



(19) 대한민국특허청(KR)  
(12) 등록특허공보(B1)

(45) 공고일자 2016년10월17일  
(11) 등록번호 10-1663699  
(24) 등록일자 2016년09월30일

- (51) 국제특허분류(Int. Cl.)  
G06F 21/32 (2013.01) G06Q 20/30 (2012.01)  
H04L 9/32 (2006.01) H04W 12/06 (2009.01)
- (52) CPC특허분류  
G06F 21/32 (2013.01)  
G06Q 20/30 (2013.01)
- (21) 출원번호 10-2015-0102505(분할)
- (22) 출원일자 2015년07월20일  
심사청구일자 2015년07월20일
- (65) 공개번호 10-2015-0090005
- (43) 공개일자 2015년08월05일
- (62) 원출원 특허 10-2009-0054667  
원출원일자 2009년06월18일  
심사청구일자 2014년06월18일
- (56) 선행기술조사문헌  
KR1020070084801 A\*  
KR1020080075956 A  
KR1020090051147 A  
\*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, 동양그라데아)

전체 청구항 수 : 총 3 항

심사관 : 문남두

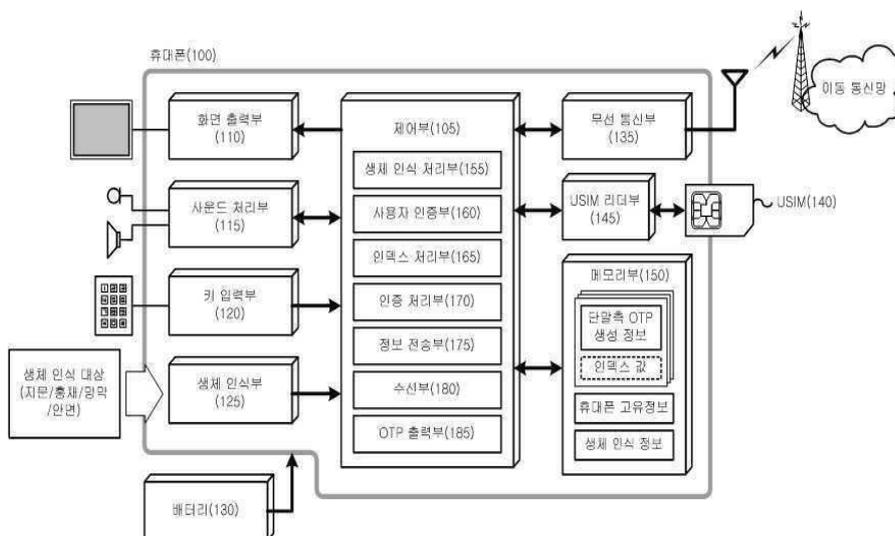
(54) 발명의 명칭 생체 인식을 이용한 네트워크 형 오티피 제공 방법

(57) 요약

본 발명의 생체 인식을 이용한 네트워크 형 오티피 제공 방법에 관한 것으로, 서버에 의해 실행되는 방법에 있어서, OTP를 구현하는 프로그램을 설치 구동한 사용자 휴대폰을 지정된 인증 절차의 OTP(One Time Password)를 구현하는 사용자 소유의 매체로 인증하기 위한 매체 정보를 확인하여 지정된 저장매체에 저장시키는 절차와, 상기

(뒷면에 계속)

대표도 - 도1



사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체 인증을 확인하기 위한 인증 정보를 확인하여 지정된 저장매체에 저장시키는 절차를 수행하고, 상기 사용자 휴대폰에서 상기 프로그램 구동 시, 상기 프로그램을 구동한 상태의 사용자 휴대폰과 통신하여 상기 매체 정보를 기반으로 상기 프로그램을 구동한 상태의 사용자 휴대폰을 상기 OTP를 구현하는 사용자 소유의 매체로 인증받기 위한 절차를 수행하고, 상기 인증 정보를 근거로 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체를 상기 사용자 휴대폰에서 구동된 상기 프로그램을 통해 인증한 결과 또는 상기 사용자 생체를 상기 사용자 휴대폰에 인터페이스된 IC칩을 통해 인증한 결과를 확인하고, 상기 프로그램을 구동한 상태의 사용자 휴대폰이 상기 OTP를 구현하는 사용자 소유의 매체로 인증되고 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체가 인증된 경우, 서버 측에서 동적 생성된  $N(N \geq 2)$ 자리수의 OTP를 확인하고, 상기 인증된 사용자 휴대폰의 프로그램으로 상기 N자리수의 OTP를 제공하는 절차를 수행하며, 상기 매체 정보는, 상기 프로그램을 설치 구동한 상태의 휴대폰을 인증하기 위해 상기 사용자 휴대폰에 상기 프로그램이 설치되어 최초 구동 시에 중복되지 않게 고유 할당되어 상기 사용자 휴대폰에 저장된 고유 값을 포함하여 이루어진다.

(52) CPC특허분류

*H04L 9/3228* (2013.01)

*H04L 9/3231* (2013.01)

*H04W 12/06* (2013.01)

## 명세서

### 청구범위

#### 청구항 1

서버에 의해 실행되는 방법에 있어서,

OTP를 구현하는 프로그램을 설치 구동한 사용자 휴대폰을 지정된 인증 절차의 OTP(One Time Password)를 구현하는 사용자 소유의 매체로 인증하기 위한 매체 정보를 확인하여 지정된 저장매체에 저장시키는 절차와, 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체 인증을 확인하기 위한 인증 정보를 확인하여 지정된 저장매체에 저장시키는 절차를 수행하는 제1 단계;

상기 사용자 휴대폰에서 상기 프로그램 구동 시, 상기 프로그램을 구동한 상태의 사용자 휴대폰과 통신하여 상기 매체 정보를 기반으로 상기 프로그램을 구동한 상태의 사용자 휴대폰을 상기 OTP를 구현하는 사용자 소유의 매체로 인증받기 위한 절차를 수행하고, 상기 인증 정보를 근거로 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체를 상기 사용자 휴대폰에서 구동된 상기 프로그램을 통해 인증한 결과 또는 상기 사용자 생체를 상기 사용자 휴대폰에 인터페이스된 IC칩을 통해 인증한 결과를 확인하는 제2 단계;

상기 프로그램을 구동한 상태의 사용자 휴대폰이 상기 OTP를 구현하는 사용자 소유의 매체로 인증되고 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체가 인증된 경우, 서버 측에서 동적 생성된  $N(N \geq 2)$ 자릿수의 OTP를 확인하는 제3 단계; 및

상기 인증된 사용자 휴대폰의 프로그램으로 상기 N자릿수의 OTP를 제공하는 절차를 수행하는 제4 단계;를 포함하며,

상기 매체 정보는, 상기 프로그램을 설치 구동한 상태의 휴대폰을 인증하기 위해 상기 사용자 휴대폰에 상기 프로그램이 설치되어 최초 구동 시에 중복되지 않게 고유 할당되어 상기 사용자 휴대폰에 저장된 고유 값을 포함하여 이루어지는 것을 특징으로 하는 생체 인식을 이용한 네트워크 형 오티피 제공 방법.

#### 청구항 2

삭제

#### 청구항 3

제 1항에 있어서, 상기 매체 정보는,

상기 휴대폰의 메모리부에 저장된 고유정보,

상기 휴대폰에 인터페이스된 IC칩으로부터 제공된 코드정보 중 하나 이상을 더 포함하여 이루어지는 것을 특징으로 하는 생체 인식을 이용한 네트워크 형 오티피 제공 방법.

#### 청구항 4

삭제

#### 청구항 5

제 1항에 있어서,

사용자 단말 또는 사용자 휴대폰으로부터 상기 사용자 휴대폰의 프로그램으로 제공된 N자리수의 OTP를 수신하는 제5 단계; 및

상기 수신된 OTP의 유효성을 인증하는 절차를 수행하는 제6 단계;를 더 포함하여 이루어지는 것을 특징으로 하는 생체 인식을 이용한 네트워크 형 오티피 제공 방법.

**청구항 6**

삭제

**발명의 설명**

**기술 분야**

[0001] 본 발명은, 서버에 의해 실행되는 방법에 있어서, OTP를 구현하는 프로그램을 설치 구동한 사용자 휴대폰을 지정한 인증 절차의 OTP(One Time Password)를 구현하는 사용자 소유의 매체로 인증하기 위한 매체 정보를 확인하여 지정한 저장매체에 저장시키는 절차와, 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체 인증을 확인하기 위한 인증 정보를 확인하여 지정한 저장매체에 저장시키는 절차를 수행하고, 상기 사용자 휴대폰에서 상기 프로그램 구동 시, 상기 프로그램을 구동한 상태의 사용자 휴대폰과 통신하여 상기 매체 정보를 기반으로 상기 프로그램을 구동한 상태의 사용자 휴대폰을 상기 OTP를 구현하는 사용자 소유의 매체로 인증받기 위한 절차를 수행하고, 상기 인증 정보를 근거로 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체를 상기 사용자 휴대폰에서 구동된 상기 프로그램을 통해 인증한 결과 또는 상기 사용자 생체를 상기 사용자 휴대폰에 인터페이스된 IC칩을 통해 인증한 결과를 확인하고, 상기 프로그램을 구동한 상태의 사용자 휴대폰이 상기 OTP를 구현하는 사용자 소유의 매체로 인증되고 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체가 인증된 경우, 서버 측에서 동적 생성된  $N(N \geq 2)$ 자리수의 OTP를 확인하고, 상기 인증된 사용자 휴대폰의 프로그램으로 상기 N자리수의 OTP를 제공하는 절차를 수행하며, 상기 매체 정보는, 상기 프로그램을 설치 구동한 상태의 휴대폰을 인증하기 위해 상기 사용자 휴대폰에 상기 프로그램이 설치되어 최초 구동 시에 중복되지 않게 고유 할당되어 상기 사용자 휴대폰에 저장된 고유 값을 포함하여 이루어지는 생체 인식을 이용한 네트워크 형 오티피 제공 방법에 관한 것이다.

**배경 기술**

[0003] 휴대폰 결제는 사용자가 사용자 단말을 통해 휴대폰번호와 가입자 정보를 입력하여 제공하면, 상기 휴대폰번호와 가입자 정보를 통해 상기 고객이 통신사의 유효한 가입자인지 인증한 후, 상기 가입자 인증 결과에 따라 소정의 인증번호를 생성하여 상기 사용자 휴대폰으로 전송한 후, 상기 사용자 단말을 통해 수신되는 인증번호와 상기 사용자 휴대폰으로 전송한 인증번호를 비교하여 매칭되면, 이를 승인하여 상기 사용자 휴대폰의 익월 통신요금에 결제금액을 과금하는 결제 방식이다(출원번호: 10-2000-0020757).

[0005] 그러나, 개인정보 유출사고가 비일비재하게 발생하고, 또한 이렇게 유출된 개인정보가 인터넷을 통해 공공연하게 거래(또는 공개)되고 있고, 휴대폰 분실 건수가 한달 평균 20만 건 이상 발생(2003.07.24자 디지털타임즈)하는 상황에서 타인의 휴대폰을 습득하거나, 또는 복제한 자는 누구라도 상기 유출된 개인정보를 이용하여 휴대폰 결제를 승인 받을 수 있는 문제점을 지니고 있다.

[0007] 특히, 상기 휴대폰 결제 승인은 실시간 이루어지지만, 결제금액에 대한 정산은 평균적으로 결제승인 후 45일 이내에 이루어지는 휴대폰 결제의 특성 상, 상기 습득/복제된 휴대폰과 유출된 개인정보를 이용한 피해가 발생할 경우, 그 피해액은 천문학적 수치에 이를 것으로 예상된다.

**발명의 내용**

**해결하려는 과제**

[0009] 본 발명의 목적은, 서버에 의해 실행되는 방법에 있어서, OTP를 구현하는 프로그램을 설치 구동한 사용자 휴대폰을 지정한 인증 절차의 OTP(One Time Password)를 구현하는 사용자 소유의 매체로 인증하기 위한 매체 정보를 확인하여 지정한 저장매체에 저장시키는 절차와, 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체 인증을 확인하기 위한 인증 정보를 확인하여 지정한 저장매체에 저장시키는 절차를 수행하는 제1 단계와 상기 사용자 휴대폰에서 상기 프로그램 구동 시, 상기 프로그램을 구동한 상태의 사용자 휴대폰과 통신하여 상기 매체 정보를 기반으로 상기 프로그램을 구동한 상태의 사용자 휴대폰을 상기 OTP를 구현하는 사용자 소유의 매체로 인증받기 위한 절차를 수행하고, 상기 인증 정보를 근거로 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체를 상기 사용자 휴대폰에서 구동된 상기 프로그램을 통해 인증한 결과 또는 상기 사용자 생체를 상기 사용자 휴대폰에 인터페이스된 IC칩을 통해 인증한 결과를 확인하는 제2 단계와 상기 프로그램을 구동한 상

태의 사용자 휴대폰이 상기 OTP를 구현하는 사용자 소유의 매체로 인증되고 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체가 인증된 경우, 서버 측에서 동적 생성된  $N(N \geq 2)$ 자리수의 OTP를 확인하는 제3 단계 및 상기 인증된 사용자 휴대폰의 프로그램으로 상기  $N$ 자리수의 OTP를 제공하는 절차를 수행하는 제4 단계를 포함하며, 상기 매체 정보는, 상기 프로그램을 설치 구동한 상태의 휴대폰을 인증하기 위해 상기 사용자 휴대폰에 상기 프로그램이 설치되어 최초 구동 시에 중복되지 않게 고유 할당되어 상기 사용자 휴대폰에 저장된 고유 값을 포함하여 이루어지는 생체 인식을 이용한 네트워크 형 오티피 제공 방법을 제공함에 있다.

**과제의 해결 수단**

[0011] 본 발명에 따른 생체 인식을 이용한 네트워크 형 오티피 제공 방법은, 서버에 의해 실행되는 방법에 있어서, OTP를 구현하는 프로그램을 설치 구동한 사용자 휴대폰을 지정된 인증 절차의 OTP(One Time Password)를 구현하는 사용자 소유의 매체로 인증하기 위한 매체 정보를 확인하여 지정된 저장매체에 저장시키는 절차와, 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체 인증을 확인하기 위한 인증 정보를 확인하여 지정된 저장매체에 저장시키는 절차를 수행하는 제1 단계와 상기 사용자 휴대폰에서 상기 프로그램 구동 시, 상기 프로그램을 구동한 상태의 사용자 휴대폰과 통신하여 상기 매체 정보를 기반으로 상기 프로그램을 구동한 상태의 사용자 휴대폰을 상기 OTP를 구현하는 사용자 소유의 매체로 인증받기 위한 절차를 수행하고, 상기 인증 정보를 근거로 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체를 상기 사용자 휴대폰에서 구동된 상기 프로그램을 통해 인증한 결과 또는 상기 사용자 생체를 상기 사용자 휴대폰에 인터페이스된 IC칩을 통해 인증한 결과를 확인하는 제2 단계와 상기 프로그램을 구동한 상태의 사용자 휴대폰이 상기 OTP를 구현하는 사용자 소유의 매체로 인증되고 상기 사용자 휴대폰의 생체 인식부를 통해 인식된 사용자 생체가 인증된 경우, 서버 측에서 동적 생성된  $N(N \geq 2)$ 자리수의 OTP를 확인하는 제3 단계 및 상기 인증된 사용자 휴대폰의 프로그램으로 상기  $N$ 자리수의 OTP를 제공하는 절차를 수행하는 제4 단계를 포함하며, 상기 매체 정보는, 상기 프로그램을 설치 구동한 상태의 휴대폰을 인증하기 위해 상기 사용자 휴대폰에 상기 프로그램이 설치되어 최초 구동 시에 중복되지 않게 고유 할당되어 상기 사용자 휴대폰에 저장된 고유 값을 포함하여 이루어지는 것을 특징으로 한다.

[0012] 삭제

[0013] 본 발명에 따른 생체 인식을 이용한 네트워크 형 오티피 제공 방법에 있어서, 상기 매체 정보는, 상기 휴대폰의 메모리부에 저장된 고유정보, 상기 휴대폰에 인터페이스된 IC칩으로부터 제공된 코드정보 중 하나 이상을 더 포함하여 이루어지는 것을 특징으로 한다.

[0014] 삭제

[0015] 삭제

[0016] 삭제

[0017] 본 발명에 따른 생체 인식을 이용한 네트워크 형 오티피 제공 방법에 있어서, 사용자 단말 또는 사용자 휴대폰으로부터 상기 사용자 휴대폰의 프로그램으로 제공된  $N$ 자리수의 OTP를 수신하는 제5 단계 및 상기 수신된 OTP의 유효성을 인증하는 절차를 수행하는 제6 단계를 더 포함하여 이루어지는 것을 특징으로 한다.

[0018] 삭제

[0019] 삭제

- [0021] 삭제
- [0022] 삭제
- [0023] 본 발명에 따른 생체 인식과 연동하는 이중 코드 생성 방식의 네트워크 형 오티피 인증을 통한 휴대폰 결제 방법은, 서버에서 OTP(One Time Password) 매체로 등록된 휴대폰 고유정보 및 사용자의 생체로부터 인식되는 생체 인식 정보를 포함하는 OTP 매체 정보와, 상기 OTP 매체로 등록된 휴대폰의 USIM(또는 메모리)에 구비된 단말측 OTP 생성 정보 및  $N(N \geq 2)$ 자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 서버측 OTP 생성 정보를 저장매체에 저장, 유지하는 단계와, OTP를 이용한 휴대폰 결제를 요청한 사용자 단말로부터 이동통신사 선택정보 및 사용자 휴대폰번호와 사용자 주민등록번호 정보가 수신되면, 서버에서 상기 이동통신사를 통한 휴대폰 가입자 인증 결과에 따라 상기 사용자의 휴대폰과 통신채널을 연결하여 상기 휴대폰의 USIM(또는 메모리)에 저장된 휴대폰 고유정보와 상기 사용자의 생체로부터 인식된 생체 인식 정보를 포함하는 OTP 매체인증 정보를 수신하는 단계와, 상기 서버에서 상기 저장매체에 저장된 OTP 매체 정보와 상기 OTP 매체인증 정보를 비교(또는 검증 연산)하여 상기 휴대폰을  $N$ 자리수의 OTP를 생성(또는 출력)하는 OTP 매체로 인증하는 단계와, 상기 휴대폰을 OTP 매체로 인증 시, 상기 서버에서 상기 수신된 단말측 OTP 생성 정보를 통해 OTP를 생성하는 단계와, 상기 서버에서 상기 저장매체로부터 상기 사용자의 생체 인식과 연계된 서버측 OTP 생성 정보와 상기 생성된 OTP를 조합하여  $N$ 자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 단계와, 상기 서버에서 상기 구성된 OTP 생성 정보를 통해  $N$ 자리수의 OTP를 생성하여 상기 휴대폰으로 전송하는 단계와, 사용자 단말, 또는 상기 휴대폰에서 상기  $N$ 자리수의 OTP를 전송하면, 서버에서 상기 저장매체로부터 상기 사용자의 생체 인식과 연계된 단말측 OTP 생성 정보를 통해 OTP를 생성하고, 상기 저장매체로부터 상기 사용자의 생체 인식과 연계된 서버측 OTP 생성 정보와 상기 생성된 OTP를 조합하여 OTP 생성 정보를 구성하는 단계와, 상기 서버에서 상기 OTP 생성 정보를 통해  $N$ 자리수의 OTP' 를 생성하는 단계 및 상기 서버에서 상기 수신된  $N$ 자리수의 OTP와 상기 생성된  $N$ 자리수의 OTP' 를 비교(또는 검증 연산)하여 상기  $N$ 자리수의 OTP의 유효성을 인증하여 상기 휴대폰 결제를 승인하는 단계를 포함하여 이루어지는 것을 특징으로 한다.
- [0025] 본 발명에 따른 생체 인식과 연동하는 이중 코드 생성 방식의 네트워크 형 오티피 인증을 통한 휴대폰 결제 방법은, 상기 생체 인식 정보에 대응하는 코드 값을 상기  $N$ 자리수의 OTP를 생성하는 정보에 포함시키는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.
- [0027] 본 발명에 따른 생체 인식과 연동하는 이중 코드 생성 방식의 네트워크 형 오티피 인증을 통한 휴대폰 결제 방법은, 휴대폰에서 USIM(또는 메모리)에 저장된 휴대폰 고유정보와 상기 사용자의 생체로부터 인식된 생체 인식 정보를 포함하는 OTP 매체인증 정보와, 단말측 OTP 생성 정보를 통신망 상의 서버로 전송하는 단계 및 상기 서버에서 상기  $N$ 자리수의 OTP를 생성하여 전송하면, 상기 휴대폰에서 상기  $N$ 자리수의 OTP를 수신하여 출력하는 단계를 포함하여 이루어지는 것을 특징으로 한다.
- [0029] 본 발명에 따른 생체 인식과 연동하는 이중 코드 생성 방식의 네트워크 형 오티피 인증을 통한 휴대폰 결제 방법에 있어서, 상기 OTP 매체인증 정보는, 사용자 비밀번호 또는 사용자 개인식별번호를 더 포함하여 이루어지는 것을 특징으로 하며, 상기 서버는 상기 사용자 비밀번호 또는 사용자 개인식별번호를 통해 상기 휴대폰을 OTP 매체로 인증하는 단계를 더 포함하여 이루어지는 것을 특징으로 한다.
- [0031] 한편, 상기 전술한 생체 인식과 연동하는 이중 코드 생성 방식의 네트워크 형 오티피 인증을 통한 휴대폰 결제 방법을 실행하는 프로그램을 기록한 것을 특징으로 하는 컴퓨터로 판독 가능한 기록매체를 포함한다.
- [0033] 한편, 본 발명에 따른 생체 인식과 연동하는 이중 코드 생성 방식의 네트워크 형 오티피 인증을 통한 휴대폰 결제 시스템은, OTP(One Time Password) 매체로 등록된 휴대폰 고유정보 및 사용자의 생체로부터 인식되는 생체 인식 정보를 포함하는 OTP 매체 정보와, 상기 OTP 매체로 등록된 휴대폰의 USIM(또는 메모리)에 구비된 단말측 OTP 생성 정보 및  $N(N \geq 2)$ 자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 서버측 OTP 생성 정보를 저장하는 저장매체와, OTP를 이용한 휴대폰 결제를 요청한 사용자 단말로부터 이동통신사 선택정보 및 사용자 휴대폰번호와 사용자 주민등록번호 정보가 수신되면, 상기 이동통신사를 통한 휴대폰 가입자 인증 결과에 따라 상기 사용자의 휴대폰과 통신채널을 연결하여 상기 휴대폰의 USIM(또는 메모리)에 저장된 휴대폰 고유정보와 상기 사용자의 생체로부터 인식된 생체 인식 정보를 포함하는 OTP 매체인증 정보를 수신하는 정보 수신수단과, 상기 저장매체에 저장된 OTP 매체 정보와 상기 OTP 매체인증 정보를 비교(또는 검증 연산)하여 상기 휴대폰을  $N$ 자리수의

OTP를 생성(또는 출력)하는 OTP 매체로 인증하는 매체 인증수단과, 상기 휴대폰을 OTP 매체로 인증 시, 상기 수신된 단말측 OTP 생성 정보를 통해 OTP를 생성하는 OTP 생성수단과, 상기 저장매체로부터 상기 사용자의 생체 인식과 연계된 서버측 OTP 생성 정보와 상기 생성된 OTP를 조합하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성하는 정보 구성수단과, 상기 구성된 OTP 생성 정보를 통해 N자리수의 OTP를 상기 휴대폰으로 전송하는 OTP 전송수단과, 사용자 단말, 또는 상기 휴대폰으로부터 N자리수의 OTP가 수신되면, 상기 서버측 OTP 생성 정보와 단말측 OTP 생성 정보를 통해 N자리수의 OTP' 를 생성하여 상기 N자리수의 OTP의 유효성을 인증하는 OTP 인증수단 및 상기 N자리수의 OTP 유효성 인증 결과에 따라 상기 휴대폰 결제를 승인하는 결제 처리수단을 구비하여 이루어지는 것을 특징으로 한다.

[0035] 본 발명에 따른 생체 인식과 연동하는 이중 코드 생성 방식의 네트워크 형 오티피 인증을 통한 휴대폰 결제 시스템에 있어서, 상기 OTP 인증수단은, 상기 저장매체로부터 상기 사용자의 생체 인식과 연계된 단말측 OTP 생성 정보를 통해 OTP를 생성하고, 상기 저장매체로부터 상기 사용자의 생체 인식과 연계된 서버측 OTP 생성 정보와 상기 생성된 OTP를 조합하여 OTP 생성 정보를 구성한 후, 상기 OTP 생성 정보를 통해 N자리수의 OTP' 를 생성하고, 상기 수신된 N자리수의 OTP와 상기 생성된 N자리수의 OTP' 를 비교(또는 검증 연산)하여 상기 N자리수의 OTP의 유효성을 인증하는 것을 특징으로 한다.

**발명의 효과**

[0038] 본 발명에 따르면, OTP를 이용하여 휴대폰 결제를 승인하되, 사용자의 휴대폰에 구비된 휴대폰의 USIM(Universal Subscriber Identity Module) 또는 메모리 영역에 상기 OTP 생성에 필요한 정보의 일부만 저장하고, OTP를 생성할 때마다 상기 휴대폰이 유효한 OTP 매체인지 인증하고, 상기 사용자의 생체(예컨대, 지문, 홍채, 망막, 안면)를 인증하고, 상기 휴대폰 사용자가 유효한 사용자인지 인증함으로써, 타인의 휴대폰과 개인 정보를 이용하여 부정하게 휴대폰 결제가 승인되는 것을 미연에 차단하는 이점이 있다.

[0040] 본 발명의 다른 목적은, OTP를 이용하여 휴대폰 결제 시, 상기 인증 결과에 따라 통신망 상의 서버에서 상기 휴대폰으로부터 제공된 단말측 OTP 생성 정보를 통해 OTP를 생성하고, 상기 휴대폰을 통해 사용자의 생체로부터 인식되는 생체 인식 정보와 연계된 서버측 OTP 생성 정보와 상기 생성된 OTP를 조합한 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰으로 제공하면, 상기 휴대폰에서 상기 N자리수의 OTP를 수신하여 출력함으로써, 유효한 OTP 매체로 등록된 휴대폰에 의해서만 휴대폰 결제를 위한 N자리수의 OTP가 생성 및 출력되도록 하는 이점이 있다.

**도면의 간단한 설명**

- [0042] 도 1은 본 발명의 실시 방법에 따라 휴대폰 결제를 인증하기 위한 OTP를 생성하는 기능 구비한 휴대폰 기능 구성을 도시한 도면이다.
- 도 2는 본 발명의 실시 방법에 따라 휴대폰 결제를 인증하기 위한 휴대폰 OTP 시스템 구성을 도시한 도면이다.
- 도 3은 본 발명의 실시 방법에 따른 OTP 매체 등록 과정을 도시한 도면이다.
- 도 4는 본 발명의 실시 방법에 따른 OTP 생성 과정을 도시한 도면이다.
- 도 5는 본 발명의 실시 방법에 따른 생체 인식 처리 과정을 도시한 도면이다.
- 도 6은 본 발명의 실시 방법에 따른 OTP 인증 과정을 도시한 도면이다.
- 도 7은 본 발명의 실시 방법에 따른 OTP 기반 휴대폰 결제 처리 시스템 구성을 도시한 도면이다.
- 도 8은 본 발명의 일 실시 방법에 따른 OTP 기반 휴대폰 결제 과정을 도시한 도면이다.
- 도 9는 본 발명의 다른 일 실시 방법에 따른 OTP 기반 휴대폰 결제 과정을 도시한 도면이다.

**발명을 실시하기 위한 구체적인 내용**

[0043] 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, 하기에 서 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.

- [0045] 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.
- [0047] 도면1은 본 발명의 실시 방법에 따라 휴대폰(100) 결제를 인증하기 위한 OTP를 생성하는 기능 구비한 휴대폰(100) 기능 구성을 도시한 도면이다.
- [0049] 보다 상세하게 본 도면1은 이동 통신망에 접속하여 데이터 통신을 제공하는 휴대폰(100)이 상기 이동 통신망을 통해 상기 휴대폰(100)이 휴대폰(100) 결제를 인증하기 위한 OTP(One Time Password)를 생성하는 OTP 에이전트가 구비한 OTP 매체임을 인증한 후, 통신망의 서버로부터  $N(N \geq 2)$ 자리수의 OTP를 제공받아 출력하는 기능을 구비한 실시 방법을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면1을 참조 및/또는 변형하여 상기 휴대폰(100) 이외에 다른 무선 통신규격의 무선 통신망에 접속한 무선통신 단말(예컨대, 휴대인터넷단말 등)에서 상기 휴대폰(100) 결제를 인증하기 위한 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.
- [0051] 본 발명의 실시 방법에 따라 휴대폰(100)은, 하드웨어적인 측면에서 외형상 몸체(Body)와 스피커와 마이크, 키패드, LCD(Liquid Crystal Display), 안테나와 배터리(130) 등을 포함하여 구성되며, 내부적으로는 CDMA(Code Division Multiple Access) 모뎀, CPU/MPU(Central Processing Unit/ Micro Processing Unit), 보코더 등의 기능을 내장한 모뎀칩(예컨대, 미국 퀄컴(Qualcomm)사의 MSM 시리즈 모뎀칩)과, 각종 메모리 소자, 하나의 안테나에서 송수신 신호를 분리해 주는 듀플렉서 필터, 송신 신호를 증폭하는 파워 앰프, 고출력 증폭기(High Power Amplifier; HPA), 고출력 송신 신호가 반대로 되돌아오는 현상을 막아주는 아이솔레이터(Isolator), 원하는 대역 외 불요파 신호를 제거하기 위한 RF/IF SAW 필터, 송신 경로의 주파수 상향회로, 수신경로의 주파수 하향 변환회로, 기준 클럭원에 해당하는 VCTXO(Voltage Controlled Temperature Compensated X-tal Oscillator), 주파수 상하향 변환의 국부신호로 사용되는 UHF 주파수 합성기, 및 아날로그 음성신호를 디지털 신호로 변환하기 위한 코덱칩을 포함하여 이루어지는 것을 특징으로 하며, 상기와 같은 내부 구성요소는 점차적으로 상기 모뎀칩에 집적화 되고 있으며, 또한 상기 모뎀칩에는 상기와 같은 이동 통신 서비스를 위한 핵심적인 구성요소 외에 각종 멀티미디어 서비스 또는 각종 부가 서비스를 위한 다양한 기능들이 함께 집적화 되고 있다.
- [0053] 도면1을 참조하면, 상기 휴대폰(100)은, 상기 구성요소에 대응하는 구조 상에서 상기 모뎀칩에 대응하는 제어부(105)와, LCD(Liquid Crystal Display)에 대응하는 화면 출력부(110)와, 마이크/스피커에 대응하는 사운드 처리부(115)와, 키패드에 대응하는 키 입력부(120)와, 안테나 및 각종 RF모듈에 대응하는 무선 통신부(135)와, 비휘발성 메모리에 대응하는 메모리부(150)와, 범용가입자식별정보를 저장하는 IC(integrated Circuit)칩에 대응하는 USIM(140)(Universal Subscriber Identity Module)과, 상기 USIM(140)에 정보(또는 데이터)를 읽고/쓰기 위한 USIM 리더부(145) 및 전원 공급을 위한 배터리(130)를 구비하여 이루어지는 것을 특징으로 하며, 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 생체 인식 대상으로부터 사용자의 생체 정보를 인식하는 생체 인식부(125)를 구비하여 이루어지는 것을 특징으로 한다.
- [0055] 본 발명의 실시 방법에 따르면, 상기 사용자의 생체 인식 대상으로부터 인식되는 생체 정보는 기 설정된 생체 인식 방식에 따라 기 설정된 데이터 구조에 대응하는 생체 인식 정보로 변환되며, 상기 생체 인식 정보는 상기 휴대폰(100)에 구비된 OTP 에이전트를 구동하거나, 또는 상기 OTP 에이전트에서 OTP를 생성하는 것을 인증하는 OTP 구동 정보로 사용되거나, 상기 휴대폰(100)에 구비된 OTP 에이전트가 통신망 상의 서버로 전송하는 OTP 매체인증 정보에 포함되거나, 상기 휴대폰(100)에 구비된 OTP 에이전트가 OTP를 생성하는 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값으로 사용되는 것 중 하나 이상의 용도로 사용되는 것을 특징으로 한다.
- [0057] 상기 제어부(105)는 하드웨어적으로 상기 모뎀칩에 구비되는 CPU/MPU를 포함하는 프로세서와 실행 메모리를 포함하고, 메모리 소자로부터 휴대폰(100) 특유의 기능을 제공하기 위한 프로그램 루틴(Routine) 또는 프로그램 데이터를 입출력하는 버스(BUS) 및 이를 위해 구비되는 전자회로(또는 집적회로)를 포함하여 이루어지는 것을 특징으로 하며, 소프트웨어적으로 상기 메모리부(150) 또는 메모리 소자(또는 칩셋)으로부터 상기 실행 메모리로 로딩되어 특유의 기능을 수행하기 위해 상기 프로세서를 통해 연산 처리되는 프로그램 루틴 또는 프로그램 데이터의 총칭(따라서, 상기 휴대폰(100) 결제를 인증하기 위한 OTP를 생성하는 기능을 위해 휴대폰(100)의 기록매체에 기록되는 OTP 에이전트에 대응하는 프로그램 루틴 구성부를 편의상 본 제어부(105) 내에 구비되는 것으로 도시하여 설명함.)으로서, 상기 제어부(105)에 구비되는 프로그램 루틴은 기본적으로 운영체제 루틴(도시

생략)과 하나 이상의 시스템 관리 루틴(예컨대, 전원관리 루틴, 채널(순방향/역방향) 관리 루틴, 핸드오프 루틴 등, 도시생략)을 포함하여 이루어지는 것을 특징으로 하며, 상기 제어부(105)에 의해 휴대폰(100)에 구현하고자 하는 다양한 기능 구성들이 실현되는 것을 특징으로 한다.

- [0059] 본 발명의 실시 방법에 따르면, 상기 휴대폰(100)에 전원이 공급된 후, 상기 운영체제 루틴(도시생략)과 하나 이상의 시스템 관리 루틴(도시생략) 및 이에 대응하는 각종 시스템 변수들이 상기 제어부(105)에 구비된 실행 메모리로 로딩 및 상기 프로세서에 의해 연산 처리됨으로써, 상기 휴대폰(100)은 부팅절차에 따라 시스템 설정 세부 상태, 파일롯 채널 획득 세부 상태, 동기 채널 획득 세부 상태 및 타이밍 변환 세부 상태를 포함하는 "이동국 초기화 상태"에 대응하는 동작모드 설정된다.
- [0061] 상기 부팅절차를 수행한 후, 상기 운영체제 루틴(도시생략)과 하나 이상의 시스템 관리 루틴(도시생략) 및 이에 대응하는 각종 시스템 변수들이 상기 제어부(105)에 구비된 실행 메모리로 로딩 및 상기 프로세서에 의해 연산 처리됨으로써, 상기 휴대폰(100)은 "이동국 통화 대기 상태", 또는 "시스템 액세스 상태", 또는 "통화 채널 상태" 등에 대응하는 동작모드로 설정됨으로써, 이동통신 기반 무선 접속 및 호처리(Call Processing) 절차를 수행한다.
- [0063] 본 발명의 실시 방법에 따르면, 상기 OTP를 생성하는 기능은 상기 휴대폰(100)이 상기 "이동국 통화 대기 상태"에 대응하는 동작모드에서 키 입력을 통해 개시(또는 실현)되는 것이 바람직하다.
- [0065] 상기 화면 출력부(110)는 상기 휴대폰(100)의 각 동작모드 운용 및 이에 대응하는 동작상태를 확인하는 화면 위한 기능 구성부로서, 상기 휴대폰(100)에 구비된 LCD를 포함하는 하나 이상의 화면 출력장치와 상기 화면 출력장치를 구동하는 드라이버를 구비하여 이루어지는 것을 특징으로 하며, 상기 제어부(105)와 연계하여 상기 키 입력부(120)를 통해 입력되는 하나 이상의 키 데이터를 출력하거나, 또는 상기 휴대폰(100)에 구비된 하나 이상의 기능(또는 프로그램)에 대응하는 메뉴 화면, 기능처리 화면 및 기능처리 결과 화면을 출력하거나, 또는 상기 휴대폰(100)에 구비된(또는 다운로드되는) 하나 이상의 콘텐츠(예컨대, 문자 콘텐츠, 이미지 콘텐츠, 멀티미디어 콘텐츠)를 출력하는 것을 특징으로 한다.
- [0067] 본 발명의 실시 방법에 따르면, 상기 화면 출력부(110)는 상기 OTP를 생성하는 기능에 대응하는 메뉴 화면, 기능처리 화면 및 기능처리 결과 화면을 출력하는 화면 출력수단의 기능을 수행하는 것이 바람직하다.
- [0069] 상기 사운드 처리부(115)는 상기 휴대폰(100)의 각 동작모드에서 사운드의 입출력을 처리하는 기능 구성부로서, 하나 이상의 부호화된 사운드 데이터를 디코딩(Decoding)하여 상기 휴대폰(100)에 구비된 스피커로 출력하거나, 또는 상기 휴대폰(100)에 구비된 마이크를 통해 입력되는 사운드 신호를 인코딩(Encoding)하여 부호화하는 보코더(Vocoder)와 코덱(Codec)을 구비하여 이루어지는 것을 특징으로 한다.
- [0071] 본 발명의 실시 방법에 따르면, 상기 사운드 처리부(115)는 상기 휴대폰(100)의 각 동작모드 중 상기 "시스템 액세스 상태"에 대응하는 동작모드에서 상기 스피커를 통해 통화연결음에 대응하는 사운드 데이터를 디코딩하여 출력하거나, 또는 상기 "통화 채널 상태"에 대응하는 동작모드에서 마이크를 통해 음성신호를 인코딩하여 입력하거나, 스피커를 통해 음성신호를 디코딩하여 출력하는 것이 바람직하다.
- [0073] 또한, 상기 사운드 처리부(115)는 상기 "이동국 통화 대기 상태"를 포함하는 하나 이상의 동작모드에서 상기 휴대폰(100)에서 구비된(또는 다운로드되는) 하나 이상의 사운드 콘텐츠 또는 멀티미디어 콘텐츠 재생시, 상기 재생되는 콘텐츠에 대응하는 사운드 데이터를 디코딩하여 출력하는 것이 바람직하다.
- [0075] 상기 키 입력부(120)는 숫자키(Number Key) 또는 문자키(Character Key) 또는 기능키(Function Key)를 포함하는 하나 이상의 키 버튼(Key Button)을 구비한 키 입력장치와, 상기 키 입력장치를 구동하는 드라이버를 구비하여 이루어지는 것을 특징으로 하며, 이에 의해 상기 키 입력장치에서 상기 키 버튼을 클릭(또는 입력)하여 발생하는 하나 이상의 키 입력신호를 검출하는 것을 특징으로 한다.
- [0077] 본 발명에 따르면, 상기 제어부(105)에 의해 제어되는 입력모드 또는 하나 이상의 동작모드에서 상기 키 입력장치에 구비된 키 버튼으로부터 키 입력신호가 검출되면, 상기 키 입력부(120)는 상기 검출된 키 입력신호에 대응하는 키 이벤트(예컨대, MH\_KEY\_PRESSEVENT, MH\_KEY\_REPEATVENT, MH\_KEY\_RELEASEEVENT)를 발생하고, 상기 발생된 키 이벤트를 상기 제어부(105)로 제공하는 것을 특징으로 하며, 상기 제어부(105)는 상기 휴대폰(100)의 현재 입력모드 또는 동작모드에서 상기 키 이벤트에 대응하는 키 데이터를 독출(예컨대, 각각의 입력모드 또는 동작모드에서 특정 키 이벤트에 대응하는 하나 이상의 키 데이터를 저장(관리)하는 키 테이블로부터 상기 키 이벤트에 키 데이터 독출)하거나, 또는 상기 키 이벤트와 매칭되어 정의된 기능을 실행하는 명령어를 독출하는 것

을 특징으로 한다.

- [0079] 본 발명의 실시 방법에 따르면, 상기 키 입력부(120)는 상기 휴대폰(100)의 각 동작모드 중 상기 "이동국 통화 대기 상태"에 대응하는 동작모드에서 전화번호를 입력하고, "통화" 버튼을 입력함으로써, 상기 휴대폰(100)의 동작모드를 "시스템 액세스 상태"에 대응하는 동작모드로 변경하는 것이 바람직하다.
- [0081] 또한, 상기 키 입력부(120)는 상기 휴대폰(100)의 각 동작모드 중 상기 "이동국 통화 대기 상태"에 대응하는 동작모드에서 기능키(예컨대, 메뉴키)를 입력함으로써, 상기 휴대폰(100)에 구비된 다양한 기능을 실행하는 것이 바람직하다.
- [0083] 본 발명의 실시 방법에 따르면, 상기 키 입력부(120)는 상기 OTP를 생성하는 기능에 대응하는 하나 이상의 키 데이터를 입력하는 키 입력수단의 기능을 수행하는 것이 바람직하다.
- [0085] 상기 생체 인식부(125)는 사용자의 지문으로부터 상기 사용자의 지문 정보에 대응하는 생체 정보를 인식하는 지문 인식부, 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 카메라부를 구비하여 이루어지는 것을 특징으로 하며, 당업자의 의도에 따라 상기 생체 인식 대상과 이에 대응하는 생체 인식부(125)는 다양하게 확장 가능하며, 생체 인식 대상과 이에 대응하는 생체 인식 방법에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.
- [0087] 상기 무선 통신부(135)는 상기 휴대폰(100)이 WCDMA를 기반으로 동작하는 이동 통신망 상의 기지국과 무선채널을 연결하는 기능 구성부로서, CDMA 모듈과 각종 RF 모듈(예컨대, 듀플렉서 필터, 파워 앰프, 고출력 증폭기(High Power Amplifier; HPA), 아이솔레이터(Isolator), RF/IF SAW 필터, 주파수 상향회로, 주파수 하향 변환회로, 기준 클럭원에 해당하는 VCTCXO, UHF 주파수 합성기 등) 및 안테나와 이를 구동하는 드라이버를 구비하여 이루어지는 것을 특징으로 하며, 상기 제어부(105)와 연계하여 상기 휴대폰(100)의 각 동작모드에 대응하여 위치등록 또는 슬롯모드(Slot Mode) 또는 전력제어(Power Control) 또는 핸드오프(Hand-off) 또는 호처리(Call Processing) 절차를 수행하는 것을 특징으로 한다.
- [0089] 본 발명의 다른 실시 방법에 따라 본 도면1에 도시된 휴대폰(100)이 휴대인터넷단말이라면 상기 무선 통신부(135)는 IEEE 802.16x 기반 휴대인터넷에 접속하여 휴대 인터넷 서비스를 제공하는 무선통신 기능 구성을 포함하여 이루어지는 것이 가능하며, 상기 휴대인터넷 이외에 무선 데이터 통신을 제공하는 다양한 형태의 다른 무선 통신 구성으로 변형하여 본 발명을 실시하는 것이 가능하고, 상기 무선 통신부(135) 구성에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.
- [0091] 상기 USIM 리더부(145)는 ISO/IEC 7816을 포함하는 규격을 통해 휴대폰(100)에 탑재 또는 이탈착되는 USIM(140)과 하나 이상의 정보(또는 데이터, 또는 명령)를 교환하는 기능 구성부로서, 상기 ISO/IEC 7816 규격에 대응하는 접촉식 IC카드 리더를 구비하여 이루어지는 것을 특징으로 하며, 상기 IC카드 리더는 APDU(Application Protocol Data Unit)를 통해 상기 USIM(140)과 하나 이상의 정보(또는 데이터, 또는 명령)를 교환하는 것을 특징으로 한다.
- [0093] 상기 휴대폰(100)에 탑재 또는 이탈착되는 USIM(140)은 상기 ISO/IEC 7816 규격을 따르는 IC칩으로서, 상기 ISO/IEC 7816 규격을 참조하면, 상기 USIM(140)은 전원 공급(VCC), 리셋 신호(RST), 클럭 신호(CLK), 접지(GND), 프로그래밍 전원 공급(VPP), 입출력(I/O) 등과 같은 접촉점을 통해 USIM 리더부(145)와 통신(예컨대, 명령 또는 데이터 교환 등)하는 입출력 인터페이스와, CPU(Central Process Unit), MPU(Micro Process Unit), 코프로세서(Coprocessor) 등을 포함하는 하나 이상의 연산 소자로 이루어진 프로세서부와, ROM(Read Only Memory), RAM(Random Access Memory), EEPROM(Electrically Erasable and Programmable Read Only Memory), FM(Flash Memory) 등을 포함하는 하나 이상의 메모리 소자로 이루어진 메모리로 이루어져 있으며, 특히 상기 메모리 소자 중에서 하나 이상의 메모리 소자(예컨대, ROM)에는 IC카드 내부 자원을 관리하고 운영하는 칩 운영체제(Chip Operating System; COS)가 저장되는데, 상기 입출력 인터페이스의 전원 공급(VCC) 접촉점을 통해 USIM 리더부(145)로부터 전원이 공급되는 경우 상기 메모리에 저장된 COS가 실행 메모리로 로딩되어 상기 USIM(140)의 전반적인 동작을 제어하고, 상기 클럭 신호(CLK) 접촉점의 클럭주파수(예컨대, 3.57MHz 또는 4.9MHz)를 기반으로 APDU(Application Protocol Data Unit)를 통해 상기 USIM(140)과 USIM 리더부(145) 사이의 정보 또는 데이터 교환을 제어한다.
- [0095] 본 발명에 따르면, 상기 USIM(140)의 메모리에는 상기 휴대폰(100)에서 상기 OTP를 생성하는데 필요한 각종 정보와 프로그램 코드를 포함하는 OTP 애플릿이 구비되는 것이 바람직하며, 상기 OTP 애플릿은 휴대폰(100)에 구

비된 프로세서에 의해 독출되어 판독 또는 사용되어지는 정보 또는 데이터에 해당하는 데이터 셋트를 저장하는 저장부(도시생략)와, 상기 프로세서부의 연산 기능과 COS가 제공하는 명령어 셋트에 의해 USIM(140) 내에서 구동 또는 실행되어 동작하며, 상기 휴대폰(100)에 구비된 프로세서에 의해 사용되는 프로그램 루틴(예컨대, 자바카드(Javacard)의 경우 자바 애플릿(JAVA Applet))으로서 상기 COS의 명령어 셋트와 상호 작용하는 명령호출코드와 프로세서부에 의해 연산 처리되는 실행코드를 포함하여 이루어진 애플리케이션에 해당하는 처리부(도시생략)가 구비되는데, 특히 상기 처리부는 APDU를 통해 상기 입출력 인터페이스를 거쳐 상기 휴대폰(100)에 구비된 프로세서로부터 제공되는 명령을 판독하고, 상기 판독된 명령을 근거로 상기 저장부에 저장되는 하나 이상의 정보 또는 데이터를 읽거나, 또는 기록하며, 그 결과 또는 읽어온 정보 또는 데이터를 APDU를 통해 상기 입출력 인터페이스를 거쳐 상기 휴대폰(100)에 구비된 프로세서로 제공하는 것을 특징으로 한다.

[0097] 본 발명의 실시 방법에 따르면, 상기 OTP 애플릿의 저장부는, 상기 휴대폰(100)에서 상기  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위해 통신망 상의 서버로부터 수신하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위해 상기 휴대폰(100)에서 상기 통신망 상의 서버로 전송하는  $m(m \geq 1)$ 개의 단말측 OTP 생성 정보를  $m$ 개의 인덱스 값과 제각기 연계하여 저장하는 것이 바람직하다.

[0099] 상기 단말측 OTP 생성 정보는, 상기 통신망 상의 서버에서 상기 휴대폰(100)으로 제공할 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한 이상의 고정 씨드(seed) 값(또는 고정 씨드 값의 일부)를 포함하거나, 또는 동적 씨드 값을 결정하기 위한 파라미터(또는 파라미터의 일부)를 포함하여 이루어지는 것이 바람직하며, 상기 통신망 상의 서버는 상기 단말측 OTP 생성 정보에 포함된 고정 씨드 값 또는 상기 단말측 OTP 생성 정보에 포함된 파라미터를 통해 결정되는 동적 씨드 값을 기 설정된 OTP 생성 알고리즘에 대입하여 OTP 생성 값을 생성하고, 상기 통신망 상의 서버에 구비된 서버측 OTP 생성 정보에 상기 생성된 OTP 생성 값을 포함하여 상기 휴대폰(100)으로 제공할 OTP 생성 정보(즉, 휴대폰(100)에 구비된 OTP 에이전트에서  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위한 하나 이상의 고정 씨드 값과 파라미터를 포함하는 정보)를 구성한다.

[0101] 예를들어, 상기 OTP가 시간-동기화 방식으로 생성된다면, 상기 단말측 OTP 생성 정보는 상기 시간-동기화 방식을 통해 생성되는 OTP를 생성하기 위한 하나 이상의 고정 씨드 값(또는 고정 씨드 값의 일부)를 포함하거나, 또는 동적 씨드 값을 결정하기 위한 파라미터(또는 파라미터의 일부)를 포함하며, 상기 단말측 OTP 생성 정보를 통해 통신망 상의 서버에서 생성되는 OTP 생성 값은 상기 서버에 구비된 서버측 OTP 생성 정보에 포함되어 상기 휴대폰(100)에서 상기 시간-동기화 방식을 통해  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위한 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 정보) 중 어느 하나로 사용되는 것이 바람직하다.

[0103] 또는, 상기 OTP가 챌린지-리스폰스 방식으로 생성된다면, 상기 단말측 OTP 생성 정보는 상기 챌린지-리스폰스 방식을 통해 생성되는 OTP를 생성하기 위한 하나 이상의 고정 씨드 값(또는 고정 씨드 값의 일부)를 포함하거나, 또는 동적 씨드 값을 결정하기 위한 파라미터(또는 파라미터의 일부)를 포함하며, 상기 단말측 OTP 생성 정보를 통해 통신망 상의 서버에서 생성되는 OTP 생성 값은 상기 서버에 구비된 서버측 OTP 생성 정보에 포함되어 상기 휴대폰(100)에서 상기 챌린지-리스폰스 방식을 통해  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위한 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터(예컨대, 상기 챌린지-리스폰스의 난수를 생성하거나, 또는 난수를 수신하기 위한 난수 생성 값) 중 어느 하나로 사용되는 것이 바람직하다.

[0105] 본 발명의 실시 방법에 따르면, 상기 단말측 OTP 생성 정보는 상기 사용자 휴대폰(100)에 다운로드되는 OTP 에이전트와 연계하여 상기 저장부에 저장(암호화 저장 가능)되는 것이 바람직하다.

[0107] 상기 인덱스 값은 상기 OTP 애플릿의 저장부에 저장된  $m$ 개의 단말측 OTP 생성 정보와 통신망 상의 서버에 구비된  $M(M \geq m)$ 개의 단말측 OTP 생성 정보를 일대일 매칭하기 위해 중복되지 않도록 단말측 OTP 생성 정보 별로 고유하게 할당된 값으로서, 동일한 인덱스 값과 연계되어 상기 OTP 애플릿의 저장부에 저장된 단말측 OTP 생성 정보와 통신망 상의 서버에 구비된 단말측 OTP 생성 정보는 동일한 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 바람직하다.

[0109] 본 발명의 다른 실시 방법에 따라 상기 OTP 애플릿의 저장부에 하나의 단말측 OTP 생성 정보가 저장되는 경우, 상기 인덱스 값은 생략 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

[0111] 본 발명의 실시 방법에 따르면, 상기 USIM(140)에 상기  $N(N \geq 2)$ 자리수의 OTP를 생성하는 기능이 구비되는 것이 가능하며, 이 경우 상기 OTP 애플릿의 처리부는, 상기 휴대폰(100)을 통해 입력되는 사용자 비밀번호 또는 사용자 개인식별번호를 통한 사용자 인증 후, 상기 휴대폰(100)을 통해 제공되는 OTP 생성 정보를 통해 상기

N(N>=2)자리수의 OTP를 생성하기 위한 하나 이상의 고정 씨드 값과 동적 씨드 값을 확인/결정하고, 상기 확인/결정된 하나 이상의 고정 씨드 값과 동적 씨드 값을 상기 설정된 OTP 알고리즘에 대입하여 상기 OTP를 생성하는 프로그램 코드를 포함하여 이루어지는 것이 바람직하다.

[0113] 본 발명의 실시 방법에 따르면, 상기 OTP 애플릿의 저장부는, 상기 휴대폰(100)에서 상기 OTP를 생성하는 것에 대한 사용자 인증을 위한 사용자 비밀번호 또는 사용자 개인식별번호를 저장(또는 암호화 저장)하는 것이 가능하며, 이 경우 상기 OTP 애플릿의 처리부는 상기 휴대폰(100)으로부터 상기 사용자 비밀번호 또는 사용자 개인식별번호가 전달되면, 기 설정된 인증 절차에 따라 상기 전달된 사용자 비밀번호 또는 사용자 개인식별번호와 상기 저장부에 저장된 사용자 비밀번호 또는 사용자 개인식별번호를 비교(또는 검증 연산)하여 상기 사용자 비밀번호 또는 사용자 개인식별번호를 통해 상기 휴대폰(100)에서 상기 OTP를 생성하는 것에 대한 사용자 인증을 처리하고, 상기 사용자 인증 결과를 상기 휴대폰(100)으로 응답하는 것이 바람직하다.

[0115] 본 발명의 실시 방법에 따르면, 상기 OTP 애플릿의 저장부는, 상기 휴대폰(100)이 상기 OTP를 생성할 수 있는 OTP 에이전트가 구비된 OTP 매체임을 인증하기 위해 통신망 상의 서버에 등록된 하나 이상의 휴대폰(100) 고유 정보를 저장하는 것이 바람직하며, 당업자의 의도에 따라 상기 휴대폰(100) 고유정보는 상기 OTP 애플릿의 저장부 이외에 상기 USIM(140) 메모리의 고정된 저장영역에 저장된 고유정보와 IC칩 정보를 포함하여 이루어질 수 있다.

[0117] 여기서, 상기 USIM(140)에 구비되는 휴대폰(100) 고유정보는, 상기 USIM(140) 메모리의 고정된 저장영역에 전화번호(Mobile Identification Number; MIN), 일련번호(ESN), 가입자식별번호, IMEI(International Mobile Equipment Identity), MSISDN(Mobile Station International ISDN Number), USIM(140)을 구성하는 IC칩 일련번호를 하나 이상 포함하거나, 또는 상기 휴대폰(100)이 상기 OTP를 생성할 수 있는 OTP 에이전트가 구비된 OTP 매체임을 인증하도록 등록된 별도의 OTP 매체 식별자(예컨대, 중복되지 않는 코드 값) 또는 USIM(140) 식별자를 포함하여 이루어지는 것이 바람직하다.

[0119] 본 발명의 실시 방법에 따르면, 상기 사용자의 생체 인식 대상으로부터 상기 사용자의 생체 정보가 인식되고, 상기 생체 정보가 생체 인식 정보로 변환되는 경우, 상기 OTP 애플릿의 저장부는, 상기 생체 인식 정보를 저장하거나, 또는 상기 생체 인식 정보를 인증하는 생체 인증 정보(예컨대, 상기 생체 인식 정보와 기 설정된 검증 연산을 통해 특정 값을 도출하는 정보)를 저장하는 것이 바람직하며, 상기 생체 인식부(125)를 통해 상기 생체 인식 대상으로부터 상기 OTP 에이전트 구동 정보에 대응하는 생체 인식 정보가 확인되면, 상기 OTP 애플릿의 처리부는, 상기 휴대폰(100)으로 상기 저장부에 저장된 생체 인식 정보(또는 생체 인증 정보)를 제공하여 상기 휴대폰(100)에서 상기 생체 인식 정보를 인증하도록 처리하거나, 또는 상기 휴대폰(100)으로부터 상기 생체 인식 정보를 제공받고, 상기 생체 인식 정보와 상기 저장된 생체 인식 정보(또는 생체 인증 정보)를 비교(또는 검증 연산)하여 상기 생체 인식 유효성이 인증되도록 처리하는 기능을 구비하는 것이 바람직하다.

[0121] 본 발명의 일 실시 방법에 따라 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트를 구동하거나, 또는 상기 OTP 에이전트에서 OTP를 생성하는 것을 인증하는 OTP 구동 정보로 사용되는 경우, 상기 생체 인식 유효성이 인증되면, 상기 OTP 에이전트가 구동되거나, 또는 상기 OTP 에이전트에서 [OTP 목적]을 위한 OTP를 생성하는 것이 개시(또는 인증)되는 것이 바람직하다.

[0123] 또는, 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트가 통신망 상의 서버로 전송하는 OTP 매체인증 정보에 포함되는 경우, 상기 생체 인식 유효성이 인증되면, 상기 생체 인식 정보를 상기 통신망 상의 서버로 전송하는 OTP 매체인증 정보에 포함시키는 것이 바람직하며, 만약 상기 생체 인식 정보에 대한 유효성을 통신망 상의 서버에서 확인하는 경우, 상기 USIM(140)을 통해 상기 생체 인식 유효성을 인증하는 것이 생략 가능하다.

[0125] 또는, 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트가 OTP를 생성하는 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값으로 사용되는 경우, 상기 생체 인식 유효성이 인증되면, 상기 생체 인식 정보는 상기 OTP 생성 정보 또는 단말측 OTP 생성 정보를 구성하는 고정 씨드 값(또는 고정 씨드 값의 일부)로 사용되는 것이 바람직하며, 상기 생체 인식 정보가 상기 고정 씨드 값으로 사용될 코드 구조를 포함하지 않는 경우, 상기 OTP 애플릿의 처리부는, 기 설정된 해시함수를 통해 상기 생체 인식 정보를 상기 고정 씨드 값으로 가공하는 기능을 더 구비하는 것이 가능하다.

[0127] 본 발명의 실시 방법에 따르면, 상기 USIM(140)의 메모리는 고정된 메모리 주소를 갖는 가입자 정보 영역과 디렉토리 파일(EFdir) 구조를 갖는 응용영역으로 나뉘며, 상기 응용영역은 ISO/IEC 10202에 기반하는 보안구조를

포함하여 이루어지는데, 이에 따르면 상기 메모리는 CSN(Chip Serial Number)와 같은 비밀정보가 저장되는 보호 영역과, COS 제어 영역, 사용자 애플리케이션 영역, 읽기/쓰기 접근 영역, 애플리케이션 프로그램 영역, 및 FAT(File Allocation Table) 관리 영역 등으로 이루어지며, 상기 OTP 애플릿은 상기 보호영역과 COS 제어 영역을 제외한 별도의 지정된 저장영역에 저장되는 것이 바람직하다.

- [0129] 또한, ISO/IEC 7816 규격에 따르면, 상기 메모리의 응용영역은 루트 파일(Root File)에 해당하는 하나의 마스터 파일(Master File; MF)과, 상기 마스터 파일 하위에 하나 이상의 저장정보에 대한 기능 정보를 포함하는 ATR(Answer To Reset)과, 각각의 ICC 저장 정보에 대응하는 하나 이상의 전용 파일(Dedicate File; DF)과, 그리고 상기 전용 파일 하위에 배치되며 스마트 카드 서비스를 위한 실질적인 정보 또는 데이터가 포함된 요소 파일(Element File; EF)로 이루어진 파일 구조를 포함하고 있는데, 상기 OTP 애플릿도 상기와 같은 파일 구조를 포함하여 이루어진다.
- [0131] 상기 메모리부(150)는 상기 휴대폰(100)에서 하나 이상의 정보(또는 데이터)를 저장하는 저장매체, 및 하나 이상의 프로그램 루틴에 대응하는 프로그램 코드를 기록하는 기록매체에 해당하는 비휘발성 메모리의 총칭으로서, 상기 읽기 전용 메모리에 해당하는 ROM(Read Only memory)과, 읽기/쓰기가 가능한 플래시 메모리(Flash Memory; FM) 및 EEPROM(Electrically Erasable and Programmable Read Only Memory) 등을 포함하여 이루어지는 것을 특징으로 한다.
- [0133] 본 발명의 실시 방법에 따르면, 상기 메모리부(150)는, 상기 휴대폰(100)에서 상기  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위해 통신망 상의 서버로부터 수신하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위해 상기 휴대폰(100)에서 상기 통신망 상의 서버로 전송하는  $m(m \geq 1)$ 개의 단말측 OTP 생성 정보를  $m$ 개의 인덱스 값과 제각기 연계하여 저장하는 것이 바람직하며, 상기 생체 인식 정보가 단말측 OTP 생성 정보로 사용 가능한 경우, 상기 메모리부(150)에 상기 단말측 OTP 생성 정보가 저장되는 것이 생략 가능하다.
- [0135] 상기 단말측 OTP 생성 정보는, 상기 통신망 상의 서버에서 상기 휴대폰(100)으로 제공할 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한 이상의 고정 씨드(seed) 값(또는 고정 씨드 값의 일부)를 포함하거나, 또는 동적 씨드 값을 결정하기 위한 파라미터(또는 파라미터의 일부)를 포함하여 이루어지는 것이 바람직하며, 상기 통신망 상의 서버는 상기 단말측 OTP 생성 정보에 포함된 고정 씨드 값 또는 상기 단말측 OTP 생성 정보에 포함된 파라미터를 통해 결정되는 동적 씨드 값을 기 설정된 OTP 생성 알고리즘에 대입하여 OTP 생성 값을 생성하고, 상기 통신망 상의 서버에 구비된 서버측 OTP 생성 정보에 상기 생성된 OTP 생성 값을 포함하여 상기 휴대폰(100)으로 제공할 OTP 생성 정보(즉, 휴대폰(100)에 구비된 OTP 에이전트에서  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위한 하나 이상의 고정 씨드 값과 파라미터를 포함하는 정보)를 구성한다.
- [0137] 상기 인덱스 값은 상기 메모리부(150)에 저장된  $m$ 개의 단말측 OTP 생성 정보와 통신망 상의 서버에 구비된  $M(M \geq m)$ 개의 단말측 OTP 생성 정보를 일대일 매칭하기 위해 중복되지 않도록 단말측 OTP 생성 정보 별로 고유하게 할당된 값으로서, 동일한 인덱스 값과 연계되어 상기 메모리부(150)에 저장된 된 단말측 OTP 생성 정보와 통신망 상의 서버에 구비된 단말측 OTP 생성 정보는 동일한 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 바람직하다.
- [0139] 본 발명의 다른 실시 방법에 따라 상기 메모리부(150)에 하나의 단말측 OTP 생성 정보가 저장되는 경우, 상기 인덱스 값은 생략 가능하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0141] 본 발명의 실시 방법에 따르면, 상기 메모리부(150)는 상기 휴대폰(100)에서 상기 OTP를 생성하는 것에 대한 사용자 인증을 위한 사용자 비밀번호 또는 사용자 개인식별번호를 암호화하여 저장하는 것이 가능하다.
- [0143] 본 발명의 실시 방법에 따르면, 상기 메모리부(150)는 상기 휴대폰(100)이 상기 OTP를 생성할 수 있는 OTP 에이전트가 구비된 OTP 매체임을 인증하도록 통신망 상의 서버에 등록된 하나 이상의 휴대폰(100) 고유정보를 저장하는 것이 바람직하다.
- [0145] 여기서, 상기 메모리부(150)에 구비되는 휴대폰(100) 고유정보는, 상기 휴대폰(100)에 구비된 메모리부(150)의 기 설정된 시스템 영역에 저장된 전화번호(Mobile Identification Number; MIN), 일련번호(ESN), 가입자식별번호, IMEI(International Mobile Equipment Identity)를 하나 이상 포함하거나, 또는 상기 휴대폰(100)이 상기 OTP를 생성할 수 있는 OTP 에이전트가 구비된 OTP 매체임을 인증하도록 등록된 별도의 OTP 매체 식별자(예컨대, 중복되지 않는 코드 값)를 포함하여 이루어지는 것이 바람직하다.
- [0147] 본 발명의 실시 방법에 따르면, 상기 사용자의 생체 인식 대상으로부터 상기 사용자의 생체 정보가 인식되고, 상기 생체 정보가 생체 인식 정보로 변환되는 경우, 상기 메모리부(150)는, 상기 생체 인식 정보를 저장하거나,

또는 상기 생체 인식 정보를 인증하는 생체 인증 정보(예컨대, 상기 생체 인식 정보와 기 설정된 검증 연산을 통해 특정 값을 도출하는 정보)를 저장하는 것이 바람직하며, 상기 생체 인식부(125)를 통해 상기 생체 인식 대상으로부터 상기 OTP 에이전트 구동 정보에 대응하는 생체 인식 정보가 확인되면, 상기 OTP 에이전트(또는 OTP 에이전트 구동 프로그램)는, 상기 OTP 에이전트(또는 OTP 에이전트 구동 프로그램)는, 상기 확인된 생체 인식 정보와 상기 메모리부(150)에 저장된 생체 인식 정보(또는 생체 인증 정보)를 비교(또는 검증 연산)하여 상기 생체 인식 유효성이 인증되도록 처리하는 기능을 구비하는 것이 바람직하다.

[0149] 본 발명의 일 실시 방법에 따라 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트를 구동하거나, 또는 상기 OTP 에이전트에서 OTP를 생성하는 것을 인증하는 OTP 구동 정보로 사용되는 경우, 상기 생체 인식 유효성이 인증되면, OTP 에이전트 구동 프로그램에 의해 상기 OTP 에이전트가 구동되거나, 또는 OTP 에이전트는 상기 OTP 에이전트에서 [OTP 목적]을 위한 OTP를 생성하는 것이 개시(또는 인증)되는 것이 바람직하다.

[0151] 또는, 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트가 통신망 상의 서버로 전송하는 OTP 매체인증 정보에 포함되는 경우, 상기 생체 인식 유효성이 인증되면, OTP 에이전트는 생체 인식 정보를 상기 통신망 상의 서버로 전송하는 OTP 매체인증 정보에 포함시키는 것이 바람직하며, 만약 상기 생체 인식 정보에 대한 유효성을 통신망 상의 서버에서 확인하는 경우, 상기 USIM(140)을 통해 상기 생체 인식 유효성을 인증하는 것이 생략 가능하다.

[0153] 또는, 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트가 OTP를 생성하는 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값으로 사용되는 경우, 상기 생체 인식 유효성이 인증되면, 상기 생체 인식 정보는 상기 OTP 생성 정보 또는 단말측 OTP 생성 정보를 구성하는 고정 씨드 값(또는 고정 씨드 값의 일부)로 사용되는 것이 바람직하며, 상기 생체 인식 정보가 상기 고정 씨드 값으로 사용될 코드 구조를 포함하지 않는 경우, 상기 OTP 에이전트(또는 OTP 애플릿의 처리부)는, 기 설정된 해시함수를 통해 상기 생체 인식 정보를 상기 고정 씨드 값으로 가공하는 기능을 더 구비하는 것이 가능하다.

[0155] 도면1을 참조하면, 상기 휴대폰(100)은, 상기 생체 인식부(125)를 통해 상기 사용자의 생체 인식 대상으로부터 생체 정보를 인식하고, 상기 인식된 생체 정보를 기 설정된 생체 인식 방식에 따라 기 설정된 데이터 구조에 대응하는 생체 인식 정보로 변환하고, 상기 생체 인식 정보를 통해 상기 휴대폰(100)에 구비된 OTP 에이전트를 구동하거나, 또는 상기 OTP 에이전트에서 OTP를 생성하는 것을 인증하는 OTP 구동 정보로 사용되도록 처리하거나, 또는 상기 휴대폰(100)에 구비된 OTP 에이전트가 통신망 상의 서버로 전송하는 OTP 매체인증 정보에 포함되도록 처리하거나, 또는 상기 휴대폰(100)에 구비된 OTP 에이전트가 OTP를 생성하는 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값으로 사용되도록 처리하는 생체 인식 처리부(155)를 구비하여 이루어지는 것을 특징으로 한다.

[0157] 상기 생체 인식 처리부(155)는 상기 화면 출력부(110)를 통해 상기 사용자의 생체 인식 대상으로부터 생체 정보를 인식하도록 요청하는 생체 인식 인터페이스를 출력하고, 상기 생체 인식부(125)를 통해 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 생체 인식 대상으로부터 사용자의 생체 정보가 인식되면, 상기 인식된 생체 정보를 기 설정된 생체 인식 방식에 따라 기 설정된 데이터 구조에 대응하는 생체 인식 정보로 변환하는 것을 특징으로 한다.

[0159] 본 발명의 일 실시 방법에 따라 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트를 구동하는 경우, 상기 생체 인식부(125)를 통해 기 설정된 생체 인식 정보가 리딩되면, 상기 생체 인식 처리부(155)는 상기 USIM(140)/메모리부(150)에 저장된 생체 인식 정보(또는 생체 인식 인증 정보)를 통해 상기 생체 인식 정보에 대한 유효성을 확인하고, 상기 생체 인식 유효성이 확인되면, 상기 휴대폰(100)에 구비된 OTP 에이전트를 구동하는 것을 특징으로 하며, 이 경우 상기 생체 인식 처리부(155)는 상기 OTP 에이전트를 구동하는 OTP 에이전트 구동 프로그램의 기능을 수행하는 것이 바람직하다.

[0161] 또는, 상기 생체 인식 정보가 상기 OTP 에이전트에서 OTP를 생성하는 것을 인증하는 OTP 구동 정보로 사용되는 경우, 상기 생체 인식부(125)를 통해 기 설정된 생체 인식 정보가 리딩되면, 상기 생체 인식 처리부(155)는 상기 USIM(140)/메모리부(150)에 저장된 생체 인식 정보(또는 생체 인식 인증 정보)를 통해 상기 생체 인식 정보에 대한 유효성을 확인하고, 상기 생체 인식 유효성 확인 결과를 상기 휴대폰(100) 결제를 인증하기 위한 N자리 수의 OTP를 생성하기 위한 사용자 인증 결과로 처리하거나, 또는 상기 휴대폰(100) 결제를 인증하기 위한 N자리 수의 OTP를 생성하기 위한 OTP 생성 유효성 결과로 사용하는 것이 바람직하다.

[0163] 본 발명의 다른 일 실시 방법에 따라 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트가 통신망

상의 서버로 전송하는 OTP 매체인증 정보에 포함되는 경우, 상기 생체 인식부(125)를 통해 기 설정된 생체 인식 정보가 리딩되면, 상기 생체 인식 처리부(155)는 상기 생체 인식부(125)를 통해 리딩된 생체 인식 정보를 상기 OTP 매체인증 정보에 포함되도록 처리하는 것이 바람직하며, 당업자의 의도에 따라 상기 생체 인식 정보를 상기 OTP 매체인증 정보에 포함하기 전에 상기 USIM(140)/메모리부(150)에 저장된 생체 인식 정보(또는 생체 인식 인증 정보)를 통해 상기 생체 인식 정보에 대한 유효성을 확인하는 기능을 더 구비하는 것이 바람직하며, 상기 생체 인식 유효성을 통신망 상의 서버에 처리하는 경우 생략 가능하다.

[0165] 본 발명의 다른 일 실시 방법에 따라 상기 생체 인식 정보가 상기 휴대폰(100)에 구비된 OTP 에이전트가 OTP를 생성하는 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값으로 사용되는 경우, 상기 생체 인식부(125)를 통해 기 설정된 생체 인식 정보가 리딩되면, 상기 생체 인식 처리부(155)는 상기 생체 인식부(125)를 통해 리딩된 생체 인식 정보를 상기 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값으로 사용되도록 처리하는 것이 바람직하며, 상기 생체 인식 정보가 상기 정보를 상기 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값으로 사용할 코드 구조를 포함하지 않는 경우, 상기 생체 인식 정보를 상기 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값에 대응하는 코드 구조로 가공하는 것이 바람직하다. 상기 생체 인식 처리부(155)는 당업자의 의도에 따라 상기 생체 인식 정보를 상기 OTP 생성 정보 또는 단말측 OTP 생성 정보의 씨드 값으로 사용하기 전에 상기 USIM(140)/메모리부(150)에 저장된 생체 인식 정보(또는 생체 인식 인증 정보)를 통해 상기 생체 인식 정보에 대한 유효성을 확인하는 기능을 더 구비하는 것이 가능하다.

[0167] 도면1을 참조하면, 상기 휴대폰(100)은, 상기 휴대폰(100) 결제를 인증하기 위한 N자리수의 OTP를 생성하기 위한 사용자 인증을 처리하는 사용자 인증부(160)를 구비하여 이루어지는 것을 특징으로 한다.

[0169] 상기 휴대폰(100)에 구비된 키 입력수단을 통해 상기 휴대폰(100) 결제를 인증하기 위한 OTP를 생성하도록 요청하는 전용 키 버튼이 입력되거나, 또는 기 설정된 메뉴 선택을 통해 상기 OTP를 생성하도록 요청되거나, 또는 상기 이동 통신망을 통해 OTP 생성 명령(또는 OTP 에이전트 구동 명령)이 수신되면, 상기 사용자 인증부(160)는 상기 화면 출력부(110)를 통해 사용자 인증을 위한 사용자 비밀번호 또는 사용자 개인식별번호를 입력하는 사용자 인증 인터페이스를 출력하고, 상기 사용자 인증 인터페이스를 통해 사용자 비밀번호 또는 사용자 개인식별번호가 입력되면, 상기 입력된 사용자 비밀번호 또는 사용자 개인식별번호를 통해 자리수의 OTP를 생성하기 위한 사용자 인증을 처리하는 것을 특징으로 하며, 상기 생체 인식 유효성 확인 결과가 상기 N자리수의 OTP를 생성하기 위한 사용자 인증 결과로 사용되는 경우, 상기 사용자 인증부(160)가 상기 사용자 비밀번호 또는 사용자 개인식별번호를 통해 사용자 유효성을 인증하는 것이 생략 가능하다.

[0171] 본 발명의 일 실시 방법에 따라 상기 USIM(140)에 상기 OTP를 생성하기 위한 사용자 인증 기능이 구비된 경우, 상기 사용자 인증부(160)는 상기 USIM 리더부(145)를 통해 상기 입력된 사용자 비밀번호 또는 사용자 개인식별번호를 상기 USIM(140)으로 전달하며, 상기 USIM(140)에 구비된 PIN 인증 기능 또는 상기 OTP 애플릿에 구비된 처리부에 의해 처리된 상기 사용자 비밀번호 또는 사용자 개인식별번호에 대한 사용자 인증 결과를 수신하고, 상기 사용자 인증 결과를 판독하여 상기 휴대폰(100)에서 상기 OTP를 생성하는 것에 대한 사용자 유효성이 인증되었는지 확인하는 것이 바람직하다.

[0173] 본 발명의 다른 일 실시 방법에 따라 상기 메모리부(150)에 상기 OTP를 생성하기 위한 사용자 인증 기능이 구비된 경우, 상기 사용자 인증부(160)는 상기 사용자 비밀번호 또는 사용자 개인식별번호가 입력되면, 기 설정된 복호화 절차에 따라 상기 메모리부(150)에 암호화되어 저장된 사용자 비밀번호 또는 사용자 개인식별번호를 복호화하고, 상기 입력된 사용자 비밀번호 또는 사용자 개인식별번호와 상기 복호화된 사용자 비밀번호 또는 사용자 개인식별번호를 비교(또는 검증 연산)하여 상기 사용자 비밀번호 또는 사용자 개인식별번호를 통해 상기 휴대폰(100)에서 상기 OTP를 생성하는 것에 대한 사용자 인증을 처리하는 것이 바람직하다.

[0175] 도면1을 참조하면, 상기 휴대폰(100)은, 상기 USIM(140)/메모리부(150)에 저장된 m개의 단말측 OTP 생성 정보 중 OTP를 생성하는데 이용할 어느 하나의 단말측 OTP 생성 정보에 대응하는 인덱스 값을 결정하고, 상기 휴대폰(100)으로 N자리수의 OTP를 전송하는 통신망 상의 서버로 상기 인덱스 값이 전송되도록 처리하는 인덱스 처리부(165)를 구비하여 이루어지는 것을 특징으로 한다.

[0177] 본 발명의 실시 방법에 따르면, 상기 인덱스 처리부(165)는 상기 USIM(140)/메모리부(150)에 저장된 m개의 단말측 OTP 생성 정보와 연계된 인덱스 값 중 임의의 인덱스 값을 결정하거나, 또는 기 설정된 순서에 따라 인덱스 값을 결정하거나, 또는 이전에 결정된 인덱스 값을 제외한 나머지 인덱스 값 중에서 어느 하나를 임의로 결정하거나, 또는 기 설정된 인덱스 정책에 따라 상기 m개의 인덱스 값 중 어느 하나를 결정하는 것이 바람직하다.

- [0179] 상기 USIM(140)/메모리부(150)에 저장된 m개의 단말측 OTP 생성 정보와 연계된 인덱스 값 중 어느 하나의 인덱스 값이 결정되면, 상기 인덱스 처리부(165)는 상기 결정된 인덱스 값이 OTP 매체인증 정보에 포함되어 상기 휴대폰(100)으로 N자리수의 OTP를 전송하는 통신망 상의 서버로 전송되도록 처리하거나, 또는 상기 휴대폰(100)이 OTP 매체로 인증된 후 상기 통신망 상의 서버와 통신채널을 연결하고, 상기 통신채널을 통해 상기 결정된 인덱스 값을 상기 통신망 상의 서버로 전송한다.
- [0181] 본 발명의 다른 실시 방법에 따라 상기 USIM(140)/메모리부(150)에 인덱스 값이 포함되지 않고 하나의 단말측 OTP 생성 정보가 저장된 경우, 상기 인덱스 처리부(165)가 상기 인덱스 값을 결정하거나, 또는 서버로 인덱스 값이 전송되도록 처리하는 것이 생략 가능하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0183] 도면1을 참조하면, 상기 휴대폰(100)은, 상기 휴대폰(100) 결제를 인증하기 위한 OTP를 생성하기 위해 상기 이동 통신망을 통해 상기 휴대폰(100)이 상기 휴대폰(100) 결제를 인증하기 위한 OTP 에이전트가 구비된 OTP 매체임을 인증하는 인증 처리부(170)를 구비하여 이루어지는 것을 특징으로 하며, 당업자에 의해 따라 상기 인증 처리부(170)는 상기 OTP 매체인증 과정에서 통신망 상의 서버로 상기 단말측 OTP 생성 정보를 전송하는 것이 가능하다.
- [0185] 상기 사용자 인증부(160)에 의해 상기 휴대폰(100)에서 상기 OTP를 생성하는 것에 대한 사용자 인증이 유효한 것으로 처리되면, 상기 인증 처리부(170)는 상기 USIM(140)/메모리부(150)에 구비된 휴대폰(100) 고유정보를 확인하고, 상기 휴대폰(100) 고유정보를 포함하는 OTP 매체인증 정보를 구성하여 상기 휴대폰(100)이 상기 휴대폰(100) 결제를 인증하기 위한 OTP 에이전트가 구비된 OTP 매체임을 인증하는 통신망 상의 서버로 전송하는 것을 특징으로 한다.
- [0187] 본 발명의 일 실시 방법에 따라 상기 USIM(140)/메모리부(150)에 인덱스 값이 저장되지 않거나, 상기 USIM(140)/메모리부(150)에 인덱스 값이 저장되더라도 상기 인덱스 처리부(165)가 상기 인덱스 값을 서버로 직접 전송하는 경우, 상기 OTP 매체인증 정보는, 상기 확인된 휴대폰(100) 고유정보를 포함하여 이루어지는 것이 바람직하며, 당업자의 의도에 따라 상기 단말측 OTP 생성 정보 또는 사용자 비밀번호 또는 사용자 개인식별번호를 더 포함하여 이루어지는 것이 바람직하다.
- [0189] 본 발명의 다른 일 실시 방법에 따라 상기 USIM(140)/메모리부(150)에 인덱스 값이 저장되고, 상기 인덱스 값이 상기 OTP 매체인증 정보에 포함되어 전송되는 경우, 상기 OTP 매체인증 정보는, 상기 확인된 휴대폰(100) 고유정보와 인덱스 값을 포함하여 이루어지는 것이 바람직하며, 당업자의 의도에 따라 상기 단말측 OTP 생성 정보 또는 사용자 비밀번호 또는 사용자 개인식별번호를 더 포함하여 이루어지는 것이 바람직하다.
- [0191] 만약 상기 생체 인식 정보가 상기 OTP 매체인증 정보에 포함되는 경우, 상기 OTP 매체인증 정보는 상기 휴대폰(100) 고유정보와 생체 인식 정보를 포함하여 이루어지는 것이 바람직하며, 상기 인덱스 값 또는 사용자 비밀번호 또는 사용자 개인식별번호는 당업자의 의도에 따라 상기 OTP 매체인증 정보에 포함될 수 있다.
- [0193] 본 발명의 실시 방법에 따르면, 상기 OTP 매체인증 정보는 상기 휴대폰(100)과 서버 사이에 설정된 보안 통신선에 의해 암호화되는 것이 바람직하다.
- [0195] 본 발명의 실시 방법에 따라 상기 OTP 매체인증 정보가 상기 휴대폰(100) 고유정보와 상기 인덱스 값을 포함하는 경우, 상기 인덱스 값과 상기 휴대폰(100) 고유정보는 기 설정된 방식에 따라 연결(또는 조합)되어 상기 OTP 매체인증 정보를 구성하거나, 또는 상기 인덱스 값과 상기 휴대폰(100) 고유정보가 기 설정된 코드 생성 알고리즘에 대입하여 생성된 코드 값을 상기 OTP 매체인증 정보로 결정되는 것이 가능하며, 상기 인덱스 값과 휴대폰(100) 고유정보를 통해 상기 OTP 매체인증 정보를 구성하는 방식에 의해 본 발명이 한정되지 아니한다.
- [0197] 예를들어, 상기 인증 처리부(170)는 상기 인덱스 값과 휴대폰(100) 고유정보 중 하나 이상의 정보를 일방향 해시 함수로 해시한 후 XOR 연산하여 매체 검증자를 생성하고, 상기 매체 검증자와 인덱스 값과 휴대폰(100) 고유정보를 연결하여 상기 OTP 매체인증 정보를 생성할 수 있다.
- [0199] 또는, 상기 OTP 매체인증 정보가 상기 휴대폰(100) 고유정보와 상기 사용자 비밀번호 또는 사용자 개인식별번호를 포함하는 경우, 상기 사용자 비밀번호 또는 사용자 개인식별번호와 상기 휴대폰(100) 고유정보는 기 설정된 방식에 따라 연결(또는 조합)되어 상기 OTP 매체인증 정보를 구성하거나, 또는 상기 사용자 비밀번호 또는 사용자 개인식별번호와 상기 휴대폰(100) 고유정보가 기 설정된 코드 생성 알고리즘에 대입하여 생성된 코드 값을 상기 OTP 매체인증 정보로 결정되는 것이 가능하며, 상기 사용자 비밀번호 또는 사용자 개인식별번호와 휴대폰(100) 고유정보를 통해 상기 OTP 매체인증 정보를 구성하는 방식에 의해 본 발명이 한정되지 아니한다.

- [0201] 예를들어, 상기 인증 처리부(170)는 상기 사용자 비밀번호 또는 사용자 개인식별번호를 일방향 해시함수를 통해 해시(Hash)하고, 상기 해시된 사용자 비밀번호 또는 사용자 개인식별번호, 적어도 하나 이상의 난수 값, 상기 휴대폰(100) 고유정보(또는 일방향 해시함수로 해시된 휴대폰(100) 고유정보)를 적어도 하나 이상 XOR 연산하여 매체 검증자를 생성하고, 상기 생성된 매체 검증자와 상기 사용자 비밀번호 또는 사용자 개인식별번호, 적어도 하나 이상의 난수 정보, 휴대폰(100) 고유정보를 포함하여 이루어진 OTP 매체인증 정보를 생성할 수 있다.
- [0203] 본 발명의 다른 실시 방법에 따르면, 상기 OTP 매체인증 정보는 상기와 같은 다양한 방식 중 어느 하나의 방식을 통해 상기 USIM(140)에 구비된 OTP 애플릿의 처리부에 의해 생성되는 것이 가능하다.
- [0205] 만약 상기 USIM(140)에 상기 휴대폰(100) 고유정보가 구비되고, 상기 OTP 애플릿의 처리부에서 상기 OTP 매체인증 정보를 생성하는 경우, 상기 OTP 애플릿의 처리부는 상기 휴대폰(100) 고유정보를 포함하는 OTP 매체인증 정보를 생성하거나, 또는 상기 사용자 인증부(160)에 의해 상기 USIM(140)으로 제공된 사용자 비밀번호 또는 사용자 개인식별번호와 휴대폰(100) 고유정보를 통해 상기 OTP 매체인증 정보를 생성하고, 상기 생성된 OTP 매체인증 정보를 상기 인증 처리부(170)로 전달하는 것이 가능하며, 당업자의 의도에 따라 상기 USIM(140)에서 상기 OTP 매체인증 정보를 암호화하는 것도 가능하다.
- [0207] 또는, 상기 메모리부(150)에 상기 휴대폰(100) 고유정보가 구비되고, 상기 OTP 애플릿의 처리부에서 상기 OTP 매체인증 정보를 생성하는 경우, 상기 인증 처리부(170)에서 상기 휴대폰(100) 고유정보를 상기 USIM(140)으로 전달하면, 상기 OTP 애플릿의 처리부는 상기 휴대폰(100) 고유정보를 포함하는 OTP 매체인증 정보를 생성하거나, 또는 상기 사용자 인증부(160)에 의해 상기 USIM(140)으로 제공된 사용자 비밀번호 또는 사용자 개인식별번호와 휴대폰(100) 고유정보를 통해 상기 OTP 매체인증 정보를 생성하고, 상기 생성된 OTP 매체인증 정보를 상기 인증 처리부(170)로 전달하는 것이 가능하며, 당업자의 의도에 따라 상기 USIM(140)에서 상기 OTP 매체인증 정보를 암호화하는 것도 가능하다.
- [0209] 상기 휴대폰(100) 고유정보를 포함하는 OTP 매체인증 정보가 생성되면, 상기 인증 처리부(170)는 상기 휴대폰(100)을 상기 휴대폰(100) 결제를 인증하기 위한 OTP 에이전트가 구비된 OTP 매체로 인증하는 통신망 상의 서버 정보를 확인하고, 상기 통신망 상의 서버와 설정된 보안 통신세션에 따라 상기 무선 통신부(135)를 통해 상기 통신망 상의 서버로 상기 생성된 OTP 매체인증 정보를 전송하는 것을 특징으로 한다.
- [0212] \*상기 OTP 매체인증 정보를 수신한 통신망 상의 서버는 상기 OTP 매체인증 정보를 수신(암호화된 경우 복호화)하고, 상기 수신된 OTP 매체인증 정보에 포함된 휴대폰(100) 고유정보와 상기 휴대폰(100)을 상기 휴대폰(100) 결제를 인증하기 위한 OTP 에이전트가 구비된 OTP 매체로 인증하도록 등록된 휴대폰(100) 고유정보를 비교(또는 검증 연산)하여 상기 휴대폰(100)을 상기 휴대폰(100) 결제를 인증하기 위한 OTP 에이전트가 구비된 OTP 매체로 인증하는 것을 특징으로 한다.
- [0214] 만약 상기 OTP 매체인증 정보에 사용자 비밀번호 또는 사용자 개인식별번호가 더 포함되고, 상기 통신망 상의 서버에 상기 사용자 비밀번호 또는 사용자 개인식별번호를 통한 사용자 인증 기능이 구비되거나, 또는 상기 사용자 비밀번호 또는 사용자 개인식별번호를 상기 통신망 상의 서버에서 상기 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하여 N자리수의 OTP를 생성할 OTP 생성 정보에 포함시킨 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(100)으로 제공하는 조건으로 이용하는 경우, 상기 통신망 상의 서버는 상기 OTP 매체인증 정보에 포함된 사용자 비밀번호 또는 사용자 개인식별번호와 상기 휴대폰(100) 고유정보와 연계하여 등록된 사용자 비밀번호 또는 사용자 개인식별번호를 비교(또는 검증 연산)하여 상기 사용자 인증을 처리하거나, 또는 상기 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하여 N자리수의 OTP를 생성할 OTP 생성 정보에 포함시킨 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(100)으로 제공하는 유효성을 확인하는 것이 바람직하다.
- [0216] 본 발명의 실시 방법에 따르면, 상기 인증 처리부(170)(또는 상기 OTP 애플릿의 처리부)는 상기 OTP 매체인증 정보에 상기 USIM(140)/메모리부(150)에 구비된 단말측 OTP 생성 정보를 더 포함시켜 통신망 상의 서버로 전송되도록 처리하는 것이 바람직하며, 상기 생체 인식 정보를 단말측 OTP 생성 정보에 포함하는 경우, 상기 생체 인식 정보를 상기 확인된 단말측 OTP 생성 정보에 포함시킨다.
- [0218] 도면1을 참조하면, 상기 휴대폰(100)은, 상기 무선 통신부(135)를 통해 상기 USIM(140)/메모리부(150)에 구비된 단말측 OTP 생성 정보를 통신망 상의 서버로 전송하는 정보 전송부(175)를 더 구비하여 이루어지는 것을 특징으로 한다.
- [0220] 상기 인증 처리부(170)를 통해 상기 OTP 매체인증 정보에 상기 단말측 OTP 생성 정보가 포함되어 상기 통신망

상의 서버로 전송되지 않은 경우, 상기 인증 처리부(170)를 통해 상기 휴대폰(100)이 상기 OTP 매체로 인증되면, 상기 정보 전송부(175)는 상기 USIM(140)/메모리부(150)에 구비된 단말측 OTP 생성 정보를 확인(상기 생체 인식 정보를 단말측 OTP 생성 정보에 포함하는 경우, 상기 생체 인식 정보를 상기 확인된 단말측 OTP 생성 정보에 포함)하고, 상기 무선 통신부(135)를 통해 상기 통신망 상의 서버로 상기 단말측 OTP 생성 정보를 전송하는 것을 특징으로 하며, 상기 인증 처리부(170)를 통해 상기 단말측 OTP 생성 정보가 상기 OTP 매체인증 정보에 포함되어 상기 통신망 상의 서버로 전송된 경우, 상기 정보 전송부(175)는 생략 가능하며, 이에 의해 본 발명이 한정되지 아니한다.

- [0222] 만약 상기 단말측 OTP 생성 정보가 수신되면, 상기 통신망 상의 서버는 상기 단말측 OTP 생성 정보부터 OTP 생성 값을 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 상기 OTP 생성 값을 생성하는 것을 특징으로 한다.
- [0224] 여기서, 상기 단말측 OTP 생성 정보를 통해 생성되는 OTP 생성 값은, 상기 통신망 상의 서버에서 상기 휴대폰(100)으로 제공하는 OTP 생성 정보(즉, 휴대폰(100)에 구비된 OTP 에이전트에서  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위한 하나 이상의 고정 씨드 값과 파라미터를 포함하는 정보)에 포함되는 정보로서, OTP 생성 방식을 통해 생성되지만, 그 자체가 OTP 인증대상으로 사용되지 않고, 상기 휴대폰(100)에 구비된 OTP 에이전트에서  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위한 씨드 값으로 사용되는 것을 특징으로 한다.
- [0226] 상기 통신망 상의 서버에서 상기 휴대폰(100)이 상기 휴대폰(100) 결제를 인증하기 위한 OTP 에이전트가 구비된 OTP 매체로 인증되고(또는 상기 휴대폰(100)을 상기 구비된 OTP 매체로 인증하고 사용자 인증이 더 처리되고), 상기 단말측 OTP 생성 정보를 통해 OTP 생성 값이 생성되면, 상기 통신망 상의 서버는 상기 휴대폰(100) 고유정보와 연계된 서버측 OTP 생성 정보를 확인한다.
- [0228] 만약 상기 통신망 상의 서버로 상기 인덱스 값이 제공된 경우, 상기 통신망 상의 서버는 상기 휴대폰(100) 고유정보와 연계된  $M(M \geq m)$ 개의 서버측 OTP 생성 정보 중 상기 인덱스 값에 대응하는 서버측 OTP 생성 정보를 확인하는 것이 바람직하다.
- [0230] 만약 상기 서버측 OTP 생성 정보가 확인되면, 상기 통신망 상의 서버는 상기 서버에 구비된 서버측 OTP 생성 정보에 상기 OTP 생성 값을 포함하여 상기 휴대폰(100)에 구비된 OTP 에이전트에서  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위한 OTP 생성 정보(즉, 휴대폰(100)에 구비된 OTP 에이전트에서  $N(N \geq 2)$ 자리수의 OTP를 생성하기 위한 하나 이상의 고정 씨드 값과 파라미터를 포함하는 정보)를 구성하고, 상기 OTP 생성 정보를 통해 상기  $N(N \geq 2)$ 자리수의 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  $N(N \geq 2)$ 자리수의 OTP를 생성하고, 상기 생성된  $N(N \geq 2)$ 자리수의 OTP를 상기 이동 통신망을 통해 상기 휴대폰(100)으로 전송하는 것을 특징으로 하며, 상기 OTP 생성 정보는 상기 휴대폰(100)과 통신망 상의 서버 사이에 구비된 보안 통신세션에 의해 암호화되어 전송되는 것이 바람직하다.
- [0232] 도면1을 참조하면, 상기 휴대폰(100)은, 상기 이동 통신망을 통해 상기  $N(N \geq 2)$ 자리수의 OTP를 수신하는 수신부(180)를 구비하여 이루어지는 것을 특징으로 한다.
- [0234] 상기 통신망 상의 서버에서 상기 휴대폰(100)이 상기 휴대폰(100) 결제를 인증하기 위한 OTP를 생성하는 OTP 에이전트가 구비된 OTP 매체로 인증됨에 의해 상기 통신망 상의 서버에서 상기 OTP 생성 정보를 통해  $N(N \geq 2)$ 자리수의 OTP를 생성하여 전송하면, 상기 수신부(180)는 상기 무선 통신부(135)를 통해 상기  $N(N \geq 2)$ 자리수의 OTP를 수신하는 것을 특징으로 하며, 상기  $N(N \geq 2)$ 자리수의 OTP가 암호화된 경우, 기 설정된 복호화 절차에 따라 복호화하는 것을 특징으로 한다.
- [0236] 도면1을 참조하면, 상기 휴대폰(100)은, 상기  $N(N \geq 2)$ 자리수의 OTP가 수신되면, 상기 OTP를 상기 화면 출력부(110)를 통해 출력하는 OTP 출력부(185)를 구비하여 이루어지는 것을 특징으로 하며, 상기 휴대폰(100)에 근거리 통신수단(도시생략)이 구비된 경우, 상기 OTP 출력부(185)는 상기 근거리 통신수단을 통해 상기 생성된 OTP를 상기 휴대폰(100)과 근거리에 위치한 단말(또는 장치)로 출력하는 것이 가능하다.
- [0238] 상기  $N(N \geq 2)$ 자리수의 OTP가 생성되면, 상기 OTP 출력부(185)는 상기 화면 출력부(110)와 연계하여 상기 수신된 OTP를 상기 휴대폰(100) 화면 상의 일정 영역에 출력하는 것을 특징으로 한다.
- [0240] 본 발명의 일 실시 방법에 따르면, 상기 OTP 출력부(185)는 상기 화면 출력부(110)와 연계하여 상기 휴대폰(100) 화면 상에 OTP 출력 화면을 출력하고, 상기 OTP 출력 화면에 상기 생성된 OTP를 출력하는 것이 바람직하다.

다.

- [0242] 본 발명의 다른 일 실시 방법에 따르면, 상기 OTP 출력부(185)는 상기 화면 출력부(110)와 연계하여 상기 휴대폰(100) 화면에 현재 출력된 화면 영역에 OTP 출력 영역을 출력(또는 할당)하고, 상기 OTP 출력 영역에 상기 생성된 OTP를 출력하는 것이 바람직하다.
- [0244] 만약 상기 휴대폰(100)에 근거리 통신수단(예컨대, 블루투스, 적외선통신, RFID통신, RF통신 등, 도시생략)이 구비된 경우, 상기 OTP 출력부(185)는 상기 근거리 통신수단을 통해 상기 생성된 OTP를 상기 휴대폰(100)과 근 거리에 위치한 단말(또는 장치)로 출력하는 것이 가능하다.
- [0246] 본 발명의 다른 실시 방법에 따르면, 상기 휴대폰(100)에서 상기 생성된 OTP를 통신망 상에 구비되어 상기 OTP를 인증하는 서버로 전송하는 경우, 상기 OTP 출력부(185)는 상기 무선 통신부(135)를 통해 상기 OTP를 인증하는 서버로 상기 OTP를 전송하기 위한 보안 통신채널(예컨대, 암호화/복호화 기반 통신채널)을 연결(기 연결된 경우 생략 가능)하고, 상기 보안 통신채널을 통해 상기 OTP를 인증하는 서버로 상기 생성된 OTP를 직접 전송하는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0248] 도면2는 본 발명의 실시 방법에 따라 휴대폰(200) 결제를 인증하기 위한 휴대폰(200) OTP 시스템 구성을 도시한 도면이다.
- [0250] 보다 상세하게 본 도면2는 상기 휴대폰(200) 결제를 인증하기 위한 OTP 매체로 등록되는 휴대폰(200)에 대응하는 OTP 매체인증 정보와 단말측 OTP 생성 정보 및 서버측 OTP 생성 정보를 연계하여 저장매체(275)에 저장하고, 상기 휴대폰(200)으로 상기 도면1에 도시된 휴대폰(200) 구성에 대응하는 OTP 에이전트를 제공(단, 상기 휴대폰(200)에 OTP 에이전트가 구비된 경우 생략 가능)한 후, 상기 휴대폰(200)을 OTP 매체로 사용시, 상기 휴대폰(200)으로부터 OTP 매체인증 정보와 단말측 OTP 생성 정보를 수신하고, 상기 OTP 매체인증 정보를 판독하여 상기 휴대폰(200)을 OTP 매체로 인증되면, 상기 수신된 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하고, 상기 저장매체(275)로부터 상기 휴대폰(200)에 대응하는 서버측 OTP 생성 정보를 확인하고, 상기 생성된 OTP 생성 값과 서버측 OTP 생성 정보를 조합(또는 연계)하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성한 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(200)으로 제공함으로써, 상기 휴대폰(200)에서 상기 휴대폰(200) 결제를 인증하기 위한 N자리수의 OTP를 출력되도록 처리하는 OTP 운영 시스템을 포함하는 휴대폰(200) OTP 시스템 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면2를 참조 및/또는 변형하여 상기 휴대폰(200) 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.
- [0252] 도면2를 참조하면, 상기 휴대폰(200) OTP 시스템은, 상기 도면1에 도시된 OTP 에이전트 구성을 구비한 휴대폰(200)과, 상기 휴대폰(200)을 소지한 사용자에게 OTP 인증을 요청하는 OTP 인증요청 서버(215)와, 상기 OTP 매체로 등록되는 휴대폰(200)에 대응하는 OTP 매체인증 정보와 단말측 OTP 생성 정보 및 서버측 OTP 생성 정보를 연계하여 저장매체(275)에 저장하고, 상기 휴대폰(200)으로 상기 도면1에 도시된 휴대폰(200) 구성에 대응하는 OTP 에이전트를 제공(단, 상기 휴대폰(200)에 OTP 에이전트가 구비된 경우 생략 가능)한 후, 상기 휴대폰(200)을 OTP 매체로 사용시, 상기 휴대폰(200)으로부터 OTP 매체인증 정보와 단말측 OTP 생성 정보를 수신하고, 상기 OTP 매체인증 정보를 판독하여 상기 휴대폰(200)을 OTP 매체로 인증되면, 상기 수신된 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하고, 상기 저장매체(275)로부터 상기 휴대폰(200)에 대응하는 서버측 OTP 생성 정보를 확인하고, 상기 생성된 OTP 생성 값과 서버측 OTP 생성 정보를 조합(또는 연계)하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성한 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(200)으로 제공함으로써, 상기 휴대폰(200)에서 상기 휴대폰(200) 결제를 인증하기 위한 N자리수의 OTP를 출력되도록 처리하는 OTP 운영 시스템을 포함하여 이루어지는 것을 특징으로 하며, 당업자의 의도에 따라 상기 휴대폰(200)을 소지한 사용자가 이용하는 사용자 단말(205)과, 상기 휴대폰(200)에서 생성된 N자리수의 OTP를 인증하는 OTP 서버(220)를 더 포함하여 이루어진다.
- [0254] 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(220), OTP 인증요청 서버(215), 상기 휴대폰(200)이 접속하는 이동 통신망에 구비된 통신사 서버(210) 중 하나 이상의 서버의 구성요소 형태로 구현되거나, 또는 상기 OTP 운영

시스템을 구성하는 각각의 수단이 상기 OTP 서버(220), OTP 인증요청 서버(215), 통신사 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.

- [0256] 상기 휴대폰(200)은, 상기 휴대폰(200) 결제를 인증하기 위한 OTP 매체로 등록됨에 의해 휴대폰(200)으로 상기 도면1에 도시된 휴대폰(200) 구성에 대응하는 OTP 에이전트를 구비하여 이루어지는 것을 특징으로 하며, 상기 휴대폰(200)에 구비된 키 입력수단을 통해 OTP를 생성하도록 요청하는 전용 키 버튼이 입력되거나, 또는 기 설정된 메뉴 선택을 통해 OTP를 생성하도록 요청되거나, 또는 상기 이동 통신망을 통해 OTP 생성 명령(또는 OTP 에이전트 구동 명령)을 수신함에 의해 사용자 인증 후, 상기 휴대폰(200)을 OTP 매체로 인증하도록 요청하는 OTP 매체인증 정보를 생성(또는 구성)하고, 상기 OTP 매체인증 정보와 단말측 OTP 생성 정보를 상기 OTP 운영 시스템으로 전송하고, 상기 OTP 운영 시스템에서 상기 휴대폰(200)을 OTP 매체로 인증하면, 상기 OTP 운영 시스템으로부터 상기 OTP 생성 정보를 통해 생성된 N자리수의 OTP를 수신하여 출력하는 것을 특징으로 한다.
- [0258] 상기 OTP 인증요청 서버(215)는, 상기 휴대폰(200)에서 생성하는 OTP를 통해 사용자, 지불결제, 금융거래를 인증하도록 요청하는 서버의 총칭으로서, 상기 휴대폰(200)에서 생성하는 OTP를 통해 사용자 인증을 처리하는 웹 서버, 상기 휴대폰(200)에서 생성하는 OTP를 통해 지불결제를 인증을 처리하는 쇼핑물 서버 또는 컨텐츠 제공 서버 또는 홈쇼핑 서버, 상기 휴대폰(200)에서 생성하는 OTP를 통해 금융거래를 인증하는 बैं킹 서버를 하나 이상 포함하여 이루어지며, 본 발명은 상기 OTP 인증요청 서버(215)의 종류와 OTP 인증요청 방식에 의해 본 발명이 한정되지 아니한다.
- [0260] 상기 사용자 단말(205)은, 상기 휴대폰(200)을 소지한 사용자가 통신망을 통해 상기 OTP 인증요청 서버(215)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 무선통신 단말(예컨대, 휴대폰(200), 휴대인터넷단말 등), 양방향 통신 기능이 구비된 디지털TV, IP-TV, 홈네트워크에 연결된 가전단말 등을 포함하여 이루어진다.
- [0262] 본 발명의 실시 방법에 따르면, 상기 사용자 단말(205)과 휴대폰(200)이 동일한 장치여도 무방하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0264] 상기 OTP 서버(220)는, 상기 휴대폰(200)에서 생성된 N자리수의 OTP를 통신망을 통해 수신하고, 상기 OTP와 매칭되는 OTP' 를 생성하고, 상기 OTP와 OTP' 를 비교(또는 검증 연산)하여 상기 휴대폰(200) 결제를 인증하기 위한 OTP 인증을 처리하는 서버의 총칭으로서, 상기 OTP 서버(220)에서 상기 OTP를 인증하는 기능은 상기 OTP 운영 시스템에 구비되어도 무방하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0266] 도면2를 참조하면, 상기 OTP 운영 시스템은, 상기 휴대폰(200)을 OTP 매체로 등록하는 OTP 등록단말로부터 상기 휴대폰(200)에 대응하는 휴대폰(200) 고유정보와 고객정보를 포함하고, 생체 인식 정보를 더 포함하는 OTP 매체 정보를 수신하고, 상기 휴대폰(200) 결제를 인증하기 위해 상기 휴대폰(200)에서 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 단말측 OTP 생성 정보와 서버측 OTP 생성 정보를 생성(또는 할당)하고, 상기 OTP 매체 정보와 상기 단말측 OTP 생성 정보 및 서버측 OTP 생성 정보를 연계하여 저장매체(275)에 저장하는 OTP 매체 등록수단(225)과, 상기 휴대폰(200)이 상기 OTP 매체로 등록되면, 상기 휴대폰(200)으로 상기 단말측 OTP 생성 정보를 제공하여 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장시키는 휴대폰 처리수단(230)을 구비하여 이루어지는 것을 특징으로 하며, 상기 휴대폰(200)에 상기 도면1에 도시된 구성을 구비한 OTP 에이전트가 구비되지 않은 경우, 상기 휴대폰 처리수단(230)은 상기 휴대폰(200)으로 상기 도면1에 도시된 구성에 대응하는 OTP 에이전트 프로그램 코드를 제공하는 것을 특징으로 한다.
- [0268] 여기서, 상기 OTP 등록단말은, 상기 휴대폰(200)을 OTP 매체로 등록하도록 요청하는 단말장치의 총칭으로서, 상기 사용자가 이용하는 사용자 단말(205), OTP 등록기관(예컨대, 국가기관, OTP 인증요청 서버(215) 운영기관, 카드사, 금융사, 증권사 등)에 구비된 단말(예컨대, 국가기관 단말, OTP 인증요청 서버(215) 운영기관 단말, 카드사 단말, 금융사 단말, 증권사 단말 등)를 하나 이상 포함하여 이루어진다.
- [0270] 상기 OTP 등록단말에서 상기 휴대폰(200)을 OTP 매체로 등록하기 위해 상기 휴대폰(200)에 대응하는 휴대폰(200) 고유정보와 고객정보를 포함하고, 생체 인식 정보를 더 포함하는 OTP 매체 정보를 입력(또는 확인)하여 통신망을 통해 전송하면, 상기 OTP 매체 등록수단(225)은 상기 통신망을 통해 상기 OTP 매체 정보를 수신하는 것을 특징으로 한다.
- [0272] 상기 OTP 매체 정보에 포함된 휴대폰(200) 고유정보는, 상기 휴대폰(200)에 구비된 메모리부의 기 설정된 시스

템 영역에 저장된 전화번호(Mobile Identification Number; MIN), 일련번호(ESN), 가입자식별번호, IMEI(International Mobile Equipment Identity)를 하나 이상 포함하거나, 또는 상기 휴대폰(200)이 상기 N자리수의 OTP를 생성할 수 있는 OTP 에이전트가 구비된 OTP 매체임을 인증하도록 등록된 별도의 OTP 매체 식별자(예컨대, 중복되지 않는 코드 값)를 포함하여 이루어지는 것이 바람직하다.

[0274] 또는, 상기 휴대폰(200) 고유정보는, 상기 휴대폰(200)에 구비된 USIM 메모리의 고정된 저장영역에 전화번호(Mobile Identification Number; MIN), 일련번호(ESN), 가입자식별번호, IMEI(International Mobile Equipment Identity), MSISDN(Mobile Station International ISDN Number), USIM을 구성하는 IC칩 일련번호를 하나 이상 포함하거나, 또는 상기 휴대폰(200)이 상기 N자리수의 OTP를 생성할 수 있는 OTP 에이전트가 구비된 OTP 매체임을 인증하도록 등록된 별도의 OTP 매체 식별자(예컨대, 중복되지 않는 코드 값) 또는 USIM 식별자를 포함하여 이루어지는 것이 바람직하다.

[0276] 본 발명의 실시 방법에 따르면, 상기 OTP 매체 정보는, 사용자의 생체 인식 대상으로부터 인식된 생체 인식 정보, 또는 상기 생체 인식 정보를 인증하는 생체 인증 정보를 더 포함하는 것이 바람직하며, 만약 상기 휴대폰(200)에 구비된 에이전트에서 상기 생체 인식 정보에 대한 유효성을 확인하거나, 또는 상기 휴대폰(200)을 OTP 매체로 사용하여 OTP를 생성하는 과정에서 상기 생체 인식 정보를 전송하는 않는 경우 생략 가능하다.

[0278] 만약 상기 휴대폰(200)에서 사용자의 생체 인식 대상으로부터 생체 정보를 인식 및 이에 대응하는 생체 인식 정보를 전송하는 경우, 상기 생체 인식 정보는 상기 OTP 매체로 등록되는 휴대폰(200)을 소지한 사용자 유효성 또는 OTP 생성 유효성을 인증하는데 사용되거나, 상기 휴대폰(200)으로부터 제공된 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하여 N자리수의 OTP를 생성할 OTP 생성 정보에 포함시킨 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(200)으로 제공하는 조건으로 이용되는 것이 바람직하다.

[0280] 본 발명의 실시 방법에 따르면, 상기 OTP 매체 정보는, 상기 사용자가 지정한 사용자 비밀번호 또는 사용자 개인식별번호를 더 포함하여 이루어지는 것이 바람직하며, 상기 사용자 비밀번호 또는 사용자 개인식별번호는 상기 OTP 매체로 등록되는 휴대폰(200)을 소지한 사용자 유효성을 인증하는데 사용되거나, 상기 휴대폰(200)으로부터 제공된 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하여 N자리수의 OTP를 생성할 OTP 생성 정보에 포함시킨 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(200)으로 제공하는 조건으로 이용되는 것이 바람직하다.

[0282] 상기 고객정보는, 상기 OTP 매체로 사용될 휴대폰(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.

[0284] 만약 상기 휴대폰(200)을 OTP 매체로 이용하여 인증하는 대상에 금융거래가 포함되는 경우, 상기 고객정보는 상기 고객정보에 대응하는 고객의 금융정보(예컨대, 계좌번호, 은행 등)를 더 포함하는 것이 바람직하다.

[0286] 또는 상기 휴대폰(200)을 OTP 매체로 이용하여 인증하는 대상에 카드거래가 포함되는 경우, 상기 고객정보는 상기 고객정보에 대응하는 고객의 카드정보(예컨대, 카드번호, 카드사 등)를 더 포함하는 것이 바람직하다.

[0288] 본 발명을 실시하는 당업자의 의도 및 상기 휴대폰(200)을 OTP 매체로 이용하는 분야에 따라 상기 고객정보는 다양한 정보(예컨대, 상기 휴대폰(200)을 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.

[0290] 상기 OTP 매체 정보가 수신되면, 상기 OTP 매체 등록수단(225)은, 상기 고객정보와 휴대폰(200) 고유정보를 통신사 서버(210)로 제공함으로써, 상기 통신사 서버(210)를 통해 상기 휴대폰(200)을 OTP 매체로 사용하는 것이 유효한지 인증하는 것이 바람직하다.

[0292] 상기 OTP 매체 정보가 수신되거나, 또는 상기 휴대폰(200)을 OTP 매체로 사용하는 것에 대한 유효성이 인증되면, 상기 OTP 매체 등록수단(225)은, 상기 휴대폰(200) 결제를 인증하기 위해 상기 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한 하나 이상  $M(M \geq m \geq 1)$ 개의 단말측 OTP 생성 정보와 M개의 서버측 OTP 생성 정보를 생성(또는 할당)한 후, 상기 생성(또는 할당)된 M개의 단말측 OTP 생성 정보와 서버측 OTP 생성 정보에 M개의 인덱스 값을 고유하게 일대일 매칭하여 할당한다.

[0294] 여기서, 상기 단말측 OTP 생성 정보는, 상기 휴대폰(200)으로 제공되어 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장(또는 암호화 저장)되며, 상기 OTP 운영 시스템에서 생성되어 상기 휴대폰(200)에 구비된 OTP 에이전

트를 통해 출력될 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 바람직하다.

- [0296] 상기 서버측 OTP 생성 정보는, 상기 OTP 운영 시스템 상에 유지되며, 상기 OTP 운영 시스템에서 생성되어 상기 휴대폰(200)에 구비된 OTP 에이전트를 통해 출력될 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 바람직하다.
- [0298] 본 발명의 다른 실시 방법에 따르면, 상기 서버측 OTP 생성 정보는, 상기 OTP 운영 시스템 상에 유지되며, 상기 OTP 운영 시스템에서 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 가능하다.
- [0300] 상기 인덱스 값은 상기  $M(M \geq m \geq 1)$ 개의 단말측 OTP 생성 정보와 서버측 OTP 생성 정보에 중복되지 않도록 고유하게 일대일 매칭하여 할당된 번호/코드 값으로서, 상기 M개의 단말측 OTP 생성 정보와 서버측 OTP 생성 정보 중 쌍을 이루는 어느 하나의 단말측 OTP 생성 정보와 서버측 OTP 생성 정보를 결정(또는 선택)하기 위한 인덱스를 포함하여 이루어진다.
- [0302] 상기 OTP 등록단말로부터 상기 OTP 매체 정보가 수신되고, 상기 단말측 OTP 생성 정보와 서버측 OTP 생성 정보가 생성(또는 할당)되면, 상기 OTP 매체 등록수단(225)은, 상기 OTP 매체 정보와 상기 M개의 단말측 OTP 생성 정보, 서버측 OTP 생성 정보 및 인덱스 값을 연계하여 저장매체(275)에 저장한다.
- [0304] 상기 OTP 매체 등록수단(225)에 의해 상기 휴대폰(200)이 상기 OTP 매체로 등록되면, 상기 휴대폰 처리수단(230)은, 이동 통신망을 통해 상기 휴대폰(200) 고유정보에 대응하는 휴대폰(200)과 통신채널을 연결하고, 상기 M개의 단말측 OTP 생성 정보, 서버측 OTP 생성 정보 및 인덱스 값 중 일부(또는 전체)에 해당하는  $m(m \leq M)$ 개의 단말측 OTP 생성 정보와 그 인덱스 값을 상기 통신채널을 통해 상기 휴대폰(200)으로 제공하여 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장시키는 것을 특징으로 하며, 상기 OTP 매체 정보에 상기 생체 인식 정보가 포함되고, 상기 휴대폰(200)에서 생체 인식 유효성을 확인하는 경우, 상기 휴대폰 처리수단(230)은 상기 생체 인식 정보(또는 상기 생체 인식 정보를 인증하는 생체 인증 정보)를 상기 휴대폰(200)으로 제공하여 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장시키는 것이 바람직하다.
- [0306] 만약 상기 휴대폰(200)에 상기 도면1에 도시된 휴대폰(200) 구성에 대응하는 OTP 에이전트가 구비되어 있지 않은 경우, 상기 휴대폰 처리수단(230)은, 상기 휴대폰(200)으로 상기 도면1에 도시된 구성에 대응하는 OTP 에이전트 프로그램 코드를 제공하여 상기 휴대폰(200)에 구비된 기록매체에 기록하는 것이 바람직하며, 상기 OTP 에이전트 프로그램 코드와 단말측 OTP 생성 정보는 별도 채널을 통해 상기 휴대폰(200)으로 제공되거나, 또는 상기 OTP 에이전트 프로그램 코드와 상기 m개의 단말측 OTP 생성 정보 및 인덱스 값을 포함(상기 OTP 매체 정보에 상기 생체 인식 정보가 포함되고, 상기 휴대폰(200)에서 생체 인식 유효성을 확인하는 경우, 상기 생체 인식 정보(또는 상기 생체 인식 정보를 인증하는 생체 인증 정보)를 더 포함)하는 패키지 데이터가 상기 휴대폰(200)으로 제공되는 것이 모두 가능하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0308] 도면2를 참조하면, 상기 OTP 운영 시스템은, 이동 통신망을 통해 상기 휴대폰(200)으로부터 상기 휴대폰(200)을 OTP 매체로 인증하도록 요청하는 OTP 매체인증 정보를 수신하는 정보 수신수단(235)과, 상기 OTP 매체인증 정보와 상기 저장매체(275)에 저장된 OTP 매체 정보를 비교(또는 검증 연산)하여 상기 휴대폰(200)을 OTP 매체로 인증하는 매체 인증수단(240)을 구비하여 이루어지는 것을 특징으로 하며, 상기 휴대폰(200)으로부터 상기 사용자 비밀번호 또는 사용자 개인식별번호가 수신되면, 상기 사용자 비밀번호 또는 사용자 개인식별번호와 상기 저장매체(275)에 저장된 사용자 비밀번호 또는 사용자 개인식별번호를 비교(또는 검증 연산)하여 상기 OTP 매체로 사용되는 휴대폰(200) 사용자 유효성을 인증하는 사용자 인증수단(245)을 더 구비하여 이루어지는 것이 바람직하다.
- [0310] 본 발명의 일 실시 방법에 따라 상기 휴대폰(200)에 구비된 키 입력수단을 통해 OTP를 생성하도록 요청하는 전용 키 버튼이 입력되거나, 또는 기 설정된 메뉴 선택을 통해 OTP를 생성하도록 요청되어 상기 휴대폰(200)에서 USIM/메모리부로부터 휴대폰(200) 고유정보를 확인(또는 추출)하고, 상기 휴대폰(200) 고유정보를 포함하고 상기 휴대폰(200)에 구비된 단말측 OTP 생성 정보를 더 포함하는 OTP 매체인증 정보를 구성하여 상기 이동 통신망을 통해 전송하면, 상기 정보 수신수단(235)은 상기 이동 통신망을 통해 상기 OTP 매체인증 정보를 수신하는 것을 특징으로 한다.
- [0312] 본 발명의 다른 일 실시 방법에 따르면, 상기 정보 수신수단(235)은 상기 휴대폰(200)에 구비된 OTP 에이전트를 구동하는 OTP 생성 명령(또는 OTP 에이전트 구동 명령)을 구성(또는 데이터베이스로부터 추출)하고, 상기 이동

통신망을 통해 상기 OTP 생성 명령(또는 OTP 에이전트 구동 명령)을 상기 휴대폰(200)으로 전송하며, 이에 대응하여 상기 휴대폰(200)에서 상기 OTP 생성 명령(또는 OTP 에이전트 구동 명령)을 통해 OTP 에이전트를 구동하고, 상기 휴대폰(200)에서 USIM/메모리부로부터 휴대폰(200) 고유정보를 확인(또는 추출)하고, 상기 휴대폰(200) 고유정보를 포함하고 상기 휴대폰(200)에 구비된 단말측 OTP 생성 정보를 더 포함하는 OTP 매체인증 정보를 구성하여 상기 이동 통신망을 통해 전송하면, 상기 정보 수신수단(235)은 상기 이동 통신망을 통해 상기 OTP 매체인증 정보를 수신하는 것을 특징으로 한다.

- [0314] 즉, 상기 OTP 매체인증 정보는 휴대폰(200) 고유정보를 포함하여 이루어지며, 또는 당업자의 의도에 따라 상기 휴대폰(200) 고유정보와 상기 휴대폰(200)에 구비된 단말측 OTP 생성 정보를 포함하여 이루어지는 것이 바람직하다.
- [0316] 만약 상기 OTP 매체인증 정보에 상기 단말측 OTP 생성 정보가 포함되지 않은 경우, 상기 휴대폰(200)은 별도의 채널을 통해 상기 단말측 OTP 생성 정보를 전송하고, 상기 정보 수신수단(235)은 별도의 채널을 통해 상기 휴대폰(200)으로부터 상기 단말측 OTP 생성 정보를 수신하는 것이 바람직하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0318] 본 발명의 실시 방법에 따르면, 상기 OTP 매체인증 정보는 사용자 비밀번호 또는 사용자 개인식별번호와 상기 휴대폰(200)에 구비된 m개의 인덱스 값 중 어느 하나에 대응하는 인덱스 값을 하나 이상 더 포함하여 이루어지는 것이 바람직하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0320] 본 발명의 다른 실시 방법에 따르면, 상기 OTP 매체인증 정보에 포함되는 휴대폰(200) 고유정보가 상기 휴대폰(200)에 할당된 전화번호인 경우, 상기 휴대폰(200) 고유정보는 상기 OTP 매체인증 정보에 직접 포함되지 않고 휴대폰(200)에 대한 발신자 정보를 통해 확인되는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0322] 본 발명의 다른 실시 방법에 따라 상기 OTP 매체인증 정보에 상기 사용자 비밀번호 또는 사용자 개인식별번호가 포함되지 않은 경우, 상기 정보 수신수단(235)은 상기 OTP 매체 인증 후 별도의 채널을 통해 상기 사용자 비밀번호 또는 사용자 개인식별번호를 수신하는 것이 바람직하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0324] 또는, 상기 OTP 매체인증 정보에 상기 휴대폰(200)에 구비된 m개의 인덱스 값 중 어느 하나에 대응하는 인덱스 값이 포함되지 않은 경우, 상기 정보 수신수단(235)은 상기 OTP 매체 인증 후 별도의 채널을 통해 상기 인덱스 값을 수신하는 것이 바람직하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0326] 만약 상기 생체 인식 정보가 상기 OTP 매체인증 정보에 포함되는 경우, 상기 OTP 매체인증 정보는 상기 휴대폰(200) 고유정보와 생체 인식 정보를 포함하여 이루어지는 것이 바람직하며, 상기 인덱스 값 또는 사용자 비밀번호 또는 사용자 개인식별번호는 당업자의 의도에 따라 상기 OTP 매체인증 정보에 포함될 수 있다.
- [0328] 상기 휴대폰(200)으로부터 OTP 매체인증 정보가 수신되면, 상기 매체 인증수단(240)은, 상기 저장매체(275)로부터 상기 OTP 매체인증 정보에 포함된 구성 정보와 매칭되는 구성 정보를 포함하는 OTP 매체 정보를 확인하고, 상기 OTP 매체인증 정보에 포함된 구성 정보와 OTP 매체 정보에 포함된 구성 정보를 비교(또는 검증 연산)하고, 상기 비교(또는 검증 연산) 결과 상기 OTP 매체인증 정보에 포함된 구성 정보와 상기 저장매체(275)에 저장된 OTP 매체 정보에 포함된 구성 정보가 일치(또는 매칭)되거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되면, 상기 OTP 매체인증 정보를 전송한 휴대폰(200)을 상기 OTP 매체 등록수단(225)에 의해 OTP 매체로 등록된 유효한 휴대폰(200)으로 인증하는 것을 특징으로 한다.
- [0330] 만약 상기 OTP 매체인증 정보에 상기 생체 인식 정보가 포함된 경우, 상기 매체 인증수단(240)은, 상기 저장매체(275)로부터 상기 OTP 매체인증 정보에 포함된 생체 인식 정보와 매칭되는 생체 인식 정보(또는 생체 인증 정보)를 확인하고, 상기 OTP 매체인증 정보에 포함된 생체 인식 정보와 OTP 매체 정보에 포함된 생체 인식 정보를 비교(또는 생체 인증 정보를 검증 연산)하고, 상기 비교(또는 검증 연산) 결과 상기 OTP 매체인증 정보에 포함된 생체 인식 정보와 상기 저장매체(275)에 저장된 OTP 매체 정보에 포함된 생체 인식 정보가 일치(또는 매칭)되거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되면, 상기 OTP 매체인증 정보를 전송한 휴대폰(200)을 상기 OTP 매체 등록수단(225)에 의해 OTP 매체로 등록된 유효한 휴대폰(200)으로 인증하거나, 상기 휴대폰(200)으로부터 제공된 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하여 N자리수의 OTP를 생성할 OTP 생성 정보에 포함시킨 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(200)으로 제공하는 유효성이 확인된 것으로 처리하는 것을 특징으로 한다.
- [0332] 상기 OTP 매체인증 정보에 사용자 비밀번호 또는 사용자 개인식별번호가 포함되거나, 또는 별도의 채널을 통해 상기 휴대폰(200)으로부터 상기 사용자 비밀번호 또는 사용자 개인식별번호가 수신되면, 상기 사용자 인증수단

(245)은, 상기 사용자 비밀번호 또는 사용자 개인식별번호와 상기 저장매체(275)에 저장된 OTP 매체 정보에 포함된 사용자 비밀번호 또는 사용자 개인식별번호를 비교(또는 검증 연산)하고, 상기 비교(또는 검증 연산) 결과 상기 사용자 비밀번호 또는 사용자 개인식별번호와 상기 저장매체(275)에 저장된 사용자 비밀번호 또는 사용자 개인식별번호가 일치(또는 매칭)되거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되면, 상기 휴대폰(200)을 소지한 사용자가 상기 OTP 매체로 등록된 휴대폰(200)의 정상적인 유효한 사용자로 인증하고 상기 휴대폰(200)으로부터 제공된 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하여 N자리수의 OTP를 생성할 OTP 생성 정보에 포함시킨 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(200)으로 제공하는 유효성이 확인된 것으로 처리하는 것을 특징으로 한다.

[0334] 도면2를 참조하면, 상기 OTP 운영 시스템은, 상기 OTP 매체인증 정보를 전송한 휴대폰(200)이 유효한 OTP 매체로 인증되면, 상기 저장매체(275)로부터 상기 OTP 매체인증 정보에 대응하는 OTP 매체 정보와 연결된 서버측 OTP 생성 정보를 확인하는 정보 확인수단(270)과, 상기 확인된 서버측 OTP 생성 정보와 상기 휴대폰(200)으로부터 수신된 단말측 OTP 생성 정보를 조합(또는 연계)하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성(또는 생성)하는 정보 구성수단(265)과, 상기 OTP 생성 정보를 통해 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 N자리수의 OTP를 생성하는 OTP 생성수단(250)과, 상기 이동통신망을 통해 상기 생성된 N자리수의 OTP를 상기 휴대폰(200)으로 전송하는 OTP 전송수단(255)을 구비하여 이루어지는 것을 특징으로 하며, 상기 정보 확인수단(270)은, 상기 휴대폰(200)으로부터 인덱스 값이 수신된 경우, 상기 저장매체(275)에 저장된 M개의 서버측 OTP 생성 정보 중 상기 인덱스 값에 대응하는 서버측 OTP 생성 정보를 확인하는 것을 특징으로 한다.

[0336] 상기 OTP 매체인증 정보를 전송한 휴대폰(200)이 유효한 OTP 매체로 인증되고, 상기 휴대폰(200) 사용자에게 대한 유효성 또는 상기 휴대폰(200)으로부터 제공된 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하여 N자리수의 OTP를 생성할 OTP 생성 정보에 포함시킨 후 상기 OTP 생성 정보를 통해 N자리수의 OTP를 생성하여 상기 휴대폰(200)으로 제공하는 유효성이 더 인증되면(생략가능), 상기 정보 확인수단(270)은, 상기 저장매체(275)로부터 상기 OTP 매체인증 정보에 대응하는 휴대폰(200) 고유정보와 연결된 서버측 OTP 생성 정보를 확인하거나, 또는 상기 사용자 비밀번호 또는 사용자 개인식별번호와 연결된 서버측 OTP 생성 정보를 확인하는 것을 특징으로 하며, 상기 휴대폰(200)으로부터 인덱스 값이 수신된 경우, 상기 저장매체(275)에 저장된 M개의 서버측 OTP 생성 정보 중 상기 인덱스 값에 대응하는 서버측 OTP 생성 정보를 확인하는 것을 특징으로 한다.

[0338] 상기 서버측 OTP 생성 정보가 확인되면, 상기 정보 구성수단(265)은, 상기 휴대폰(200)으로부터 수신된 단말측 OTP 생성 정보에 하나 이상의 고정 씨드 값을 확인하고, 상기 단말측 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 상기 서버측 OTP 생성 정보와 조합(또는 연계)될 OTP 생성 값을 생성한 후, 상기 OTP 생성 값과 상기 확인된 서버측 OTP 생성 정보를 조합(또는 연계)하여 상기 휴대폰(200)에서 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성(또는 생성)하는 것을 특징으로 한다.

[0340] 본 발명의 실시 방법에 따라 상기 생체 인식 정보가 상기 OTP 생성 정보로 사용되는 경우, 상기 정보 구성수단(265)은 상기 OTP 생성 정보에 포함된 고정 씨드 값에 상기 생체 인식 정보(또는 상기 OTP 생성 정보의 고정 씨드 값으로 사용 가능하도록 가공된 상기 생체 인식 정보)를 더 포함하는 고정 씨드 값을 확인하거나, 또는 상기 OTP 생성 정보에 별도의 고정 씨드 값이 포함되지 않고 상기 생체 인식 정보를 상기 OTP 생성 정보의 고정 씨드 값으로 사용하는 경우, 상기 생체 인식 정보(또는 상기 OTP 생성 정보의 고정 씨드 값으로 사용 가능하도록 가공된 상기 생체 인식 정보)를 상기 OTP 생성 정보의 고정 씨드 값으로 확인하는 것이 바람직하다.

[0342] 본 발명의 다른 실시 방법에 따르면, 상기 정보 구성수단(265)은, 상기 확인된 서버측 OTP 생성 정보에 포함된 하나 이상의 고정 씨드 값을 확인하고, 상기 서버측 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 상기 단말측 OTP 생성 정보를 통해 생성된 OTP 생성 값과 조합(또는 연계)될 OTP 생성 값을 생성한 후, 상기 단말측 OTP 생성 정보를 통해 생성된 OTP 생성 값과 서버측 OTP 생성 정보를 통해 생성된 OTP 생성 값을 조합(또는 연계)하여 상기 휴대폰(200)에서 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성(또는 생성)하는 것이 가능하다.

[0344] 여기서, 상기 OTP 생성 값은, 상기 서버측 OTP 생성 정보를 통해 생성되는 OTP로서, 상기 N자리수의 OTP를 생성하기 위한 제2의 씨드 값으로 사용되는 것을 특징으로 한다.

- [0346] 상기 OTP 생성 정보가 구성(또는 생성)되면, 상기 OTP 생성수단(250)은, 상기 확인된 상기 OTP 생성 정보를 통해 상기 N자리수의 OTP을 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 OTP을 생성하는 것을 특징으로 한다.
- [0348] 상기 OTP 생성 정보를 통해 N자리수의 OTP이 생성되면, 상기 OTP 전송수단(255)은, 상기 이동 통신망을 통해 상기 휴대폰(200)과 연결된 통신채널을 통해 상기 휴대폰(200)으로 상기 N자리수의 OTP을 전송하는 것을 특징으로 한다.
- [0350] 도면2를 참조하면, 상기 OTP 운영 시스템은, 통신망을 통해 상기 휴대폰(200)에 구비된 OTP 에이전트에서 생성한 N자리수의 OTP를 수신하고, 상기 OTP를 생성한 휴대폰(200) 고유정보와 연결된 단말측 OTP 생성 정보와 서버측 OTP 생성 정보를 확인하고, 상기 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성한 후 상기 OTP 생성 값과 서버측 OTP 생성 정보를 조합(또는 연계)하여 상기 OTP 생성 정보를 구성하거나, 또는 상기 정보 구성수단(265)에 의해 기 구성(또는 생성)된 OTP 생성 정보를 확인하고, 상기 OTP 생성 정보를 통해 N자리수의 OTP' 를 생성하거나, 또는 상기 OTP 생성수단(250)에 의해 기 생성된 OTP에 대응하는 N자리수의 OTP' 를 확인하고, 상기 N자리수의 OTP와 OTP' 를 비교(또는 검증 연산)하여 상기 수신된 OTP가 유효한지 인증하는 OTP 인증수단(260)을 구비하여 이루어지는 것을 특징으로 하며, 상기 OTP 인증수단(260)에서 OTP를 인증하는 기능은 별도의 OTP 서버(220)에 구현되는 것이 가능하며, 본 발명은 상기 유추 가능한 모든 실시 방법을 포함하여 이루어짐을 명백하게 밝혀두는 바이다.
- [0352] 상기 휴대폰(200)에서 상기 N자리수의 OTP를 생성하고, 상기 사용자 단말(205)에 표시된 OTP 입력 인터페이스를 통해 상기 OTP가 입력되어 전송되면, 상기 OTP 인증수단(260) 또는 OTP 서버(220)는, 통신망을 통해 상기 사용자 단말(205)로부터 상기 OTP를 수신하는 것을 특징으로 하며, 상기 OTP가 암호화되어 전송되면, 기 설정된 복호화 방식에 따라 복호화 처리한다.
- [0354] 또는, 상기 휴대폰(200)은 상기 N자리수의 OTP가 생성되면, 이동 통신망을 통해 상기 생성된 OTP를 전송하는 것이 가능하며, 상기 OTP 인증수단(260) 또는 OTP 서버(220)는, 이동 통신망을 통해 상기 휴대폰(200)으로부터 상기 OTP를 수신하는 것을 특징으로 하며, 상기 OTP가 암호화되어 전송되면, 기 설정된 복호화 방식에 따라 복호화 처리한다.
- [0356] 상기 OTP가 수신되면, 상기 OTP 인증수단(260) 또는 OTP 서버(220)는, 상기 OTP를 생성한 휴대폰(200) 고유정보와 연결된 단말측 OTP 생성 정보와 서버측 OTP 생성 정보를 확인하고, 상기 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성한 후 상기 OTP 생성 값과 서버측 OTP 생성 정보를 조합(또는 연계)하여 상기 OTP 생성 정보를 구성하는 것을 특징으로 하며, 만약 상기 OTP 운영 시스템에서 상기 휴대폰(200)으로 제공한 OTP 생성 정보를 확인할 수 있는 경우, 상기 OTP 인증수단(260)은 상기 OTP 운영 시스템에서 기 구성(또는 생성)한 제공한 OTP 생성 정보를 확인한다.
- [0358] 본 발명의 다른 실시 방법에 따라 상기 휴대폰(200)으로 제공된 OTP 생성 정보가 상기 서버측 OTP 생성 정보를 통해 생성된 OTP 생성 값을 포함하는 경우, 상기 OTP 인증수단(260) 또는 OTP 서버(220)는, 상기 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하고 상기 서버측 OTP 생성 정보를 통해 OTP 생성 값을 생성한 후 상기 생성된 각각의 OTP 생성 값을 조합(또는 연계)하여 상기 OTP 생성 정보를 구성하는 것이 가능하다.
- [0360] 만약 상기 OTP 생성 정보가 구성/확인되면, 상기 OTP 인증수단(260) 또는 OTP 서버(220)는, 상기 확인된 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 생성하며, 만약 상기 OTP 운영 시스템에서 상기 휴대폰(200)으로 제공한 OTP를 확인할 수 있는 경우, 상기 OTP 인증수단(260)은 상기 OTP 운영 시스템에서 상기 휴대폰(200)으로 제공한 OTP를 N자리수의 OTP' 로 확인한다.
- [0362] 상기 N자리수의 OTP' 가 생성되면, 상기 OTP 인증수단(260) 또는 OTP 서버(220)는, 상기 수신된 N자리수의 OTP와 상기 생성된 OTP' 를 비교(또는 검증 연산)하여 상기 휴대폰(200) 결제를 인증하기 위한 OTP 인증을 처리한다.
- [0364] 만약 상기 비교 결과 상기 OTP와 OTP' 가 일치(또는 매칭)되거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되면, 상기 OTP 인증수단(260) 또는 OTP 서버(220)는 상기 휴대폰(200) 결제를 인증하기 위한 OTP가 인증된 것으로 처리하고, 상기 OTP 인증 결과를 상기 OTP 인증 결과를 필요로 하는 OTP 인증요청 서버(215), 사용자 단

말(205), 휴대폰(200) 중 하나 이상의 OTP 인증결과 수신수단으로 제공한다.

- [0366] 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(260) 또는 OTP 서버(220)는 상기 휴대폰(200) 결제를 인증하기 위한 OTP가 인증되지 않은 것으로 처리하고, 상기 OTP 인증 결과를 상기 OTP 인증 결과를 필요로 하는 OTP 인증요청 서버(215), 사용자 단말(205), 휴대폰(200) 중 하나 이상의 OTP 인증결과 수신수단으로 제공한다.
- [0368] 도면3은 본 발명의 실시 방법에 따른 OTP 매체 등록 과정을 도시한 도면이다.
- [0370] 보다 상세하게 본 도면3은 사용자의 휴대폰(200)을 휴대폰(200) 결제를 인증하기 위한 상기 도면2에 도시된 휴대폰(200) 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.
- [0372] 이하, 본 도면3에서 상기 도면2에 도시된 OTP 운영 시스템을 편의상 "서버"라고 한다.
- [0374] 도면3을 참조하면, OTP 등록단말에서 통신망을 통해 서버에 접속하여 상기 사용자의 휴대폰(200)을 OTP 매체로 등록 요청하면(300), 상기 서버는 상기 OTP 등록단말로 사용자의 고객정보와 상기 사용자의 휴대폰(200)에 대응하는 휴대폰(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 휴대폰(200) 고유정보와 고객정보를 포함하고, 생체 인식 정보를 더 포함하는 OTP 매체 정보를 입력 및 구성하여 상기 서버로 전송한다(310).
- [0376] 상기 서버는 상기 OTP 등록단말로부터 상기 휴대폰(200) 고유정보와 고객정보를 포함하고, 생체 인식 정보를 더 포함하는 OTP 매체 정보를 수신하고, 상기 휴대폰(200) 고유정보와 고객정보를 상기 휴대폰(200) 고유정보에 대응하는 통신사 서버(210)로 제공하여 상기 휴대폰(200) 고유정보에 대응하는 휴대폰(200)을 OTP 매체로 이용하는 것에 대한 유효성을 확인한다(315).
- [0378] 만약 상기 휴대폰(200)을 OTP 매체로 이용하는 것에 대한 유효성이 확인되지 않으면(320), 상기 서버는 상기 OTP 등록단말로 OTP 매체 오류 정보를 제공하고(325), 상기 휴대폰(200)을 OTP 매체로 등록하는 과정을 종료한다.
- [0380] 반면 상기 휴대폰(200)을 OTP 매체로 이용하는 것에 대한 유효성이 확인되면(320), 상기 서버는 상기 OTP 매체에 상기 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한  $M(M \geq 1)$ 개의 단말측 OTP 생성 정보와 M개의 서버측 OTP 생성 정보를 생성(또는 할당)하고, 상기 M개의 단말측 OTP 생성 정보와 서버측 OTP 생성 정보에 대응하는 M개의 인덱스 값을 고유하게 할당한 후(330), 상기 OTP 매체 정보와 상기 할당(또는 생성)된 M개의 단말측 OTP 생성 정보, 서버측 OTP 생성 정보 및 인덱스 값을 연계하여 저장매체(275)에 저장한다(335).
- [0382] 본 발명의 실시 방법에 따르면, 상기 서버에서 오직 하나의 단말측 OTP 생성 정보와 서버측 OTP 생성 정보가 할당되는 것이 가능하며, 이 경우 상기 서버는 상기 인덱스 값을 할당되지 않아도 무방하다.
- [0384] 여기서, 상기 단말측 OTP 생성 정보는, 상기 휴대폰(200)으로 제공되어 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장(또는 암호화 저장)되며, 상기 OTP 운영 시스템에서 생성되어 상기 휴대폰(200)에 구비된 OTP 에이전트를 통해 출력될 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 바람직하다.
- [0386] 상기 서버측 OTP 생성 정보는, 상기 OTP 운영 시스템 상에 유지되며, 상기 OTP 운영 시스템에서 생성되어 상기 휴대폰(200)에 구비된 OTP 에이전트를 통해 출력될 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 바람직하다.
- [0388] 본 발명의 다른 실시 방법에 따르면, 상기 서버측 OTP 생성 정보는, 상기 OTP 운영 시스템 상에 유지되며, 상기 OTP 운영 시스템에서 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한 하나 이상의 고정 씨드 값과 동적 씨드 값을 결정하기 위한 파라미터를 포함하여 이루어지는 것이 가능하다.
- [0390] 이후, 상기 서버는 상기 휴대폰(200) 고유정보에 대응하는 휴대폰(200)에 상기 도면1에 도시된 휴대폰(200) 구

성에 대응하는 OTP 에이전트가 구비되어 있는지 확인한다(340).

- [0392] 본 발명의 실시 방법에 따르면, 상기 서버는 상기 휴대폰(200) 고유정보와 상기 휴대폰(200)에 구비된 OTP 에이전트 정보(예컨대, OTP 에이전트 버전 정보, OTP 발급사 정보, OTP 사용처 정보, OTP 에이전트 사용내역 등)를 연계하여 저장하는 데이터베이스(도시생략) 또는 OTP 서버(220) 또는 통신사 서버(210)를 통해 상기 휴대폰(200)에 상기 OTP 에이전트가 구비되어 있는지 확인하는 것이 바람직하다.
- [0394] 만약 상기 휴대폰(200)에 OTP 에이전트가 탑재되어 있지 않다면(345), 상기 서버는 상기 휴대폰(200)에 구비된 플랫폼(또는 운영체제)에서 동작 가능하며 상기 도면1에 도시된 휴대폰(200) 구성에 대응하는 OTP 에이전트 프로그램 코드와, 상기 할당된 M개의 단말측 OTP 생성 정보와 인덱스 값 중 상기 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한  $m(1 \leq m \leq M)$ 개의 단말측 OTP 생성 정보를 상기 휴대폰(200)으로 제공하고(350), 상기 휴대폰(200)은 상기 OTP 에이전트를 상기 휴대폰(200)에 구비된 기록매체(예컨대, USIM/메모리부의 프로그램 영역)에 기록하고, 상기 m개의 단말측 OTP 생성 정보와 인덱스 값을 상기 OTP 에이전트와 연결하여 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장한다(360).
- [0396] 반면 상기 휴대폰(200)에 OTP 에이전트가 탑재되어 있다면(345), 상기 서버는 상기 할당된 M개의 단말측 OTP 생성 정보와 인덱스 값 중 상기 N자리수의 OTP를 생성하는 OTP 생성 정보에 포함될 OTP 생성 값을 생성하기 위한  $m(1 \leq m \leq M)$ 개의 단말측 OTP 생성 정보와 인덱스 값을 상기 휴대폰(200)으로 제공하고(355), 상기 휴대폰(200)은 상기 m개의 단말측 OTP 생성 정보와 인덱스 값을 상기 휴대폰(200)에 구비된 기록매체(예컨대, USIM/메모리부의 프로그램 영역)에 기록되어 있는 OTP 에이전트와 연결하여 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장한다(360).
- [0398] 본 발명의 실시 방법에 따라 상기 생체 인식 정보를 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장하는 경우, 상기 서버는 상기 생체 인식 정보를 상기 휴대폰(200)으로 제공하여 상기 휴대폰(200)에 구비된 USIM/메모리부에 저장하며, 상기 생체 인식 정보는 상기 단말측 OTP 생성 정보 또는 OTP 에이전트 프로그램 코드에 포함되어 상기 휴대폰(200)으로 제공되는 것이 가능하다.
- [0400] 도면4는 본 발명의 실시 방법에 따른 OTP 생성 과정을 도시한 도면이다.
- [0402] 보다 상세하게 본 도면4는 사용자의 휴대폰(200)이 상기 도면3에 도시된 과정을 통해 OTP 매체로 등록된 후, 도면1에 도시된 휴대폰(200)에서 상기 도면2에 도시된 OTP 운영 시스템과 연계하여  $N(N \geq 2)$ 자리수의 OTP를 생성하는 과정 중 생체 인식을 이용하지 않고 OTP를 생성하는 과정을 도시한 것으로서, 본 도면4에 도시된 과정에 생체 인식을 이용하는 방법은 도면5에 도시하여 설명하기로 한다. 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.
- [0404] 예컨대, 본 도면4는 편의상 OTP 매체인증 정보에 휴대폰(200) 고유정보와 인덱스 값 및 상기 인덱스 값에 대응하는 단말측 OTP 생성 정보를 포함하여 OTP 운영 시스템으로 전송하는 것으로 도시하여 설명하지만, 이에 의해 본 발명이 한정되는 것은 결코 아니며, 상기 인덱스 값 또는 단말측 OTP 생성 정보는 상기 OTP 매체인증 정보에 포함되지 않고 별도의 채널을 통해 OTP 운영 시스템으로 전송되는 것이 가능하며, 또한 OTP 매체인증 정보는 상기 OTP 운영 시스템에서 사용자 인증을 위한 사용자 비밀번호 또는 사용자 개인식별번호를 더 포함하거나, 또는 별도의 채널을 통해 상기 사용자 비밀번호 또는 사용자 개인식별번호를 상기 OTP 운영 시스템으로 전송하는 것이 모두 가능하며, 본 발명은 본 도면4를 통해 변형 가능한 모든 실시 방법을 포함함을 명백하게 밝혀두는 바이다.
- [0407] \*이하, 본 도면4에서 상기 도면2에 도시된 OTP 운영 시스템을 편의상 "서버"라고 한다.
- [0409] 도면4를 참조하면, 사용자의 휴대폰(200)이 상기 도면3에 도시된 과정을 통해 OTP 매체로 등록된 후, 상기 휴대폰(200)은 키 입력수단을 통해 상기 휴대폰(200) 결제를 인증하기 위한 N자리수의 OTP를 생성하도록 요청하는 전용 키 버튼이 입력되거나, 또는 기 설정된 메뉴 선택을 통해 상기 N자리수의 OTP를 생성하도록 요청되거나, 또는 상기 이동 통신망을 통해 OTP 생성 명령(또는 OTP 에이전트 구동 명령)이 수신되면, 상기 도면1에 도시된 휴대폰(200) 구성에 대응하는 OTP 에이전트를 구동하여 상기 휴대폰(200)을 OTP 매체로 이용하기 위한 사용자 인증을 요청하고(400), 사용자 비밀번호 또는 사용자 개인식별번호를 통해 사용자 인증을 처리한다(405).
- [0411] 본 발명의 실시 방법에 따르면 상기 OTP 에이전트를 구동하는 과정은 도면5에 도시된 바와 같이 생체 인식 정보를 통해 구동되는 것이 가능하며, 또는 상기 사용자 인증 과정은 도면5에 도시된 바와 같이 생체 인증으로 대체

되는 것이 가능하다.

- [0413] 만약 상기 사용자 인증이 유효하게 처리되지 않는다면(410), 상기 휴대폰(200)은 사용자 인증 오류 정보를 출력하고(415), 상기 휴대폰(200) 결제를 인증하기 위한 OTP 생성 과정을 종료한다.
- [0415] 반면 상기 사용자 인증이 유효하게 처리되면(410), 상기 휴대폰(200)은 USIM/메모리부에 저장된 m개의 인덱스 값 중 휴대폰(200) 결제를 인증하기 위한 OTP 인증에 사용할 어느 하나의 인덱스 값을 결정하고, 상기 결정된 인덱스 값 및 상기 인덱스 값에 대응하는 단말측 OTP 생성 정보를 확인하고(420), 상기 휴대폰(200)에 대응하는 휴대폰(200) 고유정보와 상기 결정된 인덱스 값 및 상기 인덱스 값에 대응하는 단말측 OTP 생성 정보를 포함하는 OTP 매체인증 정보를 구성하고(425), 상기 서버와 통신채널을 연결한 후, 상기 통신채널을 통해 상기 서버로 상기 OTP 매체인증 정보를 전송한다(430).
- [0417] 본 발명의 실시 방법에 따르면 상기 OTP 매체인증 정보는 도면5에 도시된 바와 같이 생체 인식 정보를 더 포함하는 것이 가능하다.
- [0419] 상기 서버는 상기 통신채널을 통해 상기 OTP 매체인증 정보를 수신하고, 상기 수신된 OTP 매체인증 정보에 포함된 휴대폰(200) 고유정보를 판독하여 상기 휴대폰(200)을 OTP 매체로 인증한다(435).
- [0421] 본 발명의 실시 방법에 따르면, 상기 서버는 상기 저장매체(275)로부터 상기 OTP 매체인증 정보에 포함된 구성 정보와 매칭되는 구성 정보를 포함하는 OTP 매체 정보를 확인하고, 상기 OTP 매체인증 정보에 포함된 구성 정보와 OTP 매체 정보에 포함된 구성 정보를 비교(또는 검증 연산)하고, 상기 비교(또는 검증 연산) 결과 상기 OTP 매체인증 정보에 포함된 구성 정보와 상기 저장매체(275)에 저장된 OTP 매체 정보에 포함된 구성 정보가 일치(또는 매칭)되거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되면, 상기 OTP 매체인증 정보를 전송한 휴대폰(200)을 상기 OTP 매체 등록수단(225)에 의해 OTP 매체로 등록된 유효한 휴대폰(200)으로 인증하는 것이 바람직하다.
- [0423] 본 발명의 실시 방법에 따라 도면5에 도시된 과정을 통해 생체 인식 정보가 더 수신된 경우, 상기 서버는 상기 저장매체(275)로부터 상기 OTP 매체인증 정보에 포함된 생체 인식 정보와 매칭되는 생체 인식 정보(또는 생체 인증 정보)를 확인하고, 상기 OTP 매체인증 정보에 포함된 생체 인식 정보와 OTP 매체 정보에 포함된 생체 인식 정보를 비교(또는 생체 인증 정보를 검증 연산)하고, 상기 비교(또는 검증 연산) 결과 상기 OTP 매체인증 정보에 포함된 생체 인식 정보와 상기 저장매체(275)에 저장된 OTP 매체 정보에 포함된 생체 인식 정보가 일치(또는 매칭)되거나, 또는 검증 연산을 통해 기 예측된 결과가 도출되면, 상기 OTP 매체인증 정보를 전송한 휴대폰(200)을 상기 OTP 매체 등록수단(225)에 의해 OTP 매체로 등록된 유효한 휴대폰(200)으로 인증하는 것이 바람직하다.
- [0425] 만약 상기 휴대폰(200)이 유효한 OTP 매체로 인증되지 않으면(440), 상기 서버는 상기 휴대폰(200)으로 OTP 매체 오류 정보를 전송하고(445), 상기 휴대폰(200) 결제를 인증하기 위한 OTP 생성 과정을 종료한다.
- [0427] 반면 상기 휴대폰(200)이 유효한 OTP 매체로 인증되면(440), 상기 서버는 수신된 단말측 OTP 생성 정보에 하나 이상의 고정 씨드 값을 확인하고, 상기 단말측 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 상기 서버측 OTP 생성 정보와 조합(또는 연계)될 OTP 생성 값을 생성하고, 또한 상기 휴대폰(200) 고유정보를 포함하는 OTP 매체 정보와 연계되어 저장매체(275)에 저장된 M개의 서버측 OTP 생성 정보 중 상기 인덱스 값에 대응하는 서버측 OTP 생성 정보를 확인한 후(450), 상기 생성된 OTP 생성 값과 상기 확인된 서버측 OTP 생성 정보를 조합(또는 연계)하여 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성(또는 생성)한다(455).
- [0429] 본 발명의 다른 실시 방법에 따르면, 상기 서버는, 상기 확인된 서버측 OTP 생성 정보에 포함된 하나 이상의 고정 씨드 값을 확인하고, 상기 서버측 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 상기 단말측 OTP 생성 정보를 통해 생성된 OTP 생성 값과 조합(또는 연계)될 OTP 생성 값을 생성한 후, 상기 단말측 OTP 생성 정보를 통해 생성된 OTP 생성 값과 서버측 OTP 생성 정보를 통해 생성된 OTP 생성 값을 조합(또는 연계)하여 상기 휴대폰(200)에서 N자리수의 OTP를 생성하기 위한 OTP 생성 정보를 구성(또는 생성)하는 것이 가능하다.
- [0431] 여기서, 상기 OTP 생성 값은, 상기 서버측 OTP 생성 정보를 통해 생성되는 OTP로서, 상기 N자리수의 OTP를 생성

하기 위한 제2의 씨드 값으로 사용되는 것을 특징으로 한다.

- [0433] 이후, 상기 서버는 상기 구성된 OTP 생성 정보를 통해 상기 N자리수의 OTP을 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 N자리수의 OTP를 생성하고(460), 통신채널을 통해 상기 휴대폰(200)으로 상기 생성된 N자리수의 OTP를 전송하고(465), 이에 대응하여 상기 휴대폰(200)은 상기 통신채널을 통해 N자리수의 OTP를 수신하여 출력한다(470).
- [0435] 도면5는 본 발명의 실시 방법에 따른 생체 인식 처리 과정을 도시한 도면이다.
- [0437] 보다 상세하게 본 도면5는 상기 도면4에 도시된 과정에서 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 생체 인식 대상으로부터 사용자의 생체 정보를 인식하고, 상기 인식되는 생체 정보는 기 설정된 생체 인식 방식에 따라 기 설정된 데이터 구조에 대응하는 생체 인식 정보로 변환한 후, 상기 리딩된 생체 인식 정보를 상기 휴대폰(200)에 구비된 OTP 에이전트를 구동하거나, 또는 상기 OTP 에이전트에서 OTP를 생성하는 것을 인증하는 OTP 구동 정보로 사용하거나, 상기 휴대폰(200)에 구비된 OTP 에이전트가 OTP 운영 시스템으로 전송하는 OTP 매체인증 정보에 포함시키는 실시 방법을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면5를 참조 및/또는 변형하여 상기 생체 인식 처리 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.
- [0439] 이하, 본 도면5에서 상기 도면2에 도시된 OTP 운영 시스템을 편의상 "서버"라고 한다.
- [0441] 도면5를 참조하면, 상기 휴대폰(200)은 상기 사용자의 생체 인식 대상으로부터 생체 정보를 인식하도록 요청하는 생체 인식 인터페이스를 출력하고, 상기 사용자의 지문, 홍채, 망막, 안면 중 어느 하나에 대응하는 생체 인식 대상으로부터 사용자의 생체 정보를 인식한다(500). 만약 상기 사용자의 생체 인식 대상으로부터 생체 정보가 인식되면(505), 상기 휴대폰(200)은 상기 인식된 생체 정보를 기 설정된 생체 인식 방식에 따라 기 설정된 데이터 구조에 대응하는 생체 인식 정보로 변환하고(510), USIM/메모리부에 저장된 생체 인식 정보(또는 생체 인증 정보)를 통해 상기 생체 인식 유효성을 인증한다(510).
- [0443] 만약 상기 생체 인식 유효성이 인증되지 않으면(515), 상기 휴대폰(200)은 생체 인증 오류 정보를 출력하고(520), 상기 휴대폰(200)을 통해 OTP를 생성/출력하는 과정을 종료한다.
- [0445] 반면 상기 생체 인식 유효성이 인증되면(515), 상기 휴대폰(200)은 OTP 에이전트를 구동하고(525), 상기 도면4에 도시된 과정을 통해 OTP 매체인증 정보를 구성하여 상기 서버로 전송하거나, 또는 상기 OTP 에이전트가 기 구동된 경우, 상기 생체 인식 유효성 확인 결과를 사용자 인증 결과로 처리한 후, 상기 도면4에 도시된 과정을 통해 OTP 매체인증 정보를 구성하여 상기 서버로 전송하는 과정을 수행한다.
- [0447] 만약 상기 도면4에 도시된 과정 중에 OTP 매체인증 정보에 생체 인식 정보를 포함시킨다면(530), 상기 휴대폰(200)은 상기 휴대폰(200) 고유정보를 포함하는 OTP 매체인증 정보에 상기 생체 인식 정보를 더 포함하여 OTP 매체인증 정보를 구성하고(535), 상기 서버와 통신채널을 연결한 후, 상기 통신채널을 통해 상기 서버로 상기 OTP 매체인증 정보를 전송한다(540).
- [0449] 도면6은 본 발명의 실시 방법에 따른 OTP 인증 과정을 도시한 도면이다.
- [0451] 보다 상세하게 본 도면6은 상기 도면2에 도시된 OTP 운영 시스템에서 통신망을 통해 상기 도면4와 도면5에 도시된 과정을 통해 상기 도면1에 도시된 휴대폰(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.
- [0453] 이하, 본 도면6에서 상기 도면2에 도시된 OTP 운영 시스템을 편의상 "서버"라고 한다.
- [0455] 도면6을 참조하면, 상기 도면4와 도면5에 도시된 과정을 통해 상기 도면1에 도시된 휴대폰(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 수신하거나, 또는 상기 도면1에 도시된 휴대폰(200)으로부터 상기 생성된 N

자리수의 OTP를 수신하고(600), 저장매체(275)로부터 상기 N자리수의 OTP를 생성한 OTP 매체에 대응하는 M개의 단말측 OTP 생성 정보 중 상기 도면4와 도면5에 도시된 과정을 통해 확인된 인덱스 값에 대응(단, 상기 도면4와 도면5에서 인덱스 값이 확인되지 않은 경우 생략)하는 단말측 OTP 생성 정보와 서버측 OTP 생성 정보를 확인한다(605).

- [0457] 본 발명의 일 실시 방법에 따라 상기 사용자 단말(205)로부터 상기 N자리수의 OTP가 수신되는 경우, 상기 OTP 매체에 대응하는 휴대폰(200) 고유정보는 상기 N자리수의 OTP가 수신되기 전의 OTP 인증 요청 과정에서 상기 서버로 제공되거나, 또는 상기 N자리수의 OTP와 함께 상기 서버로 제공되는 것이 바람직하다.
- [0459] 본 발명의 다른 일 실시 방법에 따라 상기 사용자 단말(205)로부터 상기 N자리수의 OTP가 수신되는 경우, 상기 OTP 매체에 대응하는 휴대폰(200) 고유정보는 상기 휴대폰(200)에 대응하는 발신자 정보로부터 확인되거나, 또는 상기 N자리수의 OTP와 함께 상기 서버로 제공되는 것이 바람직하다.
- [0461] 이후, 상기 서버는 상기 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하고, 상기 OTP 생성 값과 서버측 OTP 생성 정보를 조합(또는 연계)하여 상기 OTP 생성 정보를 구성한다(610).
- [0463] 만약 상기 서버에서 상기 도면4와 도면5에 도시된 과정을 통해 상기 휴대폰(200)으로 제공한 N자리수의 OTP를 생성한 OTP 생성 정보를 확인할 수 있는 경우, 상기 서버는 상기 휴대폰(200)으로 제공한 N자리수의 OTP를 생성한 OTP 생성 정보를 확인하는 것이 가능하다.
- [0465] 본 발명의 다른 실시 방법에 따라 상기 휴대폰(200)으로 제공된 OTP 생성 정보가 상기 서버측 OTP 생성 정보를 통해 생성된 OTP 생성 값을 포함하는 경우, 상기 서버는, 상기 단말측 OTP 생성 정보를 통해 OTP 생성 값을 생성하고 상기 서버측 OTP 생성 정보를 통해 OTP 생성 값을 생성한 후 상기 생성된 각각의 OTP 생성 값을 조합(또는 연계)하여 상기 OTP 생성 정보를 구성하는 것이 가능하다.
- [0467] 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).
- [0469] 만약 상기 서버에서 상기 도면4와 도면5에 도시된 과정을 통해 상기 휴대폰(200)으로 제공한 N자리수의 OTP를 확인할 수 있는 경우, 상기 서버는 상기 휴대폰(200)으로 제공한 N자리수의 OTP를 확인하는 것이 가능하다.
- [0471] 만약 상기 N자리수의 OTP' 가 생성되면(620), 상기 서버는 상기 수신된 N자리수의 OTP와 OTP' 를 비교(또는 검증 연산)하여 상기 휴대폰(200) 결제를 인증하기 위한 OTP 유효성을 확인한다(625).
- [0473] 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 휴대폰(200) 결제를 인증하기 위한 OTP 유효성이 확인된 것으로 처리한다.
- [0475] 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(215), 사용자 단말(205), 휴대폰(200) 중 하나 이상의 포함)으로 제공한다(635).
- [0477] 반면 상기 OTP 유효성이 확인되면(630), 상기 서버는 OTP 유효성 확인에 대응하는 OTP 인증결과를 기 설정된 OTP 인증결과 수신수단(예컨대, OTP 인증요청 서버(215), 사용자 단말(205), 휴대폰(200) 중 하나 이상의 포함)으로 제공한다(640).
- [0479] 도면7은 본 발명의 실시 방법에 따른 OTP 기반 휴대폰(700) 결제 처리 시스템 구성을 도시한 도면이다.
- [0481] 보다 상세하게 본 도면7은 상기 도면2에 도시된 OTP 운영 시스템을 구비한 휴대폰(700) 결제 처리 시스템 구성을 도시한 것으로서, 소액결제 대상 웹사이트에 접속한 사용자 단말(705)로 휴대폰(700) 결제와 관련된 하나 이상의 인터페이스가 제공되도록 처리한 후, 상기 사용자 단말(705)에서 상기 인터페이스 중 OTP를 입력하는 사용자 인터페이스가 포함된 인터페이스를 통해 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하여 전송하면, 상기 사용자 단말(705)로부터 상기 OTP를 수신하고, 상기 OTP에 대한 유효성을 검증한 후, 상기 OTP 유효성 검증 결과에 따라 휴대폰(700) 결제를 처리하는 시스템 구성을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면7을 참조 및/또는 변형하여 상기 OTP 기반 휴대폰(700) 결제 처리 시스템에 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 도면7에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.

- [0483] 예컨대, 본 도면7에 도시된 휴대폰(700) 결제 처리 시스템은 결제금액을 사용자 휴대폰(700)의 통신요금에 부가하는 것을 제외하면, 고객의 결제수단을 이용해 결제를 처리하는 시스템에 적용하는 것이 가능하며, 본 발명은 상기와 같이 유추 가능한 모든 결제 처리 시스템을 포함하는 것이 당연하다.
- [0485] 도면7을 참조하면, 상기 휴대폰(700) 결제 처리 시스템은, 소액결제 대상 웹사이트에 접속한 사용자가 사용하는 사용자 단말(705) 및 상기 사용자가 소지하며 상기 도면1에 도시된 휴대폰(700)에 구비된 휴대폰(700) 구성을 구비한 사용자 휴대폰(700)을 포함하고, 상기 사용자 단말(705)을 통해 사용자에게 유형/무형의 재화를 판매하고, 상기 판매된 재화에 대한 결제금액을 사용자 휴대폰(700) 통신요금에 부과하는 휴대폰(700) 결제수단을 통해 결제할 수 있도록 하는 소액결제 대상 웹사이트를 운영하는 하나 이상의 OTP 인증요청 서버(715)와, 상기 사용자 단말(705) 및 사용자 휴대폰(700)과 연계하여 OTP 기반 휴대폰(700) 소액결제를 처리하는 휴대폰(700) 결제 시스템과, 상기 사용자 휴대폰(700)이 접속한 이동 통신망 상의 통신사 서버(710)를 포함하여 이루어지는 것을 특징으로 하며, 상기 휴대폰(700) 결제 시스템은 상기 OTP 인증요청 서버(715) 및 통신사 서버(710)와 연결된 인증서버(또는 중계서버) 형태로 구현되거나, 또는 상기 OTP 인증요청 서버(715)의 내부 구성 요소 형태로 구현되거나, 또는 상기 통신사 서버(710)의 내부 구성 요소 형태로 구현되는 것이 모두 가능하며, 이에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.
- [0487] 상기 사용자 단말(705)은, 상기 소액결제 대상 웹사이트를 운영하는 OTP 인증요청 서버(715)에 접속할 수 있는 브라우저를 구비한 개인 컴퓨터, 노트북을 하나 이상 포함하며, 상기 OTP 인증요청 서버(715) 또는 휴대폰(700) 결제 시스템으로부터 휴대폰(700) 결제를 위한 하나 이상의 인터페이스를 수신하여 출력하고, 상기 인터페이스에 포함된 사용자 인터페이스를 통해 상기 휴대폰(700) 결제를 위한 하나 이상의 정보를 입력하여 상기 OTP 인증요청 서버(715) 또는 휴대폰(700) 결제 시스템으로 전송하는 것을 특징으로 한다.
- [0489] 본 발명의 일 실시 방법에 따르면, 상기 사용자 단말(705)은 상기 OTP 인증요청 서버(715) 또는 휴대폰(700) 결제 시스템으로부터 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호를 입력하기 위한 휴대폰(700) 결제 인터페이스를 제공받아 화면 출력수단으로 출력하고, 키 입력수단을 통해 상기 휴대폰(700) 결제 인터페이스로 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 입력하여 상기 OTP 인증요청 서버(715) 또는 휴대폰(700) 결제 시스템으로 전송한 후, 상기 OTP 인증요청 서버(715) 또는 휴대폰(700) 결제 시스템으로부터 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하는 OTP 입력 인터페이스를 제공받아 화면 출력수단으로 출력하고, 키 입력수단을 통해 상기 OTP 입력 인터페이스로 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하여 상기 OTP 인증요청 서버(715) 또는 휴대폰(700) 결제 시스템으로 전송하는 것을 특징으로 한다.
- [0491] 본 발명의 다른 일 실시 방법에 따르면, 상기 사용자 단말(705)은 상기 OTP 인증요청 서버(715) 또는 휴대폰(700) 결제 시스템으로부터 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보 및 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하는 휴대폰(700) 결제 인터페이스를 제공받아 화면 출력수단으로 출력하고, 키 입력수단을 통해 상기 휴대폰(700) 결제 인터페이스로 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보 및 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하여 상기 OTP 인증요청 서버(715) 또는 휴대폰(700) 결제 시스템으로 전송하는 것을 특징으로 한다.
- [0493] 상기 OTP 인증요청 서버(715)는, 상기 사용자 단말(705)을 통해 사용자에게 유형/무형의 재화를 판매하고, 상기 판매된 재화에 대한 결제금액을 사용자 휴대폰(700) 통신요금에 부과하는 휴대폰(700) 결제수단을 통해 결제할 수 있는 소액결제 대상 웹사이트를 운영하는 서버의 총칭으로서, 상기 사용자 단말(705)에서 상기 휴대폰(700) 결제수단을 상기 결제금액에 대한 결제수단으로 선택하면, 상기 사용자 단말(705)로 상기 휴대폰(700) 결제 인터페이스를 제공하거나, 또는 상기 휴대폰(700) 결제 시스템을 통해 상기 사용자 단말(705)로 상기 휴대폰(700) 결제 인터페이스가 제공되도록 처리하는 것을 특징으로 한다.
- [0495] 상기 사용자 휴대폰(700)은, 상기 OTP 인증요청 서버(715)가 판매하는 유형/무형의 재화를 구매하는 사용자가 소지하고 있는 휴대폰(700)으로서, 상기 사용자 휴대폰(700)에 부과되는 통신요금을 이용한 결제 유효성을 인증

하기 위한 OTP 에이전트를 다운로드하는 기능과, 상기 OTP 에이전트를 구동하여 OTP를 생성하고, 상기 생성된 OTP를 출력하는 기능(예컨대, 화면출력, 또는 블루투스, 와이파이, RF통신 등과 같은 근거리통신수단을 통해 사용자 단말(705)로 출력 가능)을 구비하여 이루어지는 것을 특징으로 한다.

- [0497] 본 발명에 따르면, 상기 사용자 단말(705)은, 사용자가 통신망을 통해 서버에 접속하여 상기 서버에서 판매하는 유형/무형의 재화를 구매하는 제1 단말의 일 실시예로서, 상기 제1 단말은 상기 통신망 및 서버 종류와 특성에 따라 다양하게 변형하여 실시하는 것이 가능하다.
- [0499] 본 발명에 따르면, 상기 사용자 휴대폰(700)은, 상기 제1 단말을 통해 재화를 구매한 구매대금에 대한 결제 유효성을 인증하기 위해 OTP 에이전트가 탑재된 제2 단말의 일 실시예로서, 상기 제2 단말은 상기 제1 단말을 제외한 모든 통신단말을 포함하여 이루어질 수 있다.
- [0501] 예를들어, 상기 제1 단말이 접속하는 서버가 홈쇼핑 서버인 경우, 상기 제1 단말은 사용자의 IPTV를 포함할 수 있으며, 상기 제2 단말은 상기 IPTV 근처에 구비된 유선전화/VoIP폰을 포함할 수 있다.
- [0503] 또는, 상기 제1 단말이 접속하는 서버가 ARS 서버인 경우, 상기 제1 단말은 사용자의 유선전화/휴대폰(700)/VoIP폰을 포함할 수 있으며, 상기 제2 단말은 상기 제1 단말을 제외한 다른 음성통화단말(예컨대, 상기 제1 단말이 유선전화라면 상기 제2 단말은 휴대폰(700)/VoIP폰을 포함하고, 상기 제1 단말이 휴대폰(700)이라면 상기 제2 단말은 유선전화/VoIP폰을 포함하고, 상기 제1 단말이 VoIP폰이라면 상기 제2 단말은 유선전화/휴대폰(700)을 포함 가능)을 포함할 수 있다.
- [0505] 즉, 본원의 사용자 단말(705)이 상술된 유선단말로 한정되는 것은 결코 아니며, 본원의 사용자 휴대폰(700) 역시 휴대폰(700)으로 한정되는 것은 결코 아님을 명백하게 밝혀두는 바이다.
- [0507] 상기 통신사 서버(710)는, 상기 사용자 휴대폰(700)이 접속한 이동 통신망 상에 구비되어 상기 휴대폰(700)과 인터페이스하는 이동통신사 측 서버의 총칭으로서, 상기 휴대폰(700) 결제 시스템에서 상기 사용자 휴대폰(700)으로 제공하도록 요청하는 정보(또는 데이터)를 기 설정된 통신 프로토콜에 따라 이동통신 시스템(예컨대, 교환기, 기지국 등)을 통해 상기 사용자 휴대폰(700)으로 전송하는 메시지 서버, 데이터 교환 서버, 왓(WAP) 서버를 하나 이상 포함하여 이루어지는 것이 바람직하다.
- [0509] 본 발명의 실시 방법에 따르면, 상기 통신사 서버(710)는 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 통해 가입자 D/B(도시생략)를 조회하여 사용자를 인증하는 기능과, 상기 사용자 휴대폰(700)으로 OTP 에이전트를 제공하거나, 또는 소정의 OTP 서버(720)를 통해 상기 사용자 휴대폰(700)으로 제공된 OTP 에이전트를 관리하는 기능을 구비하는 것이 바람직하다.
- [0511] 본 발명의 실시 방법에 따르면, 상기 통신사 서버(710)는 사용자 휴대폰(700)에 OTP 에이전트가 구비되거나, 또는 상기 사용자 휴대폰(700)으로 OTP 에이전트를 제공한 경우, 상기 사용자 휴대폰(700)에 대응하는 휴대폰(700)번호와, 상기 사용자 휴대폰(700)에 구비된 OTP 에이전트에 대응하는 OTP 에이전트 정보를 연계하여 저장하는 것이 바람직하다.
- [0513] 여기서, 상기 OTP 에이전트 정보는, 상기 휴대폰(700)번호에 대응하는 사용자 휴대폰(700)에 구비된 OTP 에이전트의 버전 정보, OTP 생성 알고리즘 및 OTP 생성 방식을 하나 이상 포함하여 이루어지는 것이 바람직하다.
- [0515] 여기서, 상기 OTP 생성 알고리즘 및 OTP 생성 방식은, 각각의 OTP 에이전트마다 서로 다른 알고리즘과 생성 방식을 사용하는 것이 가능하며, 이에 의해 본 발명이 한정되지 아니한다.
- [0517] 본 발명의 일 실시 방법에 따른 도면7을 참조하면, 상기 휴대폰(700) 결제 시스템은, 상기 소액결제 대상 웹사이트에 접속한 사용자 단말(705)로 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호를 입력하기 위한 휴대폰(700) 결제 인터페이스가 제공되도록 처리하는 인터페이스 제공수단(735)과, 상기 휴대폰(700) 결제 인터페이스를 통해 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 수신하는 정보 수신수단(740)과, 상기 수신된 이동통신사 선택정보에 대응하는 통신사 서버(710)로 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 전송하고, 상기 통신사 서버(710)를 통해 사용자 휴대폰(700)번호와 사용자 주민등록번호 확인결과에 대응하는 사용자 인증결과를 수신 및 판독하여 상기 사용자를 인증하는 사용자 인증수단(745)을 구비하여 이루어지는 것을 특징으로 하며, 상기 인터페이스 제공수단(735)은 상기 사용자 단말(705)로 사용자 휴대폰(700)에 구비된 OTP 에이전트에 의해 생성되는 OTP를 입력하기 위한 OTP 입력 인터페이스가 제공되도록 처리하는 것을 특징으로 한다.

- [0519] 본 발명의 다른 일 실시 방법에 따른 도면7을 참조하면, 상기 휴대폰(700) 결제 시스템은, 상기 소액결제 대상 웹사이트에 접속한 사용자 단말(705)로 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 및 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하는 휴대폰(700) 결제 인터페이스를 제공하는 인터페이스 제공수단(735)과, 상기 휴대폰(700) 결제 인터페이스를 통해 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보 및 OTP를 수신하는 정보 수신수단(740)과, 상기 수신된 이동통신사 선택 정보에 대응하는 통신사 서버(710)로 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 전송하고, 상기 통신사 서버(710)를 통해 사용자 휴대폰(700)번호와 사용자 주민등록번호 확인결과에 대응하는 사용자 인증결과를 수신 및 판독하여 상기 사용자를 인증하는 사용자 인증수단(745)을 구비하여 이루어지는 것을 특징으로 한다.
- [0521] 본 발명에 따르면, 상기 휴대폰(700) 결제 시스템을 구성하는 각각의 수단은 각 수단 별로 별도의 서버로 구현되거나, 또는 상기 수단을 포함하는 소정의 인증서버(또는 중계서버) 형태로 구현되거나, 또는 두개 이상의 수단이 결합하여 별도 서버로 구현되거나, 또는 상기 수단들이 상기 OTP 인증요청 서버(715) 내 구성 요소 형태로 구현되거나, 또는 상기 수단들이 상기 통신사 서버(710) 내 구성 요소 형태로 구현되거나, 또는 상기 수단 중 일부는 OTP 인증요청 서버(715) 내 구성 요소로 구현되고 나머지 일부는 통신사 서버(710) 내 구성요소로 구현되거나, 또는 상기 수단 중 일부는 OTP 인증요청 서버(715) 내 구성 요소로 구현되고 나머지 일부는 통신사 서버(710) 내 구성요소로 구현되고 또다른 나머지 일부는 별도 서버 형태로 구현되는 것이 모두 가능하며, 상기 휴대폰(700) 결제 시스템을 구현하는 실시 방법에 의해 본 발명이 한정되지 아니함을 명백하게 밝혀두는 바이다.
- [0523] 본 발명의 일 실시 방법에 따르면, 상기 사용자가 상기 OTP 인증요청 서버(715)에 접속하여 유형/무형의 재화를 구매하고, 상기 재화에 대한 구매대금에 대응하는 결제금액을 상기 사용자 휴대폰(700)에 부과되는 통신요금을 통해 결제하도록 휴대폰(700) 결제수단을 선택하면, 상기 인터페이스 제공수단(735)은, 상기 사용자 단말(705)이 접속한 통신망을 통해 상기 사용자 단말(705)로 직접, 또는 상기 OTP 인증요청 서버(715)를 중계하여 상기 사용자 단말(705)로 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호를 입력하기 위한 휴대폰(700) 결제 인터페이스가 제공되도록 처리하는 것을 특징으로 한다.
- [0525] 상기 인터페이스 제공수단(735)에 의해 상기 사용자 단말(705)로 상기 휴대폰(700) 결제 인터페이스가 제공되면, 상기 정보 수신수단(740)은 상기 사용자 단말(705)로부터 상기 휴대폰(700) 결제 인터페이스를 통해 입력된 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 수신하기 위한 통신세션을 연결한다.
- [0527] 본 발명의 일 실시 방법에 따라 상기 인터페이스 제공수단(735)이 상기 사용자 단말(705)과 통신채널을 연결하고, 상기 통신채널을 통해 상기 사용자 단말(705)로 상기 휴대폰(700) 결제 인터페이스를 제공한 경우, 상기 정보 수신수단(740)은 상기 휴대폰(700) 결제 인터페이스를 상기 사용자 단말(705)로 제공한 통신채널로부터 상기 사용자 단말(705) 정보(예컨대, IP주소)를 확인하고, 상기 통신채널을 기반으로 상기 사용자 단말(705)로부터 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 수신하기 위한 통신세션(예컨대, 상기 사용자 단말(705)로부터 상기 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 수신하기 위해 할당한 메모리 영역과 통신 스레드(Thread) 코드)을 연결하는 것이 바람직하다.
- [0529] 본 발명의 다른 일 실시 방법에 따라 상기 인터페이스 제공수단(735)이 상기 OTP 인증요청 서버(715)를 통해 사용자 단말(705)로 상기 휴대폰(700) 결제 인터페이스를 제공한 경우, 상기 정보 수신수단(740)은 상기 OTP 인증요청 서버(715)로부터 상기 사용자 단말(705) 정보(예컨대, IP주소)를 제공받고, 이를 기반으로 상기 사용자 단말(705)로부터 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 수신하기 위한 통신세션(예컨대, 상기 사용자 단말(705)로부터 상기 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 수신하기 위해 할당한 메모리 영역과 통신 스레드(Thread) 코드)을 연결하는 것이 바람직하다.
- [0531] 여기서, 상기 통신세션은, 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 암호화하여 수신하고, 상기 암호화된 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 복호화하는 보안통신세션을 포함하여 이루어지는 것이 바람직하다.
- [0533] 상기 사용자 단말(705)과 통신세션이 연결되면, 상기 정보 수신수단(740)은 상기 통신세션을 통해 상기 사용자

단말(705)로부터 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 수신하는 것을 특징으로 한다.

- [0535] 상기 사용자 단말(705)로부터 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보가 수신되면, 상기 사용자 인증수단(745)은, 상기 이동통신사 선택정보에 대응하는 통신사 서버(710)로 상기 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 전송하고, 상기 통신사 서버(710)에서 가입자 D/B를 통해 상기 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보에 대한 사용자 인증결과를 구성하여 전송하면, 상기 사용자 인증수단(745)은 상기 사용자 인증결과를 수신 및 판독하여 상기 휴대폰(700) 소액결제를 요청한 사용자를 인증하는 것을 특징으로 한다.
- [0538] 상기 사용자 인증이 확인되면, 상기 OTP 인터페이스 제공수단(735)은, 상기 사용자 단말(705)로 사용자 휴대폰(700)에 구비된 OTP 에이전트에 의해 생성되는 OTP를 입력하기 위한 OTP 입력 인터페이스가 제공되도록 처리하는 것을 특징으로 한다.
- [0540] 본 발명의 실시 방법에 따르면, 상기 OTP 인터페이스 제공수단(735)은 상기 사용자 단말(705)이 접속한 통신망을 통해 상기 사용자 단말(705)로 직접, 또는 상기 OTP 인증요청 서버(715)를 중계하여 상기 사용자 단말(705)로 상기 OTP 입력 인터페이스가 제공되도록 처리하는 것이 바람직하다.
- [0542] 상기 OTP 인터페이스 제공수단(735)에 의해 상기 사용자 단말(705)로 상기 OTP 입력 인터페이스가 제공되면, 상기 OTP 수신수단은 상기 사용자 단말(705)로부터 상기 OTP 입력 인터페이스를 통해 입력된 OTP를 수신하기 위한 통신세션을 연결하며, 상기 사용자 단말(705)과 통신세션이 기 연결된 경우 생략 가능하다.
- [0544] 본 발명의 일 실시 방법에 따라 상기 OTP 인터페이스 제공수단(735)이 상기 사용자 단말(705)과 통신채널을 연결하고, 상기 통신채널을 통해 상기 사용자 단말(705)로 상기 OTP 입력 인터페이스를 제공한 경우, 상기 OTP 수신수단은 상기 OTP 입력 인터페이스를 상기 사용자 단말(705)로 제공한 통신채널로부터 상기 사용자 단말(705) 정보(예컨대, IP주소)를 확인하고, 상기 통신채널을 기반으로 상기 사용자 단말(705)로부터 상기 OTP를 수신하기 위한 통신세션(예컨대, 상기 사용자 단말(705)로부터 상기 OTP를 수신하기 위해 할당된 메모리 영역과 통신 쓰레드(Thread) 코드)을 연결하는 것이 바람직하다.
- [0546] 본 발명의 다른 일 실시 방법에 따라 상기 OTP 인터페이스 제공수단(735)이 상기 OTP 인증요청 서버(715)를 통해 사용자 단말(705)로 상기 OTP 입력 인터페이스를 제공한 경우, 상기 OTP 수신수단은 상기 OTP 인증요청 서버(715)로부터 상기 사용자 단말(705) 정보(예컨대, IP주소)를 제공받고, 이를 기반으로 상기 사용자 단말(705)로부터 상기 OTP를 수신하기 위한 통신세션(예컨대, 상기 사용자 단말(705)로부터 상기 OTP를 수신하기 위해 할당된 메모리 영역과 통신 쓰레드(Thread) 코드)을 연결하는 것이 바람직하다.
- [0548] 여기서, 상기 통신세션은, 상기 OTP를 암호화하여 수신하고, 상기 암호화된 OTP를 복호화하는 보안통신세션을 포함하여 이루어지는 것이 바람직하다.
- [0550] 본 발명의 다른 일 실시 방법에 따르면, 상기 사용자가 상기 OTP 인증요청 서버(715)에 접속하여 유형/무형의 재화를 구매하고, 상기 재화에 대한 구매대금에 대응하는 결제금액을 상기 사용자 휴대폰(700)에 부과되는 통신요금을 통해 결제하도록 휴대폰(700) 결제수단을 선택하면, 상기 인터페이스 제공수단(735)은, 상기 사용자 단말(705)이 접속한 통신망을 통해 상기 사용자 단말(705)로 직접, 또는 상기 OTP 인증요청 서버(715)를 중계하여 상기 사용자 단말(705)로 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 및 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하기 위한 휴대폰(700) 결제 인터페이스가 제공되도록 처리하는 것을 특징으로 하며, 상기 정보 수신수단(740)은 상기 휴대폰(700) 결제 인터페이스를 통해 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보 및 OTP를 수신하고, 상기 사용자 인증수단(745)은 상기 수신된 이동통신사 선택정보에 대응하는 통신사 서버(710)로 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 전송하고, 상기 통신사 서버(710)를 통해 사용자 휴대폰(700)번호와 사용자 주민등록번호 확인결과에 대응하는 사용자 인증결과를 수신 및 판독하여 상기 사용자를 인증하는 것을 특징으로 한다.
- [0552] 도면7을 참조하면, 상기 휴대폰(700) 결제 시스템은, 상기 사용자 단말(705)로 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하기 위한 인터페이스가 제공된 후, 상기 도면1에 도시된 휴대폰(700)과 연계하여 상기 휴대폰(700) 결제를 인증기 위한 OTP를 생성하고, 상기 생성된 OTP가 상기 사용자 휴대폰(700)을 통해 출력되도록 처리한 후, 상기 사용자 단말(705)(또는 휴대폰(700))으로부터 상기 생성된 OTP를 수신하고, 상기 수신된 OTP에 대한 유효성을 검증하는 OTP 운영수단(725)을

구비하여 이루어지는 것을 특징으로 한다.

- [0554] 본 도면7에서 상기 OTP 운영수단(725)은 상기 도면2에 도시된 OTP 운영 시스템을 상기 휴대폰(700) 결제 시스템의 내부 구성 요소 형태로 도시한 것으로서, 이에 대한 상세한 설명은 상기 도면2에 도시된 OTP 운영 시스템 구성을 참조하기로 한다.
- [0556] 도면7을 참조하면, 상기 휴대폰(700) 결제 시스템은, 상기 OTP 운영수단(725)에 의해 결제 유효성이 인증되면, 상기 휴대폰(700)에 부과되는 통신요금을 통해 상기 결제금액이 결제되도록 처리하는 결제 처리수단(750)을 더 구비하여 이루어지는 것이 바람직하다.
- [0558] 본 발명의 실시 방법에 따르면, 상기 결제 처리수단(750)은, 상기 OTP 인증요청 서버(715)로부터 상기 사용자 휴대폰(700) 통신요금에 부과될 결제금액을 확인하고, 상기 통신사 서버(710)와 연계하여 상기 사용자 휴대폰(700)번호에 대한 결제한도를 조회하고, 상기 결제금액과 상기 결제한도를 비교하여 상기 휴대폰(700)에 부과되는 통신요금을 통한 결제를 승인하는 것이 바람직하다.
- [0560] 본 발명의 다른 실시 방법에 따르면, 상기 결제 처리수단(750)은, 상기 사용자 휴대폰(700)번호와 이에 대응하는 결제한도 정보를 별도의 데이터베이스를 통해 저장, 관리하는 것이 가능하며, 이 경우 상기 결제 처리수단(750)은 상기 데이터베이스를 통해 상기 사용자 휴대폰(700)번호에 대한 결제한도를 조회하고, 상기 결제금액과 상기 결제한도를 비교하여 상기 휴대폰(700)에 부과되는 통신요금을 통한 결제를 승인하는 것이 가능하다.
- [0562] 상기 휴대폰(700)에 부과되는 통신요금을 이용한 결제가 승인되면, 상기 결제 처리수단(750)은, 상기 통신사 서버(710)를 통해 상기 결제금액이 상기 사용자 휴대폰(700)에 대한 통신요금에 부과되도록 처리하고, 상기 OTP 인증요청 서버(715)로 상기 결제금액에 대한 결제승인 정보를 전달한다.
- [0564] 도면8은 본 발명의 일 실시 방법에 따른 OTP 기반 휴대폰(700) 결제 과정을 도시한 도면이다.
- [0566] 보다 상세하게 본 도면8은 소액결제 대상 웹사이트에 접속한 사용자 단말(705)로 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호를 입력하기 위한 인터페이스가 제공되도록 처리한 후 상기 사용자 단말(705)로부터 상기 인터페이스를 통해 사용자 휴대폰(700)에 대응하는 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 수신하고, 상기 이동통신사 선택정보에 대응하는 통신사 서버(710)를 통해 사용자 인증이 확인되면, 상기 사용자 단말(705)로 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하는 OTP 입력 인터페이스를 제공한 후, 상기 도면4 내지 도면6에 도시된 과정을 통해 상기 OTP를 생성/인증하고, 상기 OTP 인증 결과에 따라 휴대폰(700) 결제를 처리하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면8을 참조 및/또는 변형하여 상기 OTP 검증정보를 이용한 휴대폰(700) 결제 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 도면8에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.
- [0568] 이하, 본 도면8에서 상기 도면7에 도시된 휴대폰(700) 결제 시스템을 편의상 "서버"라고 하고, 상기 도면2 또는 도면7에 도시된 OTP 인증요청 서버(715)를 편의상 "웹서버"라고 한다.
- [0570] 도면8을 참조하면, 사용자가 상기 웹서버에 접속하여 유형/무형의 재화를 구매하고, 상기 재화에 대한 구매대금에 대응하는 결제금액을 상기 사용자 휴대폰(700)에 부과되는 통신요금을 통해 결제하도록 휴대폰(700) 결제수단을 선택하면(800), 상기 서버는 상기 사용자 단말(705)이 접속한 통신망을 통해 상기 사용자 단말(705)로 직접, 또는 상기 웹서버를 중계하여 상기 사용자 단말(705)로 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호를 입력하기 위한 휴대폰(700) 결제 인터페이스가 제공되도록 처리하고(805), 상기 사용자 단말(705)로부터 상기 휴대폰(700) 결제 인터페이스를 통해 입력된 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보가 수신되는지 확인한다(810).
- [0572] 만약 상기 사용자 단말(705)로부터 이동통신사 선택정보 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보가 수신되면(815), 상기 서버는 상기 이동통신사 선택정보에 대응하는 통신사 서버(710)로 상기 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보를 전송하여 사용자 인증을 요청하고, 상기 통신사 서버(710)에서 가입자 D/B를 통해 상기 사용자 휴대폰(700)번호와 사용자 주민등록번호 정보에 대한 사용자 인증결과를 구성하여 전송하면, 상기 사용자 인증결과를 수신 및 판독하여 상기 휴대폰(700) 소액결제를 요청한 사용자를 인증한다(820).

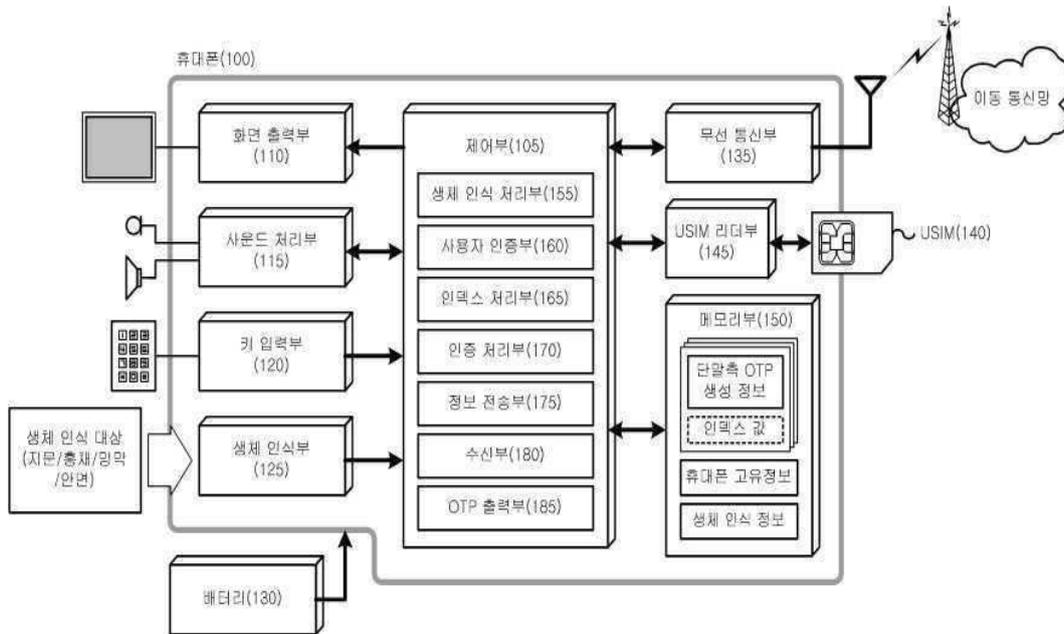
- [0574] 만약 상기 사용자가 인증되지 않으면(825), 상기 서버는 사용자 인증 오류를 생성하여 상기 사용자 단말(705) (또는 사용자 휴대폰(700))과 상기 웹서버로 전송한다(830).
- [0576] 반면 상기 사용자가 인증되면(825), 상기 서버는 상기 도면4 내지 도면6에 도시된 과정을 통해 상기 도면1에 도시된 휴대폰(700)과 연계하여 상기 휴대폰(700) 결제를 인증하기 위한 OTP를 생성하여 상기 사용자 휴대폰(700)에 출력되도록 처리하고, 상기 사용자 단말(705)(또는 휴대폰(700))으로부터 상기 OTP를 수신하여 상기 휴대폰(700) 결제를 위한 OTP 유효성을 인증한다(835).
- [0578] 만약 상기 휴대폰(700) 결제를 위한 OTP 유효성이 인증되지 않으면(840), 상기 서버는 결제 오류 정보를 생성하여 상기 사용자 유선단말(또는 사용자 휴대폰(700))과 웹서버로 전송한다(845).
- [0580] 만약 상기 휴대폰(700) 결제를 위한 OTP 유효성이 인증되면(840), 상기 서버는 상기 결제 유효성 확인결과를 생성하여 상기 사용자 유선단말(또는 사용자 휴대폰(700))과 웹서버로 전송하고(850), 상기 결제 유효성 확인결과에 대응하여 상기 사용자 휴대폰(700)의 통신요금을 통한 결제승인을 처리한다(855).
- [0582] 본 발명의 실시 방법에 따르면, 상기 서버는 상기 웹서버로부터 상기 사용자 휴대폰(700) 통신요금에 부과될 결제금액을 확인하고, 상기 통신사 서버(710)와 연계하여 상기 사용자 휴대폰(700)번호에 대한 결제한도를 조회하고, 상기 결제금액과 상기 결제한도를 비교하여 상기 휴대폰(700)에 부과되는 통신요금을 통한 결제를 승인하는 것이 바람직하다.
- [0584] 도면9는 본 발명의 다른 일 실시 방법에 따른 OTP 기반 휴대폰(700) 결제 과정을 도시한 도면이다.
- [0586] 보다 상세하게 본 도면9는 소액결제 대상 웹사이트에 접속한 사용자 단말(705)로 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 및 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하기 위한 인터페이스가 제공되도록 처리한 후, 상기 도면4 내지 도면6에 도시된 과정을 통해 상기 OTP를 생성/인증하고, 상기 OTP 인증 결과에 따라 휴대폰(700) 결제를 처리하는 과정을 도시한 것으로서, 본 발명이 속한 기술분야에서 통상의 지식을 가진 자라면, 본 도면9를 참조 및/또는 변형하여 상기 OTP 검증정보를 이용한 휴대폰(700) 결제 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 도면9에 도시된 실시 방법만으로 그 기술적 특징이 한정되지 아니한다.
- [0588] 이하, 본 도면9에서 상기 도면7에 도시된 휴대폰(700) 결제 시스템을 편의상 "서버"라고 하고, 상기 도면2 또는 도면7에 도시된 OTP 인증요청 서버(715)를 편의상 "웹서버"라고 한다.
- [0590] 도면9를 참조하면, 사용자가 상기 웹서버에 접속하여 유형/무형의 재화를 구매하고, 상기 재화에 대한 구매대금에 대응하는 결제금액을 상기 사용자 휴대폰(700)에 부과되는 통신요금을 통해 결제하도록 휴대폰(700) 결제수단을 선택하면(900), 상기 서버는 상기 사용자 단말(705)이 접속한 통신망을 통해 상기 사용자 단말(705)로 직접, 또는 상기 웹서버를 중계하여 상기 사용자 단말(705)로 상기 사용자 휴대폰(700)에 대응하는 이동통신사 선택 및 사용자 휴대폰(700)번호와 사용자 주민등록번호 및 상기 도면1에 도시된 휴대폰(700)과 상기 도면2에 도시된 OTP 운영 시스템이 연계하여 생성한 OTP를 입력하기 위한 휴대폰(700) 결제 인터페이스가 제공되도록 처리한 후(905), 상기 도면4 내지 도면6에 도시된 과정을 통해 상기 도면1에 도시된 휴대폰(700)과 연계하여 상기 휴대폰(700) 결제를 인증하기 위한 OTP를 생성하여 상기 사용자 휴대폰(700)에 출력되도록 처리하고, 상기 사용자 단말(705)(또는 휴대폰(700))으로부터 상기 OTP를 수신하여 상기 휴대폰(700) 결제를 위한 OTP 유효성을 인증한다(910).
- [0592] 만약 상기 휴대폰(700) 결제를 위한 OTP 유효성이 인증되지 않으면(915), 상기 서버는 결제 오류 정보를 생성하여 상기 사용자 유선단말(또는 사용자 휴대폰(700))과 웹서버로 전송한다(920).
- [0594] 만약 상기 휴대폰(700) 결제를 위한 OTP 유효성이 인증되면(915), 상기 서버는 상기 결제 유효성 확인결과를 생성하여 상기 사용자 유선단말(또는 사용자 휴대폰(700))과 웹서버로 전송하고(925), 상기 결제 유효성 확인결과에 대응하여 상기 사용자 휴대폰(700)의 통신요금을 통한 결제승인을 처리한다(930).
- [0596] 본 발명의 실시 방법에 따르면, 상기 서버는 상기 웹서버로부터 상기 사용자 휴대폰(700) 통신요금에 부과될 결제금액을 확인하고, 상기 통신사 서버(710)와 연계하여 상기 사용자 휴대폰(700)번호에 대한 결제한도를 조회하고, 상기 결제금액과 상기 결제한도를 비교하여 상기 휴대폰(700)에 부과되는 통신요금을 통한 결제를 승인하는 것이 바람직하다.

부호의 설명

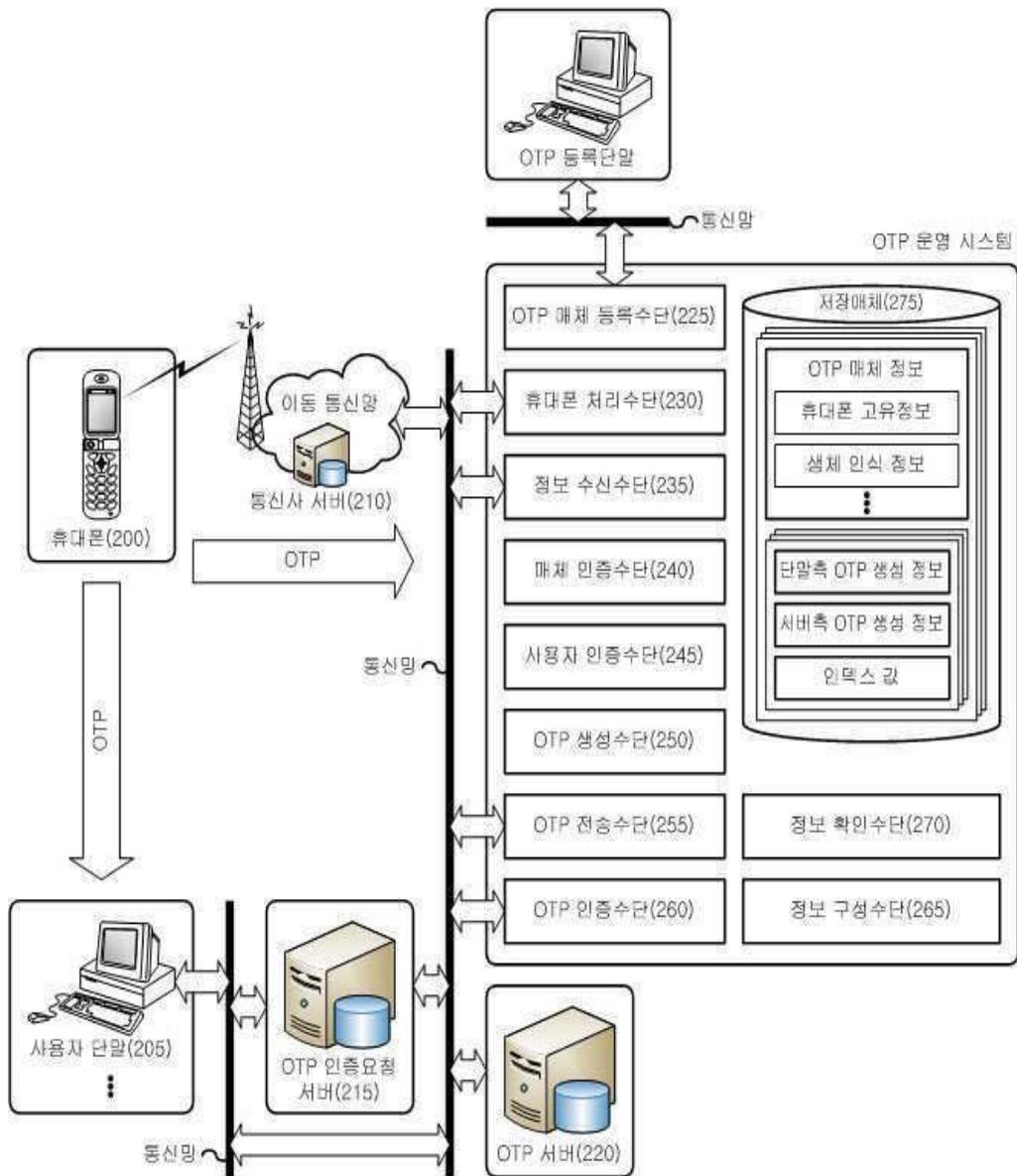
- [0598]
- |               |                 |
|---------------|-----------------|
| 100 : 휴대폰     | 105 : 제어부       |
| 110 : 화면 출력부  | 115 : 사운드 처리부   |
| 120 : 키 입력부   | 125 : 생체 인식부    |
| 130 : 배터리     | 135 : 무선 통신부    |
| 140 : USIM    | 145 : USIM 리더부  |
| 150 : 메모리부    | 155 : 생체 인식 처리부 |
| 160 : 사용자 인증부 | 165 : 인덱스 처리부   |
| 170 : 인증 처리부  | 175 : 정보 전송부    |
| 180 : 수신부     | 185 : OTP 출력부   |

도면

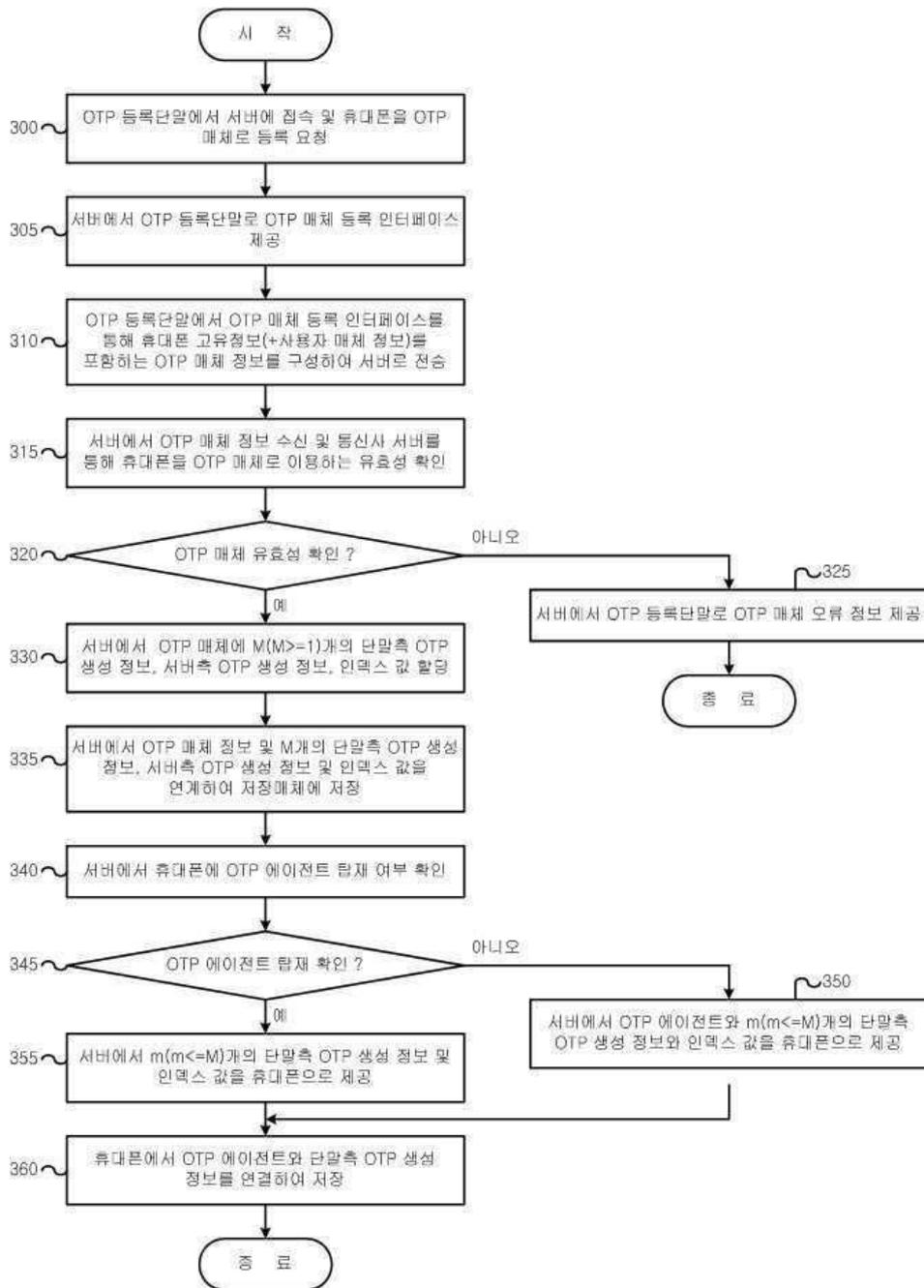
도면1



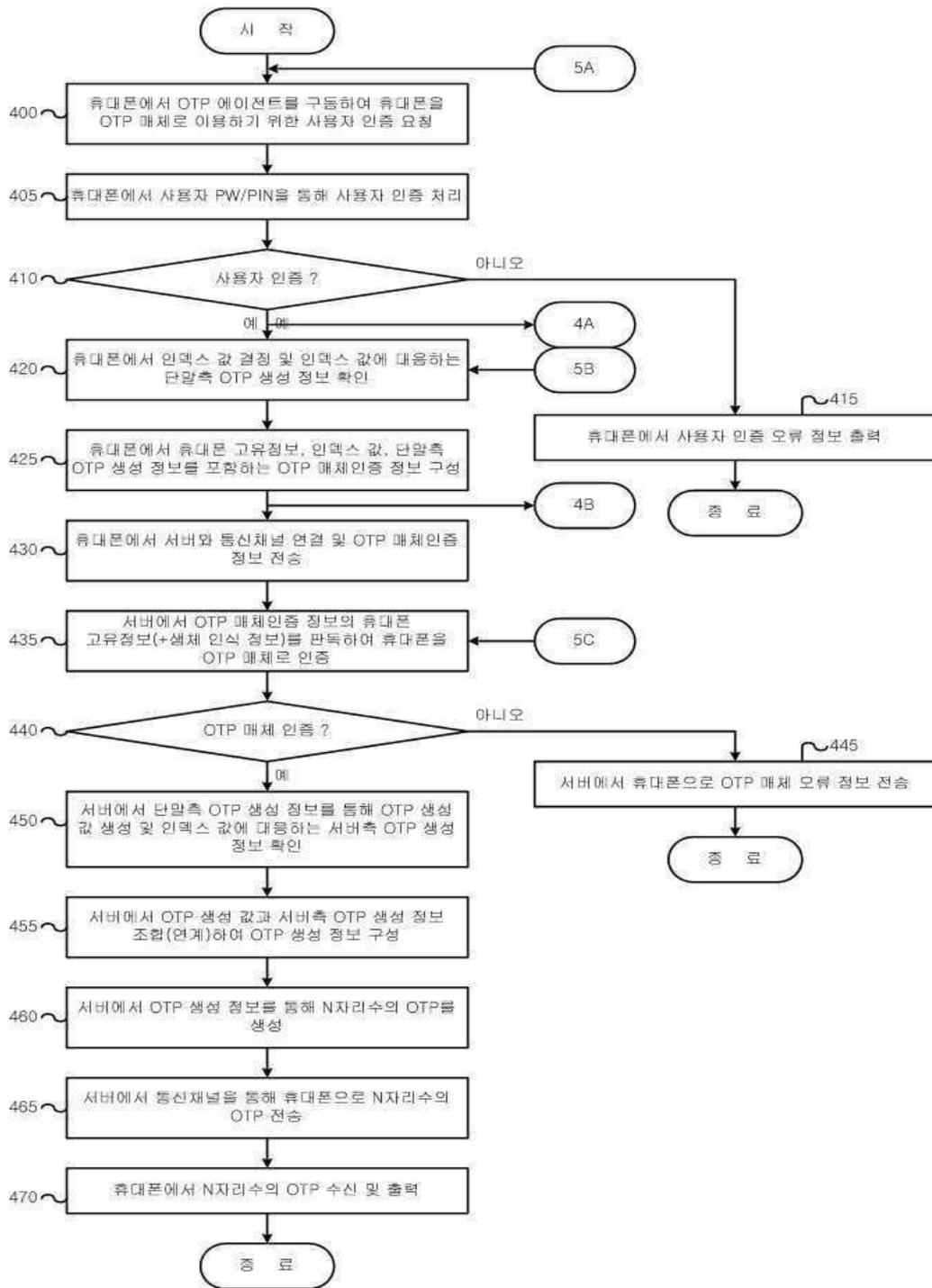
도면2



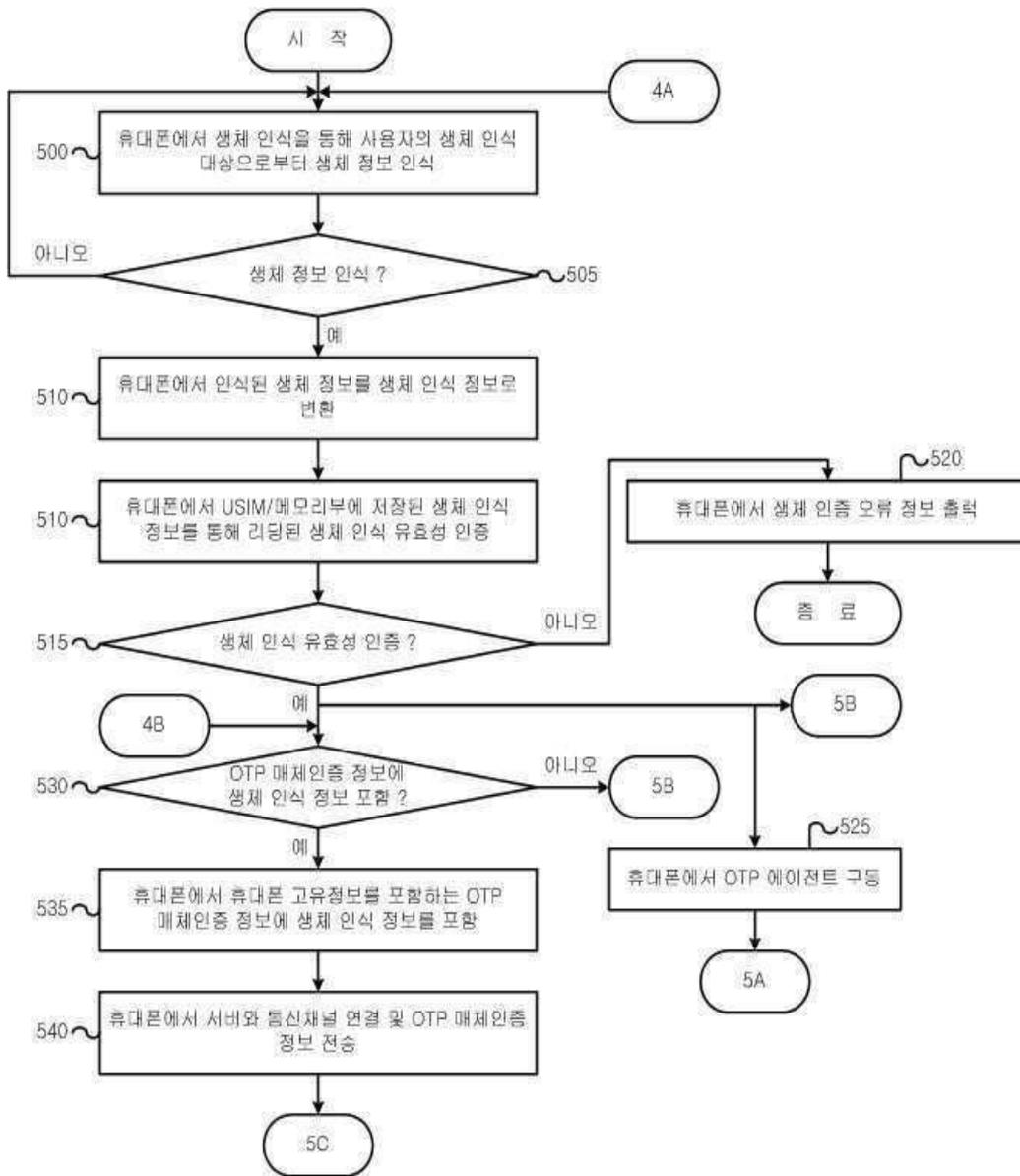
도면3



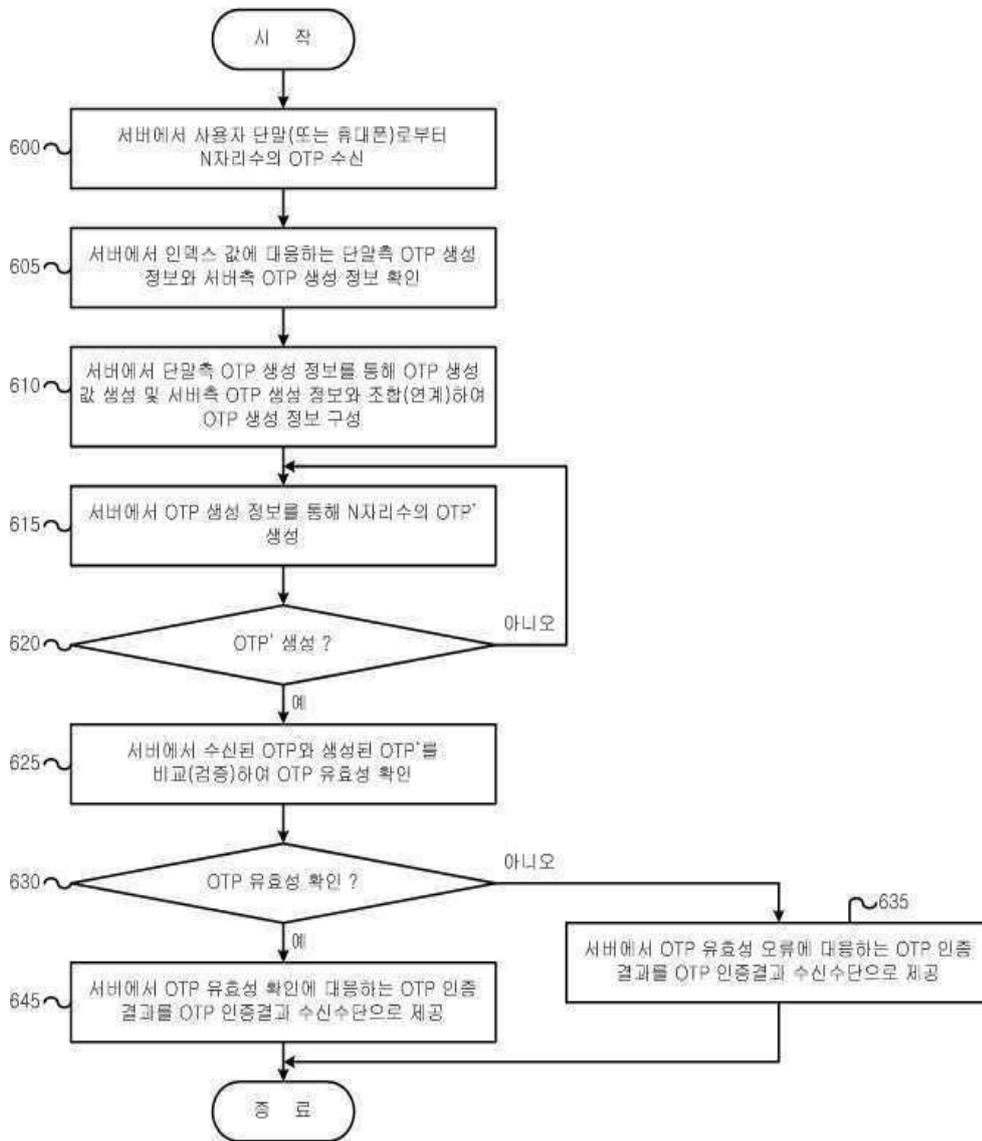
도면4



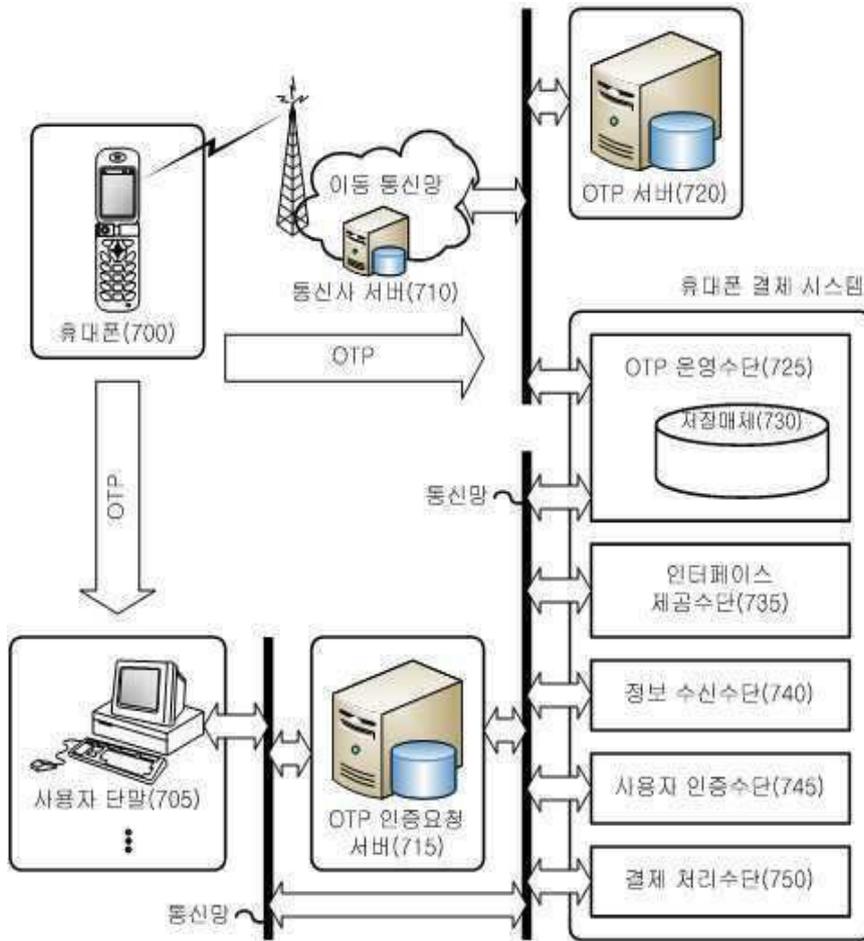
도면5



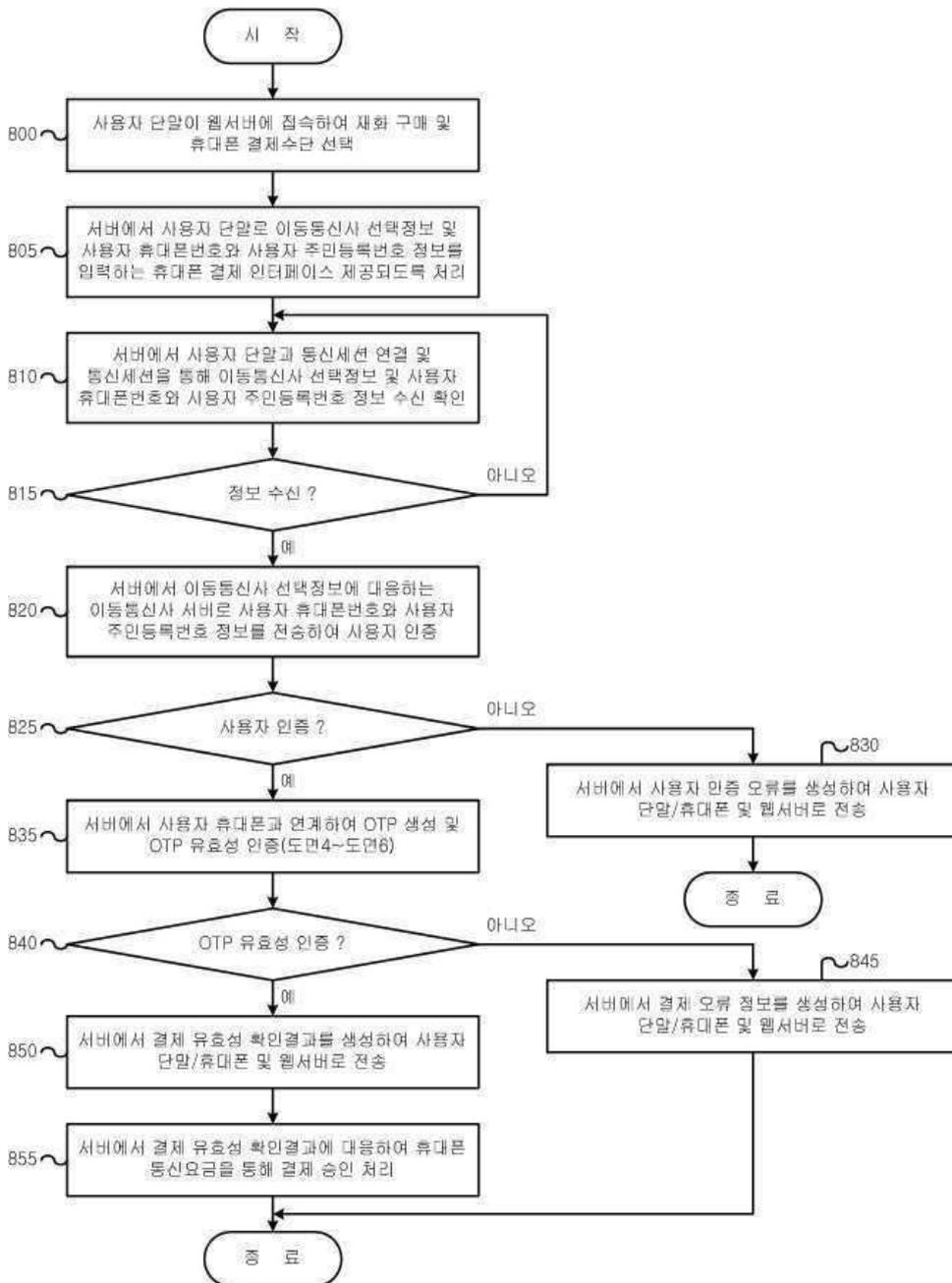
도면6



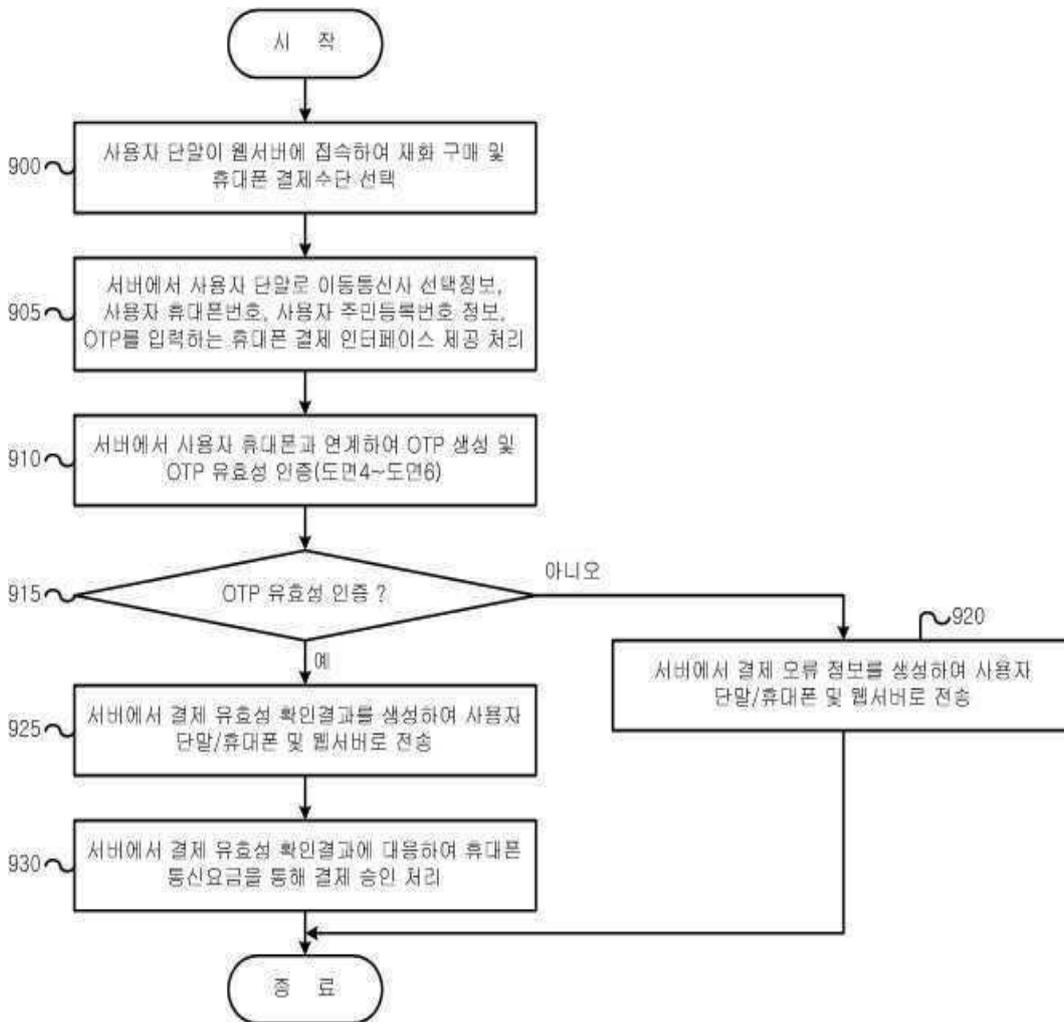
도면7



도면8



도면9



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 1

【변경전】

N(N≥2)자리수

【변경후】

N(N≥2)자릿수