(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년06월05일
(11) 등록번호 10-0834758
(24) 등록일자 2008년05월28일

(51) Int. Cl.
G06F 21/00 (2006.01) *G06F 21/22* (2006.01)
(21) 출원번호 10-2006-0063150
(22) 출원일자 2006년07월05일
심사청구일자 2006년07월05일
(65) 공개번호 10-2008-0004309
(43) 공개일자 2008년01월09일
(56) 선행기술조사문헌
KR1020030041658 A*
KR1020060014654 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성전자주식회사
경기도 수원시 영통구 매탄동 416
(72) 발명자
김명호
경기 화성시 반월동 현대아파트 202동 901호
이광용
경기 수원시 영통구 영통동 벽적골8단지아파트 823동 1504호
(뒷면에 계속)
(74) 대리인
정상빈, 특허법인가산

전체 청구항 수 : 총 18 항 심사관 : 노영철

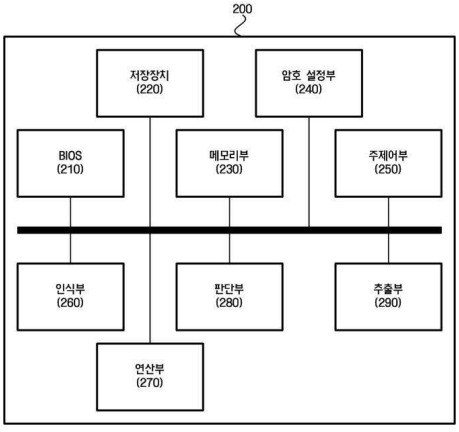
(54) 컴퓨터 시스템 보안 장치 및 방법

(57) 요 약

컴퓨터 시스템 도난시, 컴퓨터 시스템 및 상기 컴퓨터 시스템에 포함되어 있는 하드디스크에 저장되어 있는 데이터가 타인에 이해 오용되는 것을 방지할 수 있는 컴퓨터 시스템 보안 장치 및 방법이 제공된다.

본 발명의 실시예에 따른 컴퓨터 시스템 보안 장치는, 사용자 식별 정보를 인식하기 위한 인식부, 상기 인식된 사용자 식별 정보, 컴퓨터 시스템의 주변기기에 대한 고유 식별 정보, 및 상기 컴퓨터 시스템의 고유 식별 정보를 입력값으로 하는 소정 연산을 수행하여 결과값을 산출하는 연산부, 및 상기 컴퓨터 시스템에 대하여 기설정되어 있는 암호와 상기 산출된 결과값과의 일치 여부에 따라 상기 컴퓨터 시스템의 부팅을 수행하는 주제어부를 포함한다.

대표도 - 도2



(72) 발명자

조성현

서울 서초구 서초4동 서초래미안아파트 110동 801호

김태수

서울 서초구 서초4동 서초래미안아파트 101-1203

이상진

경기 수원시 영통구 매탄동 우남퍼스트빌 207동 1604호

이천무

경기 용인시 기흥구 보정동 포스홈타운아파트 212동 1702호

김은경

경기 성남시 분당구 이매동 아름마을건영아파트 112동 1104호

김수영

서울 성동구 용답동 170-5호 11/4

특허청구의 범위

청구항 1

사용자 식별 정보를 인식하기 위한 인식부;

상기 인식된 사용자 식별 정보, 컴퓨터 시스템의 주변기기에 대한 고유 식별 정보, 및 상기 컴퓨터 시스템의 고유 식별 정보를 입력값으로 하는 소정 연산을 수행하여 결과값을 산출하는 연산부; 및

상기 컴퓨터 시스템에 대하여 기설정되어 있는 암호와 상기 산출된 결과값과의 일치 여부에 따라 상기 컴퓨터 시스템의 부팅을 수행하는 주제어부를 포함하는 컴퓨터 시스템 보안 장치.

청구항 2

제 1 항에 있어서,

상기 컴퓨터 시스템의 고유 식별 정보는, 상기 컴퓨터 시스템의 시리얼 넘버인 컴퓨터 시스템 보안 장치.

청구항 3

삭제

청구항 4

제 1 항에 있어서,

상기 주변기기는 하드디스크이며, 상기 주변기기의 고유 식별 정보는, 상기 주변기기의 시리얼 넘버인 컴퓨터 시스템 보안 장치.

청구항 5

제 1 항에 있어서,

상기 사용자 식별 정보가 기록된 RFID 태그를 더 포함하는 컴퓨터 시스템 보안 장치.

청구항 6

제 1 항에 있어서,

상기 인식부는, 상기 사용자 식별 정보가 기록된 RFID 태그로부터 상기 사용자 식별 정보를 수신하는 RFID 리더인 컴퓨터 시스템 보안 장치.

청구항 7

제 1 항에 있어서,

상기 사용자 식별 정보는, 상기 사용자의 생체 정보인 컴퓨터 시스템 보안 장치.

청구항 8

제 1 항에 있어서,

상기 인식부는,

상기 사용자의 식별 정보로서 상기 사용자의 생체 정보를 입력받는 입력부; 및

상기 입력받은 생체 정보와 기저장되어 있는 생체 정보의 일치율이 소정 임계값 이상인 경우, 상기 사용자를 허가된 사용자로 판별하여, 상기 허가된 사용자에 대한 사용자 식별 정보를 출력하는 사용자 식별 정보 출력부를 포함하는 컴퓨터 시스템 보안 장치.

청구항 9

제 1 항에 있어서,

상기 컴퓨터 시스템의 부팅 암호 및 상기 주변기기의 암호 설정 여부를 판단하는 판단부; 및

상기 판단 결과, 상기 컴퓨터 시스템의 부팅 암호 및 상기 주변기기에 대한 암호가 설정되어 있지 않은 경우, 상기 산출된 결과값을 상기 컴퓨터 시스템의 부팅 암호 및 상기 주변기기의 암호로 설정하는 암호 설정부를 더 포함하는 컴퓨터 시스템 보안 장치.

청구항 10

제 1 항에 있어서,

상기 주제어부는, 상기 주변기기에 대하여 기설정되어 있는 암호와 상기 산출된 결과값의 일치하는 경우, 상기 주변기기로의 접근을 허용하는 컴퓨터 시스템 보안 장치.

청구항 11

주변기기를 포함하는 컴퓨터 시스템의 보안 방법에 있어서,

사용자 식별 정보를 인식하는 단계;

상기 인식된 사용자 식별 정보, 상기 컴퓨터 시스템의 주변기기에 대한 고유 식별 정보, 및 상기 컴퓨터 시스템의 고유 식별 정보를 입력값으로 하는 소정 연산을 수행하여 결과값을 산출하는 단계; 및

상기 컴퓨터 시스템에 대하여 기설정되어 있는 암호와 상기 산출된 결과값과의 일치 여부에 따라 상기 컴퓨터 시스템의 부팅을 수행하는 단계를 포함하는 컴퓨터 시스템 보안 방법.

청구항 12

제 11 항에 있어서,

상기 컴퓨터 시스템의 고유 식별 정보는, 상기 컴퓨터 시스템의 시리얼 넘버인 컴퓨터 시스템 보안 방법.

청구항 13

삭제

청구항 14

제 11 항에 있어서,

상기 주변기기는 하드디스크이며, 상기 주변기기의 고유 식별 정보는, 상기 주변기기의 시리얼 넘버인 컴퓨터 시스템 보안 방법.

청구항 15

제 11 항에 있어서,

상기 사용자 식별 정보가 기록된 RFID 태그를 더 포함하는 컴퓨터 시스템 보안 방법.

청구항 16

제 11 항에 있어서,

상기 인식하는 단계는, RFID 태그에 기록된 상기 사용자 식별 정보를 RFID 리더를 통해 수신하는 단계를 포함하는 컴퓨터 시스템의 보안 방법.

청구항 17

제 11 항에 있어서,

상기 사용자 식별 정보는, 상기 사용자의 생체 정보인 컴퓨터 시스템 보안 방법.

청구항 18

제 11 항에 있어서,

상기 인식하는 단계는,

상기 사용자의 식별 정보로서 상기 사용자의 생체 정보를 입력받는 단계;

상기 입력받은 생체 정보와 기저장되어 있는 생체 정보의 일치율이 소정 임계값 이상인 경우, 상기 사용자를 허가된 사용자로 판별하는 단계; 및

상기 허가된 사용자에 대한 사용자 식별 정보를 출력하는 단계를 포함하는 컴퓨터 시스템 보안 방법.

청구항 19

제 11 항에 있어서,

상기 컴퓨터 시스템의 부팅 암호 및 상기 주변기기에 대한 암호가 설정되어 있지 않은 경우, 상기 산출된 결과값을 상기 컴퓨터 시스템의 부팅 암호 및 상기 주변기기의 암호로 설정하는 단계를 더 포함하는 컴퓨터 시스템 보안 방법.

청구항 20

제 11 항에 있어서,

상기 주변기기에 대하여 기설정되어 있는 암호와 상기 산출된 결과값의 일치하는 경우, 상기 주변기기로의 접근을 허용하는 단계를 더 포함하는 컴퓨터 시스템 보안 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<15> 본 발명은 컴퓨터 보안 장치 및 방법에 관한 것으로, 보다 상세하게는 컴퓨터 도난 시에도 컴퓨터 시스템의 하드웨어 및 하드디스크에 저장되어 있는 데이터가 타인에 의해 오용되는 것을 방지할 수 있는 컴퓨터 시스템 보안 장치 및 방법에 관한 것이다.

<16> 최근 데스크탑 및 노트북 등의 개인용 컴퓨터를 사용하는 사용자가 급격하게 늘어나면서 컴퓨터 도난에 따른 보안 장치의 필요성이 급격하게 증가하고 있다.

<17> 컴퓨터에 저장되어 있는 데이터의 보안을 위해 종래에는 컴퓨터 부팅 단계에서 암호를 입력받는 기술 및/또는 하드디스크에 암호를 설정하는 기술이 사용되고 있다.

<18> 도 1은 종래 컴퓨터 보안 방법을 도시한 흐름도로서, 부팅 단계에서 암호를 입력받는 기술 및 하드디스크에 암호를 설정하는 기술이 동시에 사용되는 경우의 컴퓨터 보안 방법을 도시한 것이다.

<19> 우선, 사용자는 컴퓨터 부팅시에 필요한 부팅 암호를 설정한다. 사용자에 의해 설정된 부팅 암호는 CMOS에 저장된다. 또한, 사용자는 하드디스크에도 암호를 설정할 수 있다. 하드디스크에 대한 암호는 하드디스크에 포함된 메모리에 저장된다.

<20> 이와 같이, 부팅 및 하드디스크에 대한 암호가 설정된 상태에서 컴퓨터에 전원이 인가되면(S110), 컴퓨터는 사용자로부터 부팅 암호를 입력받아(S120), 입력받은 부팅 암호와 CMOS에 저장되어 있는 암호를 비교한다(S130).

<21> 비교 결과, 두 암호가 일치하지 않는 경우에는(S130, 아니오), 기저장되어 있는 암호와 일치하는 암호가 입력될 때까지 부팅 과정이 더 이상 진행되지 않는다. 비교 결과, 두 암호가 일치하는 경우에는(S130, 예), 부팅 과정이 계속해서 수행된다(S140).

<22> 한편, 컴퓨터 부팅이 완료된 후, 사용자가 하드디스크에 저장되어 있는 데이터를 엑세스하려는 경우, 사용자는 하드디스크에 대한 암호를 입력해야 한다(S150). 이 때, 사용자가 입력한 암호가 기설정되어 있는 하드디스크 암호와 일치하는 경우(S160, 예)에만 하드디스크로의 접근이 허용된다(S170).

<23> 그러나 종래 기술에 따르면, 컴퓨터 부팅시마다 사용자가 암호를 입력해야하는 번거로움이 있고, 컴퓨터

분실시, CMOS 배터리만 제거하면 누구나 컴퓨터의 하드웨어를 이용할 수 있다는 문제가 있다. 또한, 하드디스크에 암호를 설정하더라도, 암호가 설정된 하드디스크만 교체하면, 누구나 컴퓨터의 하드웨어를 이용할 수 있다는 문제가 있다.

발명이 이루고자 하는 기술적 과제

<24> 본 발명은 상기한 문제점을 개선하기 위해 안출된 것으로, 컴퓨터 부팅시마다 사용자가 암호를 입력해야하는 번거로움을 줄이고, 컴퓨터 도난 시에도 컴퓨터에 포함되어 있는 하드웨어 및 하드디스크에 저장되어 있는 데이터가 타인에 의해 오용되는 것을 방지할 수 있는 컴퓨터 시스템 보안 장치 및 방법을 제공하는데 목적이 있다.

<25> 그러나 본 발명의 목적들은 상기에 언급된 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

발명의 구성 및 작용

<26> 상기 목적을 달성하기 위하여 본 발명의 실시예에 따른 컴퓨터 시스템 보안 장치는, 사용자 식별 정보를 인식하기 위한 인식부, 상기 인식된 사용자 식별 정보, 컴퓨터 시스템의 주변기기에 대한 고유 식별 정보, 및 상기 컴퓨터 시스템의 고유 식별 정보를 입력값으로 하는 소정 연산을 수행하여 결과값을 산출하는 연산부, 및 상기 컴퓨터 시스템에 대하여 기설정되어 있는 암호와 상기 산출된 결과값과의 일치 여부에 따라 상기 컴퓨터 시스템의 부팅을 수행하는 주제어부를 포함한다.

<27> 또한, 상기 목적을 달성하기 위하여 본 발명의 실시예에 따른 컴퓨터 시스템 보안 방법은, 사용자 식별 정보를 인식하는 단계, 상기 인식된 사용자 식별 정보, 상기 컴퓨터 시스템의 주변기기에 대한 고유 식별 정보, 및 상기 컴퓨터 시스템의 고유 식별 정보를 입력값으로 하는 소정 연산을 수행하여 결과값을 산출하는 단계, 및 상기 컴퓨터 시스템에 대하여 기설정되어 있는 암호와 상기 산출된 결과값과의 일치 여부에 따라 상기 컴퓨터 시스템의 부팅을 수행하는 단계를 포함한다.

<28> 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범수를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

<29> 이하, 본 발명의 실시예들에 의하여 컴퓨터 시스템 보안 장치 및 방법을 설명하기 위한 블록도 또는 처리 흐름도에 대한 도면들을 참고하여 본 발명에 대해 설명하도록 한다. 이 때, 처리 흐름도 도면들의 각 블록과 흐름도 도면들의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수 있음을 이해할 수 있을 것이다.

<30> 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 흐름도 블록(들)에서 설명된 기능들을 수행하는 수단을 생성하게 된다.

<31> 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 흐름도 블록(들)에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 흐름도 블록(들)에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

<32> 또한, 각 블록은 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또, 몇 가지 대체 실행예들에서는 블록들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

<33> 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명하기로 한다.

<34> 도 2는 본 발명의 제1 실시예에 따른 컴퓨터 시스템(200)의 구조를 도시한 블록도이다.

<35> 도 2를 참조하면, 본 발명의 제1 실시예에 따른 컴퓨터 시스템(200)은 바이오스(BIOS)(210), 저장장치(220), 메모리부(230), 암호 설정부(240), 주제어부(250), 인식부(260), 추출부(290), 연산부(270) 및 판단부(280)를 포함하여 구성된다.

<36> 바이오스(Basic Input Output System; BIOS)(210)는 컴퓨터가 켜질 때 자동으로 실행되어 컴퓨터의 상태를 검사하고(Power-On Self Test, POST), 시스템을 초기화(initialize)하는 작업을 하며, 초기화 작업 중 어떠한 주변장치들이 연결되어 있는지 확인한다.

<37> 저장장치(220)는 컴퓨터 시스템(200)의 주변 장치로서, 대용량의 데이터를 저장한다. 이러한 저장장치(200)로서, CD-ROM, DVD-ROM, USB 저장장치 및 하드디스크 등을 예로 들 수 있다. 이하의 설명에서는 저장장치(200)가 하드디스크인 경우를 예로 들어 설명하기로 한다. 그러나 본 발명은 하드디스크뿐만 아니라 기타 저장장치에도 적용될 수 있음은 물론이다.

<38> 하드디스크는 제1 저장부 및 제2 저장부를 포함할 수 있다. 여기서, 제1 저장부는 운영체제 및 사용자가 저장하는 데이터를 저장하며, 제2 저장부는 하드디스크의 고유 정보 예를 들면, 시리얼 넘버 및 하드디스크의 암호를 저장한다. 제2 저장부는 예를 들어, EPROM, EEPROM 등으로 구현될 수 있으나 이에 한정되지는 않는다.

<39> 메모리부(230)는, 후술될 암호 설정부(240)에 의해 설정되는 컴퓨터 시스템(200)의 부팅 암호를 저장한다. 이를 위해 메모리부(230)는 플래시 메모리와 같은 비휘발성 메모리 소자로 구현될 수 있으나 이에 한정되지는 않는다.

<40> 암호 설정부(240)는 컴퓨터 시스템(200)의 부팅 암호 및 하드디스크의 암호가 설정되어 있지 않은 경우, 후술될 연산부(270)에 의해 산출된 결과값을 컴퓨터 시스템(200)의 부팅 암호 및 하드디스크의 암호로 설정한다. 이때, 컴퓨터 시스템(200)의 부팅 암호는 전술한 메모리부(230)에 저장되며, 하드디스크의 암호는 하드디스크 내에 포함된 제2 저장부에 저장된다.

<41> 주제어부(250)는 컴퓨터 시스템(200) 내의 구성 요소들을 서로 연결하고 관리한다. 그리고, 후술될 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 컴퓨터 시스템(200)의 부팅 암호의 일치 여부에 따라, 컴퓨터 시스템(200)의 부팅을 진행한다. 좀 더 구체적으로, 후술될 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 컴퓨터 시스템(200)의 부팅 암호가 서로 일치하는 경우, 주제어부(250)는 컴퓨터 시스템(200)의 부팅이 성공적으로 이루어질 수 있도록 한다. 만약, 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 부팅 암호가 서로 일치하지 않는 경우, 주제어부(250)는 컴퓨터 시스템(200)의 부팅이 더 이상 진행될 수 없도록 한다.

<42> 인식부(260)는 사용자 식별 정보를 인식한다. 사용자 식별 정보란, 컴퓨터 시스템(200)을 사용하는 사용자에 대한 고유 정보를 말하는 것으로서, 사용자의 지문, 홍채, 얼굴 등의 생체 정보 등을 예로 들 수 있다. 예시한 사용자 식별 정보 인식을 위해 인식부(260)는 지문 인식 모듈, 홍채 인식 모듈 및 얼굴 인식 모듈 중 어느 하나를 포함할 수 있다. 이외에도 사용자 식별 정보를 입력받기 위해 RFID 기술이 이용될 수도 있다. 이하의 설명에서는, RFID 기술을 이용하여 사용자 식별 정보를 인식하는 것을 제1 실시예로 하여 설명하기로 한다.

<43> RFID(Radio Frequency Identification)란 사물에 부착된 전자태그로부터 무선 주파수를 이용하여 정보를 송·수신하고 이와 관련된 서비스를 제공하는 기술을 말하는 것으로 바코드, 마그네틱, IC-card를 대체할 비접촉식 카드(Contectless Card)의 대표적인 기술이라고 할 수 있다. 이러한 RFID 기술을 통해 사용자 식별 정보를 입력받기 위해 인식부(260)는 RFID 리더(260)(reader)를 포함하는 것이 바람직하며, 사용자는 식별 정보가 저장된 RFID를 휴대하는 것이 바람직하다.

<44> RFID 리더(260)는 내장형 또는 외장형의 안테나를 포함하며, 이 안테나는 활성신호를 발산하여 전자기장 즉, RF 필드를 형성한다. 이 RF 필드 내에 RFID 태그(300)가 진입하면, RFID 태그(300)는 RFID 리더(260)의 안테나에서 발산된 활성 신호를 수신하고, 수신된 활성 신호를 이용하여 RFID 태그(300) 내에 저장되어 있는 정보를 RFID 리더(260)로 송신하게 된다. 이 후, RFID 리더(260)는 RFID 태그(300)에서 전송된 정보를 수신하고 분석하여, RF 태그에 저장되어 있는 사용자 식별 정보를 취득한다. RFID 태그(300) 및 RFID 리더(260)에 대한 보다 상세한 설명은 도 3 및 도 4를 참조하여 후술하기로 한다.

<45> 추출부(290)는 컴퓨터 시스템(200)의 식별 정보 및 하드디스크의 식별 정보를 추출하는 역할을 한다. 여기서, 컴퓨터 시스템(200)의 식별 정보란, 컴퓨터 시스템(200)에 대한 고유 정보를 말하는 것으로서 제품 시리얼 넘버

를 예로 들 수 있다. 마찬가지로, 하드디스크의 식별 정보란, 하드디스크에 대한 고유 정보를 말하는 것으로서, 하드디스크의 시리얼 넘버를 예로 들 수 있다.

<46> 연산부(270)는 사용이 허가된 사용자의 식별 정보, 컴퓨터 시스템(200) 정보 및 하드디스크 식별 정보에 소정 연산을 수행하여 결과값을 산출한다. 예를 들면, 연산부(270)는 전술한 세 개의 식별 정보를 모두 더해 결과값을 산출할 수 있다.

<47> 판단부(280)는 컴퓨터 시스템(200)의 부팅 암호 및 하드디스크 암호가 설정되어 있는지의 여부를 판단한다. 판단 결과, 부팅 암호 및 하드디스크 암호가 설정되어 있지 않은 경우, 판단부(280)는 판단 결과를 제어부로 제공하여, 연산부(270)에 의해 산출된 결과값이 컴퓨터 시스템(200)의 보안을 위한 암호로 설정될 수 있도록 한다. 즉, 연산부(270)에서 제공된 결과값이 각각 부팅 암호 및 하드디스크 암호로 설정될 수 있도록 한다. 판단 결과, 부팅 암호 및 하드디스크 암호가 이미 설정되어 있는 경우, 판단부(280)는 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 암호를 비교한다.

<48> 비교 결과, 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 암호가 일치하지 않는 경우, 판단부(280)는 판단 결과를 주제어부(250)로 제공하여 컴퓨터 시스템(200)의 부팅 작업이 계속 진행될 수 없도록 한다.

<49> 비교 결과, 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 암호가 일치하는 경우, 판단부(280)는 컴퓨터 시스템(200)의 부팅 작업이 정상적으로 진행될 수 있도록 한다. 이로써, 사용자가 컴퓨터 시스템(200) 및 하드디스크에 저장되어 있는 데이터에 접근하는 것을 허용한다.

<50> 도 3은 RFID 태그(300)의 구조를 도시한 블록도이고, 도 4는 RFID 리더(260)의 구조를 도시한 블록도이다.

<51> RFID 태그(300)는 앞서 언급한 바와 같이 사용자 식별 정보로 사용되는 고유 정보를 저장한다. RFID 태그(300)는 RF 필드 내에 진입하는 경우, 상기 고유 정보를 RFID 리더(260)로 전송한다. 이를 위해 RFID 태그(300)는 도 3에 도시된 바와 같이, 안테나부(320), 전원부(310), 복조부(350), 변조부(360), 제어부(330) 및 메모리부(340)를 포함하여 구성된다.

<52> 안테나부(320)는 소정의 주파수대역 예를 들어, 100~500KHz의 저주파 대역, 10~15MHz의 중간 주파수 대역, 860~960MHz 또는 2.45GHz~5.8GHz의 고주파 대역에 해당하는 RF 신호를 사용하여 RFID 리더(260)와 데이터를 송수신한다.

<53> 전원부(310)는 전원을 생성하여 RFID 태그(300) 전반에 공급함으로써, 태그의 메모리부(340)에 저장되어 있는 정보가 RFID 리더(260)로 전송될 수 있도록 한다. 전원부(310)는 태그의 종류에 따라 별도의 배터리로 구현되거나 LC 회로로 구현될 수 있다. 예를 들어, RFID 태그(300)가 능동형 태그인 경우, 전원부(310)는 별도의 배터리로 구현되어 태그 내에 포함될 수 있다. 만약 RFID 태그(300)가 수동형 태그인 경우, 전원부(310)는 LC 회로로 구현될 수 있다. 이 경우 전원부(310)에서는 RFID 리더(260)의 안테나(미도시)에 의해 생성된 자기장을 통해 소정의 유도 전압 예를 들어, 3V의 직류 전압을 발생하여 RFID 태그(300)에 공급한다.

<54> 복조부(350)는 안테나부(320)를 통해 수신되는 RF 신호를 복조한다. 또한 복조된 신호로부터 커맨드(Command)를 검출하여, 검출된 커맨드의 종류에 따라 제어부(330)가 메모리부(340)를 액세스할 수 있도록 한다. 예를 들어, 복조부(350)가 커맨드를 검출한 결과, RFID 리더(260)로부터 리드 커맨드(Read command)를 수신하였다면, 검출된 커맨드를 제어부(330)에 제공하여, 제어부(330)가 메모리부(340)를 액세스할 수 있도록 한다.

<55> 변조부(360)는 RFID 태그(300)의 메모리부(340)에 저장되어 있는 고유 정보를 RF 신호로 변조하는 역할을 한다. 다시 말해, 디지털 신호인 고유 정보를 아날로그 신호로 변환한다. 고유 정보를 아날로그 신호로 변조할 때에는 다양한 변조 방식을 이용될 수 있다. 예를 들면, 진폭 변조(Amplitude Shift Keying Modulation: ASK Modulation), 주파수 변조(Frequency Shift Keying Modulation: FSK Modulation), 위상 변조(Phase Shift Keying Modulation: PSK Modulation) 중 어느 하나의 변조 방식이 사용될 수 있다. 변조된 RF 신호는 안테나부(320)를 통해 RFID 리더(260)로 송신된다.

<56> 메모리부(340)는 태그의 고유정보 예를 들면, ID를 저장한다. 메모리부(340)는 데이터를 기록하는 방식에 따라 읽기 전용(read-only), 읽기/쓰기가 가능한 형태(read/write), 한 번 쓰고 여러 번 읽기가 가능한 형태(Write Once Read Many; WORM) 등으로 구현될 수 있으며, 이러한 메모리부(340)는 예를 들어, 레지스터(Register), ROM, EPROM, EEPROM, RAM 및 FRAM(Ferroelectric Random Access Memory; 강유전체 RAM)과 같은 형태의 메모리 소자로 구현될 수 있으나, 이에 한정되지는 않는다.

<57> 제어부(330)는 복조부(350)가 RFID 리더(260)로부터 리드 커맨드(Read command)를 수신하는 경우, 메모리부

(340)를 액세스하여 메모리부(340)에 저장되어 있는 고유 정보를 읽어온다. 이 후, 제어부(330)는 메모리부(340)로부터 읽어온 고유 정보를 변조부(360)에 제공하여, 고유 정보가 아날로그 신호로 변조될 수 있도록 한다.

<58> 이외에도 RFID 태그(300)는 제어부(330)에 일정한 주기의 클럭을 공급하는 클럭 공급부(미도시)를 포함할 수 있다.

<59> 전술한 RFID 태그(300)는 사용자가 항시 휴대하는 물품 예를 들면, 명함, 휴대 전화 등에 부착될 수 있도록 스티커와 같은 형태로 구현되어, 사용자가 RFID 태그(300)를 휴대할 수 있도록 하는 것이 바람직하다.

<60> 다음으로, RFID 리더(RF reader)(260)는 RFID 태그(300)에 RF 에너지를 공급하여 활성화되도록 하고, RFID 태그(300)에서 송신된 정보를 수신한다. 이를 위해 RFID 리더(260)는 도 4에 도시된 바와 같이, RF 신호 발신부(261), RF 신호 수신부(262) 및 제어부(263)를 포함하여 구성된다.

<61> RF 신호 발신부(261)는 도면에 도시되지는 않았으나 안테나 회로, 동조(tuning) 회로 및 RF 반송파 발생부(RF carrier generator)를 포함한다. 안테나 회로에서는 지속적으로 전파를 발산하여 전자기장을 형성하고, 동조회로는 안테나가 최상의 성능을 발휘할 수 있도록 동조를 맞춘다. RF 신호 발신부(261)는 기저신호를 고주파 신호로 변환하여 전송한다. 이 때, 소정의 변조 방식으로는 진폭 변조(Amplitude Shift Keying Modulation; ASK Modulation), 주파수 변조(Frequency Shift Keying Modulation; FSK Modulation), 위상 변조(Phase Shift Keying Modulation; PSK Modulation) 방식 등의 디지털 변조방식을 예로 들 수 있다.

<62> RFID 리더(260)의 제어부(263)는 마이크로 컨트롤러로 구현될 수 있으며, 이 마이크로 컨트롤러 내에는 펌웨어 알로리즘이 저장된다. RFID 리더(260)기는 이 알고리즘을 이용해 RF 신호를 발신하며, RF 신호 수신부(262)를 통해 수신된 신호를 디코딩하여 데이터 신호로 변환한다.

<63> 다음으로, 도 5는 본 발명의 실시예에 따른 컴퓨터 시스템의 보안 방법을 도시한 흐름도이다.

<64> 먼저, 컴퓨터 시스템에 전원이 인가되면, RFID 리더(260)는 사용자가 휴대한 RFID 태그(300)로부터 사용자 식별 정보를 인식한다(S510).

<65> 사용자 식별 정보 인식 과정을 좀 더 구체적으로 설명하면, 우선 RFID 리더(260)는 안테나(미도시)를 통해 RF 신호를 지속적으로 방출하여 전자기장 즉, RF 필드를 형성한다. 이 후, RFID 리더(260)는 RF 필드 내에 있는 RFID 태그(300)로 리드 커맨드(read command) 신호를 송신한다.

<66> 한편, RF 필드가 형성됨에 따라 RF 필드 내에 있는 RFID 태그(300)에는, RFID 태그(300)의 안테나부(320)를 통해 RF 신호가 수신되고, 수신된 신호에 의해 유도전압이 발생되어 RFID 태그(300)에 전원이 공급된다. 이 후, 수신부(320)는 수신한 RF 신호를 복조하여 커맨드 신호를 검출하고, 검출된 커맨드 신호의 종류에 따른 동작을 하게 된다. 예를 들어, 리드 커맨드(read command)가 검출된 경우, 검출된 리드 커맨드를 제어부(350)에 제공하여 메모리부(370)를 액세스할 수 있도록 한다. 제어부(350)는 메모리부(370)를 액세스하여, 디지털 신호 형태의 고유정보를 읽어와 변조부(330)로 제공한다. 변조부(330)는 제어부(350)에 의해 제공된 고유정보를 아날로그 신호로 변조한다. 이 때, 변조 방식으로는 소정의 디지털 변조 방식 예를 들면, 진폭 변조(Amplitude Shift Keying; ASK) 방식이 사용될 수 있다. 변조부(330)에 의해 변조된 신호는 안테나부(320)를 통해 RFID 리더(260)로 송신된다.

<67> 한편, RFID 리더(260)는 RFID 태그(300)로부터 수신된 신호를 복조하여 사용자 식별 정보를 검출한다. 이 후, 종료 커맨트(End command)를 송신하여 RFID 태그(300) 인식 과정을 종료한다. RFID 리더(260)에 의해 검출된 사용자 식별 정보는 연산부(270)로 제공된다.

<68> 한편, 컴퓨터 시스템(200)에 전원이 인가되면, 추출부(290)는 컴퓨터 시스템(200)의 식별 정보 및 하드디스크의 식별 정보를 추출한다(S520). 추출된 식별 정보는 연산부(270)로 제공된다.

<69> 연산부(270)는 인식된 사용자 식별 정보, 추출된 컴퓨터 시스템(200)의 식별 정보 및 하드디스크의 식별 정보를 입력값으로 하는 소정 연산을 수행하여 결과값을 산출한다(S530). 예를 들면, 세 개의 식별 정보를 모두 더하여 결과값을 산출한다.

<70> 이 후, 판단부(280)는 컴퓨터 시스템(200)의 부팅 암호 및 하드디스크 암호가 설정되어 있는지를 판단한다(S540). 판단 결과, 부팅 암호 및 하드디스크의 암호가 설정되어 있지 않은 경우(S540, 아니오), 판단부(280)는 연산부(270)에 의해 산출된 결과값을 컴퓨터 시스템(200)의 부팅 암호 및 하드디스크 암호로 설정한다

(S550). 판단 결과, 부팅 암호 및 하드디스크 암호가 이미 설정되어 있는 경우(S540, 예), 판단부(280)는 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 부팅 암호를 비교한다(S560).

<71> 비교 결과, 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 부팅 암호가 일치하지 않는 경우(S570, 아니오), 판단부(280)는 컴퓨터 시스템(200)의 부팅 작업이 계속 진행될 수 없도록 한다(S590).

<72> 비교 결과, 연산부(270)에 의해 산출된 결과값과 기설정되어 있는 부팅 암호가 일치하는 경우(S570, 예), 판단부(280)는 컴퓨터 시스템(200)의 부팅 작업이 정상적으로 진행될 수 있도록 한다(S580). 이로써, 사용자에게 컴퓨터 시스템(200) 및 하드디스크로의 접근을 허용한다.

<73> 다음으로 도 6 및 도 7을 참조하여 본 발명의 제2 실시예에 따른 컴퓨터 보안 장치 및 방법에 대해서 설명하기로 한다.

<74> 본 발명의 제2 실시예에 따른 컴퓨터 시스템(600)은 제1 실시예에 따른 컴퓨터 시스템(600)과 다음을 제외하고는 동일한 구성 요소를 포함할 수 있다. 즉, 제2 실시예에 따른 컴퓨터 시스템(600)은, 얼굴 인식 기술을 기반으로 하여 사용자 식별 정보를 출력하는 인식부(660)를 포함한다. 여기서, 도 6을 참조하여 인식부(660)에 대해 보다 구체적으로 설명하기로 한다.

<75> 도 6은 본 발명의 제2 실시예에 따른 보안 기능을 갖는 컴퓨터 시스템(600)의 구조를 도시한 블록도이다. 도 6을 참조하면, 제2 실시예에 따른 컴퓨터 시스템(600)에서 인식부(660)는 입력부(661), 변환부(662), 비교부(663) 및 사용자 식별 정보 출력부(664)를 포함하여 구성된다.

<76> 입력부(661)는 사용자의 얼굴을 촬영하기 위한 카메라 모듈을 포함할 수 있다. 카메라 모듈은 컴퓨터 시스템(600)의 소정 위치에 설치될 수 있으며, 이를 통해 사용자 얼굴의 평면적인 이미지를 획득할 수 있다. 다른 예로써, 입력부(661)는 적어도 두 개 이상의 카메라 모듈을 포함할 수 있는데, 이 경우, 서로 다른 각도에 위치한 적어도 두 개 이상의 카메라 모듈을 통해 사용자 얼굴을 입체 형상으로 읽어낼 수도 있다.

<77> 변환부(662)는 카메라 모듈를 통해 획득된 2차원 얼굴 영상 또는 3차원 얼굴 영상을 수학적 수치로 변환한다. 예를 들면, 사람의 얼굴 중 눈썹에서부터 입술 바로 밑까지를 소정 개수 예를 들면, 200개의 칸으로 분할한 후, 200개의 칸을 각각 고유한 수치로 변환한다. 이 때, 변환부(662)는 개인의 얼굴 중 가장 변화가 적은 부분, 타인과 구분이 잘되는 부분 등에 대한 가중치를 적용한다.

<78> 비교부(663)는 변환된 200개의 수치와 기저장되어 있는 데이터베이스를 비교하여, 일치율이 소정 임계값 예를 들어, 90% 이상인지를 판단한다. 판단 결과, 일치율이 90% 보다 낮은 경우, 예를 들면, 변환된 200개의 데이터 중 일치하는 수치의 개수가 180개 보다 적은 경우, 비교부(663)는 현재 사용자가 사전에 허가된 사용자가 아닌 것으로 판단한다. 판단 결과, 일치율이 90% 이상인 경우, 예를 들면, 변환된 데이터 중 일치하는 수치의 개수가 180개 이상인 경우, 비교부(663)는 현재 사용자가 사전 허가된 사용자인 것으로 판단한다.

<79> 사용자 식별 정보 출력부(664)는, 비교부(663)의 판단 결과에 따라 사용자 식별 정보로 지정된 값을 출력한다. 설명의 편의를 위해 허가된 사용자에 대해 5라는 값이 사용자 식별 정보로 지정되어 있다고 하자. 만약, 비교부(663)의 판단 결과, 현재 사용자가 허가된 사용자가 아닌 경우, 사용자 식별 정보 출력부(664)는 5 이외의 값 예를 들면, 0을 출력한다. 만약, 비교부(663)의 판단 결과, 현재 사용자가 허가된 사용자인 경우, 사용자 식별 정보 출력부(664)는 5라는 값을 출력한다. 사용자 식별 정보 출력부(664)에 의해 출력된 값은 연산부(670)로 제공된다.

<80> 도 7은 본 발명의 제2 실시예에 따른 컴퓨터의 보안 방법을 도시한 흐름도이다.

<81> 먼저, 컴퓨터 시스템(600)에 전원이 인가되면, 추출부(690)는 컴퓨터 시스템(600)의 식별 정보 및 하드디스크의 식별 정보를 추출하여 연산부(670)로 제공한다(S710).

<82> 또한, 인식부(660)는 사용자 얼굴을 인식하고, 인식 결과에 따라 사용자 식별 정보를 출력한다(S720). 여기서, 사용자 얼굴을 인식한 결과에 따라 사용자 식별 정보를 출력하는 단계 S720에 대한 보다 상세한 설명을 위해 도 8을 참조하기로 한다.

<83> 인식부(660)는 우선, 카메라 모듈을 통해 사용자 얼굴에 대한 2차원 영상 또는 3차원 영상을 입력받는다(S721). 이 후, 인식부(660)는 입력받은 얼굴 영상을 수학적 수치로 변환한다(S722).

<84> 이 후, 인식부(660)는 변환된 수치와 비교할 데이터베이스의 유무를 판단한다(S723).

<85> 데이터베이스의 유무를 판단한 결과, 기저장되어 있는 데이터베이스가 없는 경우(S723, 아니오), 인식부(660)는 허가된 사용자에 대하여 할당되어 있는 값을 사용자 식별 정보를 출력한다(S724). 예를 들어, 허가된 사용자에 대하여 할당되어 있는 값이 5인 경우, 인식부(660)는 5를 사용자 식별 정보로 출력한다.

<86> 데이터베이스의 유무를 판단한 결과, 기저장되어 있는 데이터베이스가 존재하는 경우(S723, 예), 인식부(660)는 변환된 수치와 기저장되어 있는 데이터베이스를 비교한다(S725).

<87> 비교 결과 일치율이 소정 임계값 예를 들면, 90% 보다 낮은 경우(S726, 아니오), 인식부(660)는 현재 사용자가 허가된 사용자가 아닌 것으로 판단한다. 이 경우, 인식부(660)는 허가된 사용자에 대하여 할당되어 있는 값 이외의 값을 사용자 식별 정보로 출력한다(S727). 예를 들어, 허가된 사용자에 대하여 할당되어 있는 값이 5인 경우, 인식부(660)는 0을 사용자 식별 정보로 출력한다.

<88> 비교 결과, 일치율이 90% 이상인 경우(S726, 예), 인식부(660)는 현재 사용자가 허가된 사용자인 것으로 판단한다. 이 경우, 인식부(660)는 허가된 사용자에 대하여 할당되어 있는 값을 사용자 식별 정보로 출력한다(S724).

<89> 연산부(670)는 인식부(660)에서 출력된 사용자 식별 정보, 추출부(690)에서 추출된 컴퓨터 시스템(600)의 식별 정보 및 하드디스크의 식별 정보를 입력값으로 하는 소정 연산을 수행하여 결과값을 산출한다. 예를 들면, 입력받은 세 개의 식별 정보를 모두 더하여 결과값을 산출한다(S730).

<90> 이 후, 판단부(680)는 컴퓨터 시스템(600)의 부팅 암호 및 하드디스크 암호가 설정되어 있는지의 여부를 판단한다(S740). 판단 결과, 부팅 암호 및 하드디스크의 암호가 설정되어 있지 않은 경우(S740, 아니오), 판단부(680)는 연산부(670)에 의해 산출된 결과값을 컴퓨터 시스템(600)의 부팅 암호 및 하드디스크 암호로 설정한다(S750). 판단 결과, 부팅 암호 및 하드디스크 암호가 이미 설정되어 있는 경우(S740, 예), 판단부(680)는 연산부(670)에 의해 산출된 결과값과 기설정되어 있는 컴퓨터 시스템(600)의 부팅 암호를 비교한다(S760).

<91> 비교 결과, 연산부(670)에 의해 산출된 결과값과 기설정되어 있는 부팅 암호가 일치하지 않는 경우(S770, 아니오), 판단부(680)는 컴퓨터 시스템(600)의 부팅 작업이 계속 진행될 수 없도록 한다(S790). 동시에 하드디스크에 저장된 데이터로의 접근을 불허한다.

<92> 비교 결과, 연산부(670)에 의해 산출된 결과값과 기설정되어 있는 부팅 암호가 일치하는 경우(S770, 예), 판단부(680)는 컴퓨터 시스템(600)의 부팅 작업이 정상적으로 진행될 수 있도록 한다(S780). 이로써, 사용자에게 컴퓨터 시스템(600) 및 하드디스크로의 접근을 허용한다.

<93> 전술한 바와 같은 본 발명에 의하면, 컴퓨터 시스템(600)이 도난된 경우, 기존의 하드디스크를 새로운 하드디스크로 교체하더라도 컴퓨터 시스템(600)을 사용할 수 없으며, 기존의 하드디스크를 다른 컴퓨터 시스템(600)에 연결하더라도 하드디스크에 저장되어 있는 데이터로의 접근이 불가능하다. 따라서, 컴퓨터 시스템(600) 및 하드디스크를 동시에 보호할 수 있다.

<94> 이상과 같이 예시된 도면을 참조로 하여, 본 발명에 따른 컴퓨터 시스템 보안 장치 및 방법에 대하여 설명하였으나, 본 발명은 본 명세서에 개시된 실시예와 도면에 의해 한정되지 않으며, 그 발명의 기술사상 범위 내에서 당업자에 의해 다양한 변형이 이루어질 수 있음은 물론이다.

발명의 효과

<95> 상기한 바와 같이 본 발명에 의한 컴퓨터 시스템 보안 장치 및 방법에 따르면 다음과 같은 효과가 하나 혹은 그 이상 있다.

<96> 컴퓨터 도난 시, 컴퓨터 시스템 및 하드디스크에 저장되어 있는 데이터가 타인에 의해 오용되는 것을 방지할 수 있다.

<97> 또한, 컴퓨터 시스템 및 하드디스크를 모두 보호할 수 있다.

<98> 또한, 컴퓨터 시스템의 부팅시마다, 사용자가 수동으로 암호를 입력해야하는 번거로움을 감소시킬 수 있다.

도면의 간단한 설명

<1> 도 1은 종래 기술에 따른 컴퓨터의 보안 방법을 도시한 흐름도이다.

<2> 도 2는 본 발명의 제1 실시예에 따른 컴퓨터 시스템의 구성을 도시한 블럭도이다.

<3> 도 3은 도 2의 컴퓨터 시스템에 적용된 RFID 태그의 구조를 도시한 블록도이다.

<4> 도 4는 도 2의 컴퓨터 시스템에 적용된 RFID 리더의 구조를 도시한 블록도이다.

<5> 도 5는 본 발명의 제1 실시예에 따른 컴퓨터 시스템의 보안 방법을 도시한 흐름도이다.

<6> 도 6은 본 발명의 제2 실시예에 따른 컴퓨터 시스템에서 인식부의 구조를 도시한 블록도이다.

<7> 도 7은 본 발명의 제2 실시예에 따른 컴퓨터 시스템의 보안 방법을 도시한 흐름도이다.

<8> 도 8은 도 7의 사용자 얼굴을 인식한 결과에 따라 사용자 식별 정보를 출력하는 단계 S720을 보다 상세히 도시한 흐름도이다.

<9> <도면의 주요 부분에 대한 부호의 설명>

<10> 200: 컴퓨터 시스템 220: 저장 장치

<11> 230: 메모리부 240: 암호 설정부

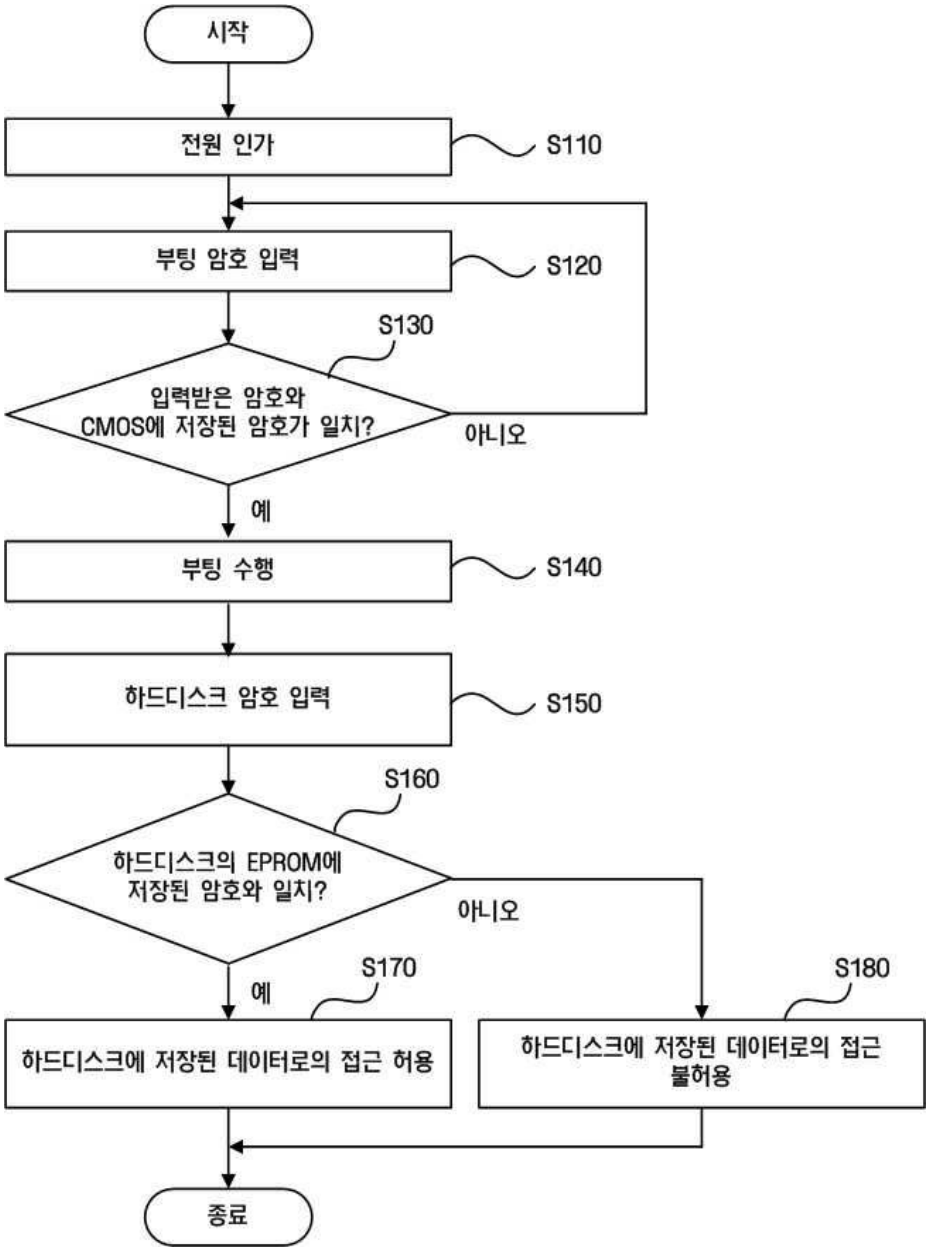
<12> 250: 주제어부 260: 인식부

<13> 270: 연산부 280: 판단부

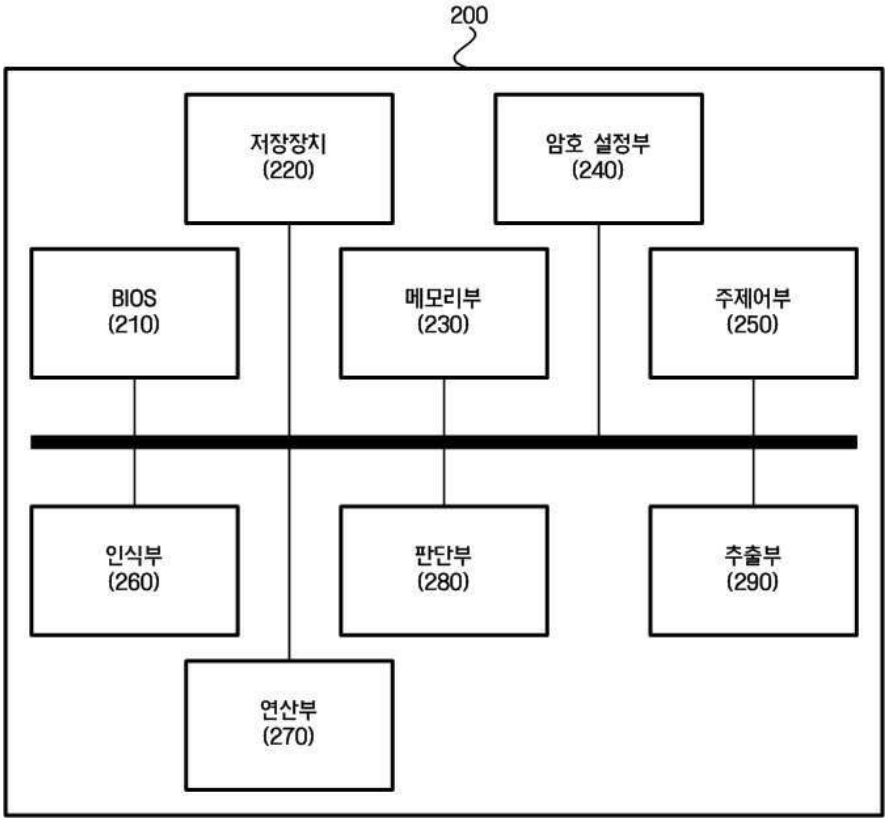
<14> 290: 추출부

도면

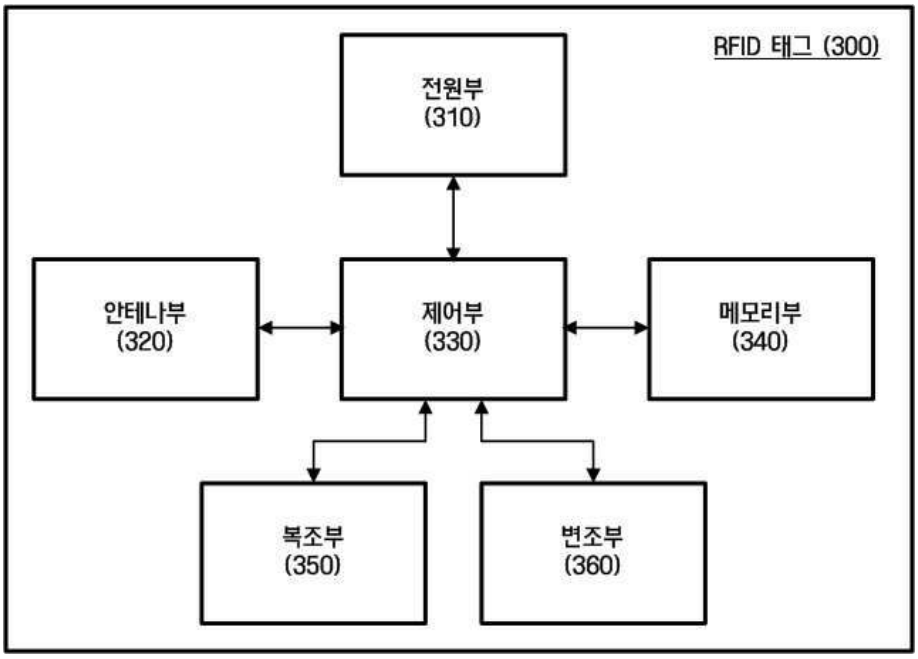
도면1


시작
전원 인가
S110
부팅 암호 입력
S120
S130
입력받은 암호와
CMOS에 저장된 암호가 일치?
아니오
예
부팅 수행
S140
하드디스크 암호 입력
S150
S160
하드디스크의 EPROM에
저장된 암호와 일치?
아니오
예
S170
S180
하드디스크에 저장된 데이터로의 접근 허용
하드디스크에 저장된 데이터로의 접근
불허용
종료

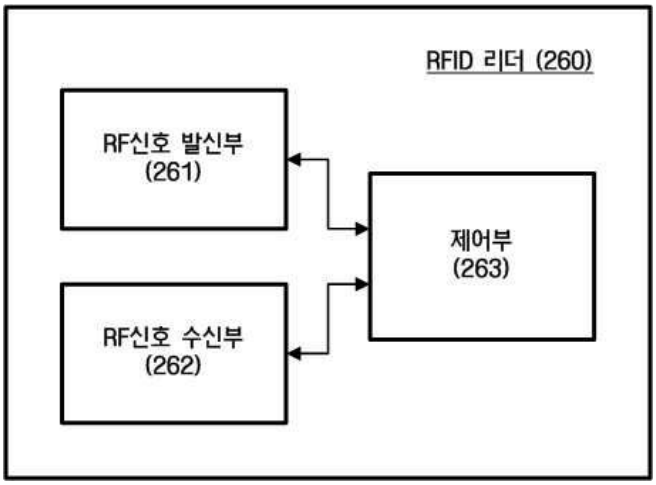
도면2


200
저장장치
(220)
암호 설정부
(240)
BIOS
(210)
메모리부
(230)
주제어부
(250)
인식부
(260)
판단부
(280)
추출부
(290)
연산부
(270)

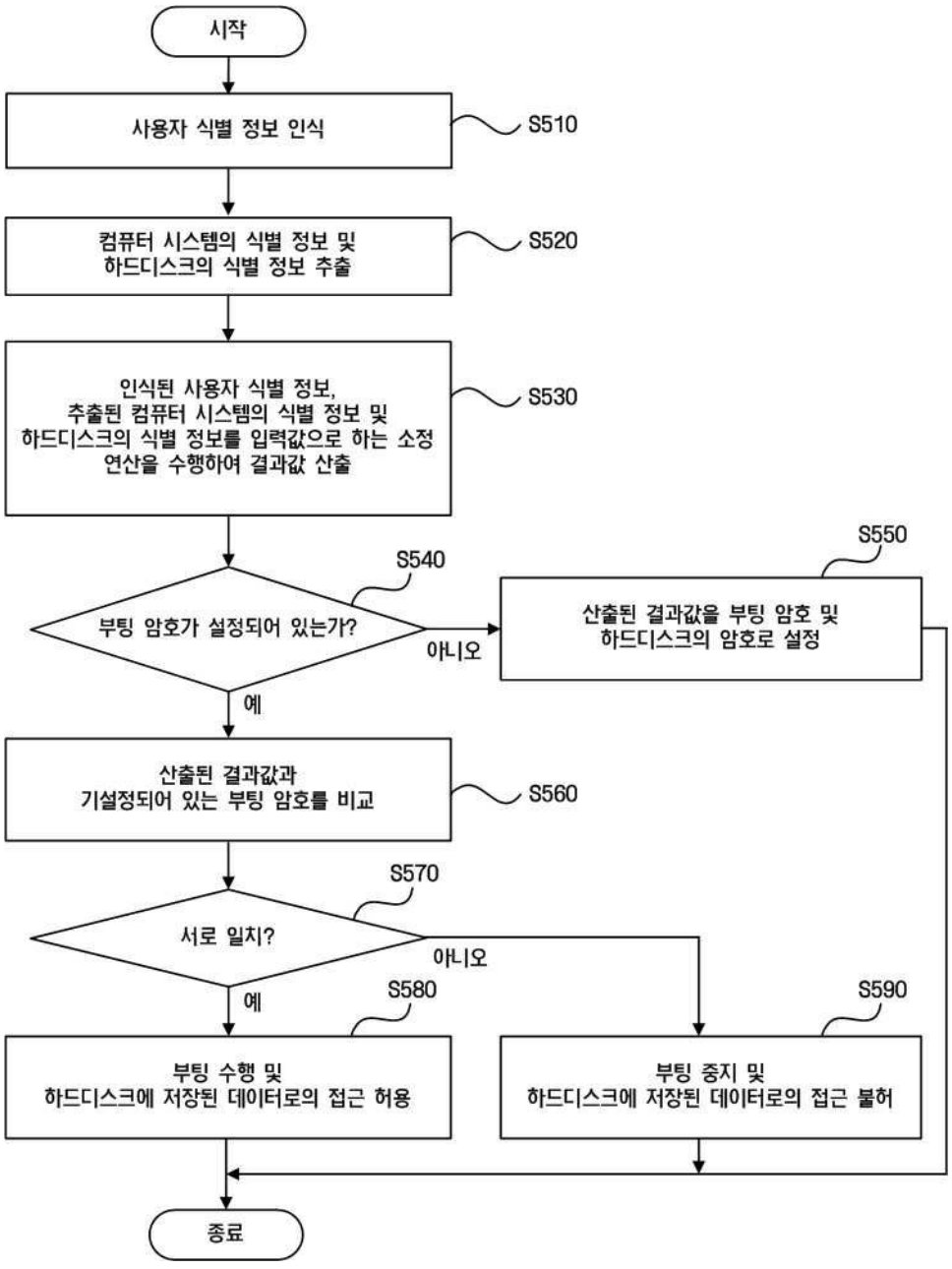
도면3


RFID 태그 (300)
전원부
(310)
안테나부
(320)
제어부
(330)
메모리부
(340)
복조부
(350)
변조부
(360)

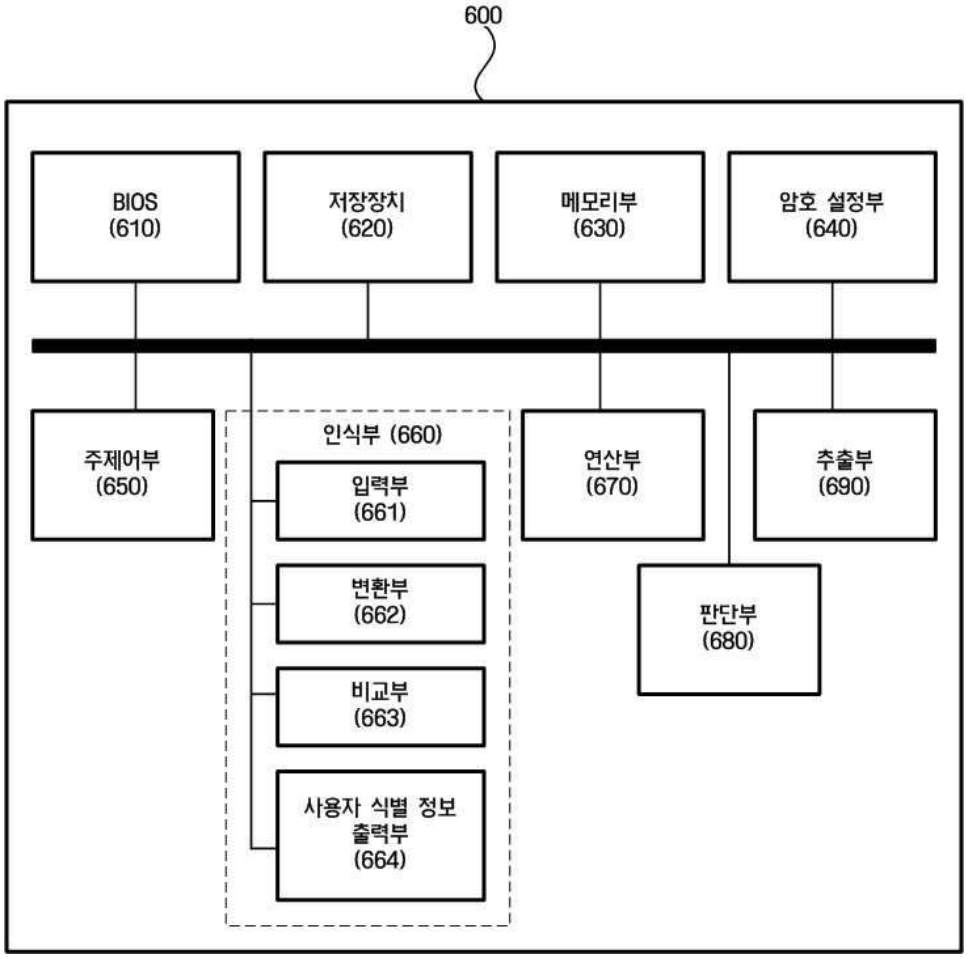
도면4



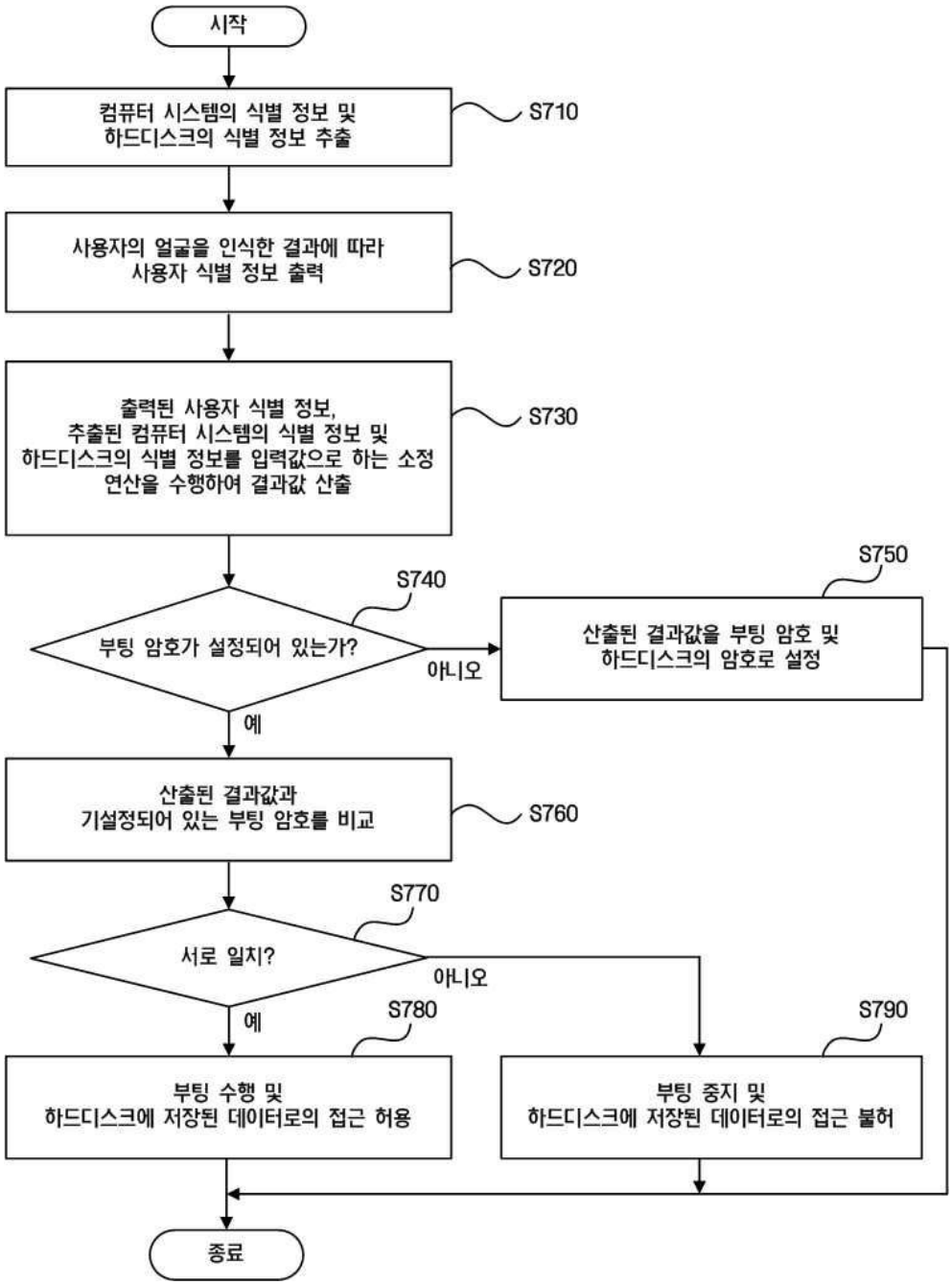
도면5


시작
사용자 식별 정보 인식
S510
컴퓨터 시스템의 식별 정보 및
하드디스크의 식별 정보 추출
S520
인식된 사용자 식별 정보,
추출된 컴퓨터 시스템의 식별 정보 및
하드디스크의 식별 정보를 입력값으로 하는 소정
연산을 수행하여 결과값 산출
S530
S540
부팅 암호가 설정되어 있는가?
아니오
S550
산출된 결과값을 부팅 암호 및
하드디스크의 암호로 설정
예
산출된 결과값과
기설정되어 있는 부팅 암호를 비교
S560
S570
서로 일치?
아니오
예
S580
부팅 수행 및
하드디스크에 저장된 데이터로의 접근 허용
S590
부팅 중지 및
하드디스크에 저장된 데이터로의 접근 불허
종료

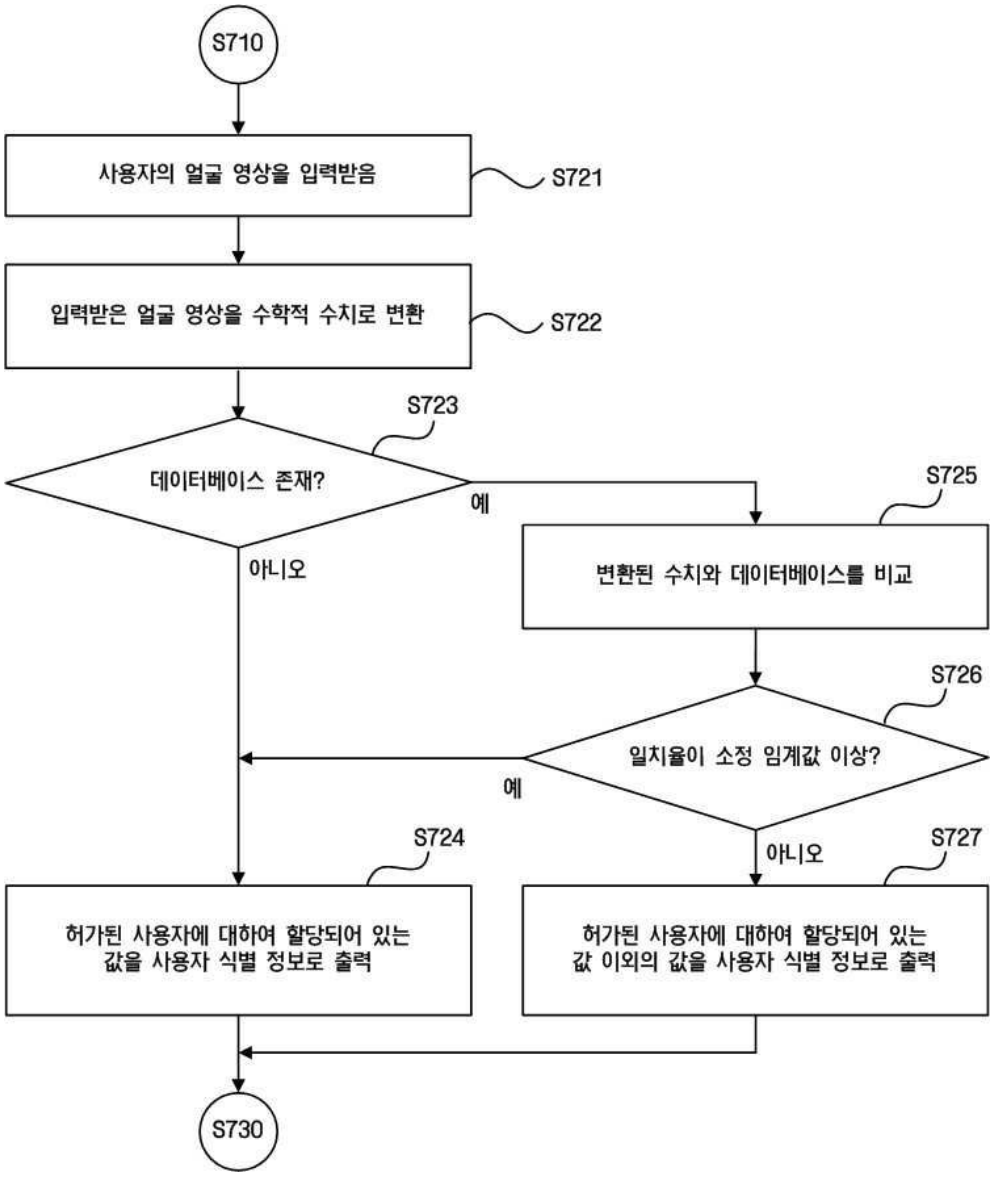
도면6


600
BIOS
(610)
저장장치
(620)
메모리부
(630)
암호 설정부
(640)
주제어부
(650)
인식부 (660)
입력부
(661)
변환부
(662)
비교부
(663)
사용자 식별 정보
출력부
(664)
연산부
(670)
판단부
(680)
추출부
(690)

도면7


시작
컴퓨터 시스템의 식별 정보 및 하드디스크의 식별 정보 추출
S710
사용자의 얼굴을 인식한 결과에 따라 사용자 식별 정보 출력
S720
출력된 사용자 식별 정보, 추출된 컴퓨터 시스템의 식별 정보 및 하드디스크의 식별 정보를 입력값으로 하는 소정 연산을 수행하여 결과값 산출
S730
S740
부팅 암호가 설정되어 있는가?
아니오
S750
산출된 결과값을 부팅 암호 및 하드디스크의 암호로 설정
예
산출된 결과값과 기설정되어 있는 부팅 암호를 비교
S760
S770
서로 일치?
아니오
예
S780
부팅 수행 및 하드디스크에 저장된 데이터로의 접근 허용
S790
부팅 중지 및 하드디스크에 저장된 데이터로의 접근 불허
종료

도면8


S710
사용자의 얼굴 영상을 입력받음
S721
입력받은 얼굴 영상을 수학적 수치로 변환
S722
S723
데이터베이스 존재?
예
아니오
S725
변환된 수치와 데이터베이스를 비교
S726
일치율이 소정 임계값 이상?
예
아니오
S724
허가된 사용자에 대하여 할당되어 있는 값을 사용자 식별 정보로 출력
S727
허가된 사용자에 대하여 할당되어 있는 값 이외의 값을 사용자 식별 정보로 출력
S730