지 않은 것으로 처리하고, 상기 OTP 유효성 인증 결과를 상기 OTP 인증 결과를 필요로 하는 OTP 인증요청 서버(210), 사용자 단말(205), OTP 장치(200) 중 하나 이상의 OTP 인증결과 수신수단으로 제공한다.

[0213] 도면3은 본 발명의 실시 방법에 따른 OTP 매체 등록 과정을 도시한 도면이다.

[0215] 보다 상세하게 본 도면3은 사용자의 OTP 장치(200)를 상기 도면2에 도시된 OTP 시스템 상의 OTP 매체로 등록하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면3을 참조 및/또는 변형하여 상기 OTP 매체 등록 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면3에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0217] 이하, 본 도면3에서 상기 도면2에 도시된 OTP 운영 시스템을 편의상 "서버"라고 한다.

[0219] 도면3을 참조하면, OTP 등록단말에서 통신망을 통해 서버에 접속하여 상기 OTP 매체에 대응하는 OTP 장치(200)를 신청하면(300), 상기 서버는 상기 OTP 등록단말로 사용자의 고객정보와 상기 사용자의 OTP 장치(200)에 대응하는 OTP 장치(200) 고유정보를 포함하는 OTP 매체 정보를 입력/등록하는 OTP 매체 등록 인터페이스를 제공하고(300), 이에 대응하여 상기 OTP 등록단말은 상기 OTP 매체 등록 인터페이스를 통해 OTP 장치(200) 고유정보와 고객정보 및 생체 인식 정보를 포함하는 OTP 매체 정보를 입력 및 구성하여 상기 서버로 전송한다(310).

[0221] 상기 서버는 상기 OTP 등록단말로부터 상기 OTP 장치(200) 고유정보와 고객정보 및 생체 인식 정보를 포함하는 OTP 매체 정보를 수신하고, 상기 OTP 매체 정보를 기반으로 OTP 장치(200)에서 상기 생체 인식 정보를 이용하여 생성하는 N자리수의 OTP를 인증하기 위한 서버측 OTP 생성 정보를 생성(또는 할당)하고(315), 상기 OTP 매체 정보와 생체 인식 정보 및 서버측 OTP 생성 정보를 연계하여 저장매체(240)에 저장한다(320).

[0223] 이후, 상기 서버는 서버측 OTP 생성 정보와 매칭되는 단말측 OTP 생성 정보를 포함하고, 상기 생체 인식 정보를 이용하여 N자리수의 OTP를 생성하는 OTP 장치(200)를 상기 사용자에게 제공되도록 처리한다(325).

[0225] 도면4는 본 발명의 일 실시 방법에 따른 OTP 생성 과정을 도시한 도면이다.

[0227] 보다 상세하게 본 도면4는 상기 도면1에 도시된 OTP 장치(200)에서 상기 생체 인식 정보를 이용하여 N자리수의 OTP를 생성하는 과정을 도시한 것으로서, 구체적으로 상기 OTP 장치(200)의 메모리부에 상기 생체 인식 정보와 비교(또는 검증 연산)될 생체 인증 정보가 구비된 경우, 상기 생체 인증 정보를 통해 상기 생체 인식 정보를 이용한 OTP 생성 유효성을 확인하는 과정을 포함하는 실시 방법을 도시한 것이다.

[0229] 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면4를 참조 및/또는 변형하여 상기 OTP 생성 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면4에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0231] 예컨대, 본 도면4는 상기 생체 인식 정보와 생체 인증 정보를 통해 상기 OTP 생성 유효성을 확인하는 과정을 포함함에 의해 사용자의 비밀번호(또는 개인식별번호)를 통한 사용자 인증 과정은 편의상 생략하였으나, 이에 의

해 본 발명이 한정되는 것은 결코 아니며, 상기 사용자 인증 과정이 더 제공되어도 무방하다.

[0233] 이하, 본 도면4에서 상기 도면2에 도시된 OTP 운영 시스템을 편의상 "서버"라고 한다.

[0235] 도면4를 참조하면, 상기 OTP 장치(200)는 키 입력수단을 통해 N자리수의 OTP를 생성하도록 요청하는 전용 키 버튼이 입력되거나, 또는 기 설정된 메뉴 선택을 통해 상기 N자리수의 OTP를 생성하도록 요청되면, 상기 OTP 장치(200)에 구비된 지문 인식모듈 또는 카메라 모듈 중 어느 하나에 대응하는 생체 인식모듈을 통해 사용자의 지문 인식 정보, 홍채 인식 정보, 망막 인식 정보, 안면 인식 정보 중 어느 하나에 대응하는 생체 인식 정보를 인식하여 획득한다(400).

[0237] 만약 상기 사용자 생체 인식 기능을 통해 상기 생체 인식 정보가 획득되면(405), 상기 OTP 장치(200)는 상기 획득된 생체 인식 정보와 상기 메모리부에 구비된 생체 인증 정보를 비교(또는 검증 연산)하여 상기 생체 인식 정보를 포함하는 OTP 생성 정보를 통해 N자리수의 OTP를 생성하는 OTP 유효성을 확인한다(410).

[0239] 만약 상기 OTP 유효성이 확인되지 않으면(415), 상기 OTP 장치(200)는 OTP 생성 유효성 오류 정보를 출력하고(420), 상기 OTP 생성 과정을 종료한다.

[0241] 반면 상기 OTP 유효성이 확인되면(415), 상기 OTP 장치(200)는 상기 생체 인식 정보를 상기 N자리수의 OTP를 생성하기 위한 고정 씨드 값으로 포함하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성한다(425).

[0243] 본 발명의 실시 방법에 따르면, 상기 OTP 장치(200)는 상기 메모리부로부터 단말측 OTP 생성 정보를 확인하며, 상기 OTP 장치(200)는 상기 생체 인식 정보를 상기 N자리수의 OTP를 생성하기 위한 고정 씨드 값으로 처리한 후, 상기 확인된 단말측 OTP 생성 정보와 상기 생체 인식 정보를 조합하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0245] 만약 상기 N자리수의 OTP가 시간-동기화 방식의 OTP라면, 상기 OTP 장치(200)는 상기 OTP 장치(200)에 구비된 타이머로부터 확인되는 시간 값(또는 특정 시간 구간에 대한 시간 값)을 결정하고, 상기 결정된 시간 값을 상기 OTP 생성 정보의 동적 씨드 값으로 포함시켜 상기 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0247] 또는, 상기 N자리수의 OTP가 챌린지-동기화 방식의 OTP라면, 상기 OTP 장치(200)는 소정의 난수 값을 생성하여 서버와 전송/교환하거나, 또는 상기 서버에서 생성한 난수 값을 수신/교환한 후, 상기 난수 값을 상기 OTP 생성 정보의 동적 씨드 값으로 포함시켜 상기 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0249] 만약 상기 생체 인식 정보를 고정 씨드 값으로 포함하는 OTP 생성 정보가 구성되면(430), 상기 OTP 장치(200)는 상기 구성된 OTP 생성 정보에 포함된 하나 이상의 고정 씨드 값을 확인하고, 상기 OTP 생성 정보에 포함된 파라미터를 통해 하나 이상의 동적 씨드 값을 결정하고, 상기 확인/결정된 하나 이상의 고정 씨드 값과 동적 씨드 값을 기 설정된 OTP 생성 알고리즘에 대입하여 N자리수의 OTP를 생성하여 출력한다(435).

[0251] 도면5는 본 발명의 다른 일 실시 방법에 따른 OTP 생성 과정을 도시한 도면이다.

[0253] 보다 상세하게 본 도면5는 상기 도면1에 도시된 OTP 장치(200)에서 상기 생체 인식 정보를 이용하여 N자리수의 OTP를 생성하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면5를 참조 및/또는 변형하여 상기 OTP 생성 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면5에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0255] 이하, 본 도면5에서 상기 도면2에 도시된 OTP 운영 시스템을 편의상 "서버"라고 한다.

[0257] 도면5를 참조하면, 상기 OTP 장치(200)는 키 입력수단을 통해 N자리수의 OTP를 생성하도록 요청하는 전용 키 버튼이 입력되거나, 또는 기 설정된 메뉴 선택을 통해 상기 N자리수의 OTP를 생성하도록 요청되면, 상기 생체 인식 정보를 이용하여 N자리수의 OTP를 생성하기 위한 사용자 인증을 요청하고(500), 비밀번호(또는 개인식별번호)를 통해 사용자 인증을 처리한다(505).

[0259] 만약 상기 사용자 인증이 처리되지 않는다면(510), 상기 OTP 장치(200)는 사용자 인증 오류 정보를 출력하고(515), 상기 OTP 생성 과정을 종료한다.

[0261] 반면 상기 사용자 인증이 처리되면(510), 상기 OTP 장치(200)는 상기 OTP 장치(200)에 구비된 지문 인식모듈 또

는 카메라 모듈 중 어느 하나에 대응하는 생체 인식모듈을 통해 사용자의 지문 인식 정보, 홍채 인식 정보, 망막 인식 정보, 안면 인식 정보 중 어느 하나에 대응하는 생체 인식 정보를 인식하여 획득한다(520).

[0263] 만약 상기 사용자 생체 인식 기능을 통해 상기 생체 인식 정보가 획득되면(525), 상기 OTP 장치(200)는 상기 생체 인식 정보를 상기 N자리수의 OTP를 생성하기 위한 고정 씨드 값으로 포함하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성한다(530).

[0265] 본 발명의 실시 방법에 따르면, 상기 OTP 장치(200)는 상기 메모리부로부터 단말측 OTP 생성 정보를 확인하며, 상기 OTP 장치(200)는 상기 생체 인식 정보를 상기 N자리수의 OTP를 생성하기 위한 고정 씨드 값으로 처리한 후, 상기 확인된 단말측 OTP 생성 정보와 상기 생체 인식 정보를 조합하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0267] 만약 상기 N자리수의 OTP가 시간-동기화 방식의 OTP라면, 상기 OTP 장치(200)는 상기 OTP 장치(200)에 구비된 타이머로부터 확인되는 시간 값(또는 특정 시간 구간에 대한 시간 값)을 결정하고, 상기 결정된 시간 값을 상기 OTP 생성 정보의 동적 씨드 값으로 포함시켜 상기 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0269] 또는, 상기 N자리수의 OTP가 챌린지-동기화 방식의 OTP라면, 상기 OTP 장치(200)는 소정의 난수 값을 생성하여 서버와 전송/교환하거나, 또는 상기 서버에서 생성한 난수 값을 수신/교환한 후, 상기 난수 값을 상기 OTP 생성 정보의 동적 씨드 값으로 포함시켜 상기 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 것이 바람직하다.

[0271] 만약 상기 생체 인식 정보를 고정 씨드 값으로 포함하는 OTP 생성 정보가 구성되면(535), 상기 OTP 장치(200)는 상기 구성된 OTP 생성 정보에 포함된 하나 이상의 고정 씨드 값을 확인하고, 상기 OTP 생성 정보에 포함된 파라미터를 통해 하나 이상의 동적 씨드 값을 결정하고, 상기 확인/결정된 하나 이상의 고정 씨드 값과 동적 씨드 값을 기 설정된 OTP 생성 알고리즘에 대입하여 N자리수의 OTP를 생성하여 출력한다(540).

[0273] 도면6은 본 발명의 실시 방법에 따른 OTP 인증 과정을 도시한 도면이다.

[0275] 보다 상세하게 본 도면6은 상기 도면2에 도시된 OTP 운영 시스템에서 통신망을 통해 상기 도면4 내지 도면5에 도시된 과정을 통해 상기 도면1에 도시된 OTP 장치(200)에 의해 생성된 N(N>=2)자리수의 OTP를 수신하고, 상기 OTP와 매칭되는 N자리수의 OTP' 를 생성하고, 상기 수신된 N자리수의 OTP와 OTP' 를 비교(또는 검증)하여 OTP 유효성을 인증하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면6을 참조 및/또는 변형하여 상기 OTP 인증 과정에 대한 다양한 실시 방법(예컨대, 일부 단계가 생략되거나, 또는 순서가 변경된 실시 방법)을 유추할 수 있을 것이나, 본 발명은 상기 유추되는 모든 실시 방법을 포함하여 이루어지며, 본 도면6에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

[0277] 이하, 본 도면6에서 상기 도면2에 도시된 OTP 운영 시스템을 편의상 "서버"라고 한다.

[0279] 도면6을 참조하면, 상기 도면4 내지 도면5에 도시된 과정을 통해 상기 도면1에 도시된 OTP 장치(200)에 의해 N자리수의 OTP가 생성/출력된 후, 상기 서버는 상기 도면2에 도시된 사용자 단말(205)로 출력된 OTP 입력 인터페이스를 통해 입력된 상기 N자리수의 OTP를 수신 및 OTP 매체 정보를 확인하고(600), 상기 OTP 장치(200)에 대한 생체 인식 정보를 확인하고, 상기 저장매체(240)로부터 상기 OTP 매체 정보와 연계된 서버측 OTP 생성 정보를 확인한 후(605), 상기 생체 인식 정보와 서버측 OTP 생성 정보를 조합(또는 연계)하여 상기 생체 인식 정보를 고정 씨드 값으로 포함하는 OTP 생성 정보를 확인/구성한다(610).

[0281] 본 발명의 실시 방법에 따라 상기 서버측 OTP 생성 정보가 상기 생체 인식 정보를 고정 씨드 값으로 기 포함하고 있으면, 상기 서버는 상기 서버측 OTP 생성 정보를 상기 N자리수의 OTP' 를 생성하기 위한 OTP 생성정보로 확인하는 것이 바람직하다.

[0283] 이후, 상기 서버는 상기 OTP 생성 정보로부터 상기 N자리수의 OTP' 을 생성하기 위한 하나 이상의 고정 씨드 값을 확인하고, 상기 OTP 생성 정보에 포함된 파라미터를 통해 하나 이상의 동적 씨드 값을 결정하고, 상기 확인/결정된 하나 이상의 고정 씨드 값과 동적 씨드 값을 기 설정된 OTP 생성 알고리즘에 대입하여 N자리수의 OTP' 를 생성한다(615).

[0285] 만약 상기 N자리수의 OTP' 가 생성되면(620), 상기 서버는 상기 수신된 N자리수의 OTP와 OTP' 를 비교(또는 검증 연산)하여 상기 OTP 유효성을 확인한다(625).

[0287] 본 발명의 실시 방법에 따르면, 상기 OTP와 OTP' 의 비교 결과 상기 OTP와 OTP' 가 일치(또는 매칭)되거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되면, 상기 서버는 상기 OTP 유효성이 확인된 것으로 처리한다.

[0289] 만약 상기 OTP 유효성이 확인되지 않으면(630), 상기 서버는 OTP 유효성 오류에 대응하는 OTP 인증 결과를 기 설정된 OTP 인증결과 수신수단(예컨대, OTP 인증요청 서버(210), 사용자 단말(205), OTP 장치(200) 중 하나 이상의 포함)으로 제공한다(635).

[0291] 반면 상기 OTP 유효성이 확인되면(630), 상기 서버는 OTP 유효성 확인에 대응하는 OTP 인증결과를 기 설정된 OTP 인증결과 수신수단(예컨대, OTP 인증요청 서버(210), 사용자 단말(205), OTP 장치(200) 중 하나 이상의 포함)으로 제공한다(640).

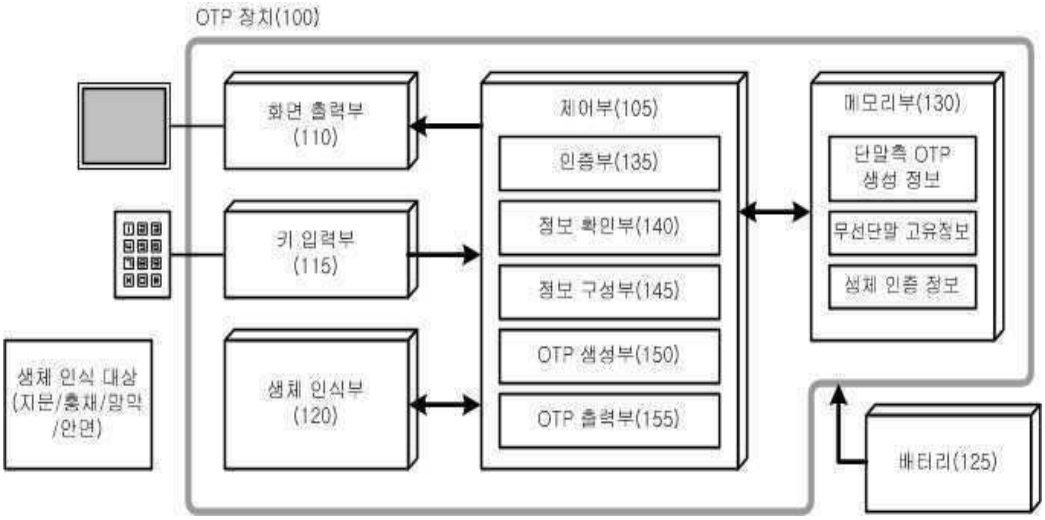
부호의 설명

[0293]

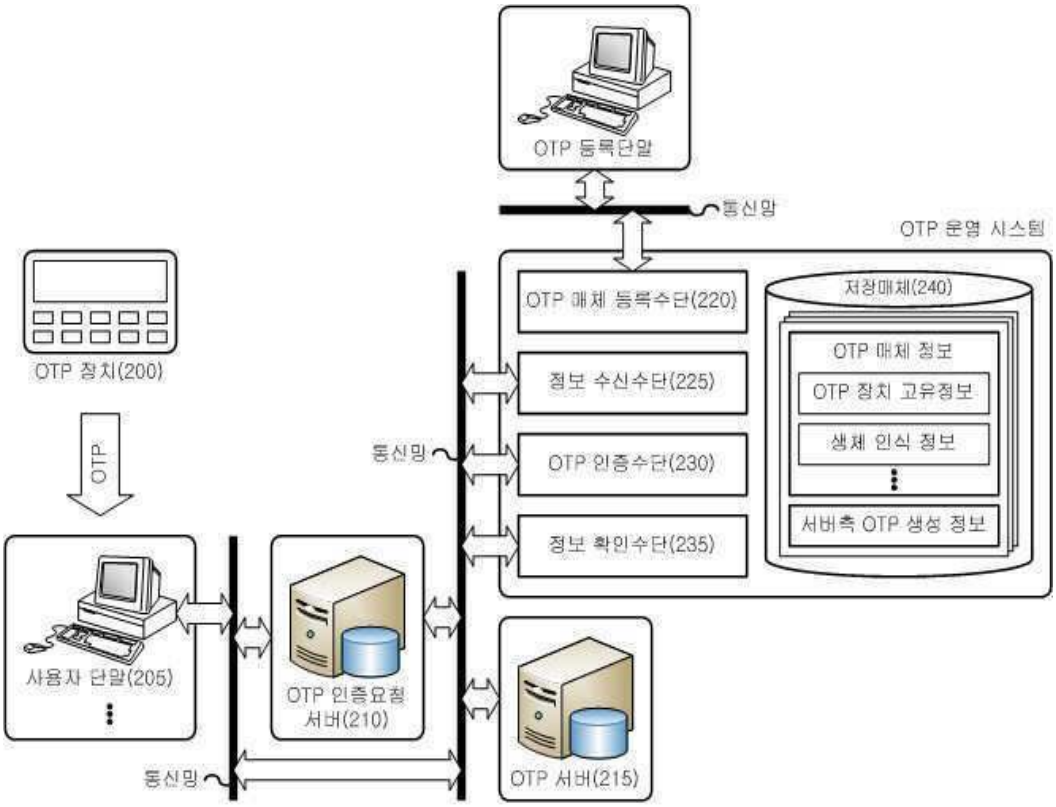
100 : OTP 장치
105 : 제어부
110 : 화면 출력부
115 : 키 입력부
120 : 생체 인식부
125 : 배터리
130 : 메모리부
135 : 인증부
140 : 정보 확인부
145 : 정보 구성부
150 : OTP 생성부
155 : OTP 출력부

도면

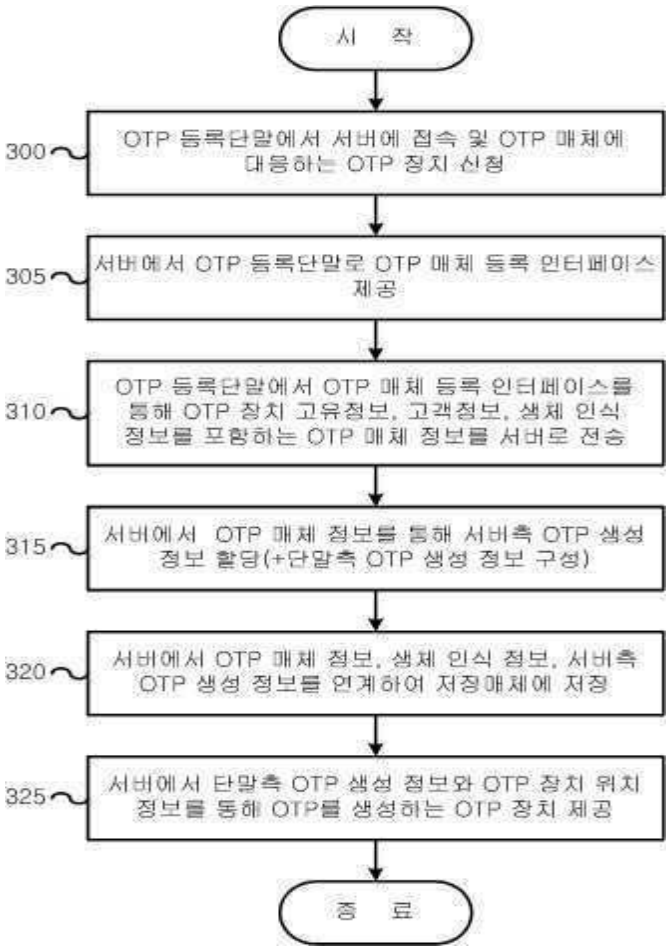
도면1



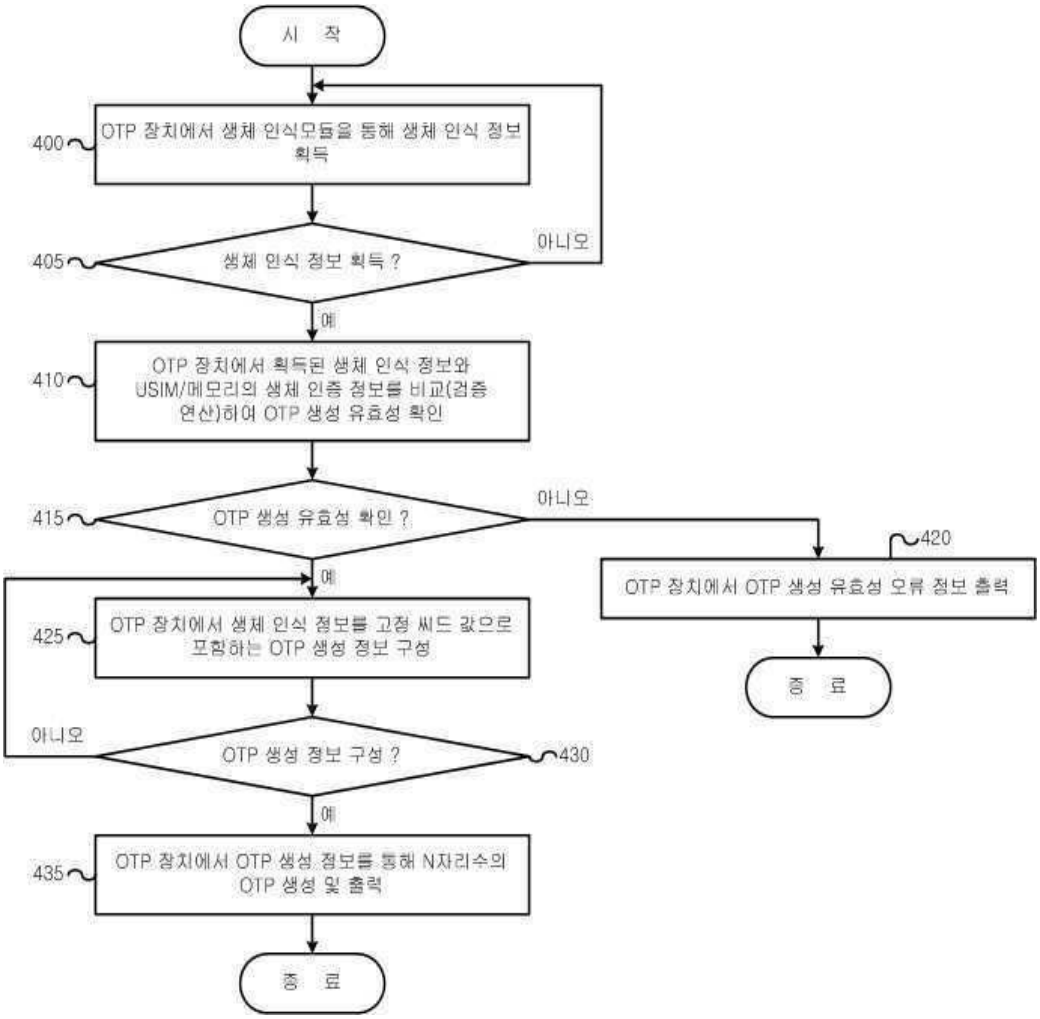
도면2


OTP 등록단말
통신망
OTP 운영 시스템
OTP 매체 등록수단(220)
정보 수신수단(225)
OTP 인증수단(230)
정보 확인수단(235)
저장매체(240)
OTP 매체 정보
OTP 장치 고유정보
생체 인식 정보
서버측 OTP 생성 정보
OTP 장치(200)
OTP
통신망
사용자 단말(205)
OTP 인증요청 서버(210)
OTP 서버(215)
통신망

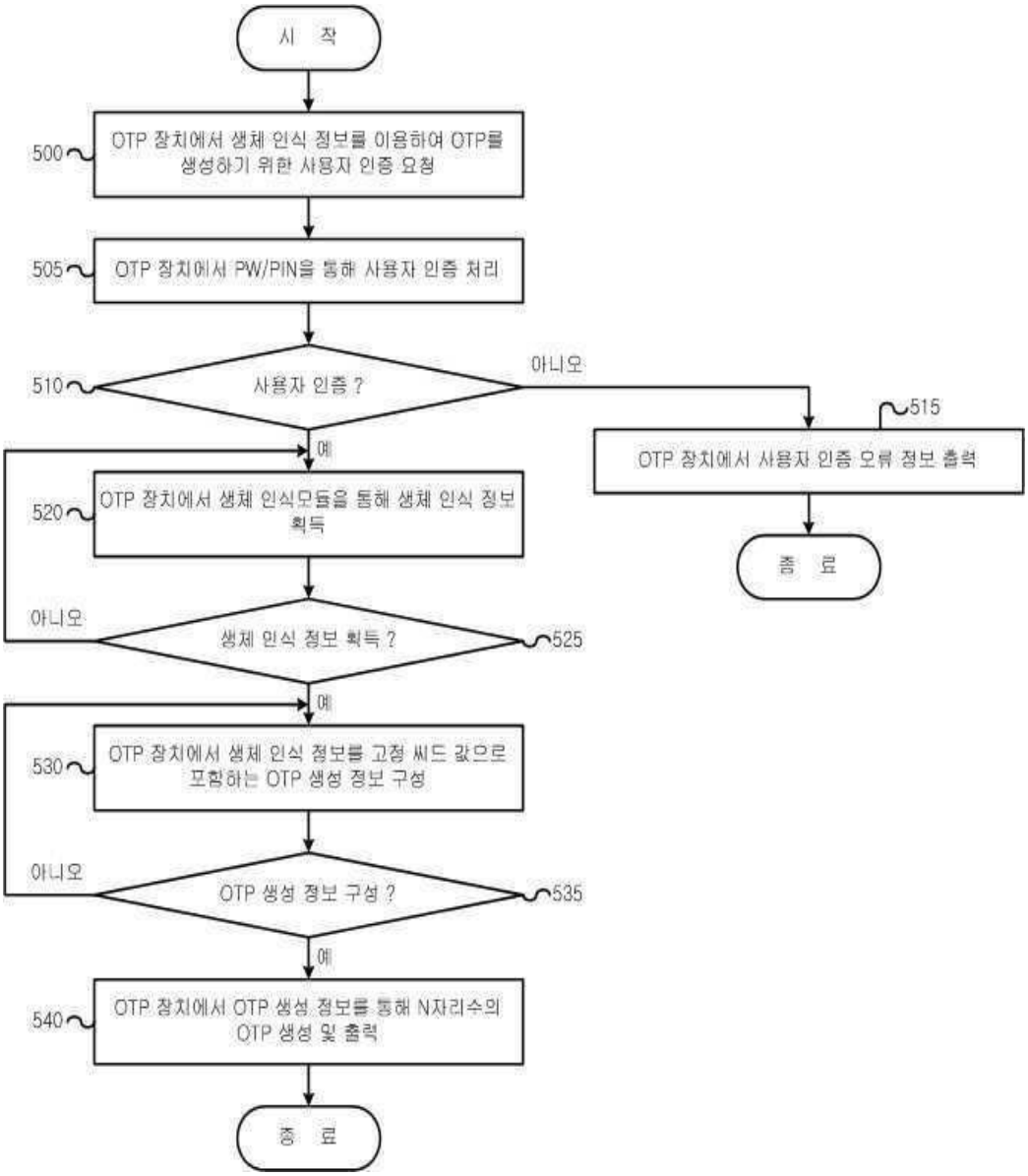
도면3


시 작
300
OTP 등록단말에서 서버에 접속 및 OTP 매체에 대응하는 OTP 장치 신청
305
서버에서 OTP 등록단말로 OTP 매체 등록 인터페이스 제공
310
OTP 등록단말에서 OTP 매체 등록 인터페이스를 통해 OTP 장치 고유정보, 고객정보, 생체 인식 정보를 포함하는 OTP 매체 정보를 서버로 전송
315
서버에서 OTP 매체 정보를 통해 서버측 OTP 생성 정보 할당(+단말측 OTP 생성 정보 구성)
320
서버에서 OTP 매체 정보, 생체 인식 정보, 서버측 OTP 생성 정보를 연계하여 저장매체에 저장
325
서버에서 단말측 OTP 생성 정보와 OTP 장치 위치 정보를 통해 OTP를 생성하는 OTP 장치 제공
종 료

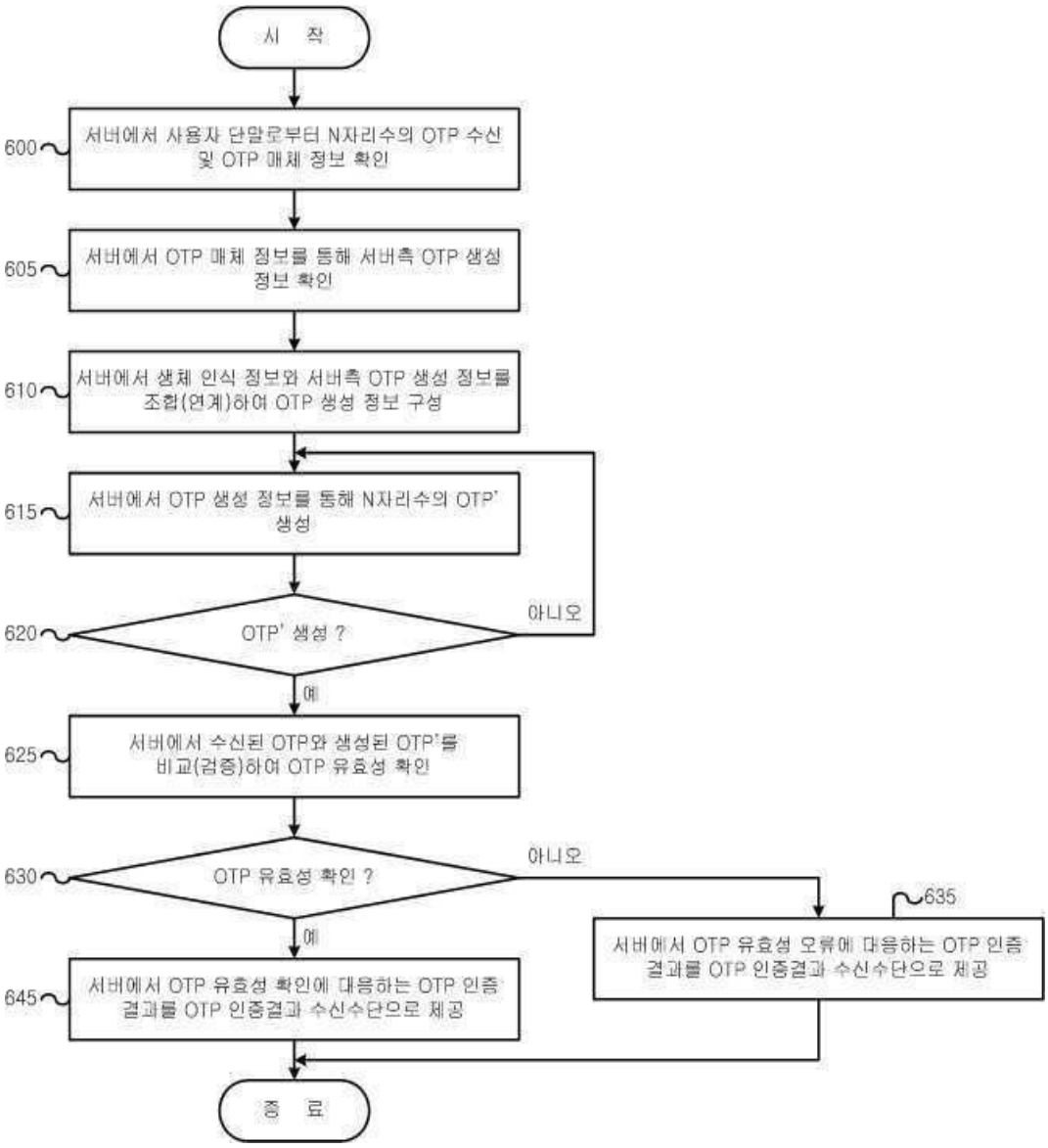
도면4


시 작
400
OTP 장치에서 생체 인식모듈을 통해 생체 인식 정보 획득
405
생체 인식 정보 획득 ?
아니오
예
410
OTP 장치에서 획득된 생체 인식 정보와 USIM/메모리의 생체 인증 정보를 비교(검증 연산)하여 OTP 생성 유효성 확인
415
OTP 생성 유효성 확인 ?
아니오
420
OTP 장치에서 OTP 생성 유효성 오류 정보 출력
종 료
예
425
OTP 장치에서 생체 인식 정보를 고정 씨드 값으로 포함하는 OTP 생성 정보 구성
아니오
OTP 생성 정보 구성 ?
430
예
435
OTP 장치에서 OTP 생성 정보를 통해 N자리수의 OTP 생성 및 출력
종 료

도면5


시 작
500
OTP 장치에서 생체 인식 정보를 이용하여 OTP를 생성하기 위한 사용자 인증 요청
505
OTP 장치에서 PW/PIN을 통해 사용자 인증 처리
510
사용자 인증 ?
아니오
515
OTP 장치에서 사용자 인증 오류 정보 출력
종 료
예
520
OTP 장치에서 생체 인식모듈을 통해 생체 인식 정보 획득
아니오
생체 인식 정보 획득 ?
525
예
530
OTP 장치에서 생체 인식 정보를 고정 씨드 값으로 포함하는 OTP 생성 정보 구성
아니오
OTP 생성 정보 구성 ?
535
예
540
OTP 장치에서 OTP 생성 정보를 통해 N자리수의 OTP 생성 및 출력
종 료

도면6


시 작
600
서버에서 사용자 단말로부터 N자리수의 OTP 수신 및 OTP 매체 정보 확인
605
서버에서 OTP 매체 정보를 통해 서버측 OTP 생성 정보 확인
610
서버에서 생체 인식 정보와 서버측 OTP 생성 정보를 조합(연계)하여 OTP 생성 정보 구성
615
서버에서 OTP 생성 정보를 통해 N자리수의 OTP' 생성
620
OTP' 생성 ?
아니오
예
625
서버에서 수신된 OTP와 생성된 OTP'를 비교(검증)하여 OTP 유효성 확인
630
OTP 유효성 확인 ?
아니오
예
635
서버에서 OTP 유효성 오류에 대응하는 OTP 인증 결과를 OTP 인증결과 수신수단으로 제공
645
서버에서 OTP 유효성 확인에 대응하는 OTP 인증 결과를 OTP 인증결과 수신수단으로 제공
종 료