

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.⁶
G06K 9/00

(11) 공개번호 10-2001-0020180
(43) 공개일자 2001년03월 15일

(21) 출원번호	10-1999-7009750	(87) 국제공개번호	WO 98/48371
(22) 출원일자	1999년10월21일	(87) 국제공개일자	1998년10월29일
번역문제출일자	1999년10월21일		
(86) 국제출원번호	PCT/US 98/03783		
(86) 국제출원출원일자	1998년02월26일		
(81) 지정국	AP ARIPO특허 : 가나 감비아 케냐 레소토 말라위 수단 스와질랜드 우간다 짐바브웨 EA 유라시아특허 : 아르메니아 아제르바이잔 벨라루스 키르기즈 카자흐 스탄 몰도바 러시아 타지키스탄 투르크메니스탄 EP 유럽특허 : 오스트리아 벨기에 스위스 리히텐슈타인 독일 덴마크 스페인 핀란드 프랑스 영국 그리스 아일랜드 이탈리아 룩셈부르크 모나코 네덜란드 포르투갈 스웨덴 OA OAPI특허 : 부르키나파소 베냉 중앙아프리카 콩고 코트디부아르 카 메룬 가봉 기네 말리 모리타니 니제르 세네갈 차드 토고 국내특허 : 알바니아 아르메니아 오스트리아 오스트레일리아 아제르바이 잔 보스니아-헤르체고비나 바베이도스 불가리아 브라질 벨라루스 캐나 다 스위스 리히텐슈타인 중국 쿠바 체코 독일 덴마크 에스토니아 스페인 핀란드 영국 그루지야 가나 감비아 기네비소 헝가리 인도네 시아 이스라엘 아이슬란드 일본 케냐 키르기즈 북한 대한민국 카자 흐스탄 세인트루시아 스리랑카 라이베리아 레소토 리투아니아 룩셈부 르크 라트비아 몰도바 마다가스카르 마케도니아 몽고 말라위 멕시코 노르웨이 뉴질랜드 폴란드 포르투갈 루마니아 러시아 수단 스웨덴 싱가포르 슬로베니아 슬로바키아 시에라리온 타지키스탄 투르크메니스 탄 터어키 트리니다드토바고 우크라이나 우간다		
(30) 우선권주장	8/837,549 1997년04월21일 미국(US)		
(71) 출원인	디지털퍼소나, 인코포레이티드 에트로 피오렐라		
(72) 발명자	미국 94063 캘리포니아주 레드우드시 베테란스 블루바드 805 스위트 226 반스씨.존 미국,94070캘리포니아,산카를로스,클리프톤애비뉴431 서지제이.베론지 미국,94709캘리포니아,버클리,하이랜드플레이스#2081771		
(74) 대리인	김윤배, 이범일		

심사청구 : 없음

(54) 지문인식시스템

요약

본 발명에 의하면, 지문인식방법 및 장치가 제공된다. 지문은 센서에 의해 검출된다(520). 그리고, 지문이 계수화된다(525). 계수화된 배경은 지문으로부터 제거되고, 이로써 차자국이 생성된다(530). 차자국은 지문 형판의 데이터 베이스와 매치된다(660).

대표도

도5

명세서

기술분야

본 발명은 생물계측학에 관한 것으로, 특히 생물계측학을 이용하는 개개인의 전자적 검증 및 식별에 관한 것이다.

배경기술

보안 컴퓨터 시스템과 전자적 처리는 전자 세대로 들어감에 따라 더욱 더 중요해지고 있다. 현존하는 패스워드와 암호화기술은 컴퓨터 시스템, 전자 상거래 및, 전자적 처리의 보안 문제를 적절히 해결하기 위한 방법으로 간주된다. 이러한 해결은 개개인과 관련한 디지털 식별 키의 세트가 전자적 처리 및 정보 교환을 안전하게 수행할 수 있는 것을 확실히 한다. 그러나, 이러한 식별 키가 정당한 소유자에 의해서만 사용될 수 있는 것을 확실히 하지 않게 한다. 이는 보안 컴퓨터 액세스, 전자 상거래, 홈뱅킹, 판매, 전자적 처리, 유사 메카니즘이 올바르게 안전하게 되면 필요로 되는 임계 링크이다.

현재, 패스워드는 이러한 대부분의 논쟁을 처리한다. 예컨대, 컴퓨터 시스템에 로그인하는 것과 같은 대부분의 전자적 처리는 패스워드를 요구하는 자동 금전 출납기, 처리 지불 카드, 전자 뱅킹 및, 유사 처리외에는 돈을 받는다. 시스템이 더욱더 보안을 요구하고, 사용자가 패스워드의 확장되는 리스트를 언제라도 저장할 수 있도록 요구되기 때문에 패스워드는 불완전한 해결이다. 더욱이, 사용자가 패스워드를 입력할 때, 패스워드는 개개인을 관측함으로써 비교적 쉽게 얻어진다. 더욱이, 사용자가 다른 사람과 패스워드를 통신하지 않게 되어 패스워드를 잃어버리거나 훔치는 것에 대해 보증이 없다. 따라서, 많은 기능에 대해 충분한 보안으로 고려되지 않게 된다.

더욱 종종, 지문 식별이 고려된다. 지문은 개개인에 대해 유일하고, 저장할 필요가 없으며, 사용하기에 비교적 어렵다는 이점이 있다. 일반적으로, 지문인식은 지문감지장치에 사용자의 손가락을 위치시키는 것을 요구한다. 각 지문은 흉과 이랑의 유일한 배열로 구성된다. 지문감지장치는 동축 케이블을 매개로 사용자의 지문의 아날로그 이미지를 컴퓨터 시스템에 전송한다. 이 때, 컴퓨터 시스템은 지문을 컴퓨터 시스템의 지문 형틀의 데이터베이스와 매치시킨다. 그러나, 종래의 지문인식방법에는 몇가지 문제가 있다.

먼저, 손가락이 위치되는 장치인 지문감지장치는 그 크기가 너무 크다. 이는 이러한 장치가 휴대용 컴퓨터, 소비자 전자제품, 또는 공간이 고가인 상황에서 이용되어지기 위해 적용할 수 없다는 것을 의미한다.

부가적으로, 일반적으로 지문장치는 컴퓨터 시스템에 연결됨과 더불어 전원에 대한 연결을 요구한다. 이는 지문장치가 사용되면 부가적인 전원이 소모됨을 의미한다. 따라서, 이러한 장치는 여분의 전원이 가능하지 않은 상황에서 이용하기 위해 적용할 수 없게 된다.

더욱이, 통상적인 지문장치는 일반적으로 동축 케이블을 매개로 지문의 아날로그 이미지를 전송하기 때문에 보안이 침해된다. 아날로그 지문 이미지는 동축 케이블상에서 전송된 이미지를 가로챌으로써 얻을 수 있다. 따라서, 거짓 사용자가 이미지 포착장치를 갖는다면, 그는 포착된 이미지를 재전송함으로써 원래의 사용자를 흉내낼 수 있게 된다. 이는 실질적인 지문감지 진행이 어느 누구에 의해 관측되지 않는 경우에 보안성을 감소시킨다.

더욱이, 일반적으로 통상적인 시스템에서의 지문 처리가 컴퓨터 시스템에서 야기되기 때문에, 컴퓨터 시스템 그 자체는 지문감지장치에 의해 제공된 보안을 헛되게 하도록 변조될 수 있다. 결국, 컴퓨터 시스템은 장치로부터 수신된 지문을 데이터베이스의 자국과 매치시킬 것인가를 결정한다. 데이터베이스가 변경될 수 있거나 데이터베이스에 대해 자국을 매치시키는 처리가 잘못된 포지티브 지시를 보내도록 변경될 수 있다. 이러한 방법에서, 지문감지시스템의 이점이 상실될 수 있다.

더욱이, 통상적인 시스템에 있어서, 사용자는 지문감지 시스템과 상호작용하는 것을 요구한다. 일반적으로, 지문을 감지하는 종래의 처리는 다음과 같다. 먼저, 사용자는 그의 손가락을 감지센서판에 위치시킨다. 지문의 이미지가 십자선과 함께 컴퓨터 모니터상에 디스플레이된다. 사용자는 십자선이 중앙에 있도록 그 손가락의 위치에 대해 묻고, 자국이 명확하게 디스플레이된다. 손가락이 적절한 위치에 있는 것을 사용자가 결정할 때, 사용자는 이것이 전송되어질 이미지이라는 것을 지시하도록 버튼을 눌러야만 한다. 사용자가 다시 한번 적절한 지문을 선택하면, 장치는 이미지를 취하고, 처리를 위해 컴퓨터 시스템에 이를 전송한다. 그러나, 이러한 거북하고, 예러가 일어나기 쉬운 진행은 사용자에게 의해 적극적 참여와 제어를 요구한다. 이러한 상호작용이 요구되지 않는다면 이점이 있다.

더욱이, 통상적인 지문장치는 사용자의 손가락이 너무 건조하거나 기름기가 많고, 또는 손가락이 놓이는 감지판이 더럽다면, 매우 정확하지 않게 된다. 이는 다양한 이유에 대해 야기된다. 일반적인 통상적 지문장치는 감지판상에 위치한 손가락의 화상을 취한다. 손가락의 이랑과 같은 감지판과 접촉하는 무엇인가가 있는 장소는 광을 반사하지 않고 흡수한다. 손가락의 흉과 같은 감지판과 접촉하는 무엇인가가 없는 장소는 광을 반사한다. 이는 감지센서판상의 흡수 및 반사된 광의 이미지를 발생시킨다. 그러나, 감지판상의 먼지 및 얼룩은 또한 광을 흡수함에 따라 잘못된 이미지를 발생시킨다. 이러한 이미지는 실질적인 이미지를 나타내는 것에 더하여 감지판상의 모든 먼지 및 얼룩을 나타낸다. 종래 기술에 있어서 이를 해결하기 위한 하나의 방법은 이미지를 포착하기 위해 손가락에 더 강한 빛을 비추는 것이다. 더 강한 빛은 감지판상의 얼룩을 통해 통과되기에 충분히 강하고, 따라서 감지판상에 어떠한 잔재가 있음에도 불구하고 광이 반사된다. 그러나, 이러한 강한 빛의 이용은 다른 문제를 야기시킨다. 더 밝은 빛은 더 많은 전력을 요구한다. 또한, 더 밝은 빛은 완전히 명확하지 않은 지문을 픽업하기 쉽게 된다. 예컨대, 사용자의 손가락이 건조하고, 이랑이 잘 정의 되지 않으면, 밝은 빛은 그를 픽업할 수 없게 된다.

따라서, 이는 더러운 감지판에 의해 반대의 영향을 주지 않고, 종래의 보안 침해를 허용하지 않는 더욱 정확한 지문감지 방법이 요구된다.

본 발명은 상기한 점을 감안하여 발명된 것으로, 지문인식을 위한 장치 및 방법을 제공함에 그 목적이 있다.

발명의 상세한 설명

상기 목적을 달성하기 위한 본 발명에 있어서, 지문이 디지털화된다. 디지털화된 배경이 지문으로부터 감해짐으로써 다른 자국을 초래한다. 다른 자국은 지문 형틀의 데이터베이스와 매치된다.

각 지문이 검출된 후, 배경은 개시시 감지판의 이미지를 취함으로써 얻어진다. 따라서, 얼룩, 평탄하지 않은 광 및 다른 요소를 포함하는 배경의 현재 상태가 검출됨과 더불어 디지털화된 지문으로부터 감해진다.

도면의 간단한 설명

도 1은 본 발명의 1실시예가 실행될 수 있는 샘플 시스템의 개략도,
 도 2는 디지털 처리 시스템과 센서의 기능블럭도,
 도 3은 네트워크 센서와 서버의 1실시예의 기능 블럭도,
 도 4는 지갑의 1실시예의 기능 블럭도,
 도 5는 센서에서 야기되는 처리를 나타낸 개략적인 플로우차트,
 도 6a 및 도 6b는 디지털 시스템에서 야기되는 처리를 나타내는 개략적인 플로우차트,
 도 7은 본 발명의 보안 처리의 1실시예를 설명하는 플로우차트,
 도 8a 및 도 8b는 본 발명의 센서의 1실시예의 도면,
 도 9는 도 8의 FPGA의 도면,
 도 10은 본 발명의 디지털 시스템의 1실시예의 도면,
 도 11a 및 도 11b는 지문을 등록하는 처리를 나타낸 플로우차트,
 도 12a는 지문 이미지를 포착하는 처리를 나타낸 플로우차트,
 도 12b는 본 발명에서 이용된 필터링처리의 도면,
 도 12c는 지문 이미지를 포착하는 동안 점진적으로 취한 지문 스냅 사진의 도면,
 도 13은 자동 착수 처리를 설명하는 플로우차트,
 도 14는 본 발명의 지문식별 시스템과 관련한 스마트카드를 이용하는 처리를 설명하는 플로우차트이다.

실시예

생물계측학을 이용하는 개개의 전자적 검증 및 식별을 위한 방법 및 장치를 설명한다. 설명의 목적을 위한 다음의 설명에 있어서, 본 발명의 이해를 통해 제공하기 위해 다양한 특정 상세가 설명된다. 그러나, 본 발명은 이러1실시예에 한정되는 것은 아니고, 본 발명의 요지를 벗어나지 않는 범위내에서 다양하게 실시할 수 있음은 물론이다.

개요

도 1은 본 발명의 1실시예를 수행할 수 있는 샘플 시스템의 개략도이다. 디지털 시스템(110)은 수신된 디지털화된 이미지와 디지털화된 형틀의 데이터베이스를 비교하고, 디지털화된 이미지를 수신하기 위한 디지털 연결을 제어하는 처리능력을 갖춘 계산 시스템이다. 본 실시예에 있어서, 디지털 연결은 통상적으로 잘 알려진 USB(universal serial bus)에 대해 확인되는 데이터 버스이다. 이러한 도면에 있어서, 디지털 시스템(110)은 컴퓨터 시스템으로 표현된다. 컴퓨터 시스템(110)은 컴퓨터 시스템(110)의 처리능력을 포함하는 보디(120)를 포함한다. 또한, 컴퓨터 시스템(110)은 디스플레이(130)를 포함한다. 디스플레이(130)는 액정디스플레이(LCD), CRT, 또는 유사한 디스플레이 메카니즘일 수 있다. 컴퓨터 시스템(110)은 데이터 입력 메카니즘(14)을 포함한다. 예컨대, 키보드(14))가 설명된다. 키보드(14)는 컴퓨터 시스템(110)과 대화하도록 사용자를 허용한다. 통상적인 커서 제어장치(145)가 더 설명된다. 커서 제어장치(145)는 마우스, 트랙볼, 펜, 또는 유사한 장치일 수 있다.

1실시예에 있어서, 센서(150)가 케이블(17)을 매개로 컴퓨터 시스템(110)에 결합된다. 한편, 센서(150)는 적외선, 라디오 주파수, 모뎀, 네트워크, 또는 다른 직간접 디지털 연결을 매개로 컴퓨터 시스템(110)에 연결될 수 있다.

본 발명의 센서(150)는 지문 인식을 위해 손가락이 위치하는 센서판(16)을 포함한다. 1실시예에 있어서, 케이블(70)은 USB 연결이다. 다른 디지털 연결이 또한 이용될 수 있음은 통상적인 기술에 의해 명백히 알 수 있다. 센서(15)는 전원에 대한 연결을 더 갖는다. 그러나, 케이블(170)이 USB 연결이라면, 전원을 제공하는 USB 연결과 같은 이러한 부가적 전원 연결을 요구하지 않는다. 도 1은 단지 본 발명이 실시되는 시스템의 1실시예를 설명하는 것을 알 수 있다. 휴대용 컴퓨터(110)와 같은 다른 구성, 도시된 모든 구성요소를 갖추지 않은 디지털 시스템 또는 다른 크기와 형태를 갖춘 센서(15)가 이용될 수 있다.

도 2는 본 발명의 디지털 시스템(210)과 센서(250)의 기능 블럭도이다. 1실시예에 있어서, 디지털 시스템(210)은 컴퓨터 시스템(110)의 예일 수 있다. 디지털 시스템(210)은 데이터를 임시 저장하기 위한 임시 데이터 저장기(215)를 포함한다. 임시 데이터 저장기(215)는 RAM 및 다양한 레지스터를 포함할 수 있다. 더욱이, 디지털 시스템(210)은 데이터베이스(220)를 포함한다. 데이터베이스(220)는 지문 형틀을 저장하기 위한 것으로, 예컨대 각 개인 누가 시스템에 등록되어 있는가에 대해 데이터를 인식한다. 비교기(225)는 지문 데이터를 비교하기 위한 것이다. 1실시예에 있어서, 비교기(225)는 데이터베이스(220)에 저장된 데이터와 임시 데이터 저장기(215)에 저장된 데이터를 비교할 수 있다. 비교기(225)는 제공된 데이터가 매치되는가의 여부를 결정하여 출력한다.

보안 유니트(230)는 라인(290)상에서 디지털 시스템(210)과 센서(250)간에서 전송된 암호 및 해독 메시지를 이용하고, 결정 및 유지함과 더불어 세션 키를 이용한다. 보안 유니트(250)에 대해 다음에 더욱 상세

히 설명한다. 인터페이스(235)는 사용자, 디지털 시스템(210)의 다른 프로그램, 센서(25)와 상호작용한다. 인터페이스(235)는 WINDOWS나 MACINTOSH 환경에서 다양한 창을 디스플레이할 수 있다. 윈도우즈는 마이크로소프트사의 상표이고, 맥킨토시는 애플 컴퓨터사의 상표이다.

카드 수신 유닛(240)는 디지털 시스템(210)과 통합될 수 있거나, 버스, 케이블, 적외선, 또는 다른 연결방법을 매개로 디지털 시스템(210)에 부착될 수 있다. 카드 수신 유닛(240)는 카드의 홀더와 관련한 개인 정보를 저장하고, 지문 정보를 포함할 수 있는 토큰, 스마트카드, 바코드, 디스켓, 또는 유사 매체를 수신하기 위한 것이다. 카드 수신 유닛(240)는 카드에 저장된 지문 정보와 관련한 카드 홀더의 식별을 검증하는데 이용될 수 있다.

등록 유닛(245)는 디지털 시스템(210)에 따라 등록하도록 사용자를 이네이블시켜 사용자의 지문 식별이 데이터베이스(220)에 위치된다. 더욱이, 디지털 시스템(210)은 USB 제어기(205)를 포함한다. 1실시에 있어서 USB 제어기(205)는 디지털 시스템(210)과 센서(250)를 결합한다. USB 제어기(205)는 데이터로 뿐만 아니라 센서(250)에 대해 전원을 제공한다. USB 제어기(205)의 기능은 1996년 1월 15일, Universal Serial Bus Specification, 개정1.0,에서 더욱 상세한 내용을 찾을 수 있다.

센서(250)는 연결(290)을 통해 디지털 시스템(210)에 결합된다. 1실시에 있어서, 연결(290)은 데이터와 전원 연결 모두를 제공하는 USB이다. 한편, 센서(250)는 분리 전원연결을 갖을 수 있다.

센서(250)는 데이터 저장유닛(255)를 포함한다. 데이터 저장유닛(255)는 RAM, 레지스터 뿐만 아니라 메모리를 포함할 수 있다. 데이터 저장유닛(255)는 자국의 중간값, 형틀, 합, 세션 키, 영구적 센서 신호 및, 유사 데이터를 저장한다.

더욱이, 센서(250)는 감지 메카니즘(260)을 포함한다. 감지 메카니즘(260)은 사용자가 식별을 위해 그 손가락을 위치시킬 수 있는 감지판을 포함한다. 감지 메카니즘(260)은 적어도 하나의 프리즘을 조사하는 빛으로 구성된 통상적인 지문감지 메카니즘일 수 있고, 이는 감지판상의 자국을 반사한다. 반사된 자국은 검출 어레이에 의해 수신된다. 한편, 감지 메카니즘(260)은 용량 센서를 포함하는 다른 감지 방법을 이용할 수 있다.

센서(250)는 더욱이 디지털타이저(265)를 포함한다. 디지털타이저(265)는 감지 메카니즘(260)으로부터 수신된 이미지를 디지털화한다. 이미지를 디지털화하는데 이용될 수 있는 메카니즘은 잘 알려진 기술이다. 1실시에 있어서, 통상적인 아날로그-디지털 변환기가 이용된다.

센서(250)는 더욱이 감산기(270)를 포함한다. 감산기(270)는 이하 설명하는 바와 같이 디지털화된 지문 이미지를 필터링하고, 자국으로부터 배경 이미지를 감하는데 이용된다.

센서(250)의 보안 유닛(275)는 디지털 시스템(210)의 보안 유닛(230)에 대응된다. 그러나, 이는 부정 사용 방지 환경에서 그 사인인 센서의 개인 키를 저장할 수 있다.

마지막으로, 센서(250)는 결정 구현 유닛(280)을 포함한다. 결정 구현 유닛(280)은 지문이 데이터베이스(220)에서의 자국과 매치되는가의 마지막 결정을 만드는데 이용될 수 있다. 결정 구현 유닛(280)은 디지털 시스템(210)이 보안화되지 않아 확고한 보안이 요구될 때 이용될 수 있다. 상기 설명한 구성 요소의 기능이 이하 상세히 설명된다.

1실시에 있어서, 디지털 시스템(210)은 컴퓨터 시스템, PCMCIA 카드, 휴대용 컴퓨터, 네트워크 스테이션 및 서버, 팜탑 컴퓨터, 또는 요구된 데이터를 처리할 수 있는 다른 시스템일 수 있다. 더욱이, 센서(250)는 디지털 시스템(210)내에 위치될 수 있다. 이 경우, 중복 메모리, 보안 유닛 및 USB 제어기가 요구되지 않는다.

도 3은 본 발명이 이용될 수 있는 네트워크를 도시한 것이다. 센서(310)가 호스트(320)에 결합된다. 호스트(320)가 네트워크(330)에 연결되도록 이네이블되고, 이는 다수의 시스템(320, 340, 350)과 함께 결합된다. 서버(340)는 센서(310)에 의해 수신된 지문과 매치되는 데이터베이스를 포함한다. 다른 시스템(350)이 그 처리능력에 대해 이용될 수 있다. 따라서, 실질적인 지문 인식 처리는 다수의 시스템(320, 340, 350)을 거쳐 분배될 수 있다. 이러한 분배된 처리는 네트워크를 통해 원격 데이터를 액세스 하기 위해 이용될 수 있다. 서버(340)도 다른 시스템(350)도 보안이 되지 않기 때문에, 보안 목적을 위해 마지막 매칭이 센서(310)에서 수행될 수 있다. 이는 처리된 데이터를 센서(310)에 다시 보냄으로써 달성된다. 따라서, 센서(310)는 매치된 엘리먼트와 원래의 지문을 수신한다. 매치된 엘리먼트가 원래의 지문과 정말로 매치되는지의 검증은 센서(310)에서 달성될 수 있는 처리이다. 따라서, 센서(310)는 매치/비매치된 신호를 보낼 수 있고, 따라서 비보안 네트워크(330)를 거쳐 보안 시스템을 야기시킨다.

도 4는 지갑(400)으로 분리워지는 단일 유닛에 센서(250)와 디지털 시스템(210)의 기능성을 조합한 시스템의 1실시의 블럭도이다. 지갑(400)은 소프트웨어 및 하드웨어의 다른 구성에 따라 실현될 수 있다. 예컨대, 전체 지갑(400)은 스마트 카드에 위치할 수 있고, 또는 스마트 카드, 데이터 베이스 및, 네트워크를 통해 분배된 매칭/제어 소프트웨어를 포함하는 분배 시스템으로서 실현될 수 있다.

감지유닛(410)은 손가락이 위치하는 감지판(415)을 갖는다. 감지 유닛(410)은 이미지를 수신하고, 디지털타이저(420)로 보낸다. 디지털타이저(420)는 지문 이미지를 디지털화하고, 매칭 유닛(425)로 보낸다. 더욱이, 매칭 유닛(425)는 형틀의 데이터베이스를 저장하는 저장 유닛(430)에 대한 액세스를 갖는다. 매칭 유닛(425)는 수신된 지문의 형상과 저장 유닛(430)의 형틀을 매치시킨다. 1실시에 있어서, 이러한 지갑(400)은 자국이 저장 유닛(430)에 저장된 오직 한 개인에 속한다. 매칭 유닛(425)는 자국 매치 여부를 예/아니오 결정에 따라 데이터 흐름 제어유닛(435)에 보낸다. 데이터 흐름 제어유닛(435)는 사용자 데이터 유닛(440)에 저장된 데이터에 대한 액세스를 제어한다. 더욱이, 데이터 흐름 제어유닛(435)는 지갑(400)에 대해 사용자의 액세스가 한번 검증되면 지갑(400)에 정보를 업로드하도록 사용자를 허용할 수 있다.

사용자 데이터 유닛(440)은 사용자의 크레딧 카드번호, 사회보장번호 및 ID 등의 정보를 수용할 수 있다. 사용자 데이터 유닛(440)은 사용자가 그 사용자 데이터 유닛(440)에 저장하기를 원하는 소정

의 정보를 더 수용할 수도 있다. 지갑(400)은 키보드, 마우스, 트랙볼, 터치 패드 등의 제어기구(445)를 더 포함할 수 있다. 사용자는 지갑(400)에 데이터를 부가하기 위해 제어메카니즘(445)을 사용할 수 있다.

도 5는 센서(250)에서 일어나는 처리의 개관을 설명하는 플로우차트이다. 블록 505에서, 센서가 턴온된다. 이것은, 디지털 시스템(210)이 최초로 턴온된 때에 일어날 수 있다. 또한, USB(universal serial bus: 통괄적인 직렬버스)(290)가 플러그 앤 플레이(plug-and-play)를 허용하기 때문에, 이것은 센서가 최초로 디지털 시스템(210)에 연결된 때에 일어날 수 있다.

블록 510에서는, 초기화 및 보안 핸드셰이크(security handshake)가 일어난다. 디지털 시스템(210)과 센서(250)의 연결이 보안연결로 되도록 설계되어 있기 때문에, 보안 핸드셰이크는 센서(250)가 대체되지 않았다는 것과, 디지털 시스템(210)이 변조되지 않았다는 것을 보증한다. 보안 핸드셰이크는 통상의 암호화 또는 공개/개인키 방법을 이용하여 실행될 수 있다.

블록 515에서는, 배경 이미지가 포착되고 계수화된다. 센서(250)가 초기화되어 있을 때, 촬상유니트(260)의 광학적인 광원이 턴온되고, 이미지가 포착된다. 이때, 센서 플레이트(sensor platen)에는 지문이 없고, 따라서 이 이미지가 배경 이미지로 된다. 계수화된 배경은 데이터 저장매체(255)에 일시적으로 저장된다. 또한, 배경 이미지는 디지털 시스템(210)으로 전송되어 데이터 저장유니트(215)에 저장되어도 좋다. 배경 이미지는 배경 잡음 및 이미지를 추정하는데에도 사용될 수 있고, 전체적인 이미지를 추정하는데도 사용될 수 있다. 1실시에에서는, 포착된 각 배경 이미지는 센서가 사용할 수도 있는 평균 배경을 산출하기 위해 더 처리된다. 이 학습처리는 이하에 좀더 상세히 설명하기로 한다.

블록 520에서는, 시스템은 센서 플레이트에 지문이 검출되어 있는지의 여부를 시험한다. 1실시에에서는, 지문검출은 센서 플레이트로부터 수신된 광의 에너지 레벨의 측정이다. 에너지 레벨이 일정 레벨 이하로 떨어지면, 지문이 검출된다. 또한, 지문은 압력센서, 열센서 또는 유사한 장치의 결과로 검출되어도 좋다.

센서 플레이트상에 검출된 지문이 없으면, 처리는 블록 515로 돌아가고, 새로운 배경 이미지가 포착되고 계수화된다. 1실시에에서는, 검출된 지문이 없으면, 대략 2초마다 새로운 배경 이미지가 포착된다. 또한, 원래의 배경을 유지해도 좋다. 지문이 검출되면, 처리는 블록 525로 계속된다.

블록 525에서는, 지문 이미지가 포착되고 계수화된다. 상술한 바와 같이, 촬상유니트(260)는 센서 플레이트상에 위치되어 검출기 어레이에 의해 포착된 지문의 이미지를 수신한다. 포착된 지문은 계수화되고 저장된다. 계수화된 지문은 센서(250) 또는 디지털 시스템(210)에 저장될 수 있다.

블록 530에서는, 계수화된 배경 이미지가 계수화된 지문으로부터 제거되어 차자국(differential print)을 생성한다. 지문 이미지로부터 배경 이미지를 제거하는 것은, 센서 플레이트상의 얼룩과 오물 또는 불규칙한 발광조건으로 인해 이미지의 레벨을 떨어뜨린다. 배경 이미지를 제거함으로써, 차자국은 센서 플레이트상에 위치되었던 지문의 더욱 뚜렷한 표현이다. 여기에서, 제거란 획득된 자국 - 배경 이미지의 차를 취하거나, 광학적으로 불완전성 및 촬상조건의 영향을 떨어뜨리는 이미지와 배경의 소정 함수를 의미한다. 1실시에에서는, 제거중에 배경의 화소값이 지문의 값보다도 높으면, 그 결과는 디폴트값(default value)으로 설정된다. 따라서, 예컨대 배경의 화소값이 150이고, 지문의 화소값이 300이면, 그 결과는 0, 30 또는 다른 디폴트값으로 설정될 수 있다. 이와 같이, 오제거(false subtraction) 및 음수가 회피된다.

블록 535에서는, 새로운 배경 이미지가 포착되고 계수화된다. 손가락을 센서로부터 치움에 따라, 새로운 배경의 이미지, 이전의 배경에 가산된 마지막 손가락의 얼룩의 결과가 새로이 포착된다.

블록 540에서는, 디지털 시스템(210)으로부터 난스(nonce)가 수신된다. 난스는 한가지 특별한 경우에만 사용되고 다시 사용되지 않는 신호 또는 코드이다. 난스는 날짜/시간 스탬프, 및 아마도 다른 데이터를 포함한다.

블록 545에서는, 차자국의 해시(hash)가 산출된다. 자국과 함께 전송되는 해시는 매치된 자국이 실제로 센서(250)에 의해 포착된 자국이라는 것을 확실하게 해준다. 부가적으로, 난스를 해시에 포함시킴으로써, 매치된 지문의 시간/날짜가 검증된다. 이것은, 사용자가 가양성표시(false positive indication)을 얻기 위해 더 오래된 자국을 재전송하는 것을 방지한다.

블록 550에서는, 해시 및 차자국이 디지털 시스템(210)으로 전송된다. 디지털 시스템(210)은 이하에 좀더 상세히 설명하는 바와 같이 또 다른 지문을 처리하기 위해 사용된다.

도 6a 및 도 6b는 디지털 시스템(210)에서 일어나는 처리의 개관을 설명하는 플로우차트이다. 디지털 시스템(210)은 컴퓨터 시스템, 컴퓨터 시스템에 연결된 서버, 자급식 PCMCIA 카드, 네트워크 또는 유사한 장치나 지문을 매치하기 위해 처리전력을 갖는 장치일 수 있다.

블록 605에서는, 시스템이 턴온 및/또는 센서에 연결된다. 1실시에에서는, 이것은 컴퓨터 시스템이나 디지털 시스템(210)의 다른 하드웨어가 실행되어 최초로 턴온된 때에 자동적으로 일어난다. 또한, 사용자는 키스트로크(keystroke), 마우스선택에 의해 본 시스템을 시작하여 센서(250)를 플러그 앤 플레이 연결이나 유사한 동작을 통해 디지털 시스템(210)에 연결할 수 있다.

블록 610에서는, USB가 초기화된다. USB는 데이터 및 전력연결을 제공하는 통신아키텍처이다. USB 제어기(205)는 USB 사양에 따라 초기화된다. 또한, 그 연결이 USB연결이 아닌 경우에는, 이 단계를 무시하거나, 다른 디지털 연결 초기화단계를 수행해도 좋다.

블록 615에서는, 초기화신호 및 전력이 센서(250)로 전송된다. 이것은, 도 5를 참조하여 상술한 바와 같이 센서(250)를 턴온한다. 프로토콜은 안전한 트랜잭션(transaction)을 위해 필요한 정보를 초기화한다. 이 처리는 후에 좀더 상세히 설명하기로 한다.

블록 620에서는, 센서(250)에 의해 지문이 검출되었다는 것을 나타내는 신호가 수신되었는지의 여부가 판단된다. 센서(250)가 지문을 검출할 때에는, 디지털 시스템(210)으로 신호를 보낸다. 그러한 신호가 수

신되지 않은 경우에는, 처리는 이 신호를 대기한다. 그 신호가 수신된 때, 처리는 블록 625로 계속된다. 1실시에에서는, 이 처리는 도 6a에서 루프로서 설명했지만, 이것은 대기중에 그 시스템이 다른 동작을 수행할 수도 있는 인터럽트 구동처리이어도 좋다. 센서(250)로부터의 신호의 도착은 그 디지털 시스템에서 디지털 시스템(210)의 적당한 소프트웨어가 그 신호에 반응하도록 활성화되는 사건(인터럽트)을 발생시킨다. 이러한 인터럽트처리는 이 기술분야에서 알려져 있다.

블록 625에서는, 난수가 센서(250)로 전송된다. 난수는 시간/날짜 스탬프, 현재의 세션 키(session key) 및 다른 정보를 포함한다. 이것은, 센서의 ID뿐만 아니라 지문의 통용기간(currency)을 검증하기 위해 사용된다.

블록 630에서는, 센서(250)로부터 차자국이 수신된다. 이것은, 한번 더 인터럽트이어도 좋다. 상술한 바와 같이, 해시는 난수와 차자국의 조합이다. 블록 635에서는, 해시가 디코드되고, 난수가 검증된다. 부가적으로, 세션 키가 검증되어도 좋다.

블록 640에서는, 차자국이 형판(template)의 데이터베이스와 비교된다. 형판의 데이터베이스는 이 시스템으로 등록된 모든 사용자를 포함한다. 수신된 자국은 데이터베이스의 자국과 비교된다. 이러한 방법은 이 기술분야에서 알려져 있다. 처리는 도 6b에 나타난 블록 A에서 계속된다.

도 6b를 참조하면, 블록 645에서는 본 발명의 처리가 예비 매치를 발견했는지의 여부가 시험된다. 매치가 발견되지 않은 경우에는, 처리는 직접 블록 670으로 계속된다. 예비 매치가 발견된 경우에는, 처리는 블록 650으로 계속되고, 최종적인 매칭을 위해 매치 및 해시가 센서로 복귀된다. 이것은, 실질 분석을 행하는 디지털 시스템이 안전하지 않은 경우에 필요하다. 자국과 매치 특성을 센서로 복귀시킴으로써, 처리를 안전하게 할 수 있다. 또한, 최적 매치는 디지털 시스템(210)에서 수행되어도 좋다.

블록 655에서는, 센서로부터 검증 매치/노매치(match/no match)신호가 수신된다. 센서는 닫혀 시스템을 안전하게 하기 때문에, 매치가 발견되었는지의 여부를 무시하고 최종 결정은 센서에 맡기고 있다. 이와 같이, 디지털 시스템(210)을 변조할 가능성이 없는 가양성신호(false positive signal)로 된다.

블록 660에서는, 최종 응답이 예스(yes)인지 노(no)이지, 즉 자국이 매치하는지 매치하지 않는지의 여부가 판단된다. 자국이 매치하지 않는 경우에는, 블록 670에서 액세스가 거절된다.

자국이 매치하는 경우에는, 블록 665에서 프로그램, 파일 또는 정보로의 액세스가 허용된다. 더욱이, 자국이 매치하면, 블록 675에서 인식한 사용자에게 대해 등록된 형판이 갱신된다. 갱신은 매치수, 즉 특징이 매치된 퍼센트를 나타내는 수에 귀착하여 양 방향으로 매칭처리를 실행함으로써 행해도 좋다. 이 수자에 기초하여 최적의 자국이 새로운 형판 자국으로서 선택되어도 좋다. 또한, 새로운 자국에서 얻어지는 정보를 부가함으로써 현재의 형판을 갱신하도록 역전파(back propagation)가 이용되어도 좋다. 또한, 현재의 형판을 갱신하기 위해 카호넨(Kahonen)형의 평범한 학습처리를 이용해도 좋다. 카호넨 학습처리는 이 기술에 정통한 자에게는 널리 알려져 있다.

도 5 및 도 6에 설명된 전체적인 매칭절차는 매우 빠르다. 1실시에에서는, 매칭절차는 대략 2분의 1초 걸린다.

보안 특징(security feature)

도 7은 본 발명에서 사용할 수 있는 보안 특징의 일례를 설명하는 플로우차트이다. 상술한 바와 같이, 반드시 디지털 시스템(210)을 안전하게 할 필요가 없기 때문에, 보안 절차는 이 시스템을 변조하는 것을 방지하기 위해 중요하다. 보안 절차의 하나는, 보안시스템에 최종 매칭을 갖게 하는 것이다. 이 보안시스템은 안전한 디지털 키와 데이터를 갖는 센서이어도 좋고, 보안 프로세서이어도 좋다. 1실시에에서는, 그러한 프로세서 및 칩은 예측이나 유사한 제거하기 어려운 재료로 그 칩을 피복함으로써 안전하게 만들어도 좋다. 또한, 센서에서는 보안시스템이 그 시스템을 부호화하기 어렵게 해도 좋다. 더욱이, 센서와 더 안전하게 처리하는데 사용되는 어떤 시스템 사이의 통신을 만들기 위해 공개키 개인키 시스템을 사용해도 좋다. 1실시에에서는, 세션 키를 이용하는 디피-헬만(Diffie-Hellman) 키교환이 이용된다. 이 기술분야에서 잘 알려진 다른 데이터 암호화방법을 이용해도 좋다. 암호화된 모든 데이터는, 본 발명에 의해 제공되는 센서와 디지털 시스템 사이에서 전송된다. 그러한 암호화는 본 발명이 안전하지 않은 환경의 넓은 범위에서 이용되는 것을 허용한다. 도 7은 디피-헬만 키교환을 설명하고 있다.

블록 710에서는, 디지털 시스템에 전력이 공급되고, 센서가 이 디지털 시스템에 연결된다. 블록 720에서는, 디지털 시스템이 인증(certificate)을 요청한다. 이 인증은 특정의 센서와 결합된 식별기(identifier)이다. 1실시에에서는, 인증은 제조시에 센서에 저장되어도 좋다. 각 센서는 특유의 인증을 가질 수 있다. 또한, 다중 센서가 동일한 시스템과 결합되어 있다면 이들 센서가 동일한 인증을 갖도록 해도 좋다. 예컨대, 큰 회사는 동일한 인증을 가짐으로써 상호 교환가능한 다중 센서를 구입해도 좋다.

블록 720에서는, 센서는 인증에 따라 반응한다. 이 점에서 센서 및 디지털 시스템이 상호 연결되어 있지만, 그들의 연결이 아직 안전하게 검증되어 있지 않다는 점에 주의해야 한다.

블록 730에서는, 디지털 시스템이 공개키를 이용하여 인증의 유효성을 시험한다. 센서는 인증의 일부인 개인키를 가지고 있다. 공개키는 개인키로 암호화된 서류를 디코드하기 위해 사용된다. 인증이 알려진 공개키를 이용하여 디코드될 수 없다면, 이것은 인증이 적절한 개인키로 암호화되지 않았기 때문에, 그 센서가 적당한 센서가 아니라는 것을 의미한다.

블록 740에서는, 디지털 시스템이 공개키를 이용하여 난수 및 시간 스탬프를 암호화하여 이것을 센서로 전송한다. 이것은, 센서만이 그 수자를 디코드할 수 있다는 것을 의미한다. 1실시에에서는, 난수는 56 비트 길이이다.

블록 750에서는, 센서에 의해 디코드된 난수는 보안을 위해 이 세션에 사용되는 세션 키이다. 따라서, 매시간마다 세션이 설정되고, 보안이 재설정된다. 부가적으로, 세션이 종료된 때에는 도둑이 그 시스템을 한번 액세스하더라도, 도둑은 제2의 세션을 액세스하기 위해 원래 얻어진 데이터를 이용할 수 없다.

센서 및 디지털 시스템

도 8은 본 발명의 센서의 일례의 블록도이다. 중앙처리장치(CPU; 810)는 USB(universal serial bus: 통괄적인 직렬버스)연결(885)과 인터페이스하기 위해 사용된다. CPU(810)는 또한 전력스위치(845) 및 전력스위치를 매개해서 광원(840)을 제어하기 위해 사용된다. 1실시예에서는, 광원(840)은 발광다이오드(LED)이다. CPU(810)는 또한 모든 다른 구성요소로의 전력을 제어한다.

CPU(810)는 FPGA(field programmable gate array; 815)에 연결되어 있다. FPGA(815)는 1실시예의 센서(250)의 모든 기능을 실행하고, RAM(random access memory)를 포함해도 좋다. FPGA(815) 및 CPU(810)는 함께 감산기, 필터, USB 인터페이스, 계수화기 및 보안시스템으로서 작용한다. FPGA(815)에 클럭신호를 공급하기 위해 FPGA(815)에 수정(crystal; 830)을 연결해도 좋다.

FPGA(815)와 CPU(810) 사이에는 EPROM(erasable programmable read only memory; 820)이 연결되어 있다. EPROM(820)은 센서(250)를 초기화하는데 필요한 정보를 포함하고 있다. EPROM(820)은 센서의 ID가 영구적으로 붙어 있는 그 특별한 센서(250)와 관련된 개인기를 더 포함해도 좋다.

FPGA(815)에는 CCD(charge-coupled device)센서(860)가 더 연결되어 있다. CCD센서(860)는 컬러나 블랙 앤 화이트를 검지할 수 있는 광감지 전자소자이다. 1실시예에서는, CCD센서(860)는 계조(gray-scale) 검지센서이다. 각 CCD센서(860)는 광감지 포토셀의 어레이로 구성된다. 1실시예에서는, 포토셀은 노광전에 전하를 줌으로써 민감해진다. CCD센서(860)를 활성화하는데 전자장치를 제공하기 위해 지원 전자장치(850)를 CCD센서(860)에 연결한다. CCD센서(860)의 출력은 신호를 명확히 하기 위해 연산증폭기(870) 및 저역통과필터(875)를 통과한다. 그후, CCD센서(860)의 명확해진 출력은 지문을 계수화하기 위해 A/D컨버터(880)를 통과한다. 이 계수화된 지문 이미지는 FPGA(815)상으로 통과된다.

도 9는 도 8의 FPGA(815)의 구성의 일례를 나타내고 있다. RAM 제어기(905)는 RAM(910)으로의 액세스를 제어한다. RAM(910)은 지문 이미지를 광학적 형태뿐만 아니라 디지털 형태로 저장하기 위해 사용된다. RAM 제어기(905)는 안정성 계산기(920)로 정보를 더 통과시킨다. 안정성 계산기(920)는 후술하는 바와 같이 수신된 지문이 안정할 때를 계산하기 위해 사용된다.

RAM 제어기(905)는 A/D컨버터(880)로부터의 데이터를 수신한다. RAM 제어기(905)는 타이밍 제어기(945)를 통해 수신된 클럭에 의해 계측된다. FPGA(815)는 멀티플렉서(MUX; 915)를 더 포함하고 있다. MUX(915)는 도 8에 나타난 바와 같이 CPU(810)로 어드레스 및 데이터선을 액세스하기 위해 사용된다.

RAM 제어기(905)는 차차곡을 결정하기 위해 지문으로부터 배경 이미지를 제거하도록 사용되는 감산기(990)를 포함하고 있다. 감산기의 출력은 안정성 계산기(920)에 연결되어 있다. 안정성 계산기(920)의 출력은 지문 이미지가 안정한 때를 표시하는 상태 레지스터인 안정성 데이터 레지스터(970)에 연결되어 있다.

압축기(925)는 지문 이미지를 병렬포트 인터페이스(930)를 통해 전송하기 전에 압축한다. 또한, 압축된 이미지는 USB 인터페이스(935)를 통해 전송되어도 좋다. 1실시예에서는, 압축기(925)는 그 정보내용에 비례하여 암호화된 심벌의 길이를 변화시키는, 즉 더욱 종종 심벌 또는 토큰을 사용할수록 이것을 압축된 스트림으로 나타내는데 사용되는 2진 스트림을 더 짧게 하는 통상적인 데이터 압축기술인 호프만 압축을 이용한다.

일반 주변장치 또는 USB 인터페이스(935)는 데이터를 USB로 통과시키기 위해 사용된다. 1실시예에서는, USB 액세스는 CPU(810)를 통해 달성된다. 그러나, USB 인터페이스(935)는 FPGA(815)내에 위치되어도 좋다.

상태 레지스터(940)는 MUX(915) 및 CPU 인터페이스에 연결되어 있다. 상태 레지스터(940)는 병렬포트, USB포트 및 프레임 포함하는 통신장치의 일반적인 상태를 표시한다. 상태 레지스터(940)는 CPU(810)에 의해 제어되고, 그 정보를 RAM 제어기(905)로 통과시킨다.

MUX(915)에는 제어 레지스터(950)도 연결되어 있다. 제어 레지스터는 FPGA(815)의 기능을 제어하도록 CPU(810)에 의해 확립된다. 어드레스 레지스터(955)는 CPU(810)가 RAM 데이터를 액세스하도록 하는 RAM(910)내의 RAM 데이터의 어드레스를 포함한다. 1실시예에서는, 어드레스 레지스터(955)는 데이터가 어드레스에 기록될 때에 자동적으로 증가된다. 어드레스 레지스터는 제어 레지스터(950)에 의해 제어된다. 독출 데이터 레지스터(965) 및 기록 데이터 레지스터(960)는 RAM(910)으로부터 독출한 데이터 또는 RAM(910)에 기록한 데이터를 버퍼링한다.

스레숄드 레지스터(975)는 안정성 계산기(920)에 의해 안정성 연산에 필요한 스레숄드 번호를 포함하고 있다. 이들 스레숄드 번호는 이하에 더 상세히 설명되고 있다. 1실시예에 있어서, 스레숄드 레지스터(975)는 CPU(810)에 의해 기록되고 있다. 포트 데이터 레지스터(985)는 CPU(810)로부터 병렬포트 인터페이스를 통해 전송되는 데이터를 위한 레지스터이다. USB 데이터 레지스터(980)는 USB인터페이스로부터의 데이터의 레지스터이다. 1실시예에 있어서, USB 데이터 레지스터는 시스템 정보를 저장하는 읽기전용 레지스터이다.

도 10은 본 발명의 디지털 시스템의 1실시예를 나타낸 도면이다. 디지털 시스템(1000)은 정보를 전달하기 위한 시스템 버스(1010)나 다른 통신수단과 정보를 처리하기 위한 시스템 버스(1010)와 결합된 프로세서(1020)를 구비하고 있다. 또, 디지털 시스템(1000)은 읽기전용메모리(ROM) 및/또는 시스템 버스(1010)에 연결된 정적정보와 프로세서(1020)의 명령을 저장하기 위한 다른 정적기억장치(1035)를 구비하고 있다. 더욱이, 디지털 시스템(1000)은 주메모리(1030)와 정보와 실행되는 명령을 저장하기 위한 동적기억장치를 구비하고 있다. 또, 주메모리(1030)는 명령의 실행동안 임시가변정보나 다른 중간정보를 저장하는데 이용된다. 1실시예에서 주메모리(1030)는 동적랜덤접근 기억장치(DRAM)이다.

게다가, 디지털 시스템(1000)은 범용 직렬버스(universal serial bus: USB)제어기(1080)와, USB(1085)를 제어하는 버스 제어기를 구비하고 있다. USB(1085)는 USB장치(1090)를 디지털 시스템(1000)에 연결하기 위한 것이다. 센서(250)는 USB(1085)를 통해 디지털 시스템에 연결된 USB장치(1090)중 하나일 수 있다.

또, 디지털 시스템(1000)은 시스템 버스(1010)를 통해 사용자에게 정보를 표시하는 음극선관(CRT)이나 액정표시(LCD) 화면 등의 표시장치(1050)에 연결될 수 있다. 통상적으로, 영숫자 입력장치(1055)는 프로세서(1020)에 정보와 명령선택을 전달하기 위해 시스템 버스(1010)에 연결되어 있다. 다른 타입의 사용자 입력장치에는 방향정보와 명령선택을 프로세서(1020)에 전달하는 마우스, 트랙볼, 트랙패드 등의 커서제어장치(1060)와 표시장치(1050)의 커서이동을 제어하는 커서방향키가 있다. 또, 철폴이나 펜 등의 다른 입력장치는 표시장치와 상호작용하는데 이용될 수 있다. 게다가, 디지털 시스템(1000)은 시스템 버스(1010)를 통해 네트워크 통신장치(1065)에 연결되어 있다. 네트워크 통신장치(1065)는 디지털 시스템을 다른 디지털 시스템, 서버 및 네트워크에 연결하기 위해 이용되고 있다.

등록

도 11a와 도 11b는 지문을 등록하는 프로세스를 나타낸 플로우차트이다. 등록은 등록인터페이스를 오픈(open)하는 사용자에게 의해 개시된다. 또, 본 시스템이 우선 개시되면, 등록프로세스는 자동적으로 오픈한다.

블록 1110에서는, 레지스터에 등록하는 사람의 신원이 요청되고 있다. 신원은 지문에 관계되는 최근의 몇몇 다른 식별자를 초기화한다. 1실시에에 있어서, 사용자의 전체이름이 여기에서 요청되고 있다. 또, 지갑이나 소지하고 있는 유사한 시스템을 위해 신원은 요청되지 않고, 이 프로세스로 등록되는 개인은 물음의 항목의 오너(owner)이다.

블록 1115에서는, 지문이 요청되고 있다. 이것은 "등록하기 위해 지금 당신의 손가락을 센서위에 대주세요." 등이나 그와 유사한 를 윈도우에 나타냄으로써 이루어진다. 또, 상기 시스템은 요청을 표시하지 않고 단지 지문을 기다릴 수 있다.

블록 1120에서는, 복수의 다른 자국이 얻어지고 있다. 상술한 바와 같이, CCD센서(860)는 지문을 검출하고, RAM의 광이미지를 복사한다. 이 경우에, 사용자가 그나 그녀의 손가락을 센서 플랫(plate)위에 대기만 하면, 복수의 자국은 얻어진다.

블록 1125에서는, 각각의 지문이 디지털화된다. 이들 자국은 센서에 일시적으로 저장된다. 또, 그것들은 디지털 시스템에 저장될 수도 있다.

블록 1130에서는, 디지털화된 배경이미지는 차분 자국을 초래하는 각각의 디지털화된 자국에서 제거된다. 상술한 바와 같이, 센서가 초기에 켜지면 다음의 지문이 획득될 때마다 디지털화된 배경이미지는 획득된다.

블록 1135에서는, 자국이 비교된다. 이것은 지문을 평가하는 공지된 기술을 이용하여 이루어진다. 예컨대, 몇개의 부합점이 자국간에서 존재하는지를 찾아내어 3개 또는 그 이상의 자국은 부합된다. 이러한 비교는 어떤 자국이 최고품질인지를 판정할 것이다.

블록 1140에서는 가장 좋은 자국이 선택된다. 등록자국은 최근의 지문과 비교되는 것이기 때문에, 가장 좋은 자국이 가능하다. 그러므로, 지문특성을 가장 뚜렷하게 표시하는 자국이 선택된다. 또, 모든 등록 자국으로부터의 정보는 데이터베이스에 저장되는 싱글 혼합자국으로 만들어진다. 또, 가장 좋은 자국 선택 외에 또, 다른 자국으로부터 학습하는 학습프로세스(learning process)를 이용하여 가장 좋은 자국은 더욱 향상된다. 게다가, 블록 675에 대해 상술한 바와 같이, 새로운 자국이 사용자로부터 얻어질 때마다 템플릿(template)은 갱신된다. 이 프로세스는 당기술분야에서 알려져 있다. 또, 이 단계는 건너뛴 수 있다.

도 11b에 나타낸 블록 1145에서는, 차분 프린터가 데이터베이스에 저장된다. 또, 이 선택프로세스는 건너뛴 수 있고, 모든 자국은 등록 데이터세트로 데이터베이스에 저장될 수 있다.

블록 1150에서는, 상기 시스템은 사용자가 지문과 신원에 관련되길 원하는 어떤 파일과 응용을 요청한다. 사용자는 성공한 지문의 타당성검사 프로세스후에 자동적으로 오픈될 수 있는 파일과 응용을 관련시킬 수 있다. 이러한 파일이 관련되지 않으면, 지문은 단지 사용자를 타당하게 하거나, 사용자 액세스가 디지털 시스템(210)이나 디지털 시스템(210)에 연결된 어떤 다른 시스템에 저장된 사용자의 자체 데이터에 대한 사용자 액세스를 허용한다.

블록 1155에서는, 어떤 파일이 사용자에게 의해 식별되었는지를 판정한다. 파일이 식별되지 않으면, 프로세스는 블록 1180에서 계속한다. 파일이 식별되면, 프로세스는 블록 1160에서 계속한다.

블록 1160에서는, 상기 시스템은 선택된 파일에 있는 보안이 어떤 종류의 것인지 판정한다. 사용자는 프로그램 파일, 응용파일이나 특정 데이터 파일 등의 파일을 선택할 수 있다. 몇몇 파일은 이미 패스워드로 보호되고 있다. 예컨대, 윈도우용 워드(Word for Windows)는 데이터파일의 패스워드 보호를 허용한다. 윈도우용 워드는 마이크로소프트사의 상표이다. 선택된 파일이 보안성을 가지고 있지 않거나 쉽게 변경할 수 있는 보안성을 가지고 있으면, 프로세스는 블록 1165에서 계속한다.

블록 1165에서는, 선택된 파일의 부트 섹터는 지문검증 또는 식별을 허용하기 위해 변경된다. 따라서, 사용자가 그 파일에 액세스하길 원하면, 사용자는 파일에 액세스하기 위해 그나 그녀의 지문을 보여야 할 것이다. 부트 섹터의 변경은 당기술분야에서 알려져 있다. 부트 섹터의 포맷은 플랫폼 종속물이기 때문에, 각 플랫폼을 위해 변경가능하다. 그러므로, 프로세스는 선택된 파일의 부트 섹터에 액세스하여 그것을 변경시킨다. 1실시에에 있어서, 이 변경은 지문식별 서브루틴에 부트 프로세스를 가리키는 단계로 이루어져 있다. 지문식별 서브루틴의 끝은 부트 섹터의 뒤를 가리킨다. 그러므로, 실행동안, 지문검증 서브루틴은 불러내어져 실행된다.

블록 1160에서는, 선택된 파일이 이미 패스워드로 보호되고 있으면, 이러한 보호는 쉽게 변경될 수 없기 때문에, 프로세스는 블록 1170에서 계속한다. 블록 1170에서는, 그 패스워드로 보호된 파일과 관련된 패스워드가 요청된다. 사용자는 파일과 관련된 패스워드를 넣어야만 한다. 따라서, 사용자가 다음번에 파일을 선택하고 지문을 사용할 때에는, 상기 시스템은 그 파일과 개인과 관련된 패스워드를 자동적으로 삼

입하여 파일을 오픈한다.

블록 1155에서는, 파일이 기입되어 있지 않으면, 프로세스는 블록 1180에서 계속한다. 블록 1180에서는, 어떤 디폴트 액세스는 식별되어 지문에 관련되어 있다. 디폴트 액세스는, 예컨대 서버나 사용자의 개인 파일을 저장하는 시스템의 특정영역에 대한 액세스를 허용하기 위해 제공된다. 그러므로, 예컨대 지문식별은 특정 파일리스트에 대한 자동 액세스를 제공한다. 1실시에에 있어서, 사용자는 이러한 영역을 규정한다. 또, 블록 1110에서 기입된 사용자 식별은 디폴트 영역 액세스를 판정하는데 이용된다. 또, 이러한 영역이 존재하지 않으면, 프로세스는 블록 1185에서 곧장 계속한다. 블록 1185에서, 등록프로세스는 완료된다.

지문포착

도 12a는 지문 이미지를 포착하는 프로세스를 나타낸 플로우차트이다. 이것은 도 5의 블록 535, 540, 545에 대해 나타낸 기능성, 즉 지문을 포착하고 자국을 디지털화하며 배경을 자국으로부터 제거하는 기능성을 더 상세히 나타낸 도면이다.

블록 1200에서는 초기 자국의 존재를 검출한다. 상술한 바와 같이, 이것은 센서의 센서 플래튼을 히트(hit)하는 에너지변화의 결과로서 검출된다. 블록 1205에서, 합계는 0으로 설정된다. 이 합계의 이용은 이하에서 명백해질 것이다.

블록 1210에서는, 자국이 포착되고 디지털화된다. 이 프로세스는 상술되어 있다. 블록 1215에서는, 디지털화된 배경이미지가 디지털화된 자국에서 제거된다. 이것은 센서 플래튼의 실제 자국의 더 명확한 표시를 초래한다.

블록 1220에서, 이미지는 모든 X번째 행과 Y번째 열을 얻고, 이들 행렬의 이들 픽셀만을 얻어 필터된다. 많은 픽셀중 1X*Y번째만이 평가될 필요가 있기 때문에, 이것은 프로세싱을 상당히 감소시킨다.

도 12b는 이 필터링 프로세스를 나타낸다. 작은 박스로 표시되는 픽처 A는 모든 픽셀을 갖는 이미지이다. 실제로는, 이것은 디지털화된 이미지이기 때문에, 이들 박스 각각은 그 특정픽셀의 강도요소에 대응한다. 픽처 B는 픽셀의 0번째와 3번째 열과 행이 선택되는 방법을 나타내는 이미지를 표시한다. 그리고, 박스로 나타낸 필터된 픽처에 있는 이들 픽셀만을 갖는 픽처 C는 필터된 이미지를 나타낸다. 1실시에에 있어서, X와 Y는 모두 4이다. 그러므로, 16픽셀의 I만이 평가된다. 더욱이, 프로세싱은 필터된 이미지로 실행된다. 이 블록은 몇몇 실시예에서는 건너뛴 수 있다.

도 12a로 돌아가서, 블록 1225에서 스레숄드 이상의 픽셀의 강도의 합이 필터된 이미지를 위해 결정된다. 1실시에에 있어서, 디지털화된 형상은 그레이 스케일 형상(gray scale figure)인 바, 이 의미하는 바는 화소가 다양한 강도를 가질 수 있다는 것이다. 이 예에서의 스레숄드는 지문의 평균 강도 에너지이다. 따라서, 예컨대 스레숄드가 3일 수 있다. 3개의 화소 2와 4 및 6에 대해, 0과 +1 및, +3이므로, 합은 4가 된다.

블록 1230에서, 이 합의 도함수가 얻어진다. 이는 합의 성장율을 결정하는 바, 이전의 합과 비교된다. 1실시에에서 도함수는 현재의 합으로부터 이전의 합을 감산함으로써 결정된다.

블록 1235에서, 도함수가 소정 스레숄드 이하인지를 결정한다. 이 스레숄드는 센서의 일반 지문의 품질에 기초하여 결정된다. 도함수가 스레숄드 이하가 아니면, 즉 합이 아직 성장하지 않으면, 처리가 블록 1210으로 되돌려지고, 다음 이미지가 포착된다. 도함수가 스레숄드 이하이면, 처리가 블록 1240으로 계속된다.

블록 1240에서 합이 소정의 최소 스레숄드 이상인지가 결정된다. 이 스레숄드는, 특정한 센서로 얻어진 지문동안, 골에 대한 평균 콘트라스트 마루이다. 1실시에에 있어서, 이 스레숄드는 나중의 결과에 기초하여 갱신될 수 있다. 합이 스레숄드 이상이 아닐 때, 처리는 블록 1210으로 되돌려지고, 다음 이미지가 선택된다. 합이 최소 스레숄드 이상이면, 지문은 충분히 크고 강하며, 처리는 블록 1245 및 블록 1250으로 계속된다. 블록 1245에서 최종 자국이 포착되고, 진행되는 처리동안 통과된다.

도 12c는 이 처리의 실례를 나타낸다. 예컨대, 사진(D)은 겨우 보이는 이미지를 나타낸다. 에너지 수준이 우선 감소될 때, 제1이미지가 포착되는 바, 이는 손가락의 부분 사진만이다. 포착되는 연속적인 사진동안, 사진(D와, E, F, G 및, H)은 지문 크기의 점진적인 증가를 나타낸다. 사진(I)이 포착될 때, 시스템은 감소의 크기를 결정한다. 지문 크기는 이전 이미지에 의해 나타난다. 사진(H)은, 그러므로 포착되고, 최적의 지문 이미지로서 간직된다.

도 12a로 돌아가서, 블록 1250에서 합이 0으로 재설정된다. 블록 1255에서 다음 이미지가 포착되고 디지털화된다. 배경은 블록 1260에서 화상으로부터 감산된다.

블록 1265에서 이미지는 필터되고, 블록1270에서 스레숄드 강도 이상의 화소의 강도의 합이 더해진다. 이 합의 도함수는 블록 1275에서 얻어진다. 블록 1280에서, 도함수가 스레숄드 이하인지 결정된다. 이 스레숄드는, 상기 언급된 형태(1235)에 대한 스레숄드보다 작다. 이미지가 감소를 정지할 때, 이미지의 도함수는 0에 가깝게 되고, 이 도함수는 스레숄드와 일치된다. 도함수가 스레숄드 이하가 아니면, 처리는 블록 1255으로 되돌려진다. 도함수가 스레숄드 이하이면, 처리는 블록 1285으로 계속된다. 블록 1285에서, 합이 소정 스레숄드 이하인지 결정된다. 합이 스레숄드 이하가 아니면, 처리는 블록 1255으로 되돌려진다. 합이 스레숄드 이하이면, 처리는 블록 1290으로 계속된다. 블록 1290에서, 새로운 배경이 포착된다. 보여지는 바와 같이, 블록 1255 내지 블록 1285는 블록 1210 내지 블록 1240의 역이다. 따라서, 새로운 배경 이미지가 얻어지는 것에 반하여 처리가 실행된다. 이 배경 이미지는 다음 처리에서 사용된다.

자동-착수 특성

도 13a는 자동-착수 응용이나 서류의 처리를 나타내는 플로우차트이다. 블록 1310에서, 응용은 초기화된다. 응용은 사용자가 파일을 선택함으로써나, 사용자가 그의 지문을 센서나 다른 수단상에 위치시킴으로

써, 초기화될 수 있다.

블록 1315에서, 초기에 언급된 바와 같이 데이터베이스내에 지문과 연관된 파일이 있는지를 결정한다. 즉, 초기화된 파일이 연관된 지문 조회/식별 요구를 갖지 않으면, 처리는 자동-착수 처리가 중지되는 블록 1320으로 계속된다.

블록 1325에서, 처리는 지문을 기다린다. 처리는, 지문을 요구한다는 표시(note)를 디스플레이 할 수 있다. 그의 손가락을 센서상에 위치시킴으로써 사용자가 처리를 초기화하면, 처리는 이 블록으로 직접 진행한다. 1실시예에 있어서, 처리는 여기서 시작되고, 블록 1310 및 블록 1315이 스킵(skip)된다. 이는, 사용자가 사용자의 특정한 저장 영역에 액세스하기를 원하거나 지문 인식을 사용하는 디폴트 파일일 때, 응용될 수 있다.

블록 1330에서, 지문은 처리되어 인식된다. 이 처리는 상기된 바와 같다.

블록 1335에서, 데이터베이스는 사용자가 선택된 파일이나 응용에 액세스할 수 있게 승인되었는지를 결정하도록 요청된다. 사용자의 식별은 블록 1330에서 결정되므로, 이는 자동화될 수 있다. 사용자가 선택된 파일에 액세스되도록 승인되지 않았으면, 처리는 블록 1340으로 계속되고, 파일이 거절되게 액세스된다. 1실시예에 있어서, 시스템은 "사용자가 선택된 파일에 액세스되도록 승인되지 않았다"란 메시지를 디스플레이 하거나 이보다 작은 메시지를 디스플레이 한다.

사용자가 선택된 파일에 액세스하도록 승인되면, 처리는 블록 1345으로 계속된다. 블록 1345에서, 파일/응용은 초기화된다. 이것이 응용 프로그램이면, 응용 프로그램이 선택된다. 이것이 파일이면, 응용 프로그램에 의해 오픈되고 파일이 발견되거나 선택된다.

블록 1350에서, 어떤 타입의 자동-착수가 선택된 파일/응용과 연관되는 지가 결정된다. 등록에 대해서 상기된 바와 같이, 도 11에서, 파일은 부트 스트랩 자동-착수되거나 패스워드 자동-착수된다.

도 13으로 돌아가서, 블록 1350에서, 처리가 패스워드 자동-착수이면, 처리는 블록 1355으로 계속된다. 블록 1360에서, 파일 및 지문과 연관된 패스워드는 데이터베이스에서 룩업(lookup)된다. 패스워드가 파일/응용을 가능하게 하는 동안, 상기된 바와 같이, 도 11에서, 패스워드는 데이터베이스에 저장된다. 블록 1365에서, 패스워드는 파일내의 적당한 위치에 삽입되고, 파일은 오픈/액세스된다.

블록 1350에서, 처리가 직접 자동-착수이면, 처리는 블록 1370으로 계속된다. 블록 1370에서, 부트스트랩은 응용을 구동하거나 파일에 액세스하도록 사용된다. 도 11에 대해 상기된 바와 같이, 파일의 부트 섹터는 지문 액세스를 가능하게 바꾸어질 수 있다. 따라서, 지문이 받아들여질때, 파일/액세스는 자동적으로 소환(call up)된다.

토큰 인터페이스

도 14는 본 발명의 지문 인식 시스템과 관련하여 토큰을 사용하는 처리를 나타낸 플로우차트이다. 토큰은 열쇠나, 바코드, 디스켓, 스마트카드, 또는 유사한 외부 데이터 컨테이너일 수 있다.

블록 1410에서, 사용자는 토큰을 삽입한다. 1실시예에 있어서, 토큰은 디지털 시스템과 결합될 필요가 있다. 다른 실시예에 있어서, 디지털 시스템은 토큰과 협동하고, 따라서 토큰은 센서와만 결합될 수 있다.

블록 1415에서, 처리는 지문 비준이 가능한지를 테스트한다. 토큰은 지문 비준없이도 사용될 수 있다. 지문 비준이 사용될 수 없으면, 처리는 블록 1420으로 계속된다. 지문 비준이 가능하지 않으므로, 블록 1420에서 처리는 종료된다. 지문 비준이 가능하면 처리는 블록 1425으로 계속된다.

블록 1425에서, 지문이 요구된다. "당신의 손가락을 센서상에 놓으세요"라는 메시지를 디스플레이하는 시스템에 의해 일어날 수 있거나, 지문 비준을 위한 대기시간일 수 있다. 따라서, 여기서 사용자는 그의 손가락을 센서상에 놓는다.

블록 1430에서, 토큰의 템플레이트(template)의 유효성이 결정된다. 토큰은 승인된 사용자의 지문의 템플레이트를 포함한다. 처리는 템플레이트가 뒤섞였는지를 테스트한다. 1실시예에 있어서, 대중-열쇠나 개인-열쇠 또는 서명의 변화가 본이 보장되는 것을 증명하는데 사용된다.

블록 1435에서, 지문은 토큰상의 본과 비교된다. 토큰은 하나 이상의 사용자에게 의해 "소유"된다. 이 단계에서, 처리는 토큰의 사용자가 그것을 사용하는 지를 결정한다.

블록 1445에서, 처리 테스트는 지문이 토큰 사용자의 자국인지를 테스트한다. 토큰 사용자의 자국은 토큰내에 등록된다. 지문이 토큰 사용자의 자국이 아니면, 처리는 블록 1450으로 계속되고, 토큰은 사용될 수 없다. 더욱이, 승인되지 않은 사용자에게 의해 토큰이 사용되고 있다는 것을 가리키는 경보가 보내질 수 있다.

지문이 토큰 사용자의 자국이면, 처리는 블록 1455으로 계속된다. 블록 1455에서, 토큰은 사용될 수 있고, 사용자는 토큰 상에 저장된 데이터에 액세스할 수 있다. 예컨대, 사용자가 신용카드인 스마트카드를 소유하면, 처리는 스마트카드가 도난된 것이 아닌 것을 증명하고, 실제로 문제의 사용자의 것인지를 증명하는데 사용될 수 있다. 도둑은 스마트카드를 동작시킬 수 없고, 따라서, 카드내에 저장된 신용정보에 액세스할 수 없다.

상기 명세서에서, 본 발명은 특정1실시예를 참조로 설명하였다. 그러나, 본 발명은, 본 발명의 기술적 사상 및 범위를 벗어나지 않고, 다양한 실시 및 변형을 할 수 있다. 따라서, 본 발명의 명세서 및 도면은 제한하기 보다는 예로서 간주되어야 한다. 본 발명은 이러1실시예와 예들에 의해 제한되는 것으로서 파악되기 보다는 이하의 청구항에 따라 파악되어야 한다.

(57) 청구의 범위**청구항 1**

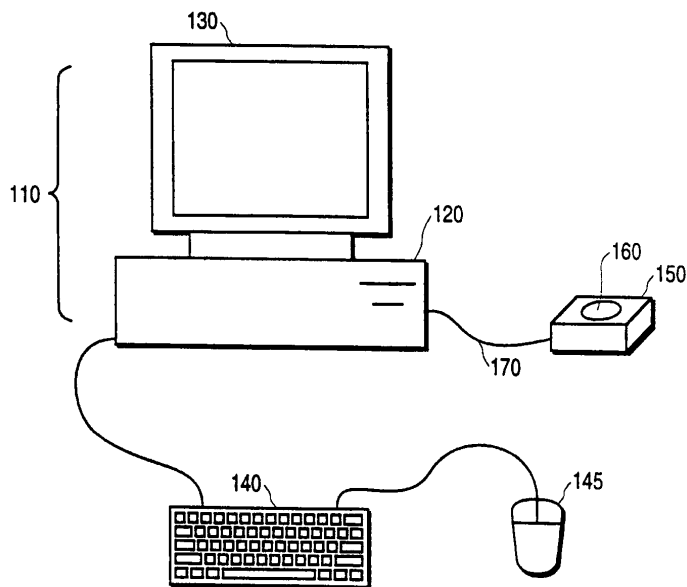
지문을 검출하는 단계와,
 상기 지문을 계수화하는 단계,
 상기 지문으로부터 계수화된 배경을 제거하여 차자국을 생성하는 단계 및,
 상기 차자국과 관련된 개체를 식별하는 단계를 구비하여 이루어진 것을 특징으로 하는 지문인식방법.

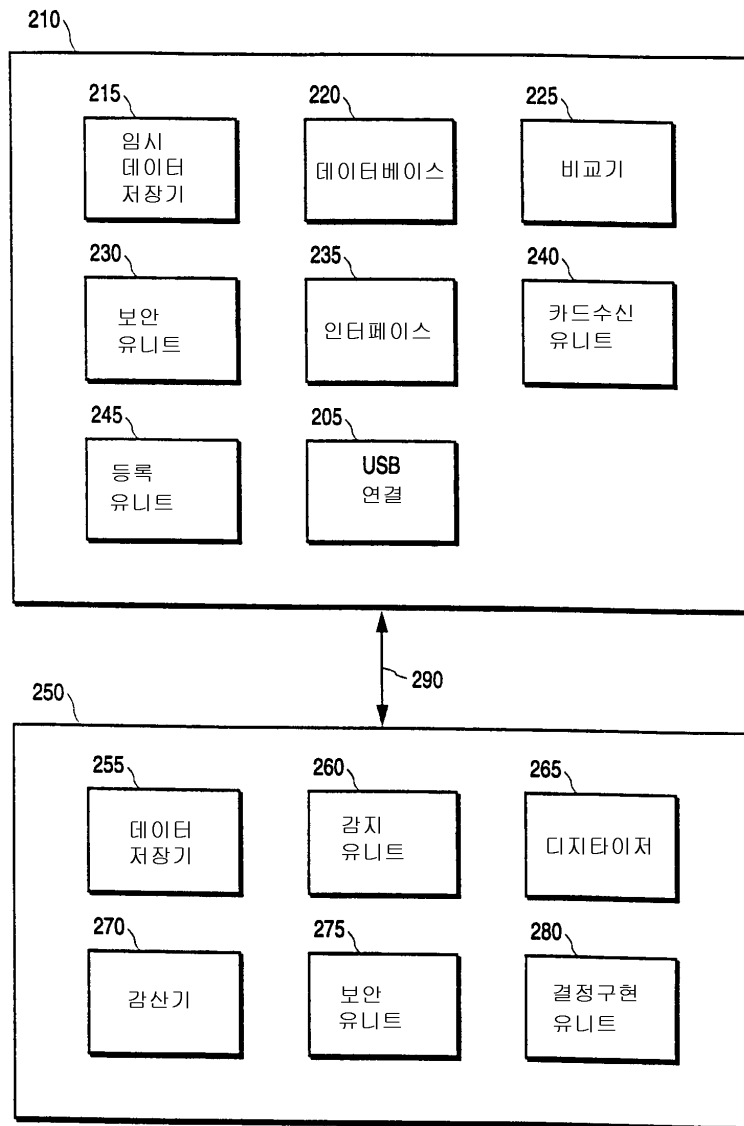
청구항 2

제1항에 있어서, 배경을 검출하는 단계와,
 상기 배경을 계수화하여 상기 계수화된 배경을 생성하는 단계를 더 구비하여 이루어진 것을 특징으로 하는 지문인식방법.

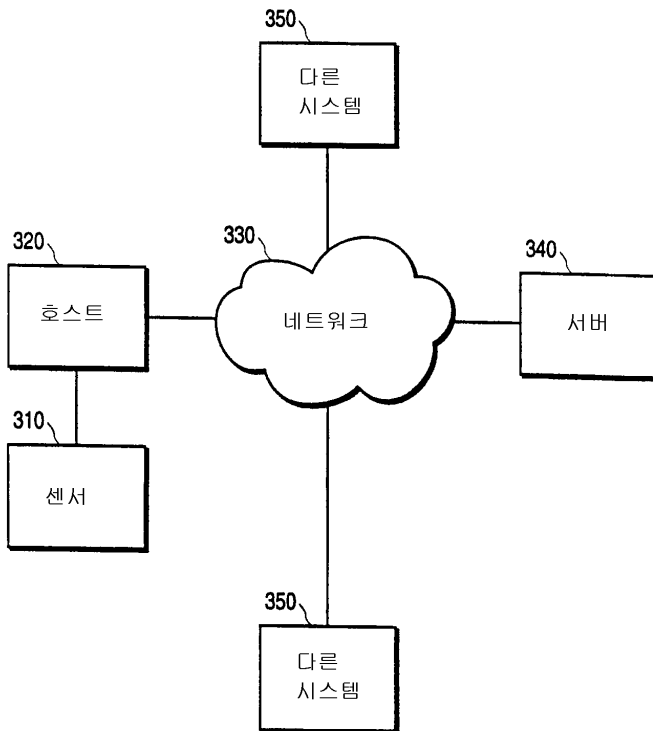
청구항 3

제1항에 있어서, 지문인식시스템이 최초로 턴온된 때에 그 지문인식시스템을 초기화하는 단계와,
 상기 지문인식시스템이 초기화되어 있을 때 제1배경을 검출하는 단계,
 상기 제1배경을 계수화하는 단계,
 지문이 검출된 후에 새로운 배경을 검출하는 단계 및,
 상기 새로운 배경을 계수화하는 단계를 더 구비하여 이루어진 것을 특징으로 하는 지문인식방법.

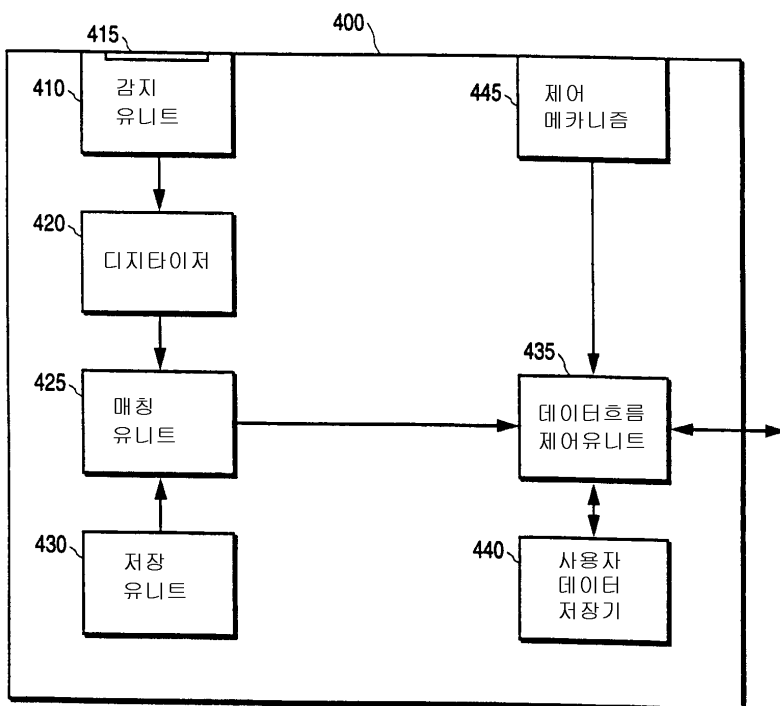
도면**도면1****도면2**



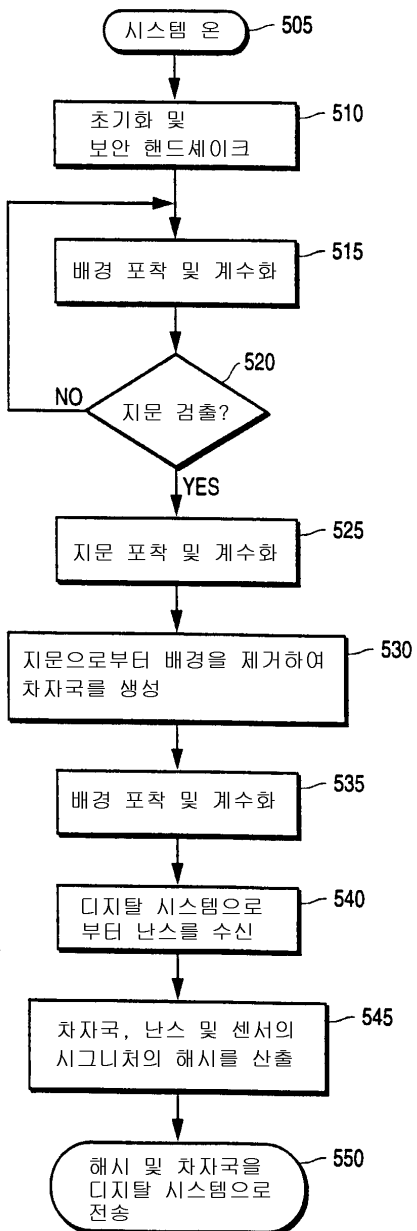
도면3



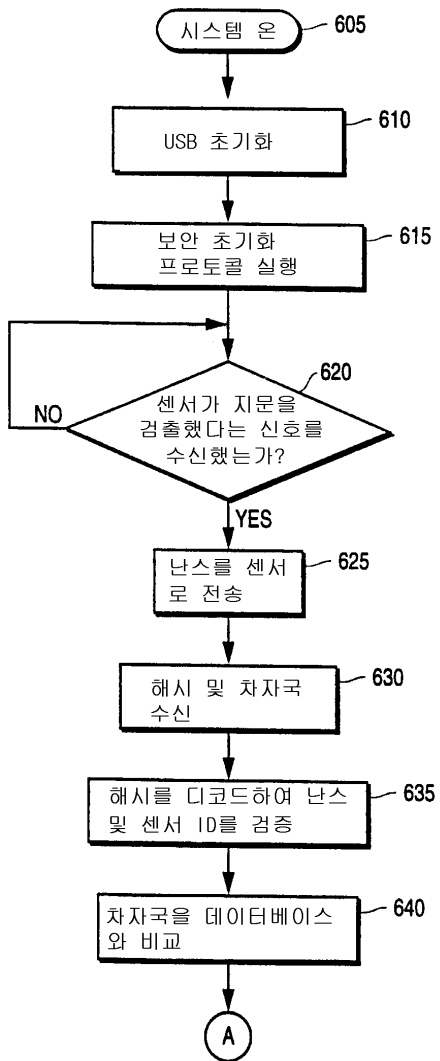
도면4



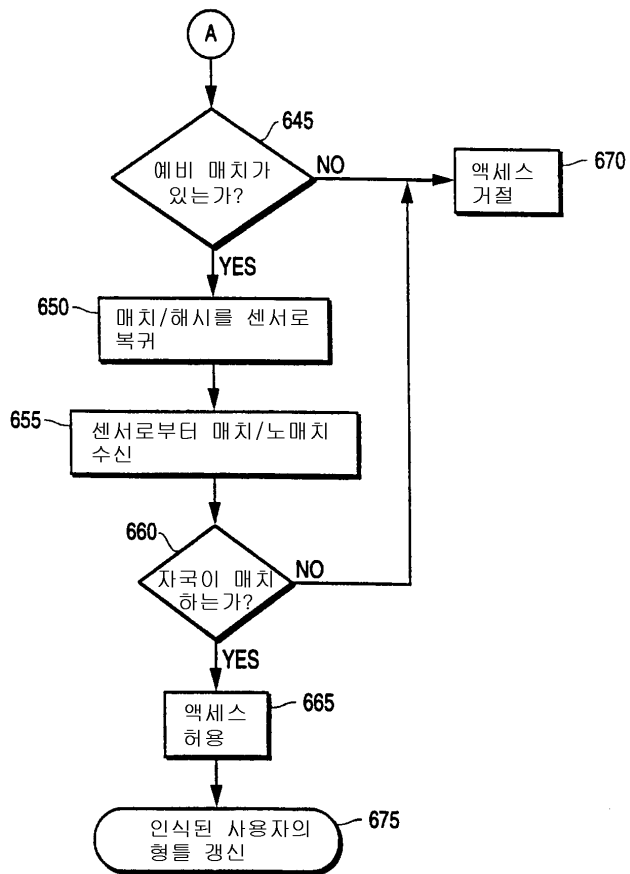
도면5



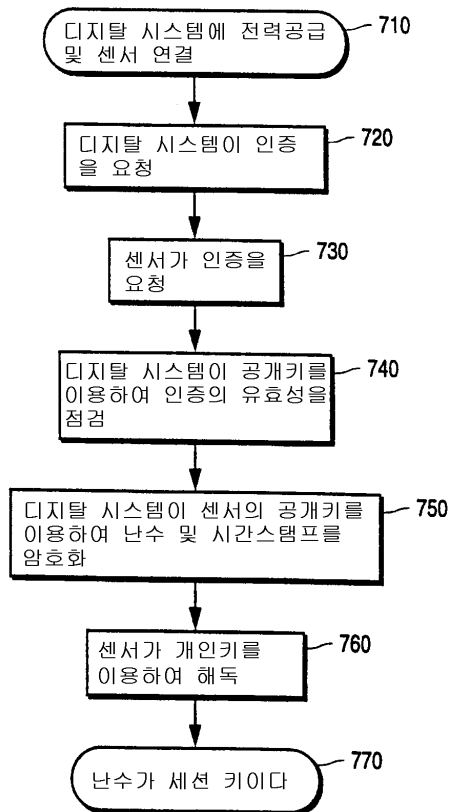
도면6a



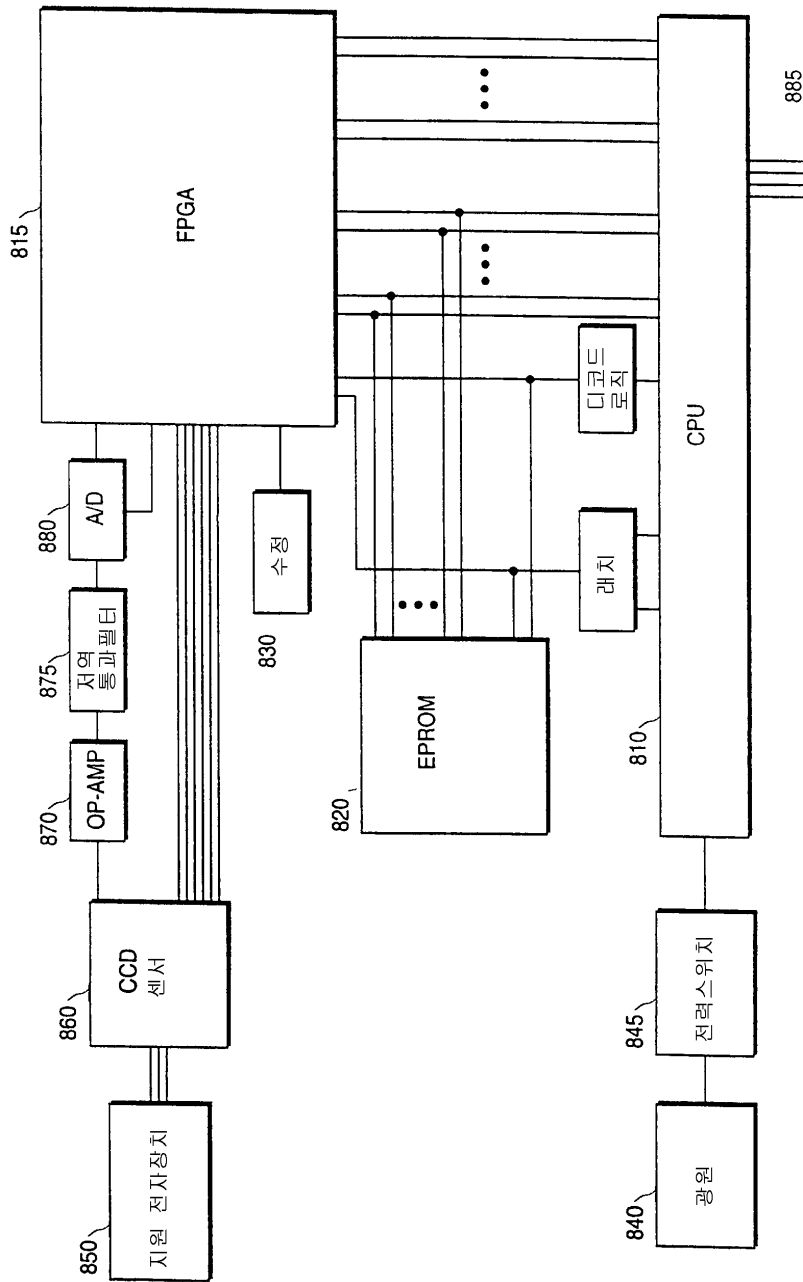
도면6b



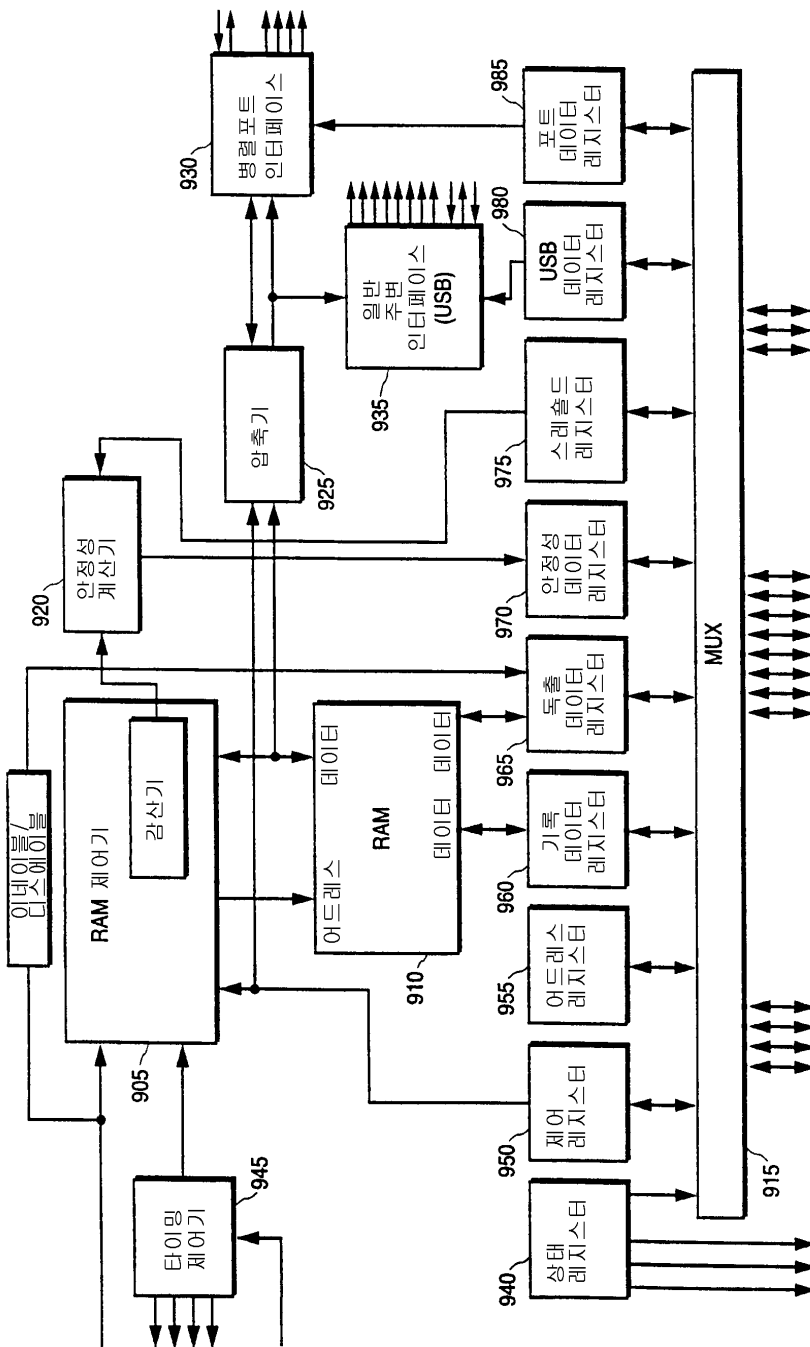
도면7



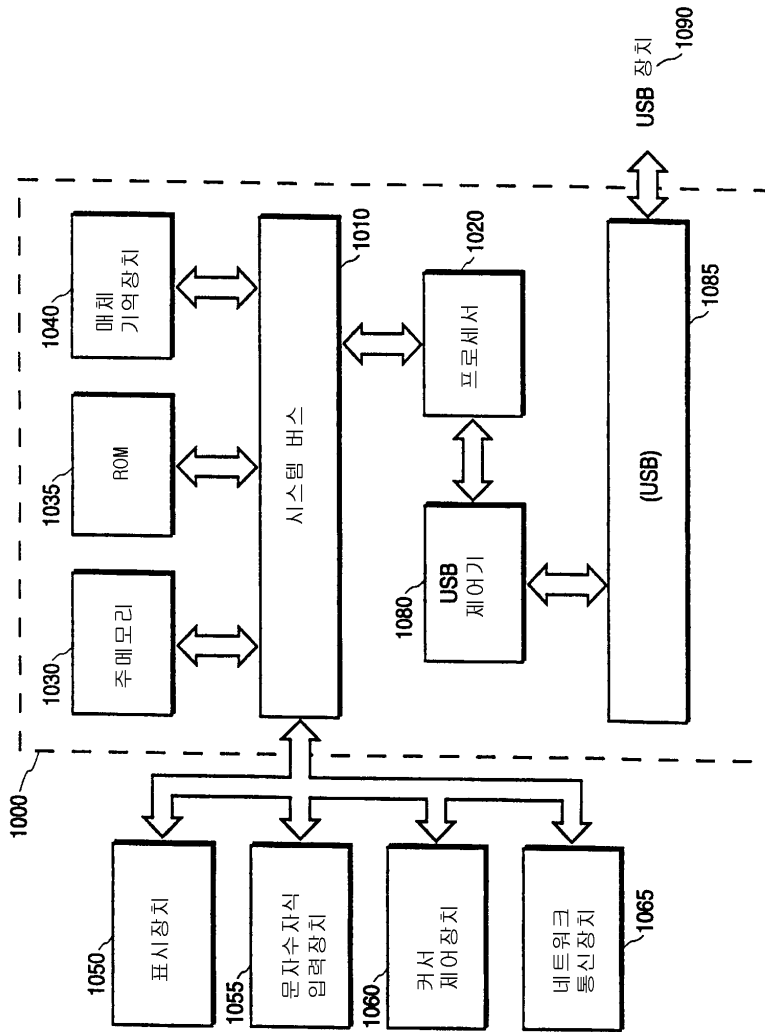
도면8



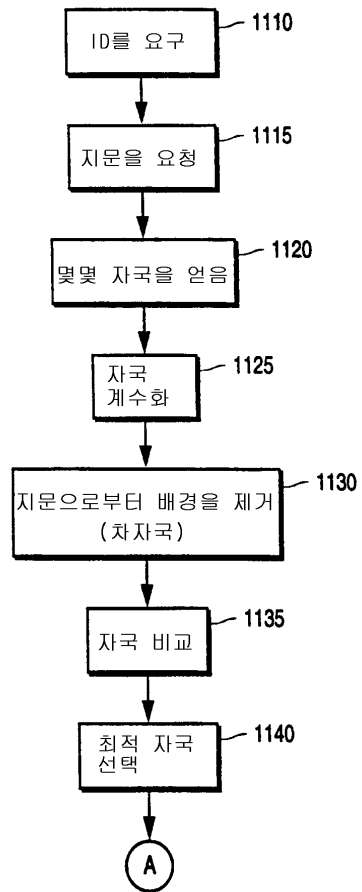
도면9



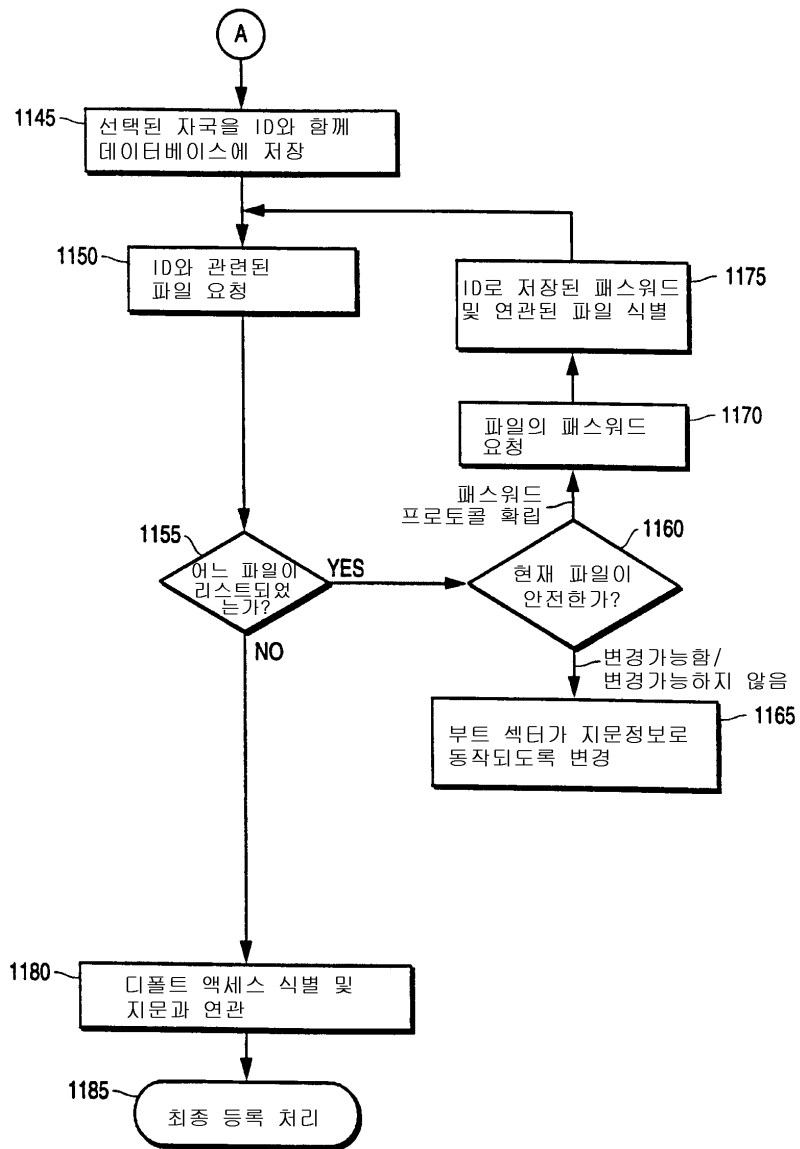
도면 10



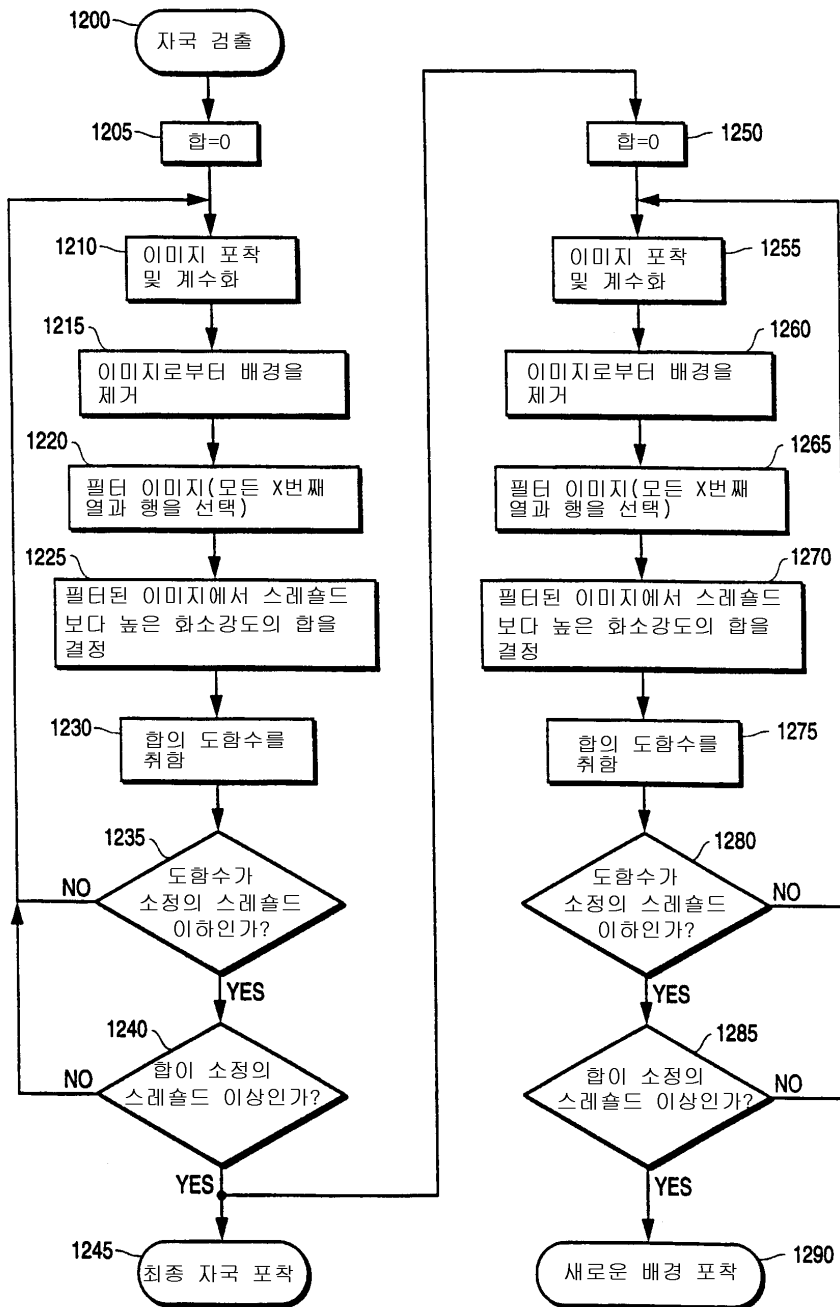
도면 11a



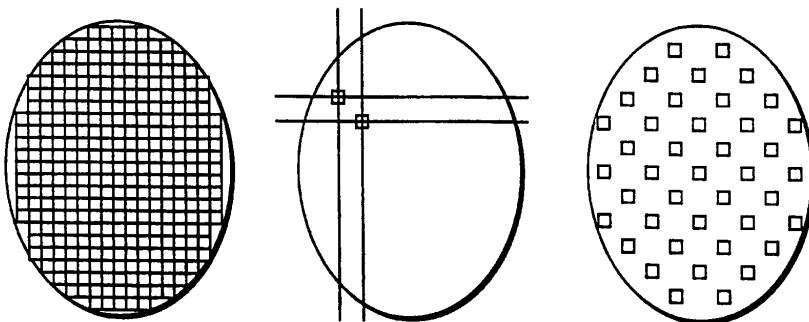
도면 11b



도면 12a



도면 12b

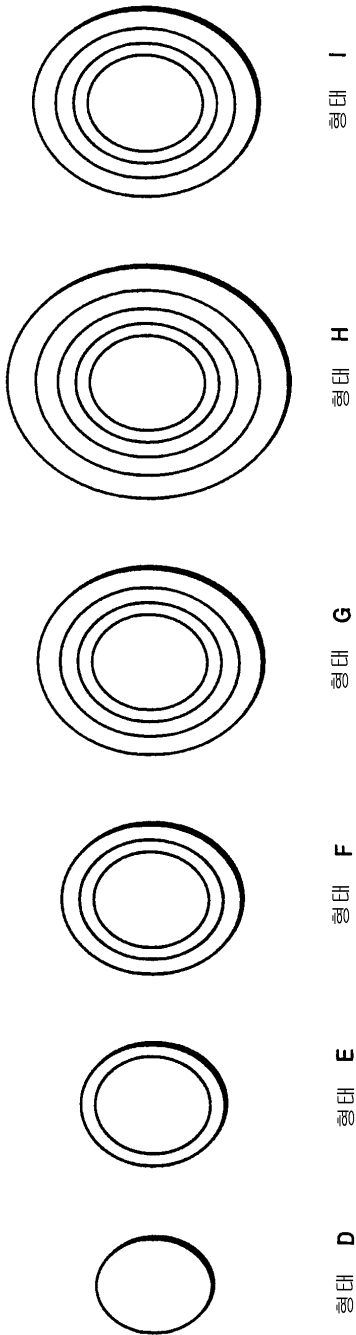


형태 A

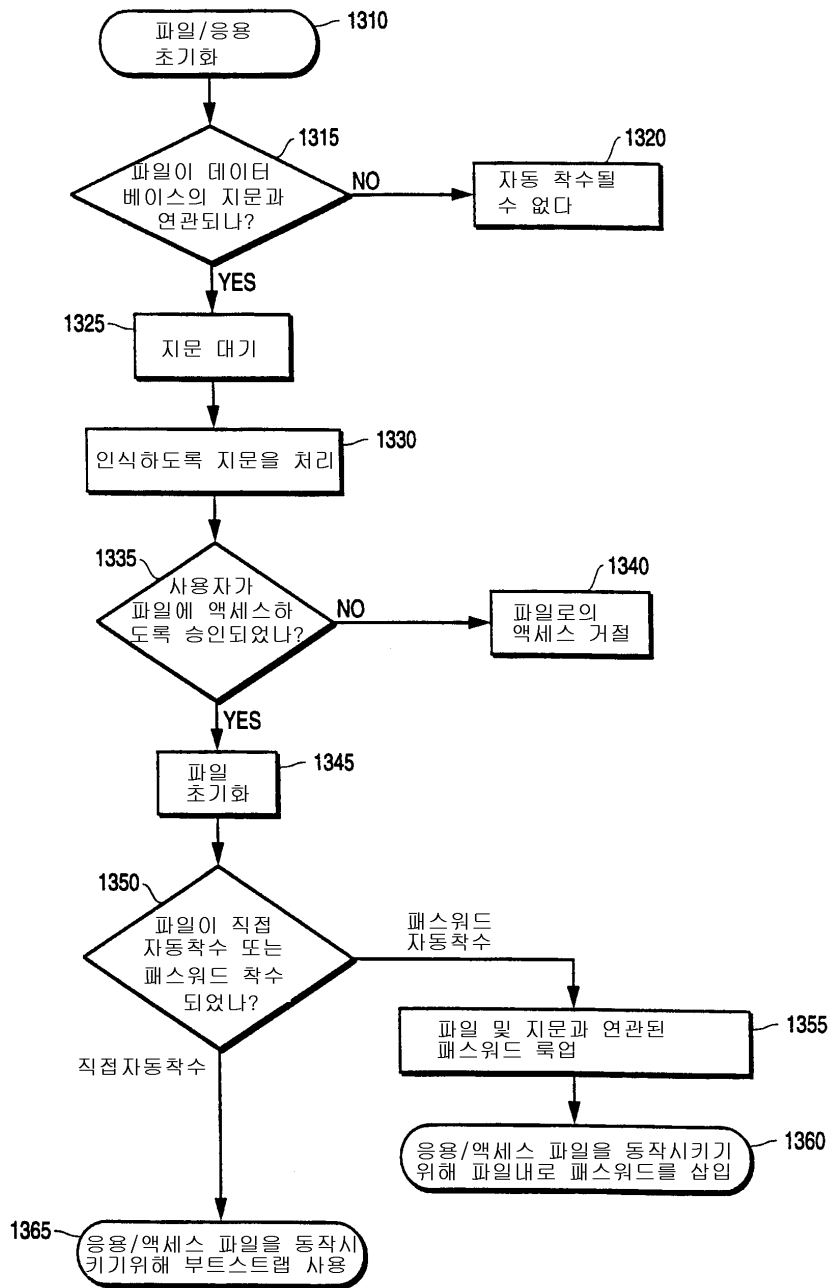
형태 B

형태 C

도면 12c



도면 13



도면 14

