(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
A61B 5/00 (2006.01)

(45) 공고일자 2007년02월07일
(11) 등록번호 10-0679762
(24) 등록일자 2007년01월31일

(21) 출원번호	10-2002-7004038	(65) 공개번호	10-2002-0064292
(22) 출원일자	2002년03월28일	(43) 공개일자	2002년08월07일
심사청구일자	2002년12월31일		
번역문 제출일자	2002년03월28일		
(86) 국제출원번호	PCT/US2000/027017	(87) 국제공개번호	WO 2001/22873
국제출원일자	2000년09월28일	국제공개일자	2001년04월05일

(81) 지정국

국내특허 : 알바니아, 아르메니아, 오스트리아, 오스트레일리아, 아제르바이잔, 보스니아 헤르체고비나, 바베이도스, 불가리아, 브라질, 벨라루스, 캐나다, 스위스, 중국, 쿠바, 체코, 독일, 덴마크, 에스토니아, 스페인, 핀란드, 영국, 그루지야, 헝가리, 이스라엘, 아이슬랜드, 일본, 케냐, 키르키즈스탐, 북한, 대한민국, 카자흐스탄, 세인트루시아, 스리랑카, 리베이라, 레소토, 리투아니아, 룩셈부르크, 라트비아, 몰도바, 마다가스카르, 마케도니아공화국, 몽고, 말라위, 멕시코, 노르웨이, 뉴질랜드, 슬로베니아, 슬로바키아, 타지키스탄, 투르크맨, 터어키, 트리니아드토바고, 우크라이나, 우간다, 미국, 우즈베키스탄, 베트남, 폴란드, 포르투칼, 루마니아, 러시아, 수단, 스웨덴, 싱가포르, 아랍에미리트, 안티구와바부다, 코스타리카, 도미니카, 알제리, 모로코, 탄자니아, 남아프리카, 벨리제, 모잠비크, 그라나다, 가나, 감비아, 크로아티아, 인도네시아, 인도, 시에라리온, 세르비아 앤 몬테네그로, 짐바브웨,

AP ARIPO특허 : 케냐, 레소토, 말라위, 수단, 스와질랜드, 우간다, 시에라리온, 가나, 감비아, 짐바브웨, 모잠비크, 탄자니아,

EA 유라시아특허 : 아르메니아, 아제르바이잔, 벨라루스, 키르키즈스탐, 카자흐스탄, 몰도바, 러시아, 타지키스탄, 투르크맨,

EP 유럽특허 : 오스트리아, 벨기에, 스위스, 독일, 덴마크, 스페인, 프랑스, 영국, 그리스, 아일랜드, 이탈리아, 룩셈부르크, 모나코, 네덜란드, 포르투칼, 스웨덴, 핀란드, 사이프러스,

OA OAPI특허 : 부르키나파소, 베닌, 중앙아프리카, 콩고, 코트디브와르, 카메룬, 가봉, 기니, 말리, 모리타니, 니제르, 세네갈, 차드, 토고, 기니 비사우,

(30) 우선권주장

60/156,488	1999년09월28일	미국(US)
09/662,246	2000년09월14일	미국(US)

(73) 특허권자

맬린크로트 인코포레이티드
미국 미주리 헤이즐우드 맥도넬 불바드 675(우:63042)

(72) 발명자

버슨,토마스,에이.
미국94301캘리포니아팔로알토포레스트애브뉴764

올슨,브라이언
미국94087캘리포니아써니베일이.레밍턴드라이브#에프-155400

페인,마이클,이.

미국94040캘리포니아마운틴뷰홀링스워쓰드라이브1613

맨하이머,폴,디.
미국94506캘리포니아댄빌슈가메이플드라이브4119

포제스,찰스,이.
미국94563캘리포니아오린다미라로마61

쉬로머,데이비드
미국66085캔자스스티웰디어본드라이브16301

(74) 대리인 남상선

심사관 : 최남호

전체 청구항 수 : 총 21 항

(54) 센서와 관련된 데이타의 디지털 서명을 가진 센서

(57) 요약

센서는 정확성이 인증될 수 있는 모니터에 대해 유용한 코드를 갖는다. 상기 센서는 계측된 생리적 특성에 대응하는 신호를 생산하고 모니터에 의해 사용될 때 정확성과 확실성이 보장될 수 있는 코드를 제공한다. 상기 센서와 관련된 메모리는 센서에 관한 데이타와 디지털 서명 둘 다를 저장한다. 상기 디지털 서명은 그것이 예정된 품질 제어를 갖는 실체에 의해 생성되었음을 보증함에 의해 상기 코드의 품질을 인증하고, 상기 코드가 정확하다는 것을 보증한다.

대표도

도 4

특허청구의 범위

청구항 1.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 맥박 산소계측기 센서; 및

상기 센서와 결합되고 센서 신호를 수신하는 모니터 외부에 위치한 메모리를 포함하며,

상기 메모리는 상기 센서와 관련된 데이타를 저장하며,

상기 데이타는 디지털 서명 및 마스킹된(masked) 데이타를 포함하며,

상기 마스킹된 데이타는 상기 디지털 서명 외부에 위치하며, 상기 디지털 서명 내에 포함된 대칭 키를 사용하여 마스킹되는 것을 특징으로 하는 맥박 산소계측기 장치.

청구항 2.

제 1항에 있어서,

상기 메모리는 상기 디지털 서명 데이타 내부에 포함되는 해시 함수(hash function)를 적용한 메시지 요약(message digest)을 저장하는 맥박 산소계측기 장치.

청구항 3.

제 2항에 있어서,

상기 대칭 키는 상기 요약으로부터 유도될 수 있는 맥박 산소계측기 장치.

청구항 4.

제 3항에 있어서,

상기 메모리는 공백(clear) 데이타를 추가로 저장하며, 상기 공백 데이타는 마스킹되지 않고(unmasked) 상기 디지털 서명 외부에 위치하며, 상기 요약은 상기 디지털 서명 데이타, 마스킹된 데이타, 및 공백 데이타로부터 형성되는 맥박 산소계측기 장치.

청구항 5.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 맥박 산소계측기 센서; 및

상기 센서와 결합되고 센서 신호를 수신하는 모니터 외부에 위치한 메모리를 포함하며,

상기 메모리는 상기 센서와 관련된 데이타를 저장하며,

상기 데이타는 디지털 서명 데이타 및 마스킹된 데이타를 포함하며,

상기 마스킹된 데이타는 상기 디지털 서명 데이타 외부에 위치하며,

상기 마스킹된 데이타를 디코딩하는데 사용되는 대칭 키는 상기 디지털 서명 데이타 내에 포함되는 맥박 산소계측기 장치.

청구항 6.

제 5항에 있어서,

메세지 요약이 적어도 소정의 데이타 정확성을 인증하기 위해 상기 서명 데이타 내에 포함되는 맥박 산소계측기 장치.

청구항 7.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 맥박 산소계측기 센서; 및

상기 센서와 결합되고 센서 신호를 수신하는 모니터 외부에 위치한 메모리를 포함하며,

상기 메모리는 상기 센서와 관련된 데이타를 저장하며,

상기 데이타는 디지털 서명을 포함하며,

상기 데이타의 필드는 강제/선택 비트 플래그를 포함하며, 상기 플래그는 상기 메모리를 판독하는 모니터에 의해 상기 데이타의 필드를 어떻게 사용할 지에 관한 정보가 상기 센서를 구비한 모니터 동작에 강제적인지 아닌지를 지시하는 맥박 산소계측기 장치.

청구항 8.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 맥박 산소계측기 센서; 및

상기 센서와 결합되고 센서 신호를 수신하는 모니터 외부에 위치한 메모리를 포함하며,

상기 메모리는 상기 센서와 관련된 데이타를 저장하며,

상기 데이타는 서명 데이타를 포함하며,

상기 서명 데이타는 포화도 계산 계수, 센서 OFF 임계치 및 서미스터 보정 계수 중 적어도 하나를 포함하는 맥박 산소계측기 장치.

청구항 9.

제 8항에 있어서,

상기 데이타는 제조일자, 로트 코드, 불량 센서 플래그, 제조 구성요소 테스트 데이타, LED 순방향 V/I 특성, LED 광전력 특성, 검출기 효율 특성, 최대 안전 LED 전력, 센서 데이타 세트 수정 레벨, 1회 기록/다수 기록 플래그, 페이지 크기, 페이지 번호, 센서 모델 유형, 최대 재순환 횟수 및 어른/신생아인지 관해 질문하는 플래그 중 적어도 하나를 포함하는 맥박 산소계측기 장치.

청구항 10.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 맥박 산소계측기 센서와 관련된 메모리를 포함하는 맥박 산소계측기 장치내 디지털 서명을 형성하는 방법으로서,

상기 디지털 서명을 형성하기 위해 상기 센서와 관련된 데이타의 적어도 일부를 사인하는 단계;

상기 메모리에 상기 디지털 서명을 저장하는 단계; 및

상기 메모리에 상기 센서와 관련된 데이타를 저장하는 단계; 및

상기 메모리 디지털 데이타로부터 유도된 메세지를 판독하고, 판독된 상기 메세지로부터 첫 번째 요약을 생성하고, 동일성 인증을 위해 상기 첫 번째 요약과 상기 디지털 서명 내부에 포함된 두 번째 요약을 비교함으로써 상기 서명을 검증 및 인증하는 단계를 포함하는 방법.

청구항 11.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 맥박 산소계측기 센서와 관련된 메모리를 포함하는 맥박 산소계측기 장치내 디지털 서명을 형성하는 방법으로서,

상기 디지털 서명을 형성하기 위해 상기 센서와 관련된 데이타의 적어도 일부를 사인하는 단계;

상기 메모리에 상기 디지털 서명 데이타를 저장하는 단계; 및

상기 메모리에 마스킹된 데이타를 저장하는 단계를 포함하며,

상기 마스킹된 데이타는 상기 디지털 서명 외부에 위치하며, 대칭 키를 이용하여 마스킹되는 것을 특징으로 하는 방법.

청구항 12.

제 11항에 있어서,

상기 디지털 서명 데이타 내에 해시 함수를 적용한 메세지 요약을 생성하는 단계를 추가로 포함하는 방법.

청구항 13.

제 11항에 있어서,

상기 대칭 키는 상기 요약으로부터 유도되는 방법.

청구항 14.

제 13항에 있어서,

언마스킹되고 상기 디지털 서명 외부에 존재하는 공백 데이타를 저장하는 단계를 추가로 포함하며, 상기 요약은 상기 디지털 서명 데이타, 마스킹된 데이타 및 공백 데이타로부터 형성되는 방법.

청구항 15.

센서를 동작시키는 방법으로서,

상기 센서와 관련된 메모리에 적어도 하나의 데이타 필드를 저장하는 단계;

상기 데이타 필드 내에 강제/선택 플래그를 저장하는 단계;

센서 판독기를 사용하여 상기 플래그를 판독하는 단계;

상기 센서 판독기가 상기 데이타 필드를 인식하지 못하고 상기 플래그가 상기 필드가 선택적이라고 지시한다면, 상기 데이타 필드를 무시하는 단계; 및

상기 센서 판독기가 상기 데이타 필드를 인식하지 못하고 상기 플래그가 상기 필드를 강제적이라고 지시한다면, 상기 센서 사용 불가능을 지시하는 에러 신호를 생성하는 단계를 포함하는 방법.

청구항 16.

제 15항에 있어서,

상기 필드와 관련된 필드 길이를 저장하는 단계;

상기 필드 길이를 판독하는 단계; 및

상기 센서 판독기가 상기 필드를 인식하지 못하고 상기 플래그가 상기 필드가 선택적임을 지시한다면, 상기 필드 길이를 사용함으로써 상기 필드를 건너뛰는 단계를 더 포함하는 방법.

청구항 17.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 센서; 및

상기 센서와 결합되고 센서 신호를 수신하는 모니터 외부에 위치한 메모리를 포함하며,

상기 메모리는 상기 센서와 관련된 데이타를 저장하며,

상기 데이타는 디지털 서명 데이타 및 마스킹된 데이타를 포함하며,

상기 마스킹된 데이타는 상기 디지털 서명 외부에 존재하며, 디지털 서명에 포함된 공개 키를 사용하여 마스킹되는 것을 특징으로 하는 장치.

청구항 18.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 센서와 관련된 메모리를 포함하는 장치내 디지털 서명을 형성하는 방법으로서,

상기 디지털 서명을 형성하기 위해 상기 센서와 관련된 데이타의 적어도 일부를 사인하는 단계;

상기 메모리에 상기 디지털 서명을 저장하는 단계; 및

상기 메모리에 마스킹된 데이타를 저장하는 단계를 포함하며,

상기 마스킹된 데이타는 상기 디지털 서명 외부에 존재하고 대칭 키를 사용하여 마스킹되는 방법.

청구항 19.

하우징;

계측된 생리적 특성에 대응하는 센서로부터의 신호를 수신하기 위한 센서 입력;

상기 센서 입력에 커플링되는 센서 프로세싱 회로;

상기 센서와 관련된 메모리에 저장된 디지털 데이타 - 상기 디지털 데이타가 디지털 서명을 포함함 -를 수신하기 위한 메모리 입력;

상기 디지털 데이타를 저장하기 위해 상기 메모리 입력에 커플링되는 제 1의 센서 판독기 메모리;

디지털 서명 검증 키를 저장하는 제 2의 센서 판독기 메모리;

상기 서명 검증키를 사용하여 상기 디지털 데이타의 상기 디지털 서명을 검증하며, 상기 디지털 서명내에 포함된 대칭 키를 사용하여 상기 디지털 서명 외부에 위치하는 마스킹된 데이타를 언마스킹하기 위한 프로그램을 저장하는 제 3의 센서 판독기 메모리; 및

적어도 상기 디지털 데이타의 일부를 상기 센서 프로세싱 회로에 제공하기 위한 전송 회로를 포함하는 센서 판독기.

청구항 20.

(a) 센서 장치로서,

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 센서; 및

상기 센서와 관련되며, 상기 센서와 관련한 디지털 데이타를 저장하는 센서 메모리 - 상기 데이타는 디지털 서명 데이타 및, 상기 디지털 서명 외부에 위치하며 상기 디지털 서명내에 포함된 대칭 키를 사용하여 마스킹되는 마스킹된 데이타를 포함함 -을 포함하는 센서 장치; 및

(b) 센서 판독기로서,

센서 판독기 하우징;

계측된 생리적인 특성에 대응하여 상기 센서로부터 상기 신호를 수신하기 위한 센서 입력;

상기 센서 입력에 커플링되는 센서 프로세싱 회로;

상기 센서 메모리로부터 상기 디지털 데이타를 수신하기 위한 메모리 입력;

상기 디지털 데이타를 저장하기 위한 상기 메모리 입력에 커플링되는 제 1의 센서 판독기 메모리;

서명 검증 키를 저장하는 제 2의 센서 판독기 메모리; 및

상기 서명 검증 키를 사용하여 상기 디지털 서명을 검증하며, 상기 디지털 서명내에 포함된 대칭 키를 사용하여 상기 디지털 서명 외부에 위치하는 마스킹된 데이타를 언마스킹하기 위한 프로그램을 저장하는 제 3의 센서 판독기 메모리를 포함하는 센서 판독기를 포함하는 시스템.

청구항 21.

측정된 생리적인 특성에 해당하는 신호를 제공하는 출력을 구비한 맥박 산소계측기 센서;

상기 센서와 관련되며, 센서 신호를 수신하는 모니터 외부에 위치하는 메모리를 포함하며,

상기 메모리는 상기 센서와 관련된 데이타를 저장하며,

상기 데이타는 디지털 서명 데이타 및 마스킹된 데이타를 포함하며, 상기 마스킹된 데이타는 상기 디지털 서명 외부에 위치하며, 상기 디지털 서명 내에 포함된 대칭 키를 사용하여 마스킹되며,

상기 데이타는 상시 센서가 환자로부터 떨어져 있는지를 지시하기 위한 센서 OFF 임계치를 포함하는 맥박 산소계측기 장치.

청구항 22.

삭제

청구항 23.

삭제

청구항 24.
삭제

청구항 25.
삭제

청구항 26.
삭제

청구항 27.
삭제

청구항 28.
삭제

청구항 29.
삭제

청구항 30.
삭제

청구항 31.
삭제

청구항 32.
삭제

청구항 33.
삭제

청구항 34.
삭제

청구항 35.
삭제

청구항 36.
삭제

청구항 37.
삭제

청구항 38.
삭제

명세서

기술분야

본 발명은 메모리를 갖는 센서에 관한 것이다. 그것은 특히 맥박 산소계측기(pulse oximeter) 센서에 관하여 설명될 것이지만, 다른 센서 유형에도 마찬가지로 동일하게 적용될 수 있다.

배경기술

맥박 산소계측

맥박 산소계측은 전형적으로 다양한 혈류 특성을 측정하기 위해 사용되고 상기 혈류 특성은 동맥혈에서의 헤모글로빈의 혈중 산소(blood-oxigen) 포화도 및 환자의 심장 박동수에 대응하는 혈액의 맥동수를 포함하나 이에 한정되지는 않는다. 이러한 특성의 측정은 비침습성(non-invasive) 센서를 사용함에 의해 수행되고, 상기 센서는 혈액이 관류하는 환자의 조직 일부를 통해 빛을 통과시키며, 광전적으로 그러한 조직에의 빛의 흡수를 감지한다. 모니터는 상기 센서와 연결되었는데, 흡수된 빛의 양을 결정하고, 측정된 혈액 성분의 양, 예를 들어, 동맥의 산소 포화도를 계산한다.

상기 조직을 통과한 빛은 하나 또는 그 이상의 파장이 되도록 선택되고, 상기 파장은 혈액 내에 존재하는 혈액 성분의 양에 대응하는 양으로 혈액에 의해 흡수된다. 조직을 통과한 투과되거나 반사된 빛의 양은 조직의 혈액 성분의 양 변화 및 관련된 빛의 흡수에 따라 변할 것이다. 혈중 산소 레벨을 측정하기 위해, 그러한 센서는 혈중 산소 포화도를 측정하기 위한 공지의 기술에 따라, 두 개의 다른 파장에서 동작하도록 적응된 광검출기 및 광소스와 함께 제공된다.

모니터에 유용한 정보를 전달하기 위해, 맥박 산소계측기 센서를 포함하는, 센서의 정보를 코딩하는 다양한 방법이 과거에 제안되어 왔다. 예를 들어, 인코딩 메커니즘이 넬코르(Nellcor) 미국 특허 제 4,700,708호에 기재되어 있고, 상기 내용의 개시는 참조 자료로서 본 명세서에 결합된다. 이러한 메커니즘은 빛을 혈액이 관류하는 조직을 통해 인도하는 한 쌍의 발광 다이오드(LED)를 사용하는 광 산소계측기 프로브에 관한 것이고, 이때 검출기는 조직에 흡수되지 않은 빛을 검출한다. 산소 포화도 계산 정확도는 상기 LED의 파장을 인지하는 것에 의존한다. LED의 파장이 변화할 수 있기 때문에, 코딩 저항기는 적어도 LED 중 하나의 실제 파장 또는 센서에 대한 LED 파장 합성에 적절한 산소계측기 산소 포화도 계산 계수를 모니터에 지시하는 저항값을 가지고 프로브에 위치한다. 산소계측기 장치가 켜질 때, 그것은 우선 전류를 코딩 저항기에 인가하고 저항값을 결정하여 프로브에서 LED의 파장에 대해 사용하기 위해 적절한 포화도 계산 계수를 결정하기 위해 전압을 측정한다.

다른 코딩 메커니즘은 또한 미국 특허 제 5,259,381호; 제 4,942,877호; 제 4,446,715호; 제 3,790,910호; 제 4,303,984호; 제 4,621,643호; 제 5,246,003호; 제 3,720,177호; 제 4,684,245호; 제 5,645,059호; 제 5,058,588호; 제 4,858,615호; 및 제 4,942,877호에 제안되었고, 상기 특허 발명의 개시는 본 명세서에서 참조 자료로 결합된다. 상기 '877 특허 발명은 산소계측에 대한 포화도 방정식의 계수를 포함하는 다양한 데이타를 특히 맥박 산소계측 센서 메모리에 저장하는 것을 개시한다.

종래의 센서 코딩 기술에 관한 문제점은 정보 인코딩의 정확성 및/또는 확실성이 종종 저하된다는 것이다. 그 결과 모니터는 때때로 환자를 충분히 판독할 수 없고, 더 나아가 부정확한 계산을 초래하며, 극단적인 예로 부정확한 코드 및 이로인한 부적절한 판독이 현저하게 환자의 안전을 해치고 안 좋은 결과를 나오게 할 수 있다. 부정확한 코드는 다양한 상황하에서 일어날 수 있다. 예를 들어, 에러는 센서의 제조 공정 또는 적재 도중 발생할 수 있다. 그러나 더 일반적인 것은 호환성 고품질의 센서를 제공하는 해당 모니터 제조자에 의해 허가받지 않거나 승인되지 않은 제 3자인 센서 제조자가 저가의 저품질로 부정확한 코드를 다소 의도적으로 사용한다는 것이다. 이러한 제 3자는 종종 연구에 최소 비용을 투자하고 모니터가 어떻게 동작하는지 또는 모니터가 어떻게 코드를 사용하는지 숙지하지 않았기 때문에 코드가 어떤 목적을 위한 것인지 알지 못한다. 그들은 상기 모니터 제조자에 의해 허가받지 않았기 때문에, 이런 정보는 일반적으로 모니터 제조자로부터 입수할 수 없다. 자주, 이러한 제 3자는 모니터가 어떻게 동작하는지와 환자의 안전을 보장하기 위해 코드가 어떻게 사용되는지에 관하여 역설계(reverse engineering) 기술 또는 독창적인 기술을 학습하는 데에 시간과 비용을 투자하지 않는다. 오히려, 그러한 제 3자는 단순히 인코딩되는 각각의 데이타 특성에 대하여 시장에서 사용되는 코드 값의 범위를 조사하고, 특정 모니터와 호환 가능하도록 모든 그들의 센서에 평균 코드 값을 취하는 예가 많다. 많은 실례에서 평균 코드 값을 사용하는 것은 단지 규격을 벗어난 판독을 야기하지만, 평균 코드 값은 모니터에 의해 사용되는 계산 알고리즘에 현저한 에러를 유발하고 심각한 환자의 안전 문제를 일으킬 수 있다. 부가하여, 제 3자가 사용한 부정확한 코드가 환자의 나쁜 결과에 원인이 될 때마다, 피해입은 환자, 또는 그의 상속인이 모니터 제조자와 직접적인 의료 제공자에 대해, 책임을 물으려는 시도를 할 수 있다. 만일 의료 제공자가 사용된 상기 낮은 품질의 제 3자 센서를 보유하고 있지 않고 그것의 사용에 대한 기록이 없다면, 모니터 제조자는 문제가 저품질의 제 3자 센서의 사용에 의해 야기된 것이고 그렇지 않았더라면 고품질의 모니터라는 것을 입증하는 것이 어려울 것이다.

의료 센서와 관련하여 저장된 디지털 데이타를 인증할 필요가 있는 또다른 이유는 공장에서 레코딩하는 시간과 환자의 상태를 모니터링하는 장치에 의한 판독 시간 사이에 데이타가 손상될 실제적인 가능성이 있기 때문이다. 그러한 손상을 야기할 수 있는 메커니즘으로 종종 인용되는 예들 중 하나는 강력한 우주선(cosmic ray)의 발생에 의해 디지털 메모리에 레코딩된 값이 변화한다는 것이다. 손상의 더 일반적인 원인은 정전기 방전에 의해 초래된 메모리 셀의 손상이다.

따라서, 정확한 계산과 모니터에 의한 정확환 환자의 모니터링을 보장하기 위해, 센서로부터 모니터에 복합 코드(complex code)를 통신하는 정확하고 확실한 방법을 고안할 필요성이 당해 기술 분야에서 존재한다.

발명의 상세한 설명

따라서, 본 발명의 목적은 정확성이 인증될 수 있는 모니터에 대해 유용한 코드를 갖는 센서를 제공하는 것이다.

이러한 목적 및 다른 목적은 환자의 계측된 생리적 특성에 대응하는 신호를 발생시키고 모니터에 의해 사용될 때 정확하고 인증되었음이 보증될 수 있는 "코드"를 제공하는 센서에 의해 달성될 수 있다. 상기 센서와 관련된 메모리는 상기 코드 및 상기 센서와 관련된 다른 데이타를 저장하고, 상기 메모리는 또한 디지털 서명을 포함한다. 디지털 서명은 그것이 소정의 품질 제어를 갖는 엔티티(entity)에 의해 생성되었음을 보장함으로써 코드 및 데이타의 품질을 인증하고, 상기 코드가 정확하다는 것을 보장한다.

하나의 실시예에서, 디지털 서명은 센서 제조 공정 중 개인 키와 공개 키 쌍 중에서 개인 키를 사용하여 생성되고, 그 다음에 상기 서명은 외부 센서 판독기(예를 들어, 모니터)내 프로세서에 삽입된 공개 키로 검증될 수 있다. 상기 서명은 상기 데이타로부터 분리될 수 있다. 또는, 서명이 데이타에 부가되는 대신, 서명 그 자체가 모든 또는 적어도 소정의 데이타를 포함할 수 있고, 이에 따라 데이타의 마스킹(masking) 레벨을 제공한다.

본 발명의 실시예 하나에 따라, 몇 개의 공지된 공개 키/개인 키 서명 방법 중 임의의 하나가 사용될 수 있다. 이것은 디피-헬만(Diffie-Hellman)(및 미국 국립표준기술 연구소로부터 나온 디지털 서명 표준과 같은 그것의 변형체, 엘 가멀(El Gamal) 및 타원 곡선 방식), RSA(MIT에서 개발됨) 및 라빈-윌리엄스(Rabin-Williams)를 포함한다.

본 발명의 부가적인 실시예에서, 사인(sign)될 데이타 부분의 요약(digest)은 데이타에 에러가 발생하지 않았음을 검증하기 위해 디지털 서명에 포함된다. 데이타의 각각의 피스(piece)는 바람직하게는 후속하는 데이타의 유형을 지시하는 필드 ID, 후속하는 데이타 길이 엘리먼트, 후속하는 데이타 피스를 포함한다. 강제 비트(mandatory bit)는 또한 바람직하게는 모니터에 의해 데이타 피스가 어떻게 사용되는지에 관한 정보가 모니터를 구비한 센서의 동작에 강제적인지 아닌지를 지시하는데 제공된다. 이런 식으로, 중요하지 않은 데이타 피스를 인식하지 못하는 구식 모니터는 간단히 그것을 무시할 수 있는데, 아마도 그것은 상기 데이타 피스에 대응하는 개량된 장치를 구현하지 않을 것이기 때문이다. 그러나 데이타 피스가 센서의 적합한 동작에 필수적이라면, 강제 비트가 설정될 것이고, 상기 센서 판독기/모니터는 그것이 플러그된(plugged in) 특정한 센서를 사용할 수 없다는 것을 표시할 것이다.

또 다른 실시예에서, 센서에 저장되는 사인된 데이타는 적어도 모니터에 의해 산소 포화도를 계산하기 위해 사용되는 센서 의존 포화도 보정계수를 포함할 것이다. 부가적으로, 상기 데이타는 센서 OFF 임계치 및 서미스터(thermistor)를 포함하는 센서에 대해 적절한 서미스터 보정 계수를 포함할 수 있다. 소정의 그러한 데이타는 상기 서명 내부에 포함될 수 있고, 이러한 또는 다른 데이타는 상기 서명 외부에 포함될 수 있다. 상기 서명 외부의 데이타는 암호화(또는 마스킹)될 수 있고, 요구된다면, 대칭 키 암호화 알고리즘, 예를 들어 NIST로부터 나온 데이타 암호화 표준(DES)으로 암호화될 수 있고, 대칭 키는 서명에 포함될 수 있다. 대안적으로, 대칭 키는 상기 요약으로부터 도출될 수 있고, 상기 요약은 상기 서명 내부에 포함된다.

본 발명의 특징과 이점을 보다 더 이해하기 위해, 도면과 함께 이하의 실시예를 참조해야 한다.

실시예

정의

사인된 데이타(SIGNED DATA)는 (해시 함수를 사용하여) 요약(digest)의 계산에 포함되는 데이타이고, 이러한 요약은 차례로 디지털 서명의 계산에 포함되며, 이에 의해 나중에 일어난 임의의 데이타 변경은 디지털 서명 검증의 실패에 의해

검출될 수 있다. 사인된 데이타는 결국 디지털 서명의 내부 아니면 외부에 존재할 수 있다. "메세지 복구를 갖는 디지털 서명"으로 알려진 프로세스에서, 데이타는 전부 디지털 서명 내부에 존재한다. 상기 서명이 검증될 때까지, 상기 데이타는 스크램블(scramble) 형태로 존재하고, 그 결과 보통 사람들은 그것을 이해할 수 없다. 서명을 검증하는 수학적 프로세스는 상기 데이타를 해독(unscramble)하거나 또는 "복구"한다. "부분적인 복구를 갖는 디지털 서명"으로 알려진 프로세스가 본 명세서에 기재된 본 발명에서 선호되는데, 사인된 데이타의 일부는 상기 서명에 포함되고, 부가적인 데이타는 서명의 외부에 존재한다. 상기 서명 내부에 존재하는 데이타 부분은 서명이 검증될 때까지 알아보기 힘든 상태로 있으나, 외부에 존재하는 부분은 마스킹 프로세스가 그것을 감추기 위해 사용되지 않는다면 쉽게 판독될 수 있다.

본 명세서에서 사용되는 **마스킹된 데이타(MASKED DATA)**라는 용어는 상기 서명 내부에 포함된 언마스킹 키(unmasking key)로 복구될 수 있도록 암호화된 데이타이다. 상기 서명을 검증하는 동안, 상기 언마스킹 키는 복구된다. 그 다음에 그러한 언마스킹 키는 마스킹된 데이타를 복호화하기 위해 사용될 수 있다. 바람직한 실시예에서, 상기 마스킹된 데이타는 대칭키로 암호화되며, 대칭키라 함은 암호화 키와 복호화 키(즉, 마스킹 키와 언마스킹 키)가 동일함을 의미한다. 특별히 바람직한 실시예에서, 디지털 서명에 통합된 메세지 요약은 상기 서명 외부의 마스킹 데이타와 언마스킹 데이타를 위한 대칭 키로서 사용된다.

센서 판독기/모니터(SENSOR READER/MONITOR)

도 1은 본 발명의 바람직한 실시예 하나를 보여주는 블록도이다. 도 1은 환자 조직(18)에 부착되는 비침습성 센서(15)에 연결되는 맥박 산소계측기(17)를 보여준다. 센서 LED(14)로부터 나온 빛은 환자의 조직(18) 내로 지나가고, 조직(18)을 통해 투과되거나 조직으로부터 반사된 이후에, 상기 빛은 광센서(16)에 의해 수용된다. 두 개 또는 그 이상의 LED가 본 발명의 실시예에 따라 사용될 수 있다. 광센서(16)는 수신한 에너지를 전기적인 신호로 변환시키고, 상기 전기 신호는 그 다음에 입력 증폭기(20)에 공급된다.

LED이외의 광 소스가 사용될 수 있다. 예를 들어, 레이저가 사용될 수 있고, 또는 백색 광소스가 적절한 파장필터와 함께 전송단 아니면 수신단에 사용될 수 있다.

시간 프로세싱 유닛(TPU)(48)은 상기 LED를 활성화하기 위해, 전형적으로 번갈아가며, 제어 신호를 LED 드라이브(32)에 보낸다. 다시, 상기 실시예에 의하면, 상기 드라이브는 두 개 또는 임의의 부가적인, 요구되는 개수의 LED를 제어할 수 있다.

입력증폭기(20)로부터 수신된 신호는 도 3의 실시예에 나타난 대로 세 개의 다른 파장에 대해서 세 개의 다른 채널을 통해 통과된다. 또한, 두 개의 파장에 대해 두 개의 채널이 사용될 수도 있고, 또는 N개의 파장에 대해 N개의 채널이 사용될 수도 있다. 각각의 채널은 아날로그 스위치(40), 저역통과 필터(42) 및 A/D 컨버터(38)를 포함한다. TPU(48)로부터 나온 제어라인은 대응하는 LED(14)가 구동되는 때에 동기하여 적합한 채널을 선택한다. 대기직렬모듈(QSM)(46)은 각각의 채널로부터 A/D 컨버터에서 나온 데이타라인을 경유하여 디지털 데이타를 수신한다. CPU(50)는 QSM(46)이 주기적으로 채워질 때마다 QSM(46)으로부터 RAM(52) 안으로 데이타를 전송한다. 하나의 실시예에서, QSM(46), TPU(48), CPU(50) 및 RAM(52)는 마이크로컨트롤러와 같은 하나의 통합된 회로의 부분이다.

센서 메모리(Sensor Memory)

센서(15)는 광검출기(16)와 LED(14)를 포함하고, 센서와 관련된 센서 메모리(12)를 갖는다. 메모리(12)는 센서 판독기 또는 모니터(17) 내의 CPU(50)와 연결된다. 상기 메모리(12)는 센서(15)의 본체 또는 센서에 연결된 전기 플러그 내에 패키지화될 수 있다. 대안으로, 상기 메모리(12)는 상기 모니터의 외부면에 부착할 수 있는 하우징 내에 패키지화될 수 있거나, 또는 상기 메모리(12)는 센서 본체와 모니터 사이의 신호 경로 내 어디든지 위치할 수 있다. 특히, 소정의 바람직한 실시예에 따르면, 센서 메모리(12)의 콘텐츠는 특별한 센서 모델과 관련된 모든 센서에 대해 일정할 수 있다. 이러한 경우에, 개개의 메모리(12)를 이 모델과 관련된 각각의 센서상에 두는 것 대신에, 상기 메모리(12)는 상기 센서 모델과 관련된 재사용 가능 연장 케이블에 대신 포함될 수 있다. 상기 센서 모델이 1회용 센서라면, 이 경우에 단일 메모리(12)는 재사용 가능 연장 케이블 내에 통합될 수 있다. 그 다음에 재사용 가능 케이블은 다수 개의 1회용 센서와 함께 사용될 수 있다.

도 2는 하나의 바람직한 실시예에 따라 도 1의 메모리(12)의 콘텐츠를 보여주는 다이어그램이다. 디지털 서명(60)은 상기 메모리의 첫 번째 부분에 위치하고, 상기의 서명은 바람직하게는 센서 관련 데이타를 포함한다. 두 번째 부분(62)은 사인되고 마스킹된 데이타를 포함한다. 세 번째 부분(64)은 사인되었으나 공백인(clear) 상태(즉, 마스킹되지 않은 상태)로 남아있는 데이타를 포함한다. 마지막으로, 일부(66)는 센서 판독기에 의해 센서 메모리에 기록되기 위해 남겨둔다. 일부(66)

는 사인되지도 마스킹되지도 않는다. 이러한 바람직한 실시예가 예시를 위해 도시되어 있지만, 메모리(12)가 디지털 서명 외부에 다른 많은 데이타 블록을 포함할 수 있다는 것이 납득되어야 하고, 상기 디지털 서명 각각은 특별한 실시예의 요구 조건에 따라 사인되거나 마스킹될 수 있다. 이러한 다른 데이타 블록은 임의의 요구되는 순서로 배열될 수 있고, 예를 들어, 다수 개의 사인된 블록과 사인되지 않은 블록이 인터리빙될 수 있고, 다수 개의 마스킹된 블록과 언마스킹 블록이 인터리빙될 수 있다. 센서 판독기에 의해 메모리(12)에 기록된 데이타는 선택 사양이며, 그러한 데이타는 선택적으로 마스킹될 수 있다는 것 역시 납득되어야 한다.

공장에서의 서명 기록

도 3은 상기 센서 메모리(12) 내부에 서명을 기록하기 위해 공장에서 사용되는 시스템의 실시예 하나에 관한 블록도이다. 도 3에 나타나 있는 것은 개인용 컴퓨터(PC)(70)와 관련 암호 보조프로세서(72)이고, 상기 암호 보조프로세서는 개인/공개 키의 쌍 중에서 개인 키를 포함하고 이용한다. 개인 키는 보조프로세서(72) 내부의 메모리 내에 포함된다. 바람직하게는 이러한 키는 보안을 유지하기 위해 누구에 의해서든지 판독가능한 것이 아니다. 대응하는 공개 키는 PC(70)와 보조프로세서(72) 양자에 의해 파악될 수 있고, 또는 보조프로세서(72)에 의해 출력될 수 있다.

보조프로세서(72)에 의해 사인되는 데이타는 하나 이상의 소스로부터 나올 수 있다. 특정 센서의 엘리먼트들의 값(78), 예를 들어 LED 파장, 서미스터 저항, 등을 결정하기 위해 센서를 테스팅하기 위한 테스터(76)가 나타나 있다. 그 다음에 이러한 데이타 값은 라인(80)을 따라 PC에 제공된다. 부가적인 정보(82)는 키보드에 의해 입력될 수 있거나 라인(84)을 따라 또다른 데이타베이스로부터 입력될 수 있다. 이러한 데이타는 예를 들어, 센서에 대한 일련 번호, 제조일자, 로트 번호(lot number), 사인될 데이타의 부분에 관한 요약, 또는 다른 정보들을 포함할 수 있다.

사인될 데이타와 메모리(12)에 포함될 다른 데이타는 PC로부터 암호 보조프로세서(72)로 전달될 수 있다. 보조프로세서(72)는 사인되는 데이타로부터 요약을 계산하고, 개인 키를 이용하여 요약과 데이타 사인이 요구되는 다른 데이타를 사인한다. 서명과 거기에 포함된 데이타는 마스킹되는 다른 데이타를 위한 대칭 키, 또는 대칭 키가 유도될 수 있는 정보를 포함할 수 있다. 보조프로세서는 PC(70)에 서명을 되돌려 전달한다. PC(70)는 바람직하게는 서명에 포함되지 않은 소정의 데이타를 마스킹하고, 마스킹된 데이타, 서명 및 공백인 데이타를 결합하여 이러한 모든 것을 라인(86) 상에서 메모리(12)에 전달한다.

도 4는 도 3의 시스템 동작을 보여주는 다이어그램이다. 도 5는 도 4의 방법에 따라 데이타 흐름을 도시한다.

우선적으로, 센서는 테스트되고, LED 파장과 같은 센서의 계측된 매개변수(88)가 제공된다. 다음으로, 임의의 다른 데이타(89)가 입력된다. 그 다음에 데이타는 정렬(sort)(단계 90)된다. 이러한 정렬의 결과로 제 1의 데이타(91)가 사인되고, 제 2의 데이타(92)는 마스킹되며, 제 3의 데이타(93)는 공백인 상태, 즉 마스킹도 되지 않고 사인도 되지 않은 상태에 있게 된다. 제조 동안 또는 뒤이어 일어나는 판독/복호화 단계 동안에 센서가 사용될 때 상기 임의의 데이타(91, 92, 93)에서 에러가 발생하지 않음을 검증하기 위해, 요약(95)은 제조 중 상기 모든 데이타(91, 92, 93)로부터 생성(단계 94)되고 서명 내부에 포함된다. 상기 요약은 상기 데이타(91, 92, 93)에 해시함수를 적용한 출력 값으로서 생성된다. 상기 요약은 복잡한 CRC에 비유될 수 있다. 상기 데이타와 요약은 이후에 복호화에 뒤이어 일어나는 모니터에 의해 판독될 때, 하나 또는 그 이상 에러 비트가 상기 데이타(91, 92, 93) 중 임의의 것에 발생한다면, 모니터가 판독된 데이타로부터 만들어내는 제 2의 요약은 상기 메모리로부터 추출된 요약에 대응하지 않을 것이고, 따라서 기록 또는 서명 검증 프로세스의 어딘가에 하나 또는 그 이상의 에러가 발생하였음을 표시할 것이다. 적절한 해시 함수의 예는 SHA-1이고, 연방정부 정보처리 표준 공보(Federal Information Processing Standard Publication) FIPS, PUB 180-1, SHA(Secure Hash Standard), 국립 표준 기술 연구소(National Institute of Standards & Techonlogy), 1995에 기재되어 있다. 요약(95)과 데이타(91)는 단계 96에서 서명(101)을 생성하기 위해 단계 100에서 부가된 포맷팅 데이타(99)를 따라 사인된다. 포맷팅 데이타는 예를 들어 국제 표준(International Standard) ISO/IEC 9796-2, 디지털 서명에 대한 표준에 따라 단계 100에서 부가된다. 상기 데이타(92)는 단계 103에서 마스킹된다. 이러한 서명(101), 마스킹된 데이타(103) 및 공백인 데이타(93)는 그 다음에 보조프로세서(72)와 PC(70)에 의해 결합되어 센서 메모리(12)에 저장된다.

삭제

데이타(91)를 사인하기 위해 사용되는 개인 키는 바람직하게는 라빈-윌리엄스(Rabin-Williams) 디지털 서명 알고리즘이고, 그 중 하나의 예가 ISO 9796-2에 기재되어 있다.

하나의 실시예에서, 사인될 데이타의 최초 블록, 블록(91)은 73 또는 이보다 적은 바이트(byte)에 요약 20바이트와 포맷팅 데이타(99) 3바이트를 더한 것이다. 이것은 96바이트의 사인된 메세지를 산출한다. 더 긴 서명이 또한 사용될 수 있는데, 예를 들어, 서명은 유용한 데이타(91)로서 수신될 수 있는 106 바이트를 갖는 128 바이트를 갖는다. 상기 서명의 길이는 요구되는 보안의 정도와 모니터의 해독 능력 정도에 의존하다.

필드에서 판독기/모니터에 의한 서명 판독

도 6은 디지털 서명을 검증하고 환자에게 사용된 센서로부터 나온 데이타를 복구하는 센서 판독기 또는 모니터(17)의 부분을 보여준다. 데이타는 CPU(50)에 의해 우선 센서 메모리로부터 검색되고 메모리(110)에 저장된다. 센서 판독기는 메모리(112)에 공개 키를 갖고, 이러한 공개키는 전형적으로 모니터를 제조할 때 로딩되거나 모니터의 업그레이드로서 제공된다. 서명 검증과 데이타 복구 프로그램은 메모리(114)의 일부에 저장된다.

도 7은 도 6에 나타난 메모리 부분의 서명 검증과 데이타 복구 프로그램(114) 동작을 보여준다. 도 8은 도 7의 플로차트에 따라 데이타의 이동을 보여주는 다이어그램이다. 데이타는 우선 단계 106에서 센서 메모리로부터 검색된다. 상기 데이타(102)는 도 8에 나타나 있고 서명(101), 마스킹된 데이타(107) 및 공백인 데이타(93)로 구성되어 있다. 그 다음에 공개 키(112)가 상기 모니터의 메모리로부터 검색된다(단계108).

그 다음에는 서명 데이타(91)와 메모리 요약(95)을 획득하기 위해 서명 및 공개 키가 암호화 변환(cryptographic transform)에 입력으로서 제공된다(단계 109). 메모리 요약은 마스킹된 데이타 대칭 키를 결정하기 위해 사용되고, 그 다음에 이러한 키는 마스킹된 데이타(107)를 복호화하여(단계 116) 마스킹된 원시 데이타(original data)(92)를 획득하기 위해 사용된다.

모든 데이타(91, 92, 93)의 정확성을 검증하기 위해, 그 다음에 제 2의 요약은 복호화된 사인된 데이타(91), 언마스킹된 데이타(92) 및 공백인 데이타(93)로부터 해시 함수(118)를 사용하여 모니터에 의해 만들어진다(단계 120). 이것은 새로운 요약(122)을 생성할 것이고 그 다음에 상기 요약은 단계 124에서 원시 요약(original digest)(95)(상기 메모리로부터 판독됨)과 비교될 수 있다. 만일 요약들이 동일하다면, 서명은 검증되고 상기 메세지(결합된 데이타(91, 92, 93))가 인증된다(단계 126). 그 다음에 모니터는 그것의 동작 중 상기 메세지를 사용한다. 반면에, 상기 요약이 동일하지 않다면, 상기 메세지는 손상된 것으로 결정되고 상기 모니터는 모니터 사용자에게 결함있는 센서 신호를 지시하고 상기 메세지를 사용하지 않는다(128).

알 수 있듯이, 본 발명은 독창적으로 디지털 서명을 센서에 적용하고 더욱 상세히는 맥박 산소계측기 센서에 적용한다. 센서에의 독창적인 적용은 상기 센서 판독기/모니터가 메세지(데이타) 정확성, 소스에 대한 인증 및 센서의 품질을 검증하도록 허용하고, 민감한 센서 사양(specification) 정보가 쉽게 누설되는 것과 개발하지 않은 센서 제조자에 의해 잘못 사용되는 것을 막아준다.

서명 필드

도 9는 디지털 서명 데이타(91), 요약(95) 및 포맷팅 데이타(99)의 일 실시예를 더욱 상세히 보여준다. 특히, 디지털 서명 데이타(91)는 CRC가 후속하는 임의의 필드 개수로 분할된다. 각각의 필드(132)는 1바이트 필드 ID(136)를 포함하고, 상기 ID는 필드에 존재하는 데이타 유형을 식별한다. 단일 비트(138)는 상기 필드가 강제적인지 아닌지를 지시한다. 다음에, 필드의 길이를 인증하는 블록(140)에 7비트가 존재한다. 마지막으로, 필드 데이타는 바이트 블록(142)에 제공된다.

동작시, 기존의 모니터 또는 센서 판독기가 특정 필드 ID(136)를 처리할 수 없거나 인식하지 못한다면, 그것은 필드 길이(140)를 보고 다음 필드에 도달하기 위해 얼마나 많은 데이타를 건너뛰어야 할지 계산할 수 있다. 그러나, 그것은 우선적으로 이 데이타가 센서를 동작하기 위해 강제적인지 아닌지를 결정하기 위해 강제 비트(138)를 체크한다. 만일 그것이 강제적이라면, 모니터 또는 센서 판독기는 부착된 센서를 적절하게 판독할 수 없음을 지시하는 에러 메세지를 생성할 것이다. 만일 그것이 강제적이지 않다면, 모니터 또는 센서 판독기는 단순히 이 데이타 필드를 무시할 것이다.

그리하여 이러한 필드 포맷은 데이타를 서명 데이타 블록 안으로 패킹(packing)하는데 있어서 유연성을 제공하고, 또한 업그레이드 가능성과 기존의 센서 판독기 및 차세대 센서와 모니터와의 호환성을 제공한다.

하나의 실시예에서, 선택된 값의 필드 식별자(field identifier)는 "이스케이프 문자(escape character)"로서 지명되고, 다음 문자가 확장된 세트의 식별자라는 것을 지시한다. 이것은 고정된 주소에 정렬할 필요없이 메세지에 포함된 필드를 추가, 삭제, 이동, 압축 또는 신장(stretch)할 능력을 허용한다.

데이타 유형

이하의 것은 하나의 실시예에서 메모리(12) 안에 포함될 수 있는 데이타 유형의 예이다.

맥박 산소계측기에 대한 포화 계산 방정식에 적용될 실제 계수 또는 데이타는 저장될 수 있다. 이러한 계수들은 계측된 LED 파장에 대응하는 값을 저장하는 대신에 저장될 수 있다. 그 결과 센서 설계에서 유연성이 크게 증가되고 보정 곡선(calibration curve)이 장치에 제공된 작은 곡선 세트에 한정되지 않는다.

대안으로 계수에 또는 거기에 부가하여, 단순히 LED 파장만이 저장될 수 있다. 또한, 제 2의 방출 파장 특성이 저장될 수 있고, 다른 LED 매개변수가 저장될 수 있다.

특정 센서는 센서 온도에 대한 보정 곡선의 보상과 같은 목적을 위해 국부적인 온도를 측정하거나 환자가 화상을 입지 않게 하는데 사용되는 서미스터를 구비할 수 있다. 서미스터에 대한 보정 계수는 저장될 수 있다.

메모리(12)에 포함될 수 있는 다른 데이타는 예를 들어, 센서 추적성(traceability)을 허용할 로트 코드, 불량 센서 플래그(flag), 제조일자, 제조 테스트 정보, 서명에 사용된 사인 소프트웨어 프로그램의 버전, LED 순방향 V/I 특성, LED 광전력 특성, 검출기 효율 특성, 최대 안전 LED 전력, 센서 데이타 세트 수정 레벨(센서에 포함된 특성을 지시), 센서 모델 ID, 어른/신생아에 관한 질문 플래그(신생아 또는 어른이 모니터되는지에 따라 맥박 산소계측기에 대해 서로 다른 표준산소포화 레벨로, 요구되는 알람 제한 범위를 트리거링하기 위함), 1회 기록/다수 기록 플래그, 페이지 크기, 페이지 번호 및 재생의 최대 횟수를 포함할 수 있다.

대안으로, 앞서 언급되거나 인용된 선행 기술 참증에 기재된 임의의 데이타 유형은 마스킹된 데이타(92), 서명 데이타(91) 또는 공백인 데이타(93)에 사용되고 저장될 수 있다.

도 10은 디지털 서명을 갖는 어댑터를 통합한 센서 시스템의 블록도이다. 도 10은 어댑터(204)에 연결된 센서(202)를 보여주고, 어댑터는 차례로 모니터(206)에 연결된다. 어댑터는 신호조정회로(208), 디지털 서명을 가진 메모리(210) 및 내부 모니터(212)를 포함한다. 그러한 어댑터는 디지털 서명 없이 상기 어댑터에 연결되도록 설계된 센서들에 대해 사용된다. 어댑터 그 자체는 외부 모니터(206)에 디지털 서명을 제공할 수 있다. 따라서, 예를 들어, 인증된 각각의 센서 대신에, 센서가 인증됨을 결정하기 위한 다른 방법이 사용될 수 있고, 이때 상기 어댑터는 외부 모니터에 인증을 제공한다.

도 10에 나타난 실시예에서, 상기 어댑터는 또한 내부 모니터(212)를 포함한다. 이러한 내부 모니터는 필드에서 외부 모니터(206)에 의해 제공된 출력과 디스플레이와는 다른 또는 그 변형인 출력 디스플레이 또는 다른 신호를 제공하는데 사용될 수 있다. 두 개의 모니터에 의한 임의의 출력이 표시와 일치함을 보장하기 위해, 신호조정 블록(208)은 센서 신호를 수정할 수 있고, 이에 의해 그것의 수정된 형태로, 외부 모니터(206)에 대한 라인(214)상의 신호 출력은 외부 모니터(206)가 내부 모니터(212)에 의해 생성된 것에 대응하는 출력 신호를 만들어 내게 한다. 예를 들어, 환자로부터의 신호는 맥박 산소계측 값에 대응하는 센서(202)로부터 얻어질 수 있다. 포화도와 심장 박동수 판단은 내부 모니터(212)상에서 발생될 수 있고, 이때 블록(208)은 그것이 외부 모니터(206)에 보내는 합성 AC 신호를 생성한다. 합성 신호의 구성은 외부 모니터가 내부 모니터(212)와 유사한 심장 박동수 및 포화도를 계산하는 것을 보장하기 위해서이다.

디지털 서명은 필터링되지 않은 환자 데이타, 필터링된 환자 데이타, 합성된 환자의 생리적 신호 또는 임의의 다른 데이타를 포함하는 임의의 데이타의 서명일 수 있다.

당업자가 알 수 있듯이, 본 발명은 본 발명의 필수적인 특성에서 벗어나지 않고 다른 특정한 형태로 구현될 수 있다. 따라서, 앞서 말한 것은 예시적인 것이며, 발명의 범위는 이하의 청구범위에 의해 정해진다.

도면의 간단한 설명

도 1은 본 발명을 통합시키는 센서와 센서 판독기 시스템의 블록도이다.

도 2는 도 1의 센서 메모리의 콘텐츠에 관한 블록도이다.

도 3은 센서의 제조 도중 데이타를 사인하는 것에 대한 시스템을 보여주는 블록도이다.

도 4는 도 3의 시스템에 의해 사인하는 메커니즘을 보여주는 도면이다.

도 5는 도 4의 방법으로 생성된 데이타를 보여주는 데이타 순서도이다.

도 6은 센서 판독기 또는 모니터의 일 실시예를 보여주는 도면이고, 다른 소프트웨어 모듈을 보여준다.

도 7은 본 발명에 따른 센서의 판독을 보여주는 순서도이다.

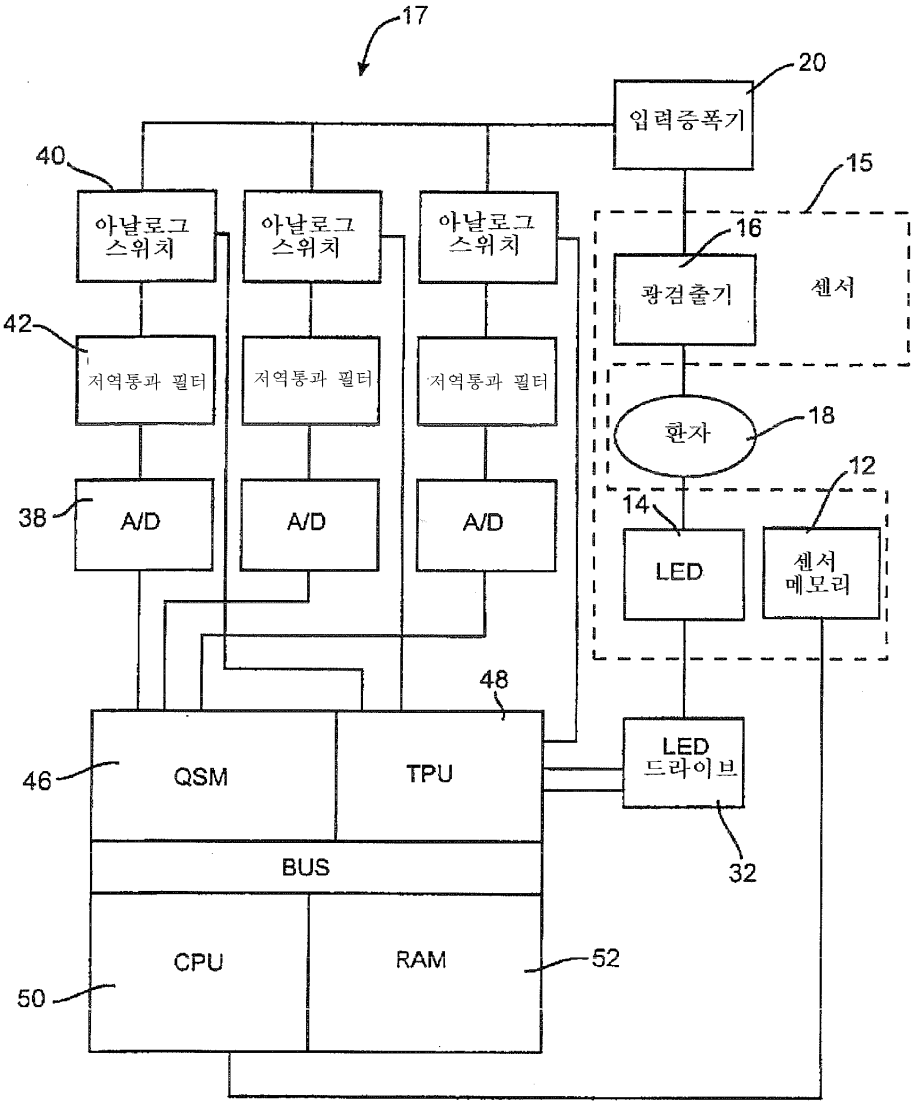
도 8은 도 7의 방법으로 판독된 데이타의 흐름을 보여주는 도면이다.

도 9는 데이타에서의 다른 필드에 관한 도면이다.

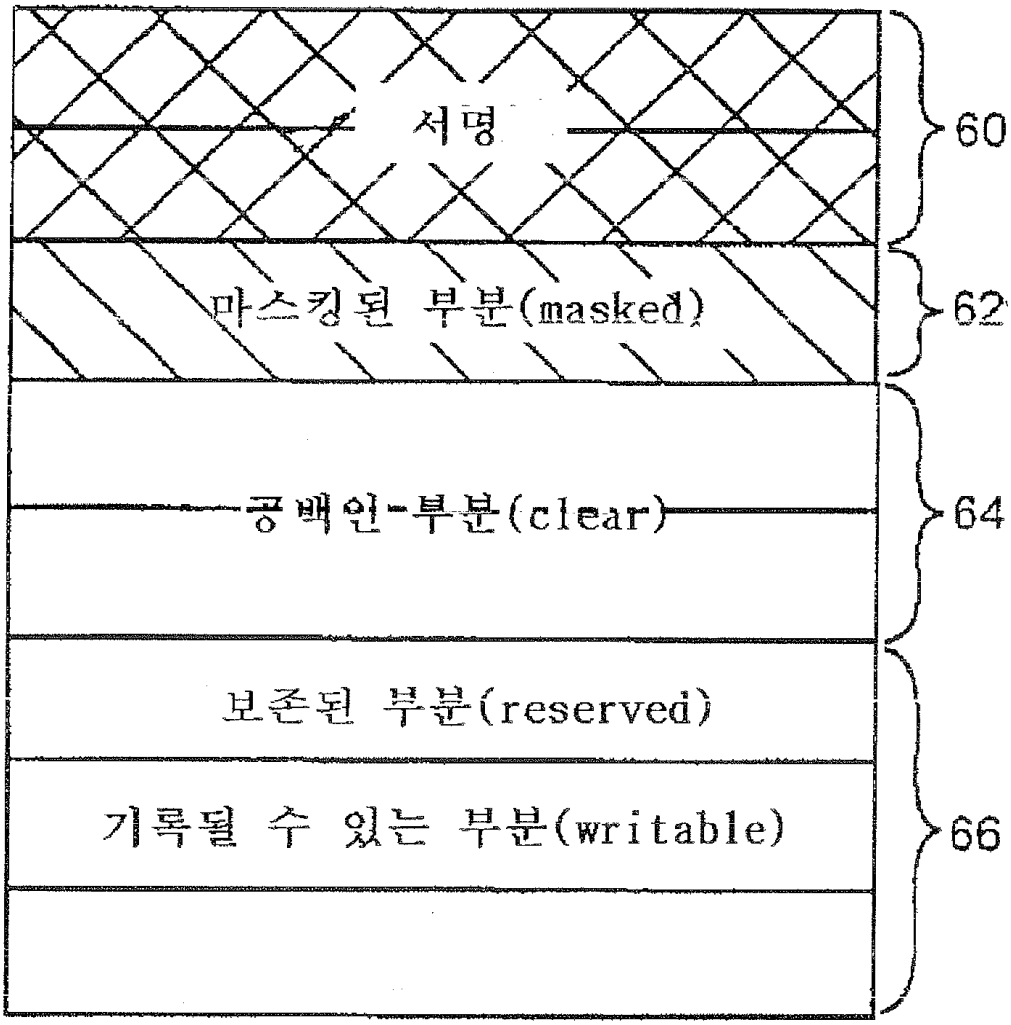
도 10은 디지털 서명을 가진 어댑터를 사용하는 센서 시스템의 블록도이다.

도면

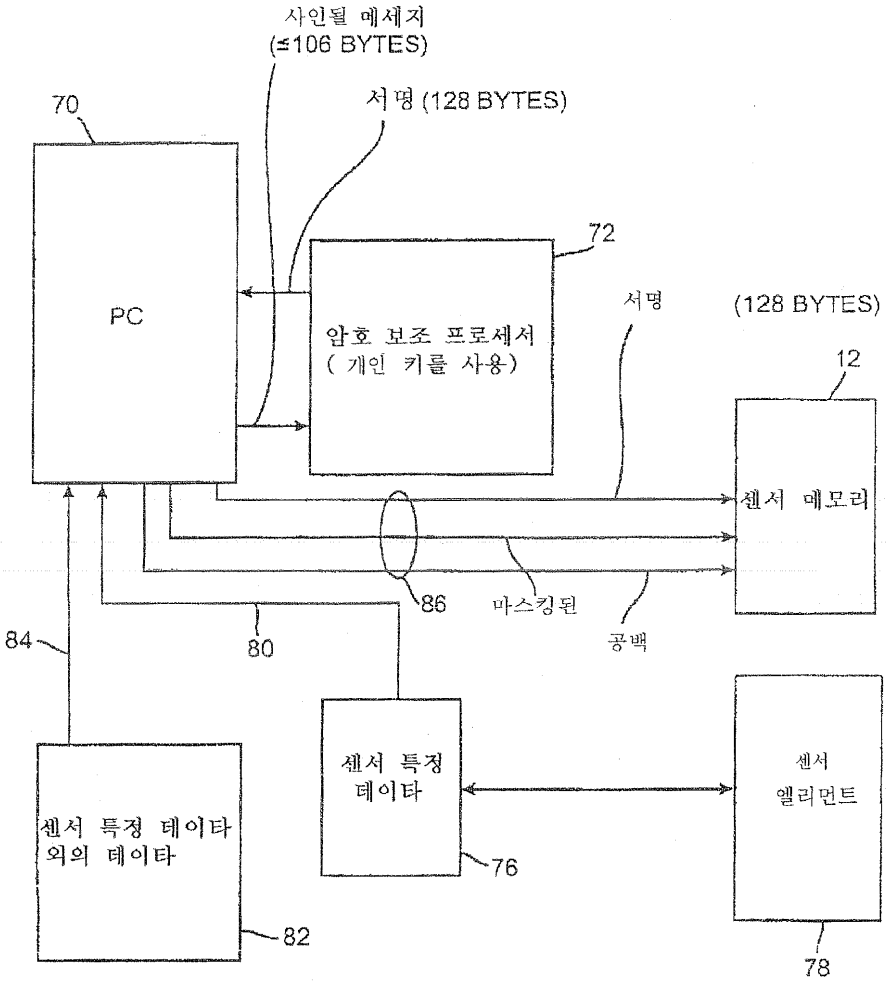
도면1


17
20
입력증폭기
40
아날로그 스위치
아날로그 스위치
아날로그 스위치
15
16
광검출기
센서
42
저역통과 필터
저역통과 필터
저역통과 필터
환자
18
12
14
38
A/D
A/D
A/D
LED
센서 메모리
48
46
QSM
TPU
LED 드라이브
32
BUS
CPU
RAM
52
50

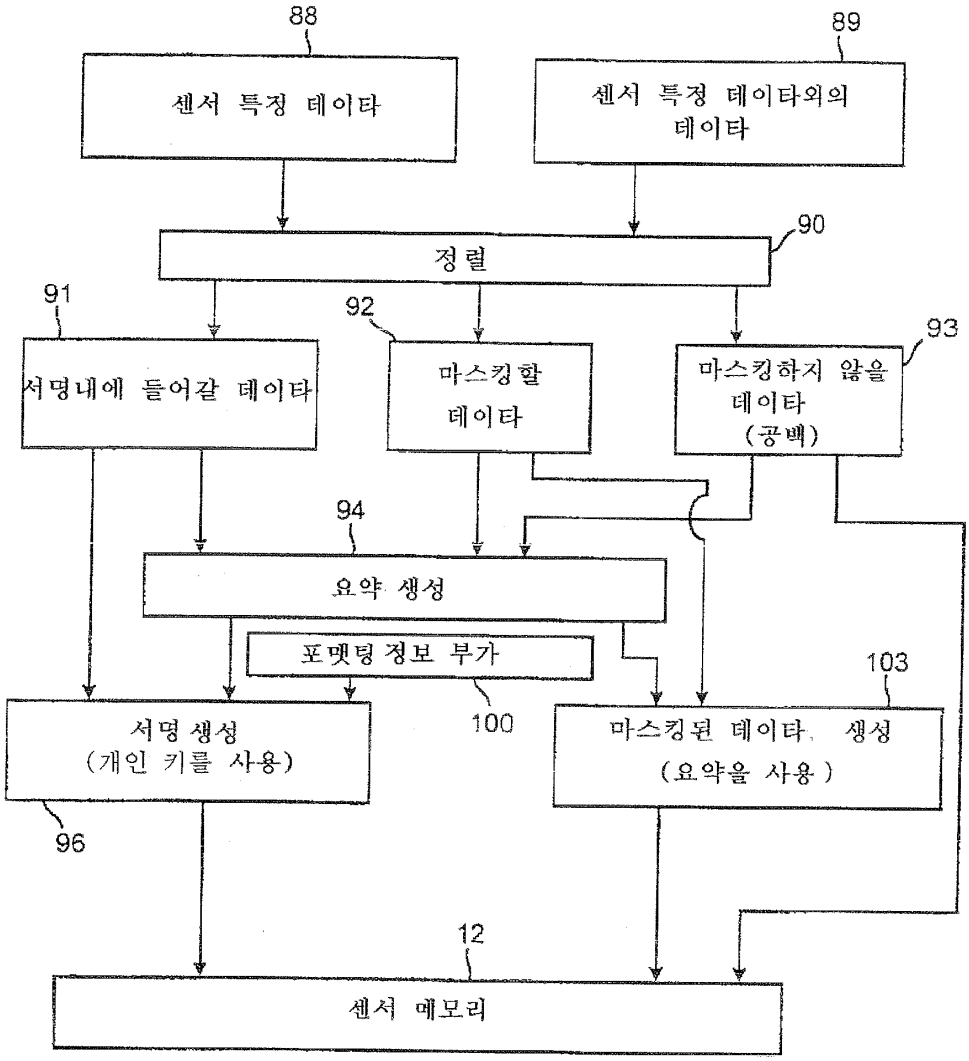
도면2


서명
60
마스킹된 부분(masked)
62
공백인-부분(clear)
64
보존된 부분(reserved)
기록될 수 있는 부분(writable)
66

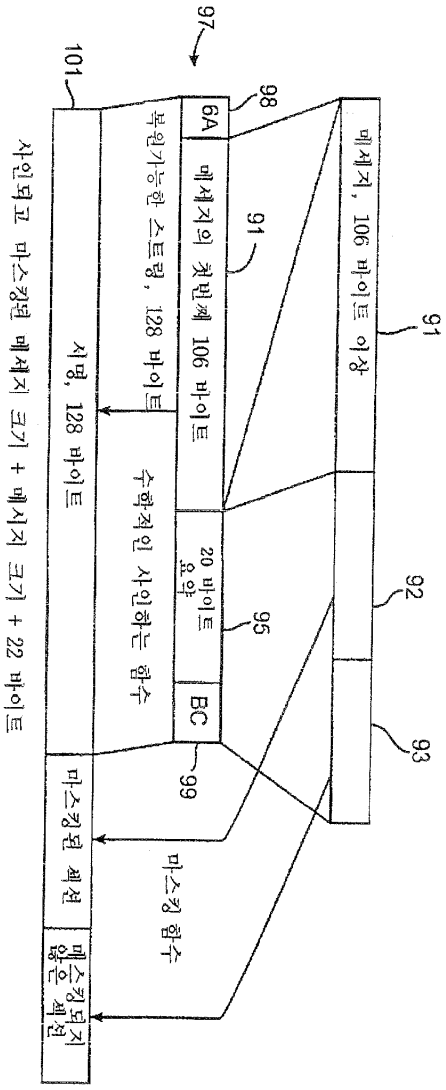
도면3


사인될 메세지
(≤106 BYTES)
서명 (128 BYTES)
70
PC
72
암호 보조 프로세서
(개인 키를 사용)
서명
(128 BYTES)
12
센서 메모리
86
마스킹된
공백
84
80
센서 특정 데이타
외의 데이타
82
센서 특정
데이타
76
센서
엘리먼트
78

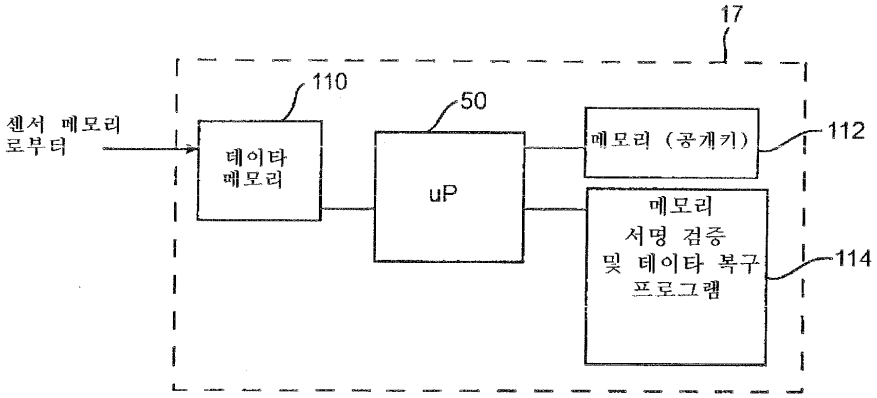
도면4


88
센서 특정 데이타
89
센서 특정 데이타외의 데이타
90
정렬
91
서명내에 들어갈 데이타
92
마스킹할 데이타
93
마스킹하지 않을 데이타 (공백)
94
요약 생성
포맷팅 정보 부가
100
103
서명 생성 (개인 키를 사용)
96
마스킹된 데이타 생성 (요약을 사용)
12
센서 메모리

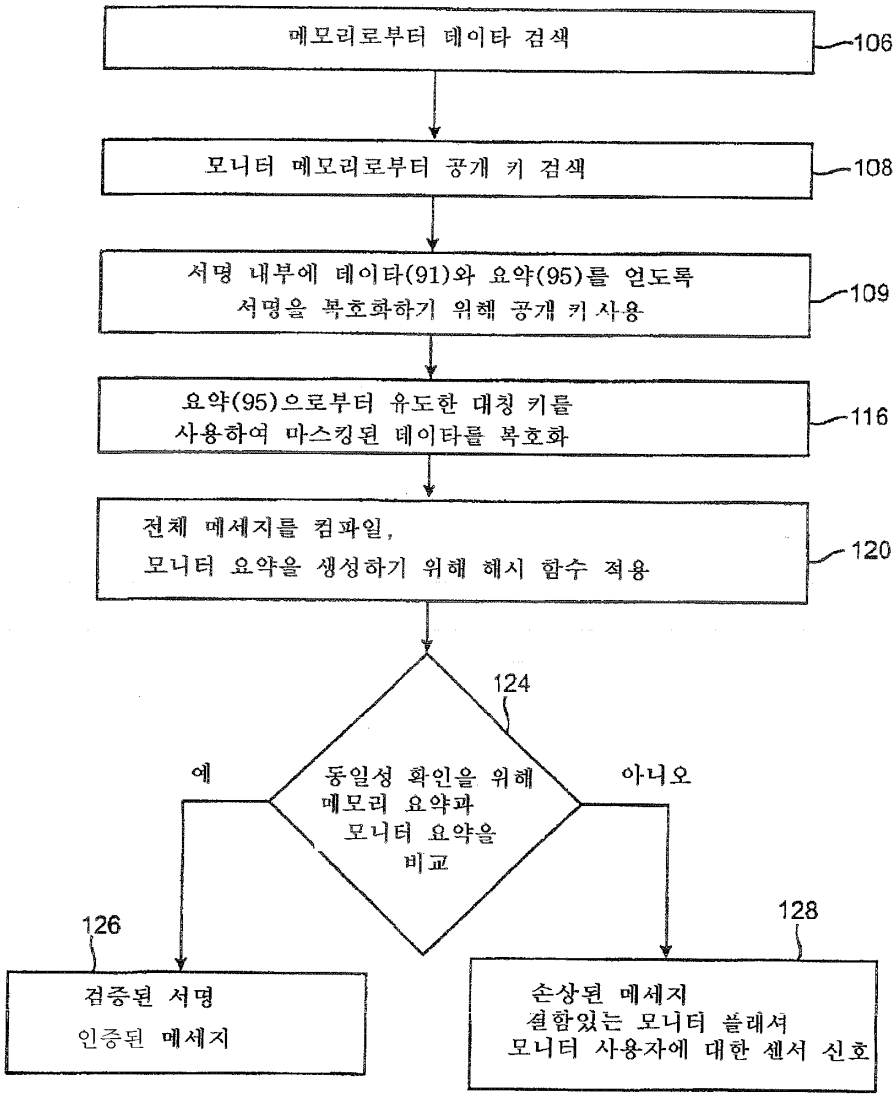
도면5


97
101
98
6A
복원가능한 스트링, 128 바이트
메세지의 첫번째 106 바이트
91
메세지, 106 바이트 이상
91
서명, 128 바이트
수학적인 사인하는 함수
20 바이트 요약
95
BC
92
93
99
마스킹된 섹션
매스킹되지 않은 섹션
마스킹 함수
사인되고 마스킹된 메세지 크기 + 메시지 크기 + 22 바이트

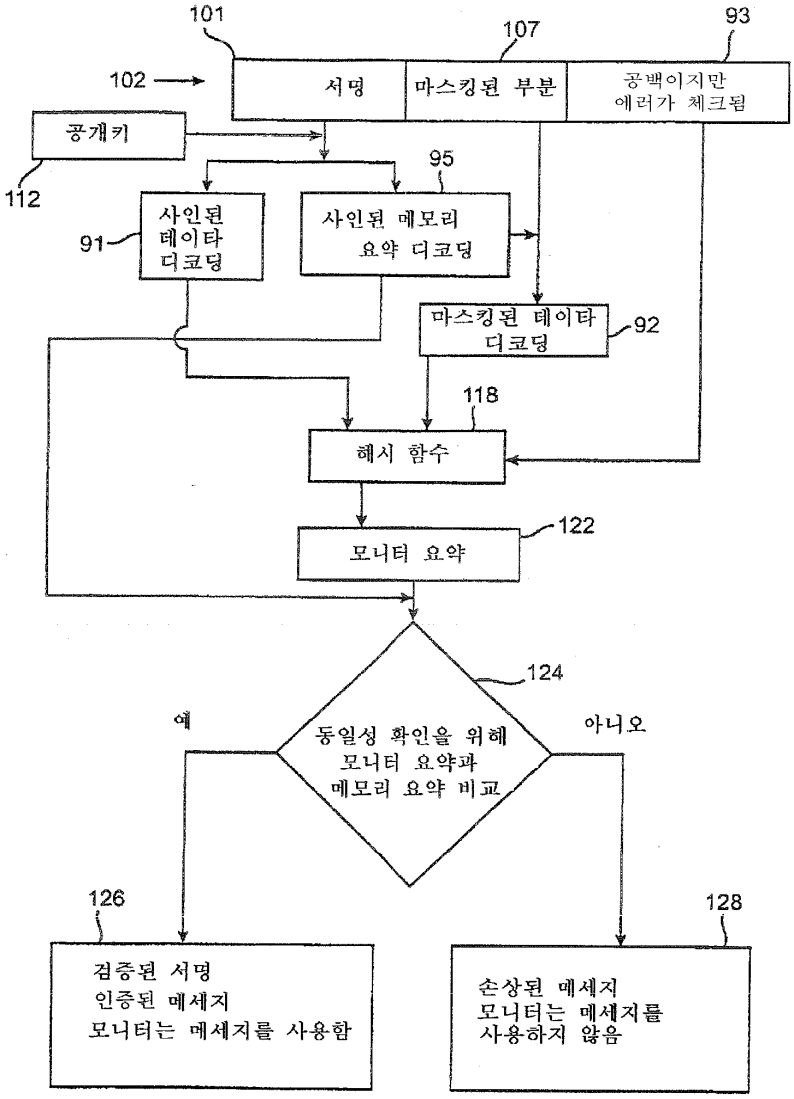
도면6


17
110
50
센서 메모리 로부터
데이타 메모리
uP
메모리 (공개키)
112
메모리 서명 검증 및 데이타 복구 프로그램
114

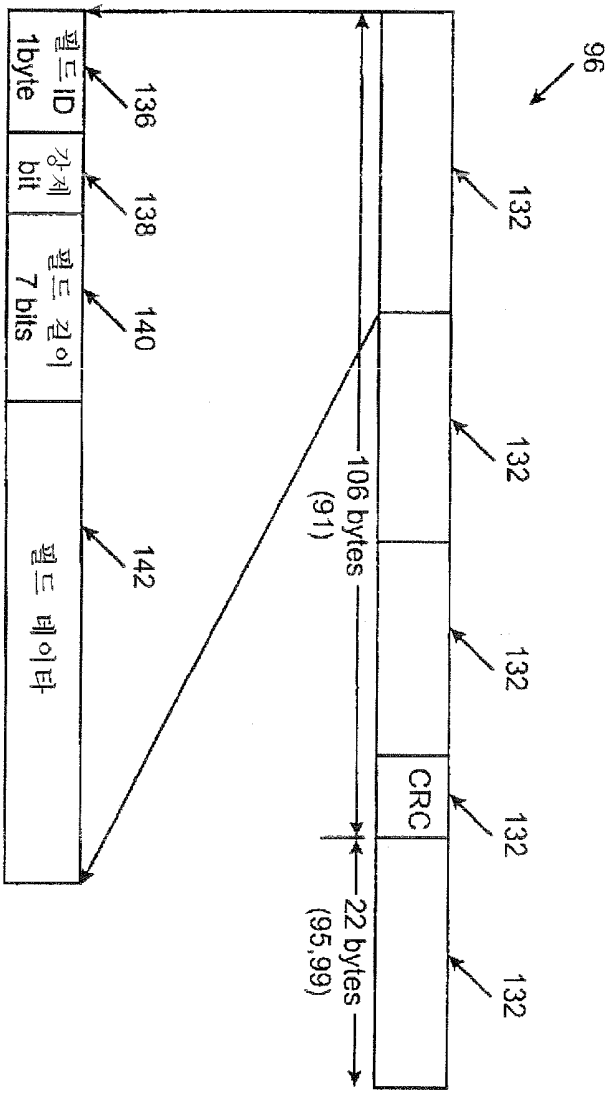
도면7


메모리로부터 데이타 검색
106
모니터 메모리로부터 공개 키 검색
108
서명 내부에 데이타(91)와 요약(95)를 얻도록
서명을 복호화하기 위해 공개 키 사용
109
요약(95)으로부터 유도한 대칭 키를
사용하여 마스킹된 데이타를 복호화
116
전체 메세지를 컴파일,
모니터 요약을 생성하기 위해 해시 함수 적용
120
124
동일성 확인을 위해
메모리 요약과
모니터 요약을
비교
예
아니오
126
검증된 서명
인증된 메세지
128
손상된 메세지
결함있는 모니터 플래셔
모니터 사용자에 대한 센서 신호

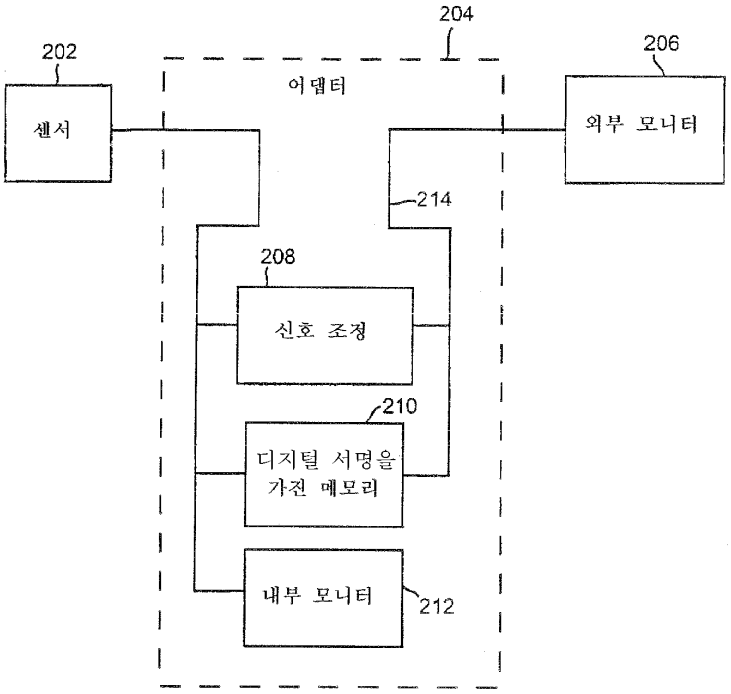
도면8


101
107
93
102
서명
마스킹된 부분
공백이지만
에러가 체크됨
공개키
112
95
91
사인된
데이타
디코딩
사인된 메모리
요약 디코딩
마스킹된 데이타
디코딩
92
118
해시 함수
122
모니터 요약
124
예
동일성 확인을 위해
모니터 요약과
메모리 요약 비교
아니오
126
검증된 서명
인증된 메세지
모니터는 메세지를 사용함
128
손상된 메세지
모니터는 메세지를
사용하지 않음

도면9


96
132
132
132
132
CRC
132
106 bytes
(91)
22 bytes
(95,99)
필드 ID
1byte
136
강제
bit
138
필드 길이
7 bits
140
필드 데이타
142

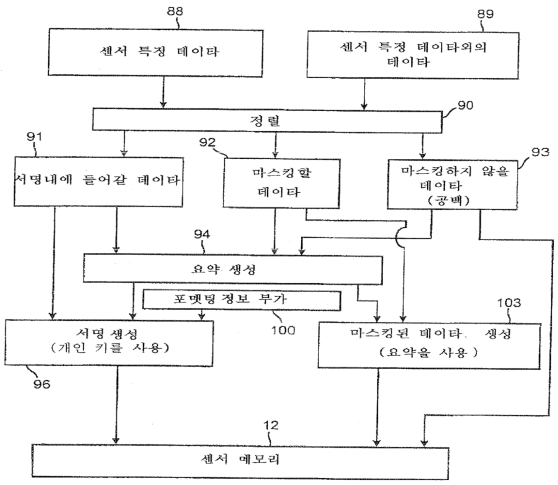
도면10


204
202
206
어댑터
센서
외부 모니터
214
208
신호 조정
210
디지털 서명을
가진 메모리
내부 모니터
212

专利名称(译)	具有与传感器相关的数据的数字签名的传感器		
公开(公告)号	KR100679762B1	公开(公告)日	2007-02-07
申请号	KR1020027004038	申请日	2000-09-28
[标]申请(专利权)人(译)	马林克罗特公司		
申请(专利权)人(译)	每天的大批量埃尔埃尔先生		
当前申请(专利权)人(译)	每天的大批量埃尔埃尔先生		
[标]发明人	BERSON THOMAS A 버슨토마스에이 OLSON BRYAN 올슨브라이언 FEIN MICHAEL E 페인마이클이 MANNHEIMER PAUL D 맨하이머폴디 PORGES CHARLES E 포제스찰스이 SCHLOEMER DAVID 쉬로머데이비드		
发明人	버슨,토마스,에이. 올슨,브라이언 페인,마이클,이. 맨하이머,폴,디. 포제스,찰스,이. 쉬로머,데이비드		
IPC分类号	A61B5/00 A61B5/145 A61B5/1455 G06F1/00 G06F12/14 G06F21/24 H04L9/32		
CPC分类号	A61B5/14551 A61B2562/08 G06F21/64 G06F2211/008 G06F2221/2107 H04L9/3247 H04L2209/805 A61B2562/085 G06F21/6209 H04L2209/88		
优先权	09/662246 2000-09-14 US 60/156488 1999-09-28 US		
其他公开文献	KR1020020064292A		
外部链接	Espacenet		

摘要(译)

前述内容为空，前述内容是说明性的，并且本发明的范围由以下权利要求限定。


88
센서 특정 데이타
89
센서 특정 데이타외의 데이타
90
정렬
91
서명내에 들어갈 데이타
92
마스킹할 데이타
93
마스킹하지 않을 데이타 (공백)
94
요약 생성
포맷팅 정보 부가
100
103
서명 생성 (개인 키를 사용)
96
마스킹된 데이타 생성 (요약을 사용)
12
센서 메모리