(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년09월12일
(11) 등록번호 10-1657005
(24) 등록일자 2016년09월06일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *A61B 5/00* (2006.01)
A61B 5/0402 (2006.01) *A61B 5/117* (2016.01)
(52) CPC특허분류
H04L 9/3231 (2013.01)
A61B 5/0402 (2013.01)
(21) 출원번호 10-2015-0082898
(22) 출원일자 2015년06월11일
심사청구일자 2015년06월11일
(56) 선행기술조사문헌
KR1020130140439 A*
KR1020140105903 A*
KR1020150029105 A*
WO1999034554 A2*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
전문석
서울특별시 양천구 목동동로 350, 목동신시가지아파트 531-303 (목동)
(72) 발명자
전문석
서울특별시 양천구 목동동로 350, 목동신시가지아파트 531-303 (목동)
(74) 대리인
특허법인이룸리온, 특허법인리온

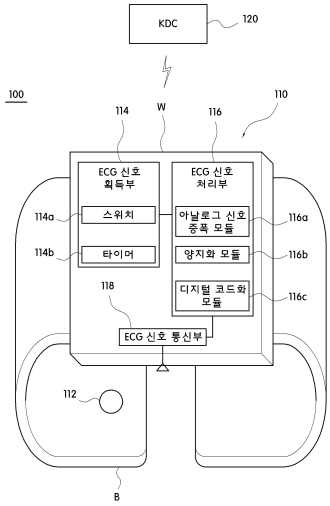
전체 청구항 수 : 총 2 항 심사관 : 양종필

(54) 발명의 명칭 **심전도 생체 인증 방법**

(57) 요 약

본 발명의 심전도 생체 인증 시스템은, 클라이언트 개인별로 고유 값을 가지는 생체 정보를 이용하여 생체 인증하는 생체 인증 시스템에 있어서, 하나 이상의 클라이언트 단말기, 및 상기 클라이언트 단말기의 심전도(electrocardiogram: ECG) 정보를 이용하여 전자 인증서를 발급하는 키 관리 센터를 포함한다. 이와 같은 발명의 구성에 의하면, 보안성이 강화된다.

대 표 도 - 도2



(52) CPC특허분류
A61B 5/117 (2013.01)
A61B 5/6831 (2013.01)
H04L 9/0819 (2013.01)
H04L 9/0825 (2013.01)

명 세 서

청구범위

청구항 1

삭제

청구항 2

삭제

청구항 3

삭제

청구항 4

삭제

청구항 5

삭제

청구항 6

삭제

청구항 7

삭제

청구항 8

삭제

청구항 9

삭제

청구항 10

클라이언트 단말기가 ECG를 이용하여 키 관리 센터(KDC)로부터 인증서를 발급받는 방법에 있어서,

상기 클라이언트 단말기는 상향 펄스 및 하향 펄스가 연속적인 곡선으로 표시되는 아날로그 ECG 파형 정보를 수집하는 단계;

상기 아날로그 ECG 파형 정보가 비연속적이고 유니크한 ECG 정보 값을 가지도록 양자화 하는 단계;

양자화를 통하여 유니크한 ECG 정보 값을 이진화 하여 바이너리 코드를 생성하는 단계;

상기 바이너리 코드를 개인키로 변경하여 암호화 하는 단계;

상기 클라이언트 단말기는 상기 암호화 결과를 상기 키 관리 센터로 전송하는 단계;

상기 키 관리 센터는 상기 암호화 결과를 R.S.A/E.C.C 알고리즘에 적용하여 공개키를 복구화 하는 단계;

상기 키 관리 센터는 상기 공개키를 상기 클라이언트 단말기로 전송하는 단계; 및

상기 클라이언트 단말기는 상기 공개키를 이용하여 인증을 실행하는 단계를 포함하여 구성됨을 특징으로 하는 심전도 생체 인증 방법.

청구항 11

삭제

청구항 12

제 10 항에 있어서,

상기 키 관리 센터는 암호화 결과를 복구화 하여 공개키를 생성함에 있어서, R.S.A/E.C.C 알고리즘을 이용하여, 심전도 생체 개인키 검증(Verification), 인증서(X.509 Certificate)를 발급하는 것을 특징으로 하는 심전도 생체 인증 방법.

발명의 설명

기 술 분 야

[0001] 본 발명은, ECG 생체 인증 단말기, 시스템, 및 방법에 관한 것으로, 더 구체적으로는 심장의 심방/심실에서 탈분극과 재분극이 이루어지면 몸에 흐르는 전류를 발생시키고, 이러한 전류의 변화를 측정하여 파형으로 표현한 아날로그 그래프는 오직 이미지를 통하여 그 유사도를 판단할 수 있기 때문에 처리 방법이 복잡하고 신뢰할 수 없지만, 이를 양자화 하여 디지털 바이너리 코드로 변환하게 되면, 그 유사도를 판단하기 매우 용이하고 신뢰성이 증진되며, 이로써 본 발명은 클라이언트 단말기를 클라이언트의 피부에 접촉하여 사용되는 스마트 워치(Smart Watch) 형태로 제공하고 ECG 정보를 추출함에 있어서 개인별로 유니크한 QRS 콤플렉스 정보를 디지털 코드로 변경하며, R.S.A/E.C.C 알고리즘을 이용하여 공개키와 개인키가 쌍을 구성하는 비대칭 암호 시스템의 개인키로 QRS 콤플렉스 디지털 ECG 정보를 활용하여 인증 절차를 실행하는 심전도 생체 인증 단말기, 이를 이용한 생체 인증 시스템, 및 그 방법에 관한 것이다.

배 경 기 술

[0002] 일반적으로 생체로부터 추출할 수 있는 다양한 신호나 데이터를 활용하여 이를 각종 시스템에서 이용하는 기술이 발전하고 있다. 가령, 생채 신호나 데이터를 이용하여 보안 시스템을 구축하는 생체 인증 기술이 최근 각광을 받고 있다.

[0003] 생체 인증 기술이란 사용자로부터 생체와 연관된 신호나 데이터를 추출하여 이를 기존에 저장된 데이터와 비교하고 본인임을 확인하여 사용자로 인증하는 기술을 말한다. 생체 인식 기술은 ID 카드나 비밀번호와는 달리 개인의 고유 생체 신호나 데이터를 이용하기 때문에 도난이나 분실의 염려가 없고 위조 또는 변조가 어렵기 때문에 보안 분야에서 각광을 받고 있다.

[0004] 또한 이러한 생체 인식 기술은 금융 서비스, 통신 서비스, 정보 보안, 의료, 치안 관리, 전자 상거래 등의 분야에서도 응용이 가능하다. 그리고 휴대용 단말기에서도 사용자를 인증하는 방법에는 비밀번호 입력이나 패턴 그리기 등이 있지만, 사용자 인증의 정확도를 높이기 위하여 최근 생체 인증 기술을 이용한 사용자 인증 방법이 개발되고 있는 실정이다.

[0005] 생체 인증 기술에서는 지문, 정맥, 홍채, 음성, 얼굴, 또는 손금 등이 보통 활용되고 있다. 특히 보안 시스템에 적용되고 있는 생체 인증 방법 중 가장 대중적인 방법은 지문 인식 기술이다. 지문은 평생 변하지 않는 특성을 갖고 있기 때문에 생체 인증 방법으로 오래전부터 사용되어 왔으나, 지문이 닳아지거나 건조할 때, 또는 이물질이 손에 묻은 경우 정확도가 떨어진다는 문제점이 있다.

[0006] 또한 생체 인증 기술로서 억양과 말하는 습관에 따른 음의 높낮이 정보를 이용한 음성 인식 기술이 있다. 음성 인식 기술을 통하면 원격지에서도 사용자 인증이 가능하고 사용방법에 대한 별도의 교육이 필요 없는 장점이 있으나, 감기 등의 요인으로 인하여 목이 쉬는 경우 인증이 어렵게 되는 단점이 있고 타인이 목소리를 흉내 내거나 주변 소음이 심한 경우 인식의 정확도가 떨어지게 되는 문제점도 있다.

[0007] 따라서 최근 상기와 같은 생체 인증 기술의 문제점들을 해결하고자 생체 신호 중에서 심전도(Electrocardiogram)를 이용하여 생체를 인식하는 기술이 개발되고 있다.

[0008] 도 1에는 통상의 심장박동과 그 결과로 발생하는 전기적 신호를 나타내는 심전도 아날로그 신호가 P, QRS, T, U

파형으로 표시되어 있다.

[0009] 심전도(ECG)란 심장에서 발생하는 전기적 신호를 기록한 것을 말한다. 심장 안에는 동방결절(Sinoauricular node)이라고 명명되는 부분이 있는데, 동방결절은 주기적으로 전기를 생성하여 심장 수축을 유도함으로써 심장 박동을 조절하는 심장의 특정 부분이다.

[0010] 동방결절로부터 만들어진 전기적 신호는 심장 내의 전기 전도 시스템을 따라 심장 전체에 전달된다. 이렇게 심장의 각 부위에 전달된 전기 신호에 의해 심장 근육을 이루는 세포가 수축하게 되고 이로 인해 심장이 뛰게 된다. 이때 심장에 전달된 전기적 신호를 피부에 부착한 전극을 통해 기록한 것을 심전도(ECG)라고 한다. 전극은 신체의 여러 부위에 부착하는데, 이를 통해 심장 각 부위의 전기적 현상을 잘 이해할 수 있다.

[0011] 이러한 심전도를 이용한 생체 인증 기술은 보안 기술에서 활용될 수 있다. 즉, 사용자로부터 심전도 신호를 추출하여, 추출된 심전도 신호를 기저장된 등록 사용자의 심전도 신호와 비교하여 사용자를 인증하는 기술로 활용할 수 있다. 그런데 이때 심전도 신호를 사용자 인증 및 보안 기술로서 활용하기 위해서는 우수한 인증의 정확도가 요구된다. 상기 인증의 정확도를 높이기 위해서는, 추출된 사용자의 심전도 신호와 기저장된 등록 사용자의 심전도 신호의 유사도를 결정하는 방법이 중요시된다. 즉, 심전도를 사용자 인증 기술로 이용하기 위해서는 상기 신호들의 유사도를 결정하는 방법의 정확도를 높일 필요성이 있다.

[0012] 종래에 아날로그 심전도 파형으로부터 이미지 패턴을 추출하여 패턴의 유사도를 대비하여 심전도를 인증 기술에 이용하기도 하였으나, 이미지 패턴을 대비하여 유사도를 판단하는 점에 오류가 빈번하여 신뢰할 수 없다.

[0013] 특히 이미지 패턴을 이용하여 생체 인증을 이용하는 경우 복제가 가능하여 안정성이 취약하다.

선행기술문헌

특허문헌

[0014] (특허문헌 0001) KR 공개번호: 10-2013-0140439

발명의 내용

해결하려는 과제

[0015] 따라서 본 발명은 상기한 바와 같은 종래 기술의 문제점을 해결하기 위하여 안출된 것으로, 심장은 수축할 때마다 미량의 활동 전류를 내보내며, 도 1에 도시된 바와 같이 이러한 심장 박동에 따라 발생하는 전기적 변화를 심전계를 이용하여 파형 곡선으로 신체 표면에서 기록하는 것이 심전도인데, 심전도 측정은 신체 표면을 통하여 간편하게 시행할 수 있고, 그 결과는 심장 활동에 대한 많은 정보와 함께 개인별로 고유성을 가지고 있기 때문에 본 발명의 목적은 클라이언트를 확인하는 생체 인증에 활용하는 심전도 생체 인증 단말기, 이를 이용한 생체 인증 시스템, 및 그 방법을 제공하는 것이다.

[0016] 본 발명의 다른 목적은, 클라이언트 신체 표면에 항상적으로 혹은 필요에 따라 접촉하여 사용되는 스마트 기기에 심전도 측정 및 처리 기술을 접목하여 클라이언트 본인을 실시간으로 확인할 수 있는 심전도 생체 인증 단말기, 이를 이용한 생체 인증 시스템, 및 그 방법을 제공하는 것이다.

[0017] 본 발명의 또 다른 목적은, R.S.A/E.C.C 알고리즘을 이용하여 공개키와 개인키가 페어(Pair)로 구성되는 비대칭 암호 시스템의 개인키로 클라이언트 심전도 정보를 활용하여 보안성을 강화하는 심전도 생체 인증 단말기, 이를 이용한 생체 인증 시스템, 및 그 방법을 제공하는 것이다.

과제의 해결 수단

[0018] 전술한 바와 같은 목적을 달성하기 위한 본 발명의 특징에 따르면, 본 발명의 심전도 생체 인증 시스템은, 클라이언트 개인별로 고유 값을 가지는 주기적인 생체 전압 정보를 이용하여 생체 인증하는 생체 인증 시스템에 있어서, 하나 이상의 클라이언트 단말기, 및 상기 클라이언트 단말기의 심전도(electrocardiogram: ECG) 정보를 이용하여 전자 인증서를 발급하는 키 관리 센터를 포함한다.

[0019] 본 발명의 다른 특징에 의하면, 본 발명의 심전도 생체 인증 단말기는, 클라이언트의 팔목을 감싸고, 상기 팔목 안쪽 피부와 접하는 하나 이상의 생체 전극이 탑재되며, 상기 생체 전극을 통하여 아날로그 심전도(ECG) 전기적

신호가 검출되는 스마트 밴드, 및 상기 생체 전극과 전기적으로 연결되어 상기 아날로그 ECG 신호를 수집하고 상기 아날로그 ECG 전기적 신호를 디지털 신호로 코드화 하는 스마트 워치를 포함한다.

[0020] 본 발명의 또 다른 특징에 의하면, 본 발명의 심전도 생체 인증 방법은, 클라이언트 단말기가 ECG를 이용하여 키 관리 센터(KDC)로부터 인증서를 발급받는 방법에 있어서, 상기 클라이언트 단말기는 상향 펄스 및 하향 펄스가 연속적인 곡선으로 표시되는 아날로그 ECG 파형 정보를 수집하는 단계, 상기 아날로그 ECG 파형 정보가 비연속적이고 유니크한 ECG 정보 값을 가지도록 양자화 하는 단계, 및 양자화를 통하여 유니크한 ECG 정보 값을 이진화 하여 바이너리 코드를 생성하는 단계를 포함한다.

발명의 효과

[0021] 위에서 설명한 바와 같이, 본 발명의 구성에 의하면 다음과 같은 효과를 기대할 수 있다.

[0022] 첫째, 심전도 생체 인증 단말기가 클라이언트 피부에 항상적으로 접촉하고 있어 실시간 인증에 편리하고, 클라이언트로부터 분리 시 인증이 원천적으로 불가능하여 보안성이 대폭 강화되는 작용 효과가 기대된다.

[0023] 둘째, 개인별로 고유성을 가지는 QRS 콤플렉스 정보를 양자화 과정을 통하여 양자화 디지털 코드로 처리하여 생성된 개인키를 공개키-개인키 조합을 이용하는 공개키 알고리즘에 적용함으로써 보안성이 한층 더 강화되는 작용 효과가 기대된다.

도면의 간단한 설명

[0024] 도 1은 종래 기술에 의한 ECG 아날로그 신호를 구성하는 P, QRS, T, U 파형을 나타내는 그래프 및 그 원인이 되는 심장도.

도 2는 본 발명에 의한 ECG 생체 인증 시스템의 구성을 나타내는 블록도.

도 3은 본 발명에 의한 생체 전극으로부터 특정 전압 파형의 아날로그 ECG 전기적 신호를 나타내는 그래프.

도 4는 본 발명에 의한 특정 전압 파형의 아날로그 ECG 전기적 신호를 양자화 하여 개인키 및 공동키를 생성하는 디지털 코드를 나타내는 개념도.

도 5는 본 발명에 의한 다양한 실시예에 의한 디지털 코드의 유형을 나타내는 개념도.

도 6은 본 발명에 의한 ECG 생체 인증을 나타내는 과정을 나타내는 순서도.

발명을 실시하기 위한 구체적인 내용

[0025] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해 질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려 주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 도면에서 층 및 영역들의 크기 및 상대적인 크기는 설명의 명료성을 위해 과장된 것일 수 있다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0026] 이하, 상기한 바와 같은 구성을 가지는 본 발명에 의한 심전도 생체 인증 시스템의 바람직한 실시예를 첨부된 도면을 참고하여 상세하게 설명한다.

[0027] 도 2에는 본 발명에 의해서 심전도 생체 인증 단말기가 키 관리 센터와 네트워크 연결되어 심전도 생체 인증하는 시스템의 구성이 블록도로 도시되어 있다.

[0028] 도 2를 참조하면, 본 발명의 심전도 생체 인증 시스템(100)은, 하나 이상의 클라이언트 단말기(110), 및 심전도 생체 정보를 이용하여 클라이언트의 생체 인증을 실시하는 키 관리 센터(120)를 포함한다. 본 발명은 여러 가지 생체 인증(뇌전도, 심전도, 근전도, 안전도 등)이 있지만, 그 중에서도 심장 박동 횟수에 따른 전기적 변화를 표시함으로써 일상에서도 용이하게 취득 가능하고 특히 복제가 어려운 심전도(electrocardiogram: ECG) 인증을 이용한다.

[0029] 클라이언트 단말기(110)는, ECG 측정 센서(112), ECG 신호 획득부(114), ECG 신호 처리부(116), 및 ECG 신호 통신부(118)를 포함한다.

[0030] ECG 측정 센서(112)는, 하나 이상의 생체 전극으로 구성된다. 생체 전극은, 클라이언트의 피부 자극 없이 장시

간 사용 가능한 스냅 전극으로 구성될 수 있다.

[0031] ECG 신호 획득부(114)는, ECG 측정 센서(112)와 유선으로 연결되어 생체 전극으로부터 ECG 신호를 수집하고 처리한다. ECG 신호 획득부(114)에서 수집되는 ECG 신호는 아날로그 전기적 신호이다. 도 2에 도시된 바와 같이 생체 전극으로부터 특정 전압 파형의 아날로그 전기적 신호가 제공된다.

[0032] ECG 신호 획득부(114)는, ECG 신호를 측정하여 생체 인증에 필요한 디지털 코드로 전환할 필요성이 있다고 판단할 때 실시간으로 측정 시점을 결정하는 스위치(114a)를 포함할 수 있다. 혹은 주기적으로 측정이 필요할 때 측정 주기를 결정할 수 있는 타이머(114b)를 포함할 수 있다.

[0033] 가령, ECG 측정은 휴식 상태에서 실시하는 것과 운동 후에 실시하는 것, 누워서 측정하는 것과 앉아서 측정하는 것, 혹은 식사/음료 전에 측정하는 것과 식사/음료 후에 측정하는 것에 약간의 차이가 발생할 수 있다. 이에 스위치(114a) 혹은 타이머(114b)를 이용하여 적절한 측정 시점을 선택하거나 혹은 일정한 시간 혹은 반복 측정을 통하여 획득된 정보의 평균값을 이용하여 생체 인증을 실시하여 인증 에러를 방지할 수 있다.

[0034] ECG 신호 처리부(116)는 연속적인 시간 축 상에 연속적으로 변화하는 진폭(전압 레벨)을 가지는 아날로그 전기적 신호를 소정 단위로 정수배로 변화하는 비연속적인 디지털 신호(코드)로 변환하는 기능을 수행한다.

[0035] 이를 위하여, ECG 신호 처리부(116)는 아날로드 신호 증폭 모듈(116a)을 통하여 1차적으로 아날로그 전기적 신호의 크기를 증폭한다. 양자화 모듈(116b)을 통하여 도 4에 도시된 바와 같이 특정 파형의 아날로그 전기적 신호를 양자화 한다. 이와 같이 연속적인 아날로그 전기적 신호는 일정한 전압 레벨을 기준으로 양자화(Quantization) 되어 P(+0.37100), Q(-0.22010), R(+0.98010), S(-0.41010), T(+0.28100), QRS(+0.34990) 등으로 표시될 수 있다. 이때 QRS = (Q + R + S)로 표시된다. 디질털 코드화 모듈(116c)을 통하여 양자화 결과는 "1(혹은 high)", "0(혹은 middle)" 과 "-1(혹은 low)"만으로 이루어지는 소수 5자리, 양자화 디지털 코드(Quantum Code)로 출력될 수 있다.

[0036] 심장(도 1 참조)은 2심방과 2심실로 되어 있다. 심장은 음식물에서 얻은 에너지로 일정 주기마다 미세 전기를 발생시켜, P, QRS, T 순서대로 박동된다. 이와 같이, 심장은 소정 심박에서 다음 심박까지 심장 주기를 갖게 되는데, 이러한 심장 주기는 심방 수축기, 심실 수축기, 및 심방/심실 이완기로 구분된다. 심방 수축기에서 좌심방 및 우심방이 수축하고, 좌심실 및 우심실이 이완되며, 심실 수축기에서 좌심방 및 우심방이 이완되고, 좌심실 및 우심실이 수축되고, 심방/심실 이완기에서 좌우 심방 및 좌우 심실이 모두 이완된다.

[0037] 다시 도 3 참조하면, ECG는 심장 수축에 따른 활동 전류 및 활동 전위차를 파상 곡선으로 기록한 파형(wave frequence)으로 표현된다. 이러한 ECG 파형은 상향 펄스와 하향 펄스가 교대로 반복하는데, 이들 펄스는 순서대로 P 웨이브, Q 웨이브, R 웨이브, S 웨이브, 및 T 웨이브라고 명명하기고 한다.

[0038] 여기서 도 3의 P 웨이브는 좌우 심방의 수축 과정을 기록한 파형이고, QRS 콤플렉스는 좌우 심실의 수축 과정을 기록한 파형이며, T 웨이브는 좌우 심실이 이완되는 과정을 기록한 파형으로서, P 웨이브는 심방의 탈분극 시기에 발생하고, QRS 콤플렉스는 심실 탈분극 시기에 발생하며, T 웨이브는 심실 재분극 시기에 발생한다.

[0039] 이러한 심장의 심방 및 심실 탈분극과 심실 재분극은 클라이언트의 피부 표면에서 측정될 수 있다. 따라서 본 발명은 심전도 측정 센서(112)를 이용하여 이와 같은 탈분극과 재분극의 영향을 클라이언트 단말기(110)를 이용하여 측정하고자 한다.

[0040] 다시 도 4를 참조하면, 이러한 아날로그 ECG 파형은 양자화 과정을 거쳐 바이너리 디지털 코드로 변경된다. ECG 디지털 정보는, P 웨이브 정보(32비트), Q 웨이브 정보(32비트), R 웨이브 정보(32비트), S 웨이브 정보(32비트), T 웨이브 정보(32비트), QRS 콤플렉스 정보(32비트), PIN 정보(64비트)의 양자화 디지털 코드로 구성되어 256비트 정보를 표현할 수 있다.

[0041] 가령, ECG 파상 곡선으로부터 상향 펄스에서 하향 펄스(혹은 하향 펄스에서 상향 펄스)로 변경되는 변곡점에서 P 웨이브, Q 웨이브, R 웨이브, S 웨이브, T 웨이브, 및 QRS 콤플렉스를 각각 검출하고 그 변곡점(특징점)을 추출하여 양자화 한 결과, P 웨이브 정보 값은 “+0.37100”, Q 웨이브 정보 값은 “-0.22010”, R 웨이브 정보 값은 “+0.98010”, S 웨이브 정보 값은 “-0.41010”, T 웨이브 정보 값은 “+0.28100”, QRS 콤플렉스 정보 값은 “+0.34990”로 표시되는 것을 알 수 있다. 가령, 도 2와 같이 그리드 박스(Grid Box)를 이용하여 각 펄스 값을 양자화 할 수 있다.

[0042] 또 다른 경우로, 도 5에 도시된 바와 같이, P 웨이브, Q 웨이브, R 웨이브, S 웨이브, T 웨이브, 및 QRS 콤플렉스 말고도 U 웨이브를 더 포함할 수 있다. 다만, U 웨이브는 QRS 콤플렉스 파형과 비교하여 상향 펄스 및 하향

펄스가 명확하고 규칙적이지 않은 단점이 있다. 따라서 도 5를 계속해서 참조하면, U 웨이브와 QRS 콤플렉스를 모두 사용할 수 있다.

[0043] 이와 같은 ECG 아날로그 파형으로부터 추출되는 양자화 디지털 코드의 정보 값은 클라이언트 개인별로 유니크한 값을 가지게 되며, 상기 유니크한 값은 본 발명의 생체 인증을 위한 정보로 이용될 수 있다.

[0044] ECG 신호 통신부(118)는 이동 통신망(Network)을 통한 통신이나 근거리 무선 통신 등 다양한 통신 기능을 가지고 있어 무선 데이터 통신이 가능한 블루투스 모듈, 적외선 통신 모듈, 지그비 모듈 등 무선 통신 모듈을 구비한 키 관리 센터(120)와 실시간 통신할 수 있다.

[0045] 다시 도 2를 참조하면, 본 발명의 클라이언트 단말기(110)는 스마트 워치(Smart Watch)를 이용할 수 있다. 즉, 클라이언트 단말기(110)는, 스마트 워치(W), 스마트 워치(W)를 팔목에 고정하는 스마트 밴드(B)를 포함한다. ECG 측정 센서(112) 즉, 생체 전극은 팔목 안쪽의 피부와 접촉하는 스마트 밴드(B)에 설치될 수 있다. 스마트 밴드(B)는 유연하고 수축 가능한 폐쇄 링 타입일 수 있다. 스마트 밴드(B)는 하드하고 탄성을 가지는 개방 링 타입일 수 있다. 혹은 선택적으로 개방 혹은 폐쇄할 수 있는 체결 타입일 수 있다.

[0046] 스마트 워치(W)는 스마트폰(smart phone), PDA(personal digital assistant), 핸드 헬드(handheld) PC, 핸드폰, 홈 서버 PC 등이 사용될 수 있다.

[0047] 스마트 밴드(B)는 심장의 탈분극와 재분극의 영향을 가장 효과적으로 검출할 수 있는 피부에 잘 접촉할 수 있도록 패치 형태로 제공될 수 있다. 스마트 밴드(B)는 클라이언트의 팔목을 감싸며 생체 전극은 팔목 안쪽에 대응되도록 한다.

[0048] 따라서 클라이언트 단말기(110) 구성 중 ECG 측정 센서(112)는 스마트 밴드(B)에 탑재되고, ECG 신호를 수집하고 처리하며 통신하는 ECG 신호 획득부(114), ECG 신호 처리부(116), 및 ECG 신호 통신부(118)는 스마트 워치(W)에 각각 탑재되며, ECG 측정 센서(112)와 ECG 신호 획득부(114)는 스마트 밴드(B)를 통해 유무선으로 상호 통신할 수 있다.

[0049] 계속해서 도 4를 참조하면, 본 발명은 위와 같은 방법을 통하여 확정된 양자화 디지털 코드를 개인키(Private Key)의 암호화에 활용할 수 있다.

[0050] 본 발명은 데이터를 암호화하는데 있어서 특정 알고리즘을 사용한다. 여기서 데이터 암호화란 특정 알고리즘을 사용하여 데이터를 변형함으로써 데이터의 암호화는 권한 없는 자가 데이터로 접근하는 것을 막는 일종의 자물쇠이다. 이때, 사용되는 특정 알고리즘은 자물쇠를 잠그는 키(Key) 역할을 하게 된다.

[0051] 반대로, 전술한 암호화 데이터를 재생하기 위해서는, 상기 암호화에 사용된 특정 알고리즘을 해독할 수 있는 수단이 제공되어야 한다. 특정 알고리즘 해독 수단은 자물쇠를 여는 일종의 키(Key) 역할을 하게 된다. 즉, 키(Key)가 제공되면, 상기 키를 사용하여 데이터 암호화에 사용된 알고리즘을 해독하고, 상기 데이터를 원래 형태로 복구화(Decryption) 할 수 있다. 따라서 데이터 암호화 및 복호화에 사용되는 상기한 알고리즘을 키(Key)라 한다.

[0052] 본 발명은 암호화할 때 사용하는 키와 복호화할 때 사용하는 키가 다른 암호화 기법인 비대칭 암호 시스템(Asymmetric Cryptographic System)을 사용한다. 이러한 비대칭 암호 시스템은 암호화할 때 사용하는 키와 복구화할 때 사용하는 키가 다른 암호화 기법으로서, 공개키 암호 체계라 불리기도 한다.

[0053] 가령, 비대칭 암호 시스템은 일반적으로 공개키 기반 구조(Public Key Infrastructure; PKI)인 것을 특징으로 한다. 두 개의 큰 소수(보통 140자리 이상 수)의 곱과 추가연산을 통하여 공개키와 개인키를 구성하고, 전자 인증서(digital certificate)를 통해 사용자를 인증(authentication)한다.

[0054] 이하, 클라이언트 단말기가 ECG를 이용하여 키 관리 센터(KDC)로부터 인증서를 발급받는 과정을 도면을 참조하여 설명한다.

[0055] 도 6을 참조하면, 상/하향 펄스가 연속적인 곡선으로 표시되는 아날로그 ECG 파형 정보를 양자화 한다. 양자화되어 비연속적인 ECG 정보 값은 유니크한 값을 가지게 된다.

[0056] 양자화를 통하여 유니크하게 된 ECG 각 파형 정보 값을 이용하여 256비트의 개인키를 생성한다. 이 정도의 개인키는 모든 동물를 유니크한 키로 사용할 수 있는 충분한 숫자이다.

[0057] 개인키와 공개키로 구성되는 키 쌍을 생성하여 암호화한다. 암호화 결과를 키 관리 센터(120)로 전송한다.

[0058] 키 관리 센터(120)는 암호화 결과를 복구화하여 공개키를 생성한다. 이때, R.S.A/E.C.C 알고리즘을 이용하여 인증서를 발급한다. 여기서 R.S.A/E.C.C 알고리즘을 이용하여 공개키를 제공함으로써 PKI 인증을 실시한다.

[0059] 클라이언트 단말기(110)는 인증서를 전송받아 인증 절차에 이용한다. 이와 같이 인증서는 특정 클라이언트 단말기(110)가 해당 공개키를 소유하고 있음을 입증하는 전자 문서이다.

[0060] 한편, 클라이언트 단말기(110)가 키 관리 센터(120)로부터 전술한 전자 인증서 발급 절차를 통하여 인증을 완료한 후에 전자 인증서를 갱신할 필요성이 있을 때 인증 절차를 새롭게 시작할 수 있다. 이때 타이머(114b)를 통하여 1시간을 설정하고, 그 시점에서 클라이언트 단말기(110)로부터 ECG 정보에 기초하여 개인키가 키 관리 센터(120)에 수신되지 않으면, 인증 절차를 모두 취소하고 원점에서 인증 절차를 새롭게 실시하도록 하여 보안성을 한 층 강화할 수 있다.

[0061] 본 발명의 ECG 생체 인증 단말기는 스마트 워치 형태로 제공하되, 특정 범죄자에게 24시간 착용하여 감시하는 전자 팔찌에 적용될 수 있다. 범죄자 개인의 ECG 정보가 실시간 혹은 주기적으로 키 관리 센터에 전송됨으로써, 전자 팔찌의 착용 상태를 원격에서 확인할 수 있다.

[0062] 이상에서 살펴본 바와 같이, 본 발명은 심전도 생체 인증 단말기를 스마트 워치 형태로 제공함으로써, 클라이언트의 팔목에 항상적으로 접촉하는 밴드에 심박을 측정하는 생체 전극을 설치할 수 있고, 아날로그 ECG 파형을 양자화 하여 디지털 코드로 변환 처리하는 기능을 스마트 기기 본체에 구비함으로써 스마트 기기의 본래 기능과 함께 스마트 기기를 이용하여 처리하는 모바일 뱅킹 기타 결제 시 인증에 그대로 활용할 수 있으며, ECG 파형을 처리하여 획득된 디지털 코드를 R.S.A/E.C.C 알고리즘에 활용하여 보안성이 강화되는 구성을 기술적 사상으로 하고 있음을 알 수 있다. 이와 같은 본 발명의 기본적인 기술적 사상의 범주 내에서, 당업계의 통상의 지식을 가진 자에게 있어서는 다른 많은 변형이 가능할 것이다.

부호의 설명

[0063]

100: ECG 생체 인증 시스템 110: ECG 생체 인증 단말기

112: ECG 측정 센서 114: ECG 신호 획득부

114a: 스위치 114b: 타이머

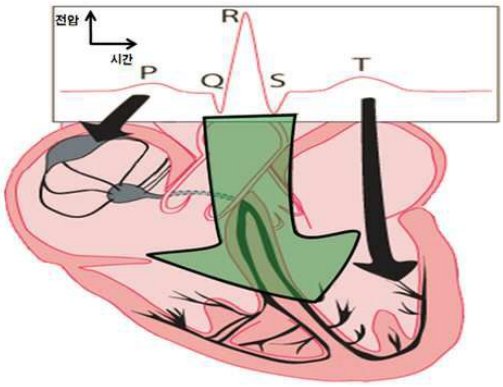
116: ECG 신호 처리부 116a: 아날로그 신호 증폭 모듈

116b: 양자화 모듈 116c: 디지털 코드화 모듈

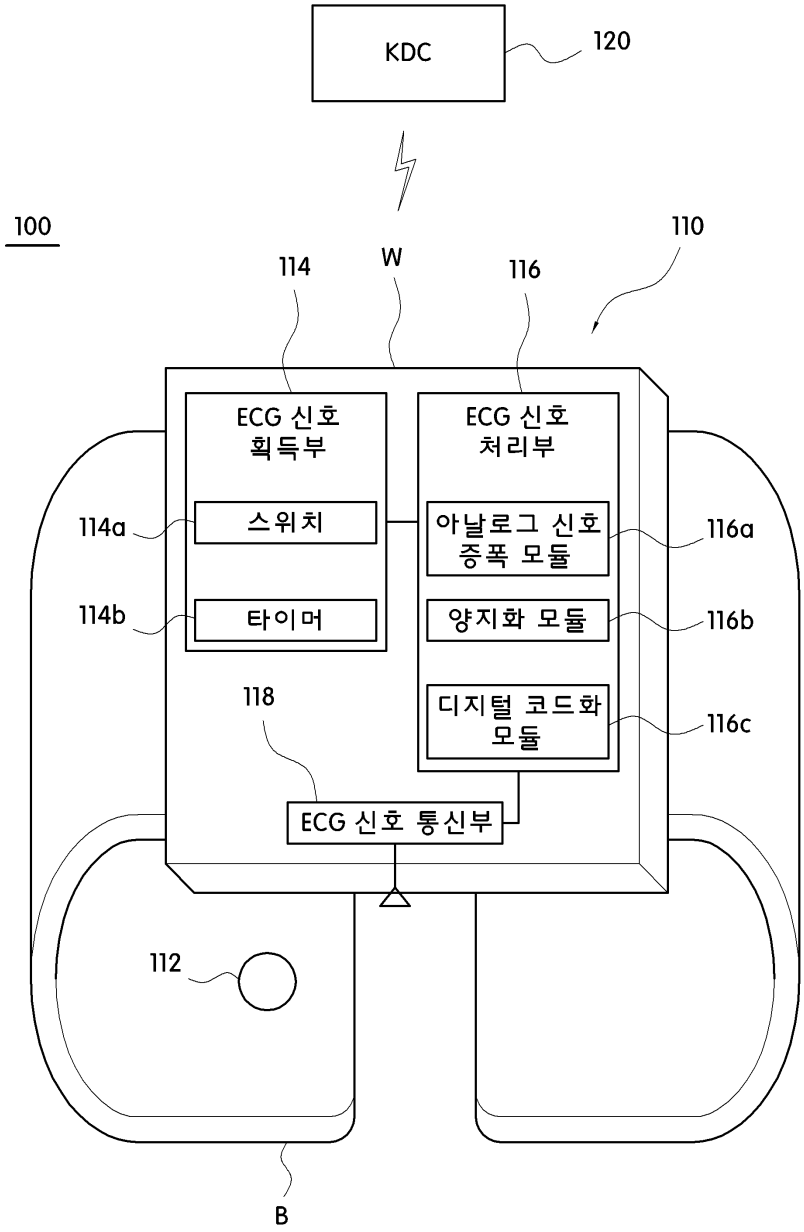
120: 키 관리 센터

도면

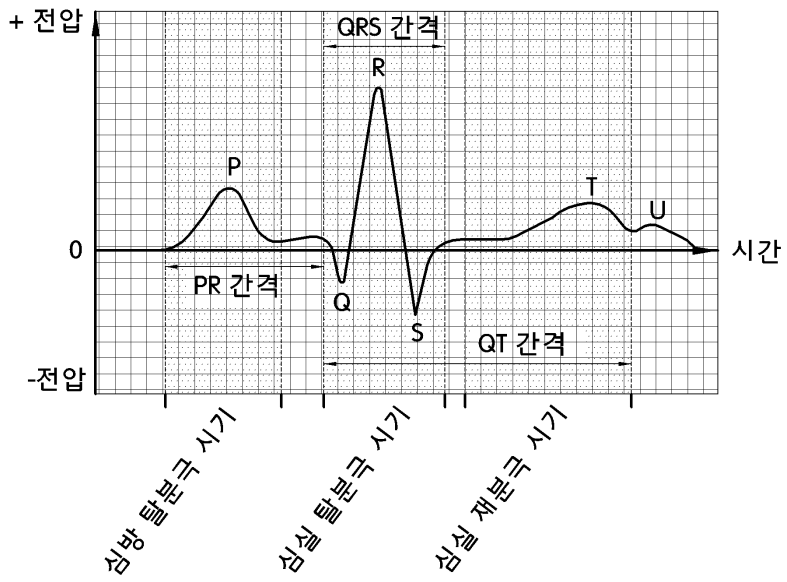
도면1



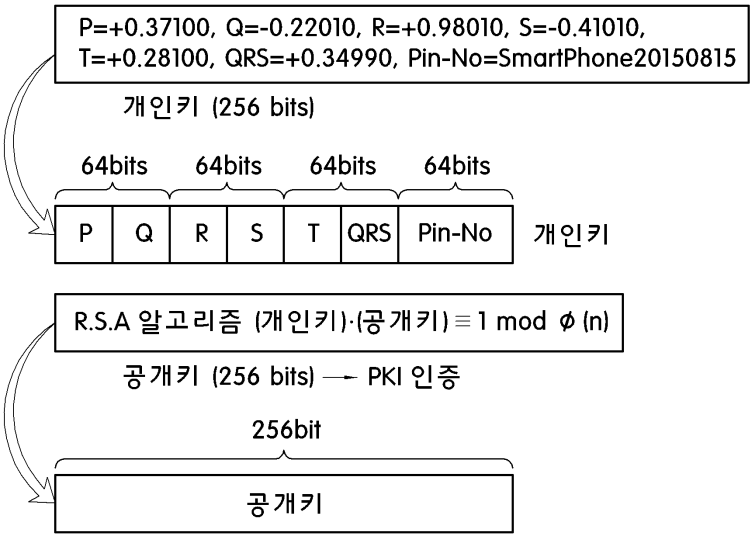
도면2


KDC
120
100
110
114
W
116
ECG 신호
획득부
ECG 신호
처리부
114a
스위치
아날로그 신호
증폭 모듈
116a
114b
타이머
양지화 모듈
116b
118
디지털 코드화
모듈
116c
ECG 신호 통신부
112
B

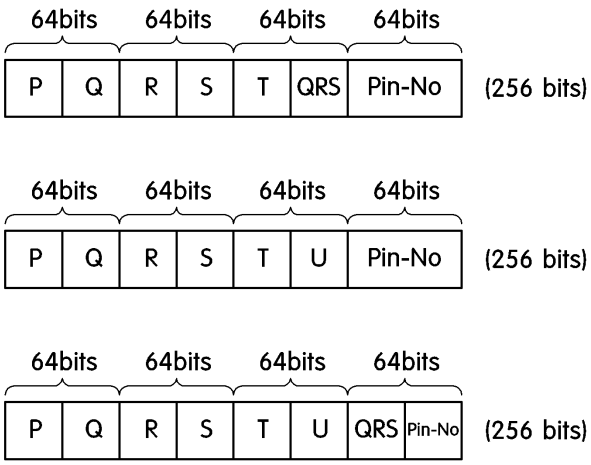
도면3


+ 전압
QRS 간격
R
P
T
U
0
시간
PR 간격
Q
S
QT 간격
-전압
심방 탈분극 시기
심실 탈분극 시기
심실 재분극 시기

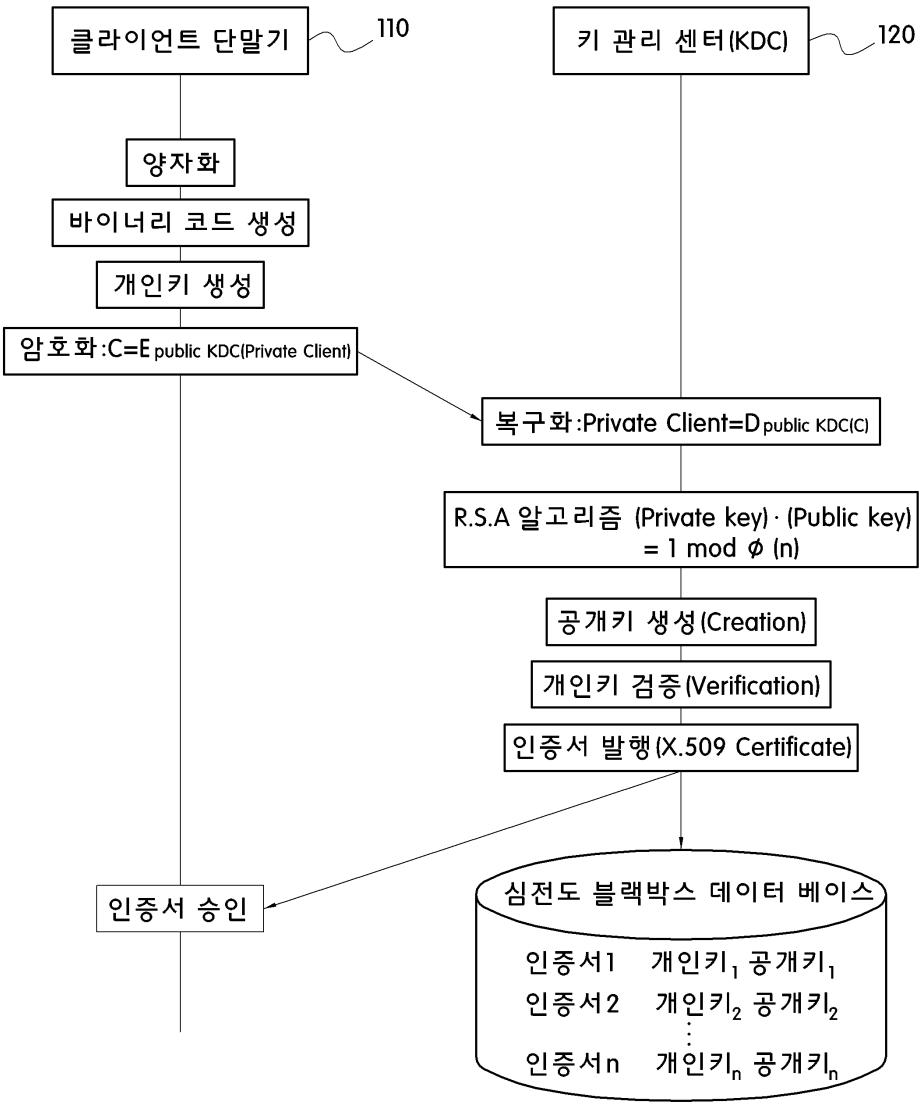
도면4


P=+0.37100, Q=-0.22010, R=+0.98010, S=-0.41010,
T=+0.28100, QRS=+0.34990, Pin-No=SmartPhone20150815
개인키 (256 bits)
64bits
64bits
64bits
64bits
P
Q
R
S
T
QRS
Pin-No
개인키
R.S.A 알고리즘 (개인키)·(공개키) ≡ 1 mod ϕ (n)
공개키 (256 bits) → PKI 인증
256bit
공개키

도면5


64bits
64bits
64bits
64bits
P
Q
R
S
T
QRS
Pin-No
(256 bits)
64bits
64bits
64bits
64bits
P
Q
R
S
T
U
Pin-No
(256 bits)
64bits
64bits
64bits
64bits
P
Q
R
S
T
U
QRS
Pin-No
(256 bits)

도면6


클라이언트 단말기
110
키 관리 센터(KDC)
120
양자화
바이너리 코드 생성
개인키 생성
암호화:C=E public KDC(Private Client)
복구화:Private Client=D public KDC(C)
R.S.A 알고리즘 (Private key) · (Public key)
= 1 mod ϕ (n)
공개키 생성(Creation)
개인키 검증(Verification)
인증서 발행(X.509 Certificate)
인증서 승인
심전도 블랙박스 데이터 베이스
인증서1 개인키1 공개키1
인증서2 개인키2 공개키2
인증서n 개인키n 공개키n

专利名称(译)	发明名称心电图生物特征认证方法		
公开(公告)号	KR101657005B1	公开(公告)日	2016-09-12
申请号	KR1020150082898	申请日	2015-06-11
[标]申请(专利权)人(译)	JUN MOON SEOG Jeonmunseok		
申请(专利权)人(译)	Jeonmunseok		
当前申请(专利权)人(译)	Jeonmunseok		
[标]发明人	JUN MOON SEOG 전문석		
发明人	전문석		
IPC分类号	H04L9/32 A61B5/00 A61B5/0402 A61B5/117		
CPC分类号	H04L9/3231 A61B5/117 A61B5/0402 A61B5/6831 H04L9/0819 H04L9/0825 A61B5/04012 A61B5/04085 A61B5/04525 A61B5/0456 A61B5/681		
代理人(译)	专利法的人		
外部链接	Espacenet		

摘要(译)

本发明的心电图生物特征认证系统是用于生物特征认证的生物特征认证系统，其使用对于每个个体客户具有唯一值的生物特征信息，该生物特征认证系统包括至少一个客户端和心电图（ECG）。并且是发布电子证书的关键管理中心。根据本发明的配置，增强了安全性。