(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 특2000-0035093
(43) 공개일자 2000년06월26일

(51) 국제분류코드
H04L 9/00 (2006.01)

(21) 출원번호 10-1999-0047105

(22) 출원일자 1999년10월28일

(30) 우선권주장 9/182,342
1998년10월29일
미국(US)

(71) 출원인
데이텀 인크
미국 매사추세츠주 베드포드 미들섹스 턴파이크 54, 미국

(72) 발명자
하스팅스토마스마크
미국메사추세츠주02420렉싱톤메리암스트리트38, 미국
맥닐마이클이
미국캘리포니아주95018펠톤로스트아크레드라이브1271, 미국
글래시토드에스
미국캘리포니아주95066스코츠밸리블루보넷래인109에이, 미국
윌렛제랄드엘
미국메사추세츠주02148말덴#1하바드스트리트189, 미국

(74) 대리인
이상섭
나영환

(77) 심사관
없음

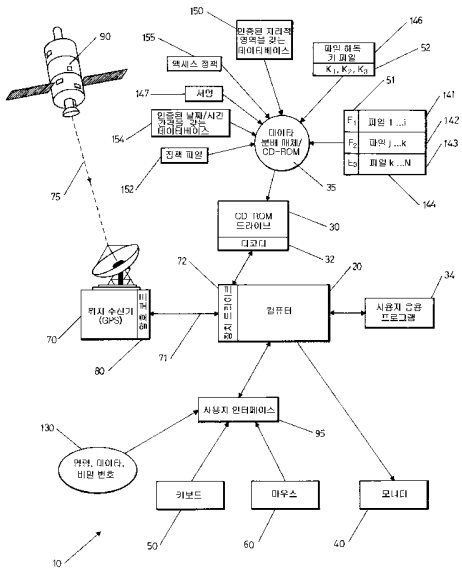
전체 청구항 수 : 총 28 항

(54)저장된 정보에 대한 액세스를 제어하는 방법 및 장치

(57)요 약

본 발명에 따르면, 사용자에 의해 저장된 정보의 액세스는 실제 지리적 위치 및/또는 실제 날짜/시간을 저장된 정보에 대한 액세스가 인증된 지리적 영역 및/또는 날짜/시간 간격과 비교함으로써 제어된다. 저장된 정보가 위치하는 실제 지리적 위치 및 실제 날짜/시간은, 예컨대 GPS 수신기와 같은 신뢰할 수 있는 위치 및 시간 정보를 제공하는 수신기에서 수신된 신호를 기초로 결정될 수 있다. 실제 지리적 위치 및/또는 날짜/시간이 인증된 지리적 및/또는 날짜/시간 간격 내에 있으면, 저장된 정보에 대한 액세스가 인증된다. 수신기에 의해 제공되는 그 위치 및 날짜/시간 정보는 암호적으로 서명되고 암호화될 수 있다.

대 표 도 - 도 2



청구의 범위

청구항 1

저장된 정보에 대한 액세스(access)를 제어하는 방법에 있어서,

신뢰할 수 있는 위치 정보를 제공하는 수신기에서 수신된 신호를 기초로 상기 저장된 정보가 위치하는 실제 지리적 위치를 결정하는 단계와,

상기 실제 지리적 위치와 상기 저장된 정보에 대한 액세스가 인증된 지리적 영역과를 서로 비교하는 단계와,

상기 실제 지리적 위치가 상기 인증된 지리적 영역 내에 위치하면 상기 저장된 정보에 대한 액세스를 허용하는 단계

를 포함하는 것을 특징으로 하는 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 2

제1항에 있어서, 상기 수신기는 GPS 수신기를 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 3

제1항에 있어서, 상기 정보는 컴퓨터로 판독 가능한 매체에 저장되는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 4

제3항에 있어서, 상기 컴퓨터로 판독 가능한 매체는 휴대 가능한 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 5

제3항에 있어서, 상기 컴퓨터로 판독 가능한 매체는 대용량 디스크를 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 6

제1항에 있어서, 상기 저장된 정보는 파일을 포함하며, 이 각 파일은 액세스가 허용되는 연관된 지리적 영역을 갖는 것으로서,

상기 실제 지리적 위치가 상기 파일에 대하여 상기 인증된 지리적 영역 내에 위치하면 그 파일에 대한 액세스를 허용하는 단계

를 더 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 7

제6항에 있어서, 상기 실제 지리적 위치가 상기 인증된 지리적 영역 내에 위치하지 않으면 상기 저장된 정보에 대한 액세스를 거부하는 단계

를 더 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 8

제1항에 있어서, 암호 키(encryption key)를 사용하여 상기 저장된 정보를 암호화하는 단계와,

상기 실제 지리적 위치가 상기 인증된 지리적 영역 내에 위치하면 상기 저장된 정보의 해독을 허용하는 해독 키를 제공하는 단계

를 더 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 9

제1항에 있어서, 상기 실제 지리적 위치를 수신기 암호 키로 암호적으로 서명하는 단계와,

그 실제 지리적 위치를 상기 인증된 지리적 영역과 비교하기 전에, 수신기 해독 키로 수신기 서명을 조회하는 단계

를 더 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 10

제1항에 있어서, 상기 저장된 정보는 정보의 부 세트(set)로 분할되며, 최소한 하나의 부 세트는 기타 부세트와는 상이한 인증된 영역을 갖는 것으로서, 인증된 지리적 영역이 실제 지리적 위치 내에 위치하는 부 세트에 대해서 액세스가 허가되지만, 인증된 지리적 영역이 실제 지리적 위치 내에 위치하지 않는 부 세트에 대해서는 액세스가 허용되지 않는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 11

제6항에 있어서, 상기 파일과 인증된 지리적 영역간의 연관 관계는 정책(policy) 파일로서 상기 저장된 정보와 함께 저장되는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 12

저장된 정보에 대한 액세스를 제어하는 장치에 있어서,

상기 저장된 정보가 위치하는 실제 지리적 위치를 결정하기 위하여 신뢰할 수 있는 위치 정보를 제공하는 수신기와,

상기 실제 지리적 위치를 상기 저장된 정보에 대한 액세스가 인증된 지리적 영역과 비교하는 컴퓨터

를 포함하는 것으로서,

상기 컴퓨터는 상기 실제 지리적 위치가 상기 인증된 지리적 영역 내에 위치할 때 상기 저장된 정보에 대한 액세스를 허용하는 것을 특징으로 하는 저장된 정보에 대한 액세스를 제어하는 장치.

청구항 13

제12항에 있어서, 상기 수신기는 GPS 수신기인 것인 저장된 정보에 대한 액세스를 제어하는 장치.

청구항 14

제12항에 있어서, 상기 수신기는 실제 지리적 위치를 암호적으로 서명하기 위한 수신기 암호 키를 제공하는 수신기 암호화 메카니즘을 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 장치.

청구항 15

제14항에 있어서, 상기 저장된 정보를 판독하는 판독기를 더 포함하는 것으로서, 이 판독기는 상기 암호적으로 서명된 실제 위치를 확인하기 위한 수신기 해독 키를 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 장치.

청구항 16

제15항에 있어서, 상기 판독기는 상기 수신기로 전송되어 실제 지리적 위치에 더해지는 위치 오프셋(offset)을 제공하는 초기화 벡터를 발생시키는 것인 저장된 정보에 대한 액세스를 제어하는 장치.

청구항 17

제16항에 있어서, 상기 위치 오프셋을 암호적으로 서명하기 위한 수신기 암호 키를 제공하는 수신기 암호화 메카니즘을 더 포함하는 것으로서, 그 위치 오프셋 서명은 위치 오프셋이 실제 지리적 위치에 더해지기 전에 수신기에 의해 해당 판독기 해독 키로 확인되는 것인 저장된 정보에 대한 액세스를 제어하는 장치.

청구항 18

저장된 정보의 더 큰 파일의 세트에 속하는 파일의 부 세트에 대한 액세스를 제어하는 방법에 있어서,

고유의 파일 암호 키를 상기 더 큰 파일의 세트로부터의 각 파일과 연관시키고 이 연관된 암호 키를 사용하여 그 파일을 암호화하는 단계와,

상기 더 큰 파일의 세트로부터의 각 파일을 상기 저장된 정보에 대한 액세스가 인증된 최소한 하나의 인증된 지리적 영역을 연관시키는 단계와,

신뢰할 수 있는 위치 정보를 제공하는 수신기에서 수신된 신호를 기초로 상기 저장된 정보가 위치하는 실제 지리적 위치를 결정하는 단계와,

상기 실제 지리적 위치와 상기 인증된 지리적 영역과를 서로 비교하는 단계와,

상기 실제 지리적 위치가 상기 파일의 부 세트에 속하는 파일에 대하여 인증된 지리적 영역에 위치할 때, 그 파일의 부 세트에 속하는 파일에 대한 액세스를 인증하고 그 파일의 해독을 허용하는 파일 해독 키를 제공하는 단계

를 포함하는 것을 특징으로 하는 저장된 정보의 더 큰 파일의 세트에 속하는 파일의 부 세트에 대한 액세스를 제어하는 방법.

청구항 19

제18항에 있어서, 상기 파일 및 인증된 지리적 영역간의 연관 관계는 정책 파일을 포함하는 정책으로서 저장되며, 인증된 지리적 영역 내에 위치하는 실제 지리적 위치가 그 파일과 연관될 때 각 정책 파일은 사용자 비밀 번호로 액세스 가능하고, 사용자 비밀 번호가 유효하다면 상기 정책 파일 내의 파일에 대한 액세스를 인증하는 것인 저장된 정보의 더 큰 파일의 세트에 속하는 파일의 부 세트에 대한 액세스를 제어하는 방법.

청구항 20

제19항에 있어서, 상기 정책은 저장된 정보와 함께 저장되는 것인 저장된 정보의 더 큰 파일의 세트에 속하는 파일의 부 세트에 대한 액세스를 제어하는 방법.

청구항 21

저장된 정보에 대한 액세스를 제어하는 방법에 있어서,

신뢰할 수 있는 시간 정보를 제공하는 수신기에서 수신된 신호를 기초로 상기 저장된 정보의 위치에서 실제 날짜 또는 시간을 결정하는 단계와,

상기 실제 날짜 또는 시간을 상기 저장된 정보에 대한 액세스가 인증된 소정의 날짜 또는 시간 간격과 비교하는 단계와,

상기 실제 날짜 또는 시간이 상기 인증된 날짜 또는 시간 간격 내에 있으면 상기 저장된 정보에 대한 액세스를 허용하는 단계

를 포함하는 것을 특징으로 하는 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 22

제21항에 있어서, 상기 실제 날짜 또는 시간이 상기 인증된 날짜 또는 시간 간격 내에 있지 않으면 상기 저장된 정보에 대한 액세스를 거부하는 단계

를 더 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 23

제21항에 있어서, 상기 정보는 파일을 포함하며, 이 각 파일은 액세스가 허용되는 연관되는 인증된 날짜 또는 시간 간격을 갖는 것으로서,

상기 실제 날짜 또는 시간이 상기 연관되는 인증된 날짜 또는 시간 간격 내에 있으면 상기 파일에 대한 액세스를 허용하는 단계

를 더 포함하는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 24

제21항에 있어서, 상기 저장된 정보는 정보의 부 세트로 분할되며, 최소한 하나의 부 세트는 기타 부 세트와는 상이한 인증된 날짜 또는 시간 간격을 갖는 것으로서, 인증된 날짜 또는 시간 간격이 실제 날짜 또는 시간 간격에 부합하는 부 세트에 대해서 액세스가 허가되지만, 인증된 날짜 또는 시간 간격이 실제 날짜 또는 시간 간격에 부합하지 않는 부 세트에 대해서는 액세스가 허용되지 않는 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 25

저장된 정보에 대한 액세스를 제어하는 방법에 있어서,

상기 정보를 인증된 지리적 영역 및 인증된 시간 간격과 연관시키는 정책을 형성하는 단계와,

상기 정책 및 정보를 암호적으로 서명하는 단계와,

상기 서명된 정책을 상기 서명된 정보와 함께 저장하는 단계와,

상기 정책을 해제하기 위한 비밀 번호를 제공하는 단계와,

신뢰할 수 있는 위치 정보를 제공하는 수신기에서 수신된 신호를 기초로 상기 저장된 정보가 위치하는 실제 지리적 위치를 결정하는 단계와,

실제 시간을 결정하는 단계와,

상기 실제 지리적 위치 및 실제 시간과 상기 정책의 인증된 지리적 영역 및 인증된 시간과를 서로 비교하는 단계와,

상기 실제 지리적 위치 및 실제 시간이 상기 정책의 인증된 지리적 영역 및 인증된 시간 간격 내에 있으면 상기 저장된 정보에 대한 액세스를 허용하는 단계

를 포함하는 것을 특징으로 하는 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 26

제1항에 있어서, 상기 신뢰할 수 있는 위치 및 시간의 소스(source)는 글로벌 궤도 순회 네비게이션 위성 시스템(Global Orbiting Navigation Satellite System)인 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 27

제1항에 있어서, 상기 신뢰할 수 있는 위치 및 시간의 소스는 관성 네비게이션 시스템인 것인 저장된 정보에 대한 액세스를 제어하는 방법.

청구항 28

제1항에 있어서, 상기 신뢰할 수 있는 위치 및 시간의 소스는 위성 기반형 위치 결정 시스템인 것인 저장된 정보에 대한 액세스를 제어하는 방법.

명세서

발명의 명칭

저장된 정보에 대한 액세스를 제어하는 방법 및 장치{CONTROLLING ACCESS TO STORED INFORMATION}

도면의 간단한 설명

도 1은 컴퓨터 시스템의 사시도.

도 2는 저장된 정보에 대한 액세스를 제어하는 컴퓨터 기반형 시스템의 블록도.

도 3은 각 파일이 서명 및 암호화되어 CD-ROM에 저장되는 단계를 설명하는 흐름도.

도 4는 본 발명에 따른 저장된 정보에 대한 액세스의 제어를 설명하는 흐름도.

도 5는 도 4의 레벨 1 및 레벨 2를 상세히 설명하는 흐름도.

도 6은 암호화 소자의 블록도.

도면의 주요 부분에 대한 부호의 설명

10 : 컴퓨터 시스템

20 : 컴퓨터

30 : CD-ROM 드라이브

40 : 모니터

50 : 키보드

60 : 마우스

70 : GPS 수신기

80 : 암호 보드

90 : GPS 위성

발명의 상세한 설명

본 발명은 저장된 정보에 대한 액세스의 제어에 관한 것이다.

CD-ROM과 같은 데이타 분배 매체는 많은 수의 파일을 저장할 수 있다. CD-ROM의 제작자는 보안상 또는 요금 청구의 문제 때문에 사용자에 의한 특정 파일에 대한 액세스의 제어를 소망할 수 있다.

사용자에게 CD-ROM 제작자로부터 얻은 비밀 번호의 입력을 요구함으로써 액세스를 제어할 수 있다. 상이한 비밀 번호는 상이한 파일 또는 상이한 파일의 부 세트(subset)를 해제할 수 있다. 파일은 암호적으로 서명될 수 있으며, 보안을 더욱 강화하기 위해 암호화될 수 있다. 본 명세서의 일부를 이루는

미국 특허 제5,646,992호에 개시된 방법에 있어서, 각 파일은 제작자에 의해 제작자만이 알고 있는 유일한 키(key)로 암호화된다. 사용자는 암호화된 항목을 수신하고, 그의 액세스에 대한 요청이 제작자에 의해 처리된 후에 개별적인 암호화 파일을 해독하는 데 사용되는 해독 키, 즉 비밀 번호를 수신한다. 그 비밀 번호는 액세스가 요청된 파일만을 해독한다.

통상적으로, 본 발명의 제1 특징에 따르면, 본 발명은 신뢰할 수 있는 위치 정보를 제공하는 수신기에서 수신된 신호를 기초로 저장된 정보가 위치하는 실제 지리적 위치를 결정함으로써 저장된 정보에 대한 액세스를 제어하는 것을 특징으로 한다. 그 다음, 그 실제 지리적 위치는 저장된 정보에 대한 액세스가 승인된 지리적 영역과 비교된다. 실제 지리적 위치가 승인된 지리적 영역 내에 위치한다면, 사용자에게는 저장된 정보에 대한 액세스가 허용된다.

본 발명의 실시예는 아래의 특징을 포함한다. 위치 정보를 제공하는 수신기는 위성 기반형 위치 판정 시스템 또는 관성 네비게이션(navigation) 시스템으로부터 위치 정보를 수신할 수 있다. 그 정보는 대용량 디스크와 같은 컴퓨터로 판독 가능한 매체에 기록될 수 있다. 저장된 정보는 파일을 포함하며, 이 각 파일은 액세스가 허용되는 연관된 지리적 영역을 갖는다. 실제 지리적 위치가 이 파일에 대한 승인된 지리적 영역 내에 위치하면, 사용자는 특정 파일 또는 파일들에 대한 액세스를 갖게 된다. 저장된 정보는 암호화될 수 있으며, 사용자는 실제 지리적 위치가 승인된 지리적 위치 내에 위치하면 해독 키에 대한 액세스를 갖게 된다. 또한, 저장된 정보는 정보의 부 세트로 분할되는데, 최소한 하나의 부 세트는 기타 부세트와 상이한 인증된 지역을 갖는다. 파일과 인증된 지리적 영역간의 연관 관계는 저장된 정보와 함께 정책(policy) 파일로서 저장될 수 있다.

통상적으로, 제2 특징에 따르면, 본 발명은 신뢰할 수 있는 시간 정보를 제공하는 수신기에서 수신된 신호를 기초로 저장된 정보의 위치에서의 실제 날짜 또는 시간을 결정한다. 실제 날짜 또는 시간은 저장된 정보에 대한 액세스가 인증되는 소정의 날짜 또는 시간 간격과 비교된다. 사용자는 실제 날짜 또는 시간이 인증된 날짜 또는 시간 간격 내에서 발생하면 저장된 정보를 액세스할 수 있다.

통상적으로, 제3 특징에 따르면, 본 발명은 저장된 정보가 위치하는 실제 지리적 위치를 결정하는 신뢰할 수 있는 위치 정보를 제공하는 수신기를 포함한다. 컴퓨터는 저장된 정보에 대한 액세스가 인증된 지리적 영역과 함께 위치 정보를 수신하고, 실제 지리적 위치가 인증된 지리적 영역 내에 위치하면 저장된 정보에 대한 액세스를 허용한다. 본 발명의 실시예는 아래의 특징을 포함한다. 수신기는 수신기 암호 키로 실제 지리적 위치를 암호적으로 서명하고 실제 지리적 위치가 인증된 지리적 영역과 비교되기 전에 수신기 해독 키로 수신기 서명을 조회하는 수신기 암호화 메카니즘을 포함한다.

통상적으로, 제4 특징에 따르면, 본 발명은 암호적으로 서명된 실제 위치를 조회하기 위한 해당 수신기 해독 키를 갖는 판독기를 포함한다.

본 발명의 실시예는 아래의 특징을 포함한다. 그 판독기는 수신기로 전송되어 실제 지리적 위치에 더해지는 위치 오프셋(offset)을 제공하는 초기화 벡터를 발생한다. 판독기는 판독기 암호 키로 그 위치 오프셋을 암호적으로 서명한다. 수신기는 위치 오프셋이 실제 지리적 위치에 더해지기 전에 해당 판독기 해독 키로 위치 오프셋 서명을 조회한다.

통상적으로, 제5 특징에 따르면, 본 발명은 정보를 인증된 지리적 영역 및 인증된 시간 간격과 연관시키는 정책을 형성하고 그 정책 및 정보를 암호적으로 서명하는 것을 특징으로 한다. 서명된 정책은 서명된 정보와 함께 저장된다. 사용자는 제조자로부터 정책을 해독하기 위한 비밀 번호를 얻고, 실제 지리적 위치 및 실제 시간이 그 정책의 인증된 지리적 영역 및 인증된 시간 간격 내에 있으면 저장된 정보에 대한 액세스를 얻는다.

본 발명의 장점은 아래의 하나 또는 그 이상의 것을 포함한다.

저장된 정보의 제조자는 지정된 지리적 영역 내로 그 정보의 사용을 제한할 수 있으며, 또한 그 사용이 허용되지 않는 지정된 영역을 차단할 수 있다. 예컨대, CD-ROM에 저장된 자동차에 대한 서비스 매뉴얼은 해당 특정 국가 및/또는 지역에 적용 가능한 상이한 정보의 부분을 포함할 수 있다. 사용자는 그의 현재 지리적 위치에 적용되는 정보의 부분만을 보도록 허용될 것이다. 이와 같이, 감응 통합 리포트에 대한 액세스는 특정 플랜트(plant) 위치로 제할될 수 있다. 시간 반응 정보에 대한 액세스는 특정 날짜 이전 또는 이후에 거부될 수 있으며 허용된 기간으로 제한될 수 있다. 인증된 지리적 영역 및 시간 간격에 관한 정보를 CD-ROM에 저장되고 사용자 비밀 번호로 액세스되는 정책 파일과 연관시킴으로써, CD-ROM 제조자는 사용자가 정책 파일의 특정 세트를 액세스하는 것을 허용하는 새로운 비밀 번호를 발행할 수 있으며, 따라서 해당 지역 및 날짜/시간에 대해 그 정보는 인증된다.

기타 장점 및 특징은 후술하는 설명 및 청구 범위로부터 명백해질 것이다.

도 1 내지 도 3에 도시된 바와 같이, 데이타 분배 매체(35)의 기능을 하는 컴퓨터로 기록 가능한 휴대용 CD-ROM에 저장된 정보에 대한 액세스는 정보가 액세스될 컴퓨터 시스템(10)의 실제 지리적 위치 및 정보가 액세스될 시간을 기초로 제어될 수 있다.

컴퓨터 시스템(10)에 있어서, 컴퓨터(20)는 키보드(50), 마우스(60), 모니터(40) 및 CD-ROM 드라이브(30)에 접속되어 있다. GPS 수신기(70)는 신뢰할 수 있는 위치 및 시간 정보의 소스(source)의 기능을 한다. 이 수신기(70)는 컴퓨터 시스템(10)의 실제 지리적 위치에 위치하며, 궤도상의 GPS 위성(90)(하나만이 도시됨)으로부터 신호(75)를 수신한다. 그 수신기(70)는 수신된 신호(75)를 경도, 위도 및 고도의 수 미터의 오차 내의 지리적 위치 데이타(71) 및 수 마이크로초의 오차 내의 날짜/시간 데이타(71)로 변환한다. 이 데이타(71)는 장치 드라이버(72)를 경유하여 컴퓨터(20)로 전달된다.

수신기 암호 보드(crypto-board)(80)는 도 6에 도시된 바와 같이 제조자에 의해 서명된 공중 키 인증(81) 및 해당 개인 키(82)를 포함할 수 있다. 따라서, 지리적 위치 및 날짜/시간 데이타(71)는 그 데이타의 진위 여부를 인증하기 위해 개인 키(82)로 서명될 수 있다.

또한, CD-ROM 드라이브(30)는 하드웨어 또는 소프트웨어 중 어느 하나로 구현될 수 있는 암호 및 서명 능력[디코더(decoder)(32)]을 포함할 수 있다. 이 디코더(32)는 도 6에 도시된 바와 같이 인증(81)과 동일한 암호 보드 공중 키 인증(83), 제조자의 신원을 조회하기 위한 제조자 인증(84) 및 제조자에 의해 서명된 분배 매체 정책 해독 키(86)를 포함한다. 암호 보드 인증(83)은 개인 키(82)로 서명된 암호 보드(80)의 서명을 조회한다. 정책 해독 키(86)는 CD-ROM(35)에 저장된 액세스 정책(155)을 해독한다.

컴퓨터 시스템(10)은 아래의 예에 설명된 레벨 1 및 레벨 2와 같은 몇몇 보안 레벨을 가질 수 있다.

보안 레벨 1의 시스템에서, 수신기(70)는 종래 장치 드라이버(72)를 통해 컴퓨터(20)와 통신하며, CD-ROM 드라이브(30)는 종래 CD-ROM이다. 수신기(70) 또는 CD-ROM 드라이브(30) 중 어느 것도 추가적인 암호화/해독 능력을 갖지 않는다. 강화된 보안 때문에, 레벨 1의 시스템의 컴퓨터(20)는 데이타를 인증 및/또는 암호화할 수 있는 "신뢰 받는" 컴퓨터가 될 수 있다. 레벨 2의 시스템의 한층 강화된 보안에서, 수신기(70)는 암호 보드(80)를 포함할 수 있으며, CD-ROM 드라이브(30)는 디코더(32)를 포함할 수 있다. 레벨 2의 시스템은 수신기(70) 및 디코더(32)간의 암호화된 데이타 전송 및 데이타 인증을 제공하도록 설계된다. 그러면, 컴퓨터(20)는 데이타 인증 및 암호화가 없는 임의의 통상의 컴퓨터가 될 수 있다.

키보드(50) 및 마우스(60)를 통해 입력된 데이타는 사용자 인터페이스(interface)(95)를 통해 입력되는 통상의 명령어 및 데이타 입력(130)[응용 프로그램(34)에 의해 제공됨] 및 사용자가 데이타 분배 매체(35)에 저장된 정보에 대한 액세스를 얻을 수 있도록 허용하는 하나 또는 그 이상의 비밀 번호(130)를 포함할 수 있다.

CD-ROM(35)은 정보(144)를 담은 파일, 인증된 지리적 영역의 목록(150), 인증된 날짜/시간 간격의 목록(154), 하나 또는 그 이상의 파일 해독 키 파일(146), 하나 또는 그 이상의 정책 파일(152) 및 전체 CD-ROM(35)에 대한 서명(147)과 같은 상이한 형태의 정보를 저장한다. 도 3에 도시된 바와 같이, 파일(144, 146, 150, 152, 154, 155)은 서명 및 암호화될 수 있다.

파일(144)은 부 세트(141, 142, 143)로 분류될 수 있다. 파일은 하나 이상의 부 세트에 속할 수 있다. 이하에서는, 파일은 파일 및 파일의 부 세트 둘 모두를 지칭하기로 한다. 각 파일(141, 142, 143)은 고유의 파일 암호 키(51)(E_1, E_2, E_3)로 암호화될 수 있다. 해당 파일 해독 키(52)(K_1, K_2, K_3)는 CD-ROM(35) 상에 파일 해독 키 파일(146)로 저장된다. 해독 키 및 해독 키 파일에 관한 추가적인 정보는 미국 특허 제5,464,992호에 개시되어 있다.

CD-ROM(35) 상의 각 파일(141, 142, 143)은 인증된 지리적 영역의 목록(150)에 저장된 0, 1 또는 그 이상의 인증된 지리적 영역과 연관되어 있다. 예컨대, 수신기가 뉴욕시의 엠파이어 스테이트 빌딩(Empire State Building) 내부의 어떠한 사무소 영역에 위치하고 있을 때 이 지역과 연관된 파일만이 오픈(open)되도록, 그 영역은 엠파이어 스테이트 빌딩의 넓이에 해당하는 위도 및 경도 및 50 미터 내지 60 미터의 고도에 의해 경계 지워질 수 있다.

마찬가지로, 각 파일(141, 142, 143)은 인증된 날짜/시간 간격의 목록(154)에 저장된 0, 1 또는 그 이상의 인증된 날짜/시간 간격과 연관될 수 있다.

각 GPS 위성(90)은 매우 정확한 시계를 보유한다. 수신기(70)는 신호(75)의 일부로서 GPS 시계 신호를 수신하거나, 또는 국부적인 원자 시계가 유사한 시계 신호를 제공할 수 있다. 시계 신호는 정보에 대한 액세스가 시도될 때 정확한 시간을 기초로 정보에 대한 액세스의 제어를 가능하게 한다. 예컨대, 제조자는 액세스가 (1) 소정의 날짜/시간 이전이나, (2) 소정의 날짜/시간 이후에만, 또는 (3) 소정의 날짜/시간 기간 동안에만 허용되도록 특정할 수 있다.

제조자는 사용자가 키보드(50)로 입력하는 비밀 번호(130)를 통해 파일(141, 142, 143)과 목록(150, 154) 내의 특정 항목을 연관시킬 수 있다. 그 비밀 번호(130)는 하나 이상의 액세스에 대해 유효한 사용자 비밀 번호이거나 1회용 비밀 번호일 수 있다. 이와 달리, 제조자는 정책 파일(152)을 통해 목록(150, 154)의 특정 지리적 영역/날짜/시간 정보와 파일(141, 142, 143)을 연관시킬 수 있다. 유효한 사용자 비밀 번호(130)는 하나 또는 그 이상의 정책 파일(152)을 해제할 수 있다. 사용자의 실제 지리적 위치 및 현재 날짜 및 시간이 사용자 비밀 번호(150)에 해당하는 인증된 지리적 영역 및 인증된 날짜/시간 내에 있으면, 사용자는 사용자 인터페이스(95)를 통해 선택된 파일을 액세스할 수 있다. 그 다음, 선택된 정보는 출력 장치(40)에 디스플레이된다.

예컨대, 표 1은 CD-ROM(35)에 저장되고 해당 인증된 지리적 영역 및 날짜/시간과 연관된 5 개의 암호화된 파일(A 내지 F)이 어떻게 액세스될 수 있는 지를 보여주고 있다. 각 파일은 4 개의 상이한 파일 해독 키(K1 내지 K4) 중 하나와 연관된다. L1 및 L2는 2 개의 상이한 인증된 지리적 영역이고, T1, T2 및 T3는 3 개의 상이한 인증된 날짜/시간 간격이다. 파일 해독 키(K1), 즉 비밀 번호를 소유하고 있는 사용자는 T1의 시간에서 L1 및 L3의 지리적 영역 내의 매뉴얼 A를 해독할 수 있다. 또한, 동일한 사용자는 동일한 T1의 시간에서 L2 및 L3의 영역(L1의 영역 제외)의 매뉴얼 D를 해독할 수 있다. 이와 같이, K2의 키를 사용하는 사용자는 동일하지 않은 시간에 L2의 영역 내의 이미지 B 및 이미지 E를 해독할 수 있다. 도면 C는 임의의 위치에서 K3의 키로 해독될수 있지만 T3의 시간에서만 가능하며, 사업 보고서 F는 K4의 키를 요구하며 임의의 시간에서 해독 될 수 있으나 L1의 영역 내에서만 가능하다.

암호화된 파일	파일 해독 키	인증된 지리적 영역	인증된 날짜/시간 간격
매뉴얼 A	K1	L1, L3	T1
이미지 B	K2	L2	T1, T3
도면 C	K3	--	T3

매뉴얼 D	K1	L2, L3	T1
이미지 E	K2	L2	T2
보고서 F	K4	L1	--

도 3에 도시된 바와 같이, 선택적인 암호화로 암호화 서명을 하기 위하여, 제조자는 CD-ROM(35) 상에 기록될 소스 파일(144')을 선택하고 인증된 지리적 영역(150')의 목록 및 인증된 날짜 및 시간 간격(154')의 목록을 특정한다. 제조자는 표 1에서와 같이 파일의 각 부 세트를 0, 1 또는 그 이상의 지리적 영역(150') 및 0, 1 또는 그 이상의 날짜/시간 간격(154')과 연관시키고 이 연관 관계를 정책 파일(152')에 저장한다. 각 파일(144', 150', 152', 154')은 단계(53, 340, 350, 360)에서 해당 각 암호키(51, 345, 355, 365)로 서명 및 암호화될 수 있다. 그 다음, 해당 암호화된 파일(150, 152, 154)은 서명되고 암호화된 지역/시간/파일 액세스 정책(155)으로서 CD-ROM(35)에 함께 저장된다. 전술한 바와 같이, CD-ROM(35)에는 서명된/암호화된 파일(144), 서명된/암호화된 대칭적 파일 해독 키 파일(146) 및 전체 CD-ROM(35)을 서명하도록 제조자에 의해 사용되는 서명(147)이 저장된다.

도 4 및 도 5에 도시된 바와 같이, 서명된/암호화된 파일(144)에 대한 액세스를 얻기 위해서, 사용자는 제조자로부터 비밀 번호를 얻고(도면 부호 400의 단계) 그 비밀 번호(130)를 키보드(50)로 입력시킨다(도면 부호 410의 단계). 비록 1 세션(session) 이상에 대해 유효한 사용자 비밀 번호를 사용할 수 있지만, 이 비밀 번호(130)는 1 회용으로 가정한다.

도 4에 도시된 바와 같이, 레벨 1 및 레벨 2에 대한 처리 흐름의 초기 부분은 거의 동일하다.

도면 부호 420의 단계에서 비밀 번호(130)가 조회되고, 그 다음 시스템 구성에 따라 도면 부호 440의 단계(추가적인 보안이 없는 레벨 1) 또는 도면 부호 450의 단계(수신기/CD-ROM 드라이브 보안이 있는 레벨 2) 중 어느 하나의 처리가 수행된다. 도면 부호 440 및 450의 단계는 도 5에 보다 상세하게 나타나 있으며, 이제 이에 대해 설명한다.

도 5에 도시된 바와 같이, 도면 부호 440의 처리 단계에서 사용자 비밀 번호(130)는 장치 드라이버(72)로 전송된다(도면 부호 510의 단계). 1 회용 비밀 번호(130)에 응답하여, 장치 드라이버(72)는 사용자 비밀 번호(130)로부터 자신의 1 회용 비밀 번호를 발생시키고(도면 부호 520의 단계), 사용자가 올바른 1 회용 비밀 번호(130)를 제대로 입력했는 지를 확인하여(도면 부호 530의 단계), 대화형 세션에 대한 사용자를 인증한다(도면 부호 532의 단계). 비밀 번호가 유효하지 않으면, 액세스는 거부된다(도면 부호 535의 단계).

일단 비밀 번호(130)가 사용자를 인증하면, 장치 드라이버(72)는 현재 위치 및 날짜/시간에 대해 수신기(70)에 질문 신호를 보낸다(도면 부호 540의 단계). 그 다음, 장치 드라이버(72)는 수신기(70)에 의해 복귀된 시간 및 위치 데이타를 파일(144) 또는 파일의 부 세트(141, 142, 143)에 적용하는 정책(155)과 비교한다(도면 부호 460의 단계). 사용자가 파일(144)을 액세스하도록 인증되면, 데이타는 해제되고(도 4의 도면 부호 470의 단계), 해독 키(52)로 해독되어(도면 부호 480의 단계), 사용자 응용 프로그램(34)에 제공 및 디스플레이된다(도면 부호 490의 단계).

레벨 2의 시스템에서, 수신기(70)는 암호화 수신기 보드(80)(이하에서는 "암호 보드"라고 지칭함)를 포함한다. 전술한 바와 같이, 암호 보드(80)는 메시지를 서명 및 암호화/해독할 수 있다. CD-ROM 드라이브(30)는 암호 보드(80)에 의해 서명되고 그로부터 수신된 위치 데이타를 디코딩하는 디코더(32)를 포함한다.

도 5에 도시된 바와 같이, 도면 부호 450의 단계에서 사용자 비밀 번호(130)는 이 비밀 번호(130)를 수신하여 이를 변경되지 않은 상태로 디코더(32)에 전달하는 장치 드라이버(72)로 전송된다(도면 부호 550의 단계). 그 다음, 이 드라이버(32)는 내부적으로 개인 키(86)로 사용자 비밀 번호에 해당하는 그 자신의 1 회용 비밀 번호를 발생시키고(도면 부호 560의 단계) 올바른 비밀 번호(130)가 장치 드라이

버(72)에 의해 통신되었는 지를 확인하여(도면 부호 570의 단계), 대화형 세션에 대한 사용자를 인증한다(도면 부호 572의 단계). 비밀 번호가 유효하지 않으면, 액세스는 거부된다(도면 부호 575의 단계).

일단 암호 회로(32)가 사용자를 인증하면, 드라이버(32)는 장치 드라이버(72)를 거쳐 암호 보드(80)에 수신기(70)로부터의 현재 시간 및 위치 정보에 대한 질문 신호를 보낸다(도면 부호 580의 단계). 디코더 유닛(30)은 "초기화 벡터", 즉 위치 오프셋을 형성하도록 암호 보드(80)에 서명된 임의의 또는 기타 비트 패턴을 제공하는데(도면 부호 580의 단계), 장치 드라이버(72)는 상기 초기화 벡터를 시간 및 위치에 대한 요구에 따라 암호 보드(80)로 전달한다(도면 부호 590의 단계).

암호 보드(80)는 현재 시간 및 경도 및 위도 그리고 고도 내의 실제 지리적 위치를 포함하는 미리 형성된 데이타 포맷에 따라 패킷(packet)을 준비함으로써 응답한다(도면 부호 600의 단계). 또한, 상기 미리 형성된 데이타 포맷에는 위성이 위치 데이타 및 기타 계산에 필요한 데이타를 전송하는 것을 확인하는 정보가 포함될 수 있다. 또한, 암호 보드(80)는 상기 제공된 초기화 벡터를 상기 패킷 내의 알려진 오프셋에 저장하고, 암호화 서명을 그 패킷의 내용에 적용한다. 예컨대, 그 암호화 서명은 패킷 데이타의 메시지 다이제스트(digest)/해쉬(hash)에 일부 소정의 키에 따른 메시지 다이제스트의 암호화를 더한 것일 수 있으며, 암호 보드(80) 상에 저장된 키 또는 인증에 따라 대칭 또는 비대칭일 수 있다.

그 다음, 암호 보드(80)는 서명된 시간/위치 패킷을 그 패킷을 디코더(32)/CD-ROM 드라이브(30)에 중계하는 장치 드라이버(72)에 전송한다. 디코더(32)는 암호 보드(80)로부터 수신된 패킷의 서명을 디코더(32)에 저장된 서명과 비교한다(도면 부호 610의 단계). 그 서명이 적절히 확인되면(도면 부호 620의 단계), 패킷 내의 초기화 벡터는 이 초기화 벡터가 디코더(32)가 암호 도면 부호 590의 단계에서 암호 보드(80)에 제공한 초기화 벡터와 동일한 지를 판정하도록 검사된다. 만약 동일하다면, 디코더(32)에 의해 수신된 패킷은 최근의 것이고 참된 것이며, 시간 및 위치 데이타는 유효한 것으로 받아들여 진다.

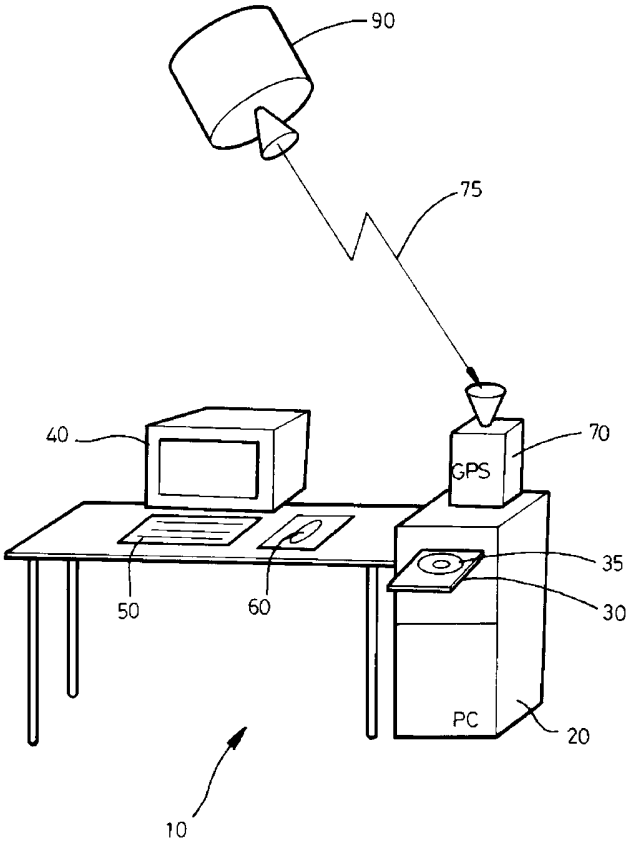
일단 암호 보드(80)로부터의 패킷이 서명 및 초기화 벡터를 기초로 인증되면, 디코더(32)는 암호 보드(80)로부터 수신된 시간 및 위치 데이타를 파일(144) 또는 파일(144)의 부 세트에 적용시키는 정책과 비교한다(도면 부호 460의 단계). 사용자가 파일(144)을 액세스하도록 인증되면, 데이타는 해제되고(도면 부호 470의 단계), 해독 키(52)로 해독되며(도면 부호 480의 단계), 사용자 응용 프로그램에 제공되어 디스플레이된다(도면 부호 490의 단계).

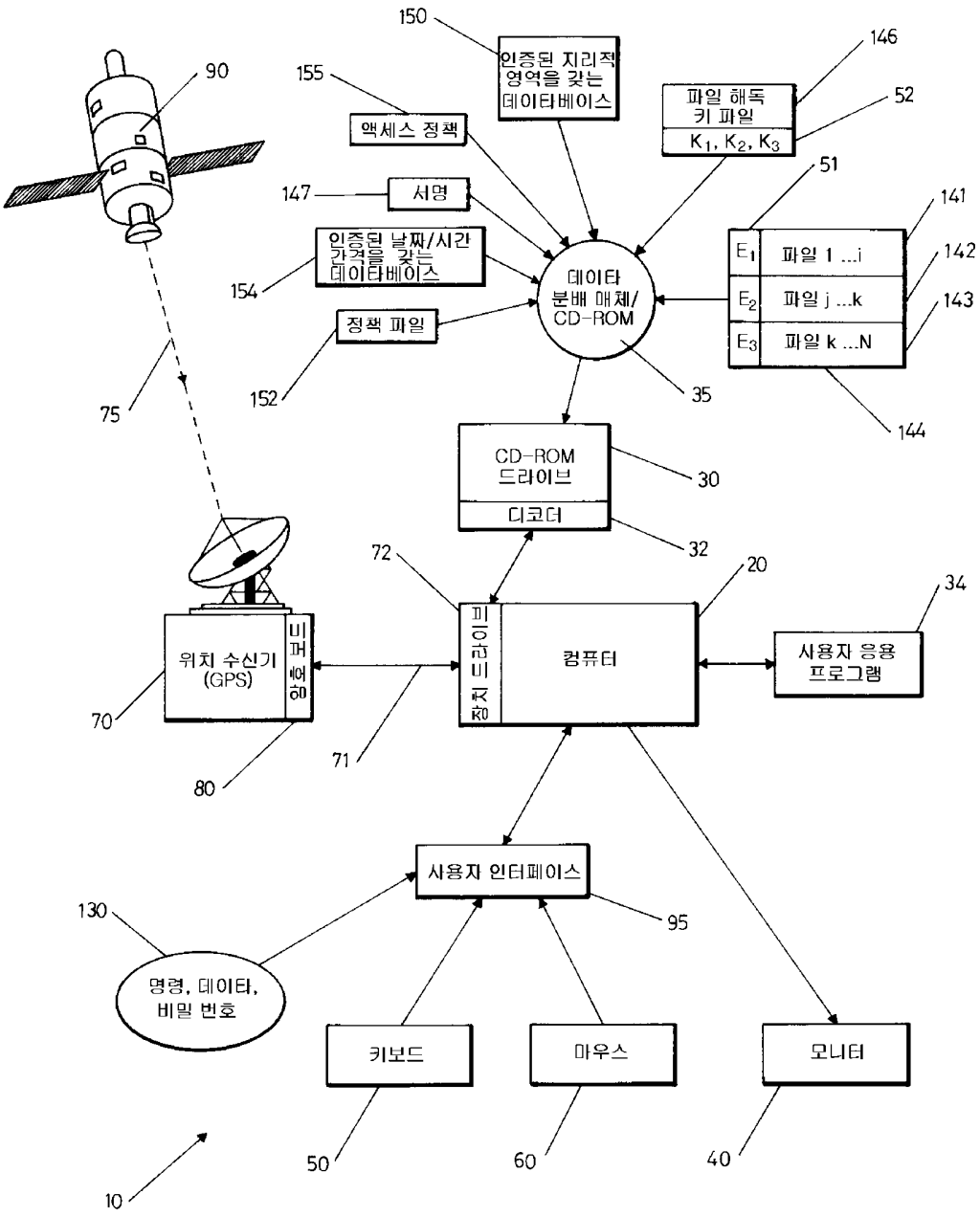
기타 실시예는 아래의 청구 범위 내에 속한다. 예컨대, GPS 수신기는 데이타 분배 매체 판독기의 정확한 위치에 위치할 필요는 없으나, 판독기와 관련된 알려진 위치(빌딩 내의 LAN에 컴퓨터 서비스를 제공하는 제어 서버를 포함하는 방과 같은 위치)에 있을 수 있다.

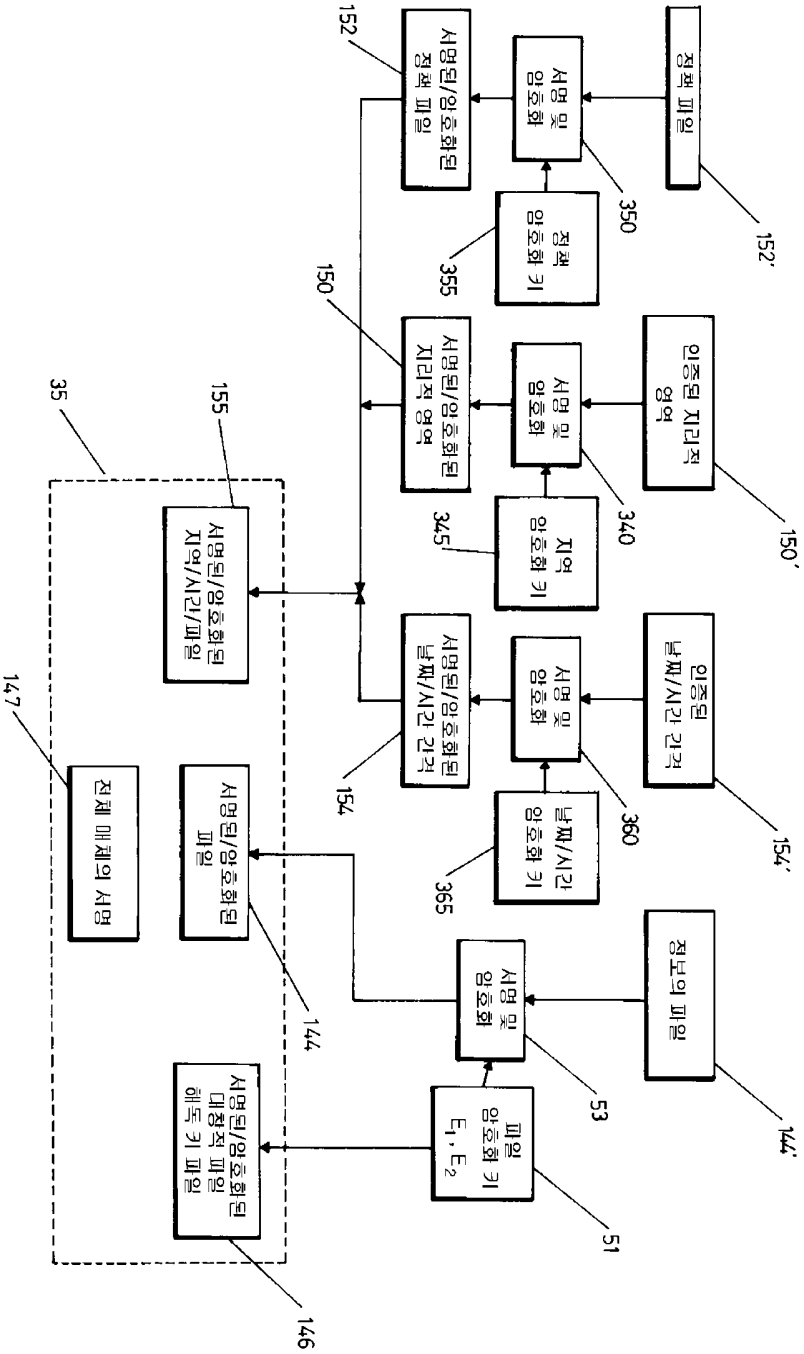
또한, 정책 파일(152')은 특정 파일(144)에 대한 액세스가 거부된 지리적 영역을 지정할 수 있다.

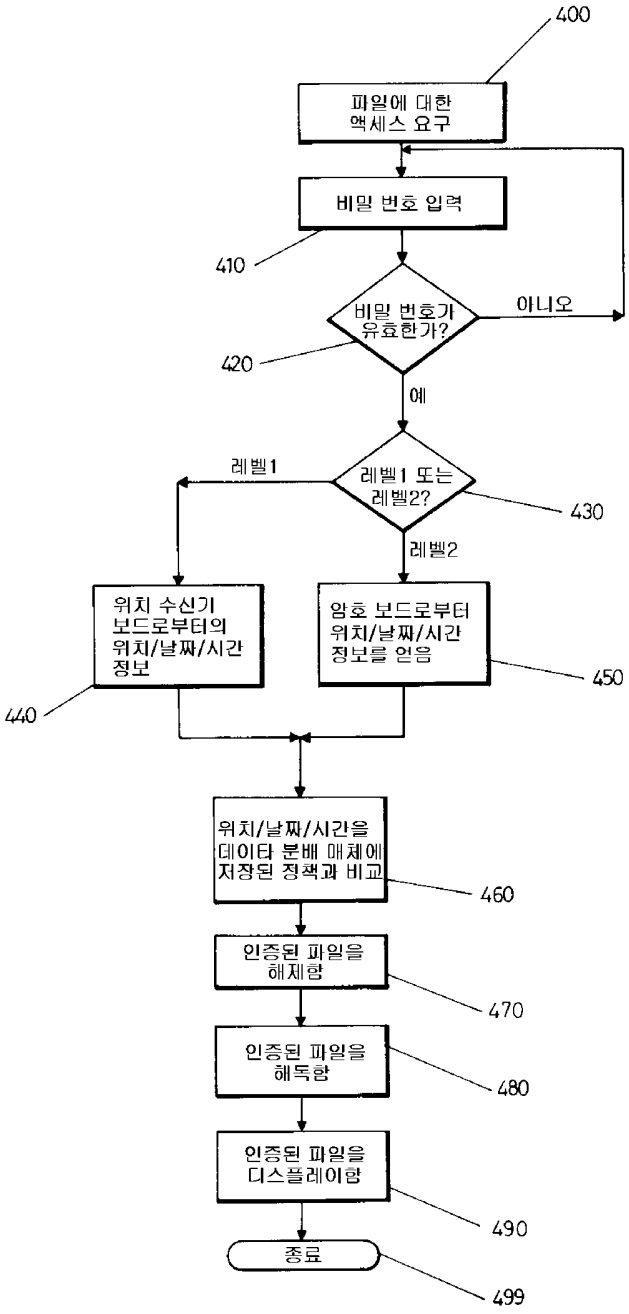
파일의 액세스에 대한 제어는 제작자에 의해 제공되고 키보드를 통해 입력된 비밀 번호를 사용하는 것에 제한되지 않는다. 비밀 번호를 대신하여 또는 이에 부가하여, 예컨대 얼굴 형상, 지문 및/또는 성문(聲紋)과 같은 특정 생물 측정의 특성을 사용할 수 있다.

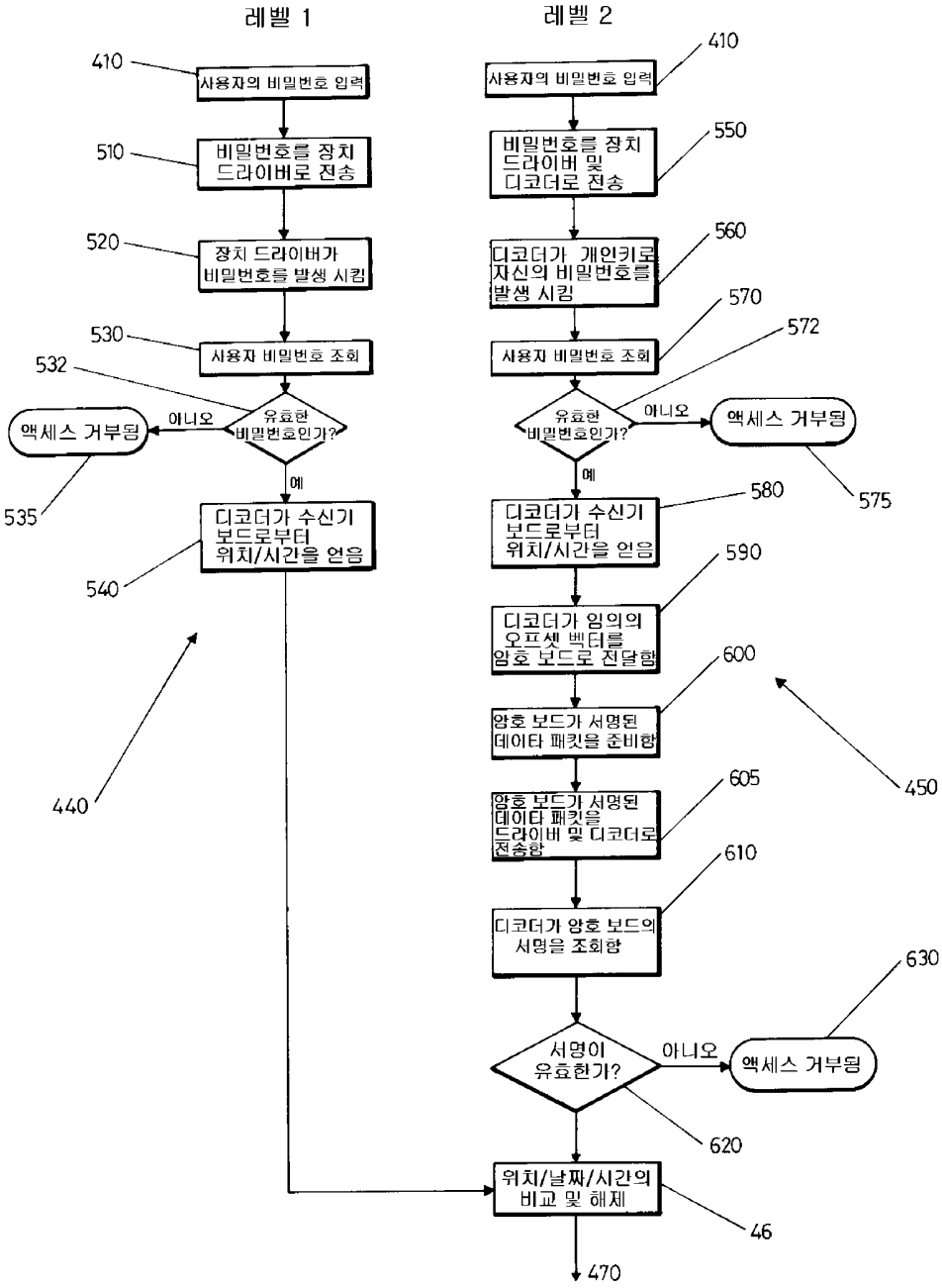
본 발명에 따라 저장된 정보에 대한 액세스를 제어하면, 저장된 정보의 제조자는 그 정보의 사용을 지정된 지리적 영역 내로 제한할 수 있거나 그 사용이 허용되지 않는 지정된 영역을 차단할 수 있다. 또한, 시간 반응 정보에 대한 액세스는 특정 날짜 이전 또는 이후에 거부될 수 있으며 허용된 기간으로 제한될 수 있다. 인증된 지리적 영역 및 시간 간격에 관한 정보를 CD-ROM에 저장되고 사용자 비밀 번호로 액세스되는 정책 파일과 연관시킴으로써, CD-ROM 제조자는 사용자가 정책 파일의 특정 세트를 액세스하는 것을 허용하는 새로운 비밀 번호를 발행할 수 있으며, 따라서 해당 지역 및 날짜/시간에 대해 그 정보는 인증되게 된다.

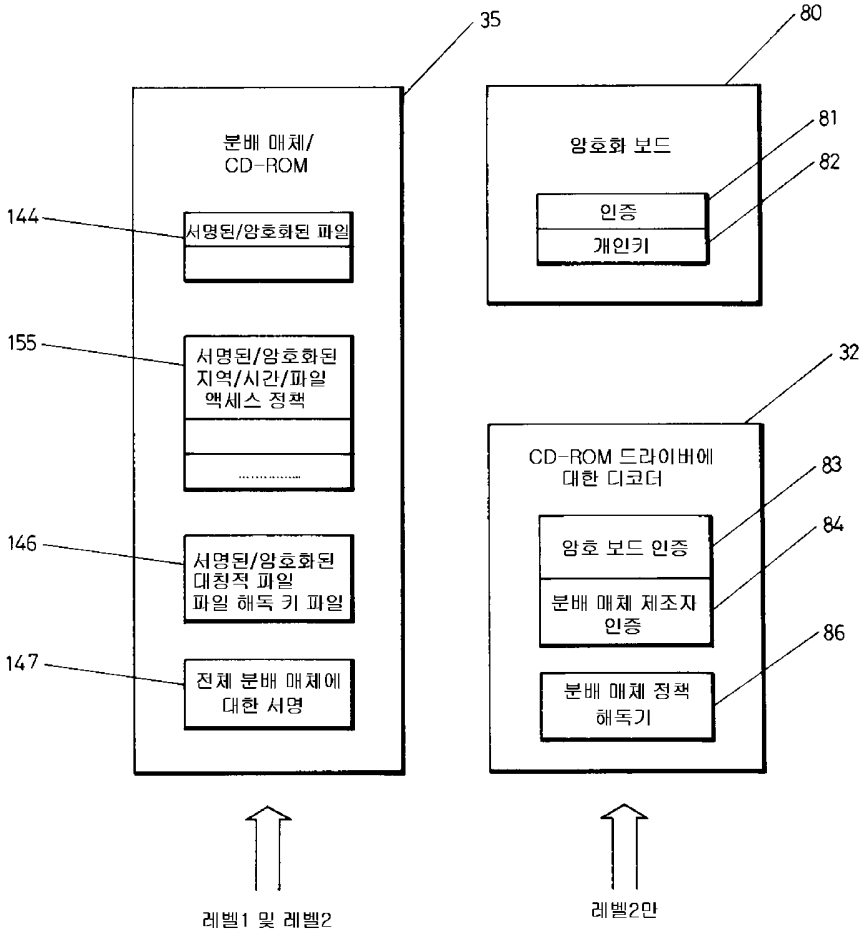

90
75
40
70
GPS
35
30
50
60
PC
20
10


150
인증된 지리적 영역을 갖는 데이터베이스
146
파일 해독 키 파일
K_1, K_2, K_3
52
155
액세스 정책
90
147
서명
51
141
인증된 날짜/시간 가격을 갖는 데이터베이스
154
데이터 분배 매체/ CD-ROM
E_1 파일 1 ...i
142
E_2 파일 j ...k
143
E_3 파일 k ...N
정책 파일
152
35
144
75
CD-ROM 드라이브
30
디코더
32
72
20
34
위치 수신기 (GPS)
안테나
컴퓨터
사용자 응용 프로그램
I/O 장치 드라이버
70
71
80
사용자 인터페이스
130
95
명령, 데이터, 비밀 번호
키보드
마우스
모니터
50
60
40
10


정책 파일
152'
서명 및 암호화
350
정책 암호화 키
355
서명된/암호화된 정책 파일
152
인증된 지리적 영역
150'
서명 및 암호화
340
지역 암호화 키
345'
서명된/암호화된 지리적 영역
150
인증된 날짜/시간 간격
154'
서명 및 암호화
360
날짜/시간 암호화 키
365
서명된/암호화된 날짜/시간 간격
154
정보의 파일
144'
서명 및 암호화
53
파일 암호화 키 E_1, E_2
51
35
서명된/암호화된 지역/시간/파일
155
서명된/암호화된 파일
144
서명된/암호화된 대칭적 파일 해독 키 파일
146
전체 매체의 서명
147


400
파일에 대한 액세스 요구
비밀 번호 입력
410
비밀 번호가 유효한가?
420
아니오
예
레벨1
레벨1 또는 레벨2?
430
레벨2
위치 수신기 보드로부터의 위치/날짜/시간 정보
440
암호 보드로부터 위치/날짜/시간 정보를 얻음
450
위치/날짜/시간을 데이타 분배 매체에 저장된 정책과 비교
460
인증된 파일을 해제함
470
인증된 파일을 해독함
480
인증된 파일을 디스플레이함
490
종료
499


레벨 1
레벨 2
410
사용자의 비밀번호 입력
510
비밀번호를 장치 드라이버로 전송
520
장치 드라이버가 비밀번호를 발생 시킴
530
사용자 비밀번호 조회
532
유효한 비밀번호인가?
아니오
액세스 거부됨
535
예
디코더가 수신기 보드로부터 위치/시간을 얻음
540
440
410
사용자의 비밀번호 입력
550
비밀번호를 장치 드라이버 및 디코더로 전송
560
디코더가 개인키로 자신의 비밀번호를 발생 시킴
570
572
사용자 비밀번호 조회
유효한 비밀번호인가?
아니오
액세스 거부됨
575
예
580
디코더가 수신기 보드로부터 위치/시간을 얻음
590
디코더가 임의의 오프셋 벡터를 암호 보드로 전달함
600
암호 보드가 서명된 데이타 패킷을 준비함
450
605
암호 보드가 서명된 데이타 패킷을 드라이버 및 디코더로 전송함
610
디코더가 암호 보드의 서명을 조회함
630
서명이 유효한가?
아니오
액세스 거부됨
620
위치/날짜/시간의 비교 및 해제
46
470


35
분배 매체/
CD-ROM
144
서명된/암호화된 파일
155
서명된/암호화된
지역/시간/파일
액세스 정책
146
서명된/암호화된
대칭적 파일
파일 해독 키 파일
147
전체 분배 매체에
대한 서명
80
암호화 보드
81
82
인증
개인키
32
CD-ROM 드라이버에
대한 디코더
83
84
86
암호 보드 인증
분배 매체 제조자
인증
분배 매체 정책
해독기
레벨1 및 레벨2
레벨2만