(19)대한민국특허청(KR)
(12) 등록특허공보(B1)

(51) 。Int. Cl.
G06K 9/00 (2006.01)
G06T 7/00 (2006.01)

(45) 공고일자 2007년08월03일
(11) 등록번호 10-0745625
(24) 등록일자 2007년07월27일

(21) 출원번호 10-2005-0095875
(22) 출원일자 2005년10월12일
심사청구일자 2005년10월12일

(65) 공개번호 10-2006-0093263
(43) 공개일자 2006년08월24일

(30) 우선권주장 JP-P-2005-00043371 2005년02월21일 일본(JP)

(73) 특허권자 히타치 오므론 터미널 솔루션즈 가부시키가이샤
일본 도쿄도 시나가와꾸 오오사끼 1쪼메 6반 3고

(72) 발명자 오가따 히사오
일본 도쿄도 지요다꾸 마루노우찌 1쪼메 6-1가부시키가이샤 히타치세이사쿠쇼 지적재산권본부 내

이마이즈미 아쯔히로
일본 도쿄도 지요다꾸 마루노우찌 1쪼메 6-1가부시키가이샤 히타치세이사쿠쇼 지적재산권본부 내

마끼모또 에이지
일본 도쿄도 지요다꾸 마루노우찌 1쪼메 6-1가부시키가이샤 히타치세이사쿠쇼 지적재산권본부 내

나가따 고우헤이
일본 도쿄도 지요다꾸 마루노우찌 1쪼메 6-1가부시키가이샤 히타치세이사쿠쇼 지적재산권본부 내

(74) 대리인 구영창
이중희
장수길

(56) 선행기술조사문헌
KR1020030070284 A
KR1019990073820 A
US2003172279 A
WO2004013744 A
KR1019970029655 A
WO2004010373 A
EP1612714 A
US6084968 A

심사관 : 전창익

전체 청구항 수 : 총 19 항

(54) 생체 인증 장치, 단말 장치 및 자동 거래 장치

(57) 요약

인증용 생체 특징량을 IC 카드에 등록할 때에는, 생체 인증 장치가 생체 특징량을 취득하여 암호화하고, 제어 컴퓨터를 통하지 않고 직접 IC 카드 장치에 저장한다. 또한, 인증 시에는 IC 카드에 등록되어 있는 암호화 생체 특징량을 생체 인증 장치에 입력함과 함께, 생체 인증 장치 내에서 생체 특징량을 추출하여, 입력된 생체 특징량과 대조하여 인증한다. 또한, 인증 장치가 기동하고 있지 않을 때에는, 장치 내의 생체 인증용 프로그램을 암호화하여 저장한다.

대표도

도 1

특허청구의 범위

청구항 1.

삭제

청구항 2.

개인의 생체 정보를 이용하여 본인 확인을 행하기 위한 생체 인증 장치로서,

생체 정보를 취득하는 센서와,

취득한 센서 정보로부터 인증을 행하기 위한 생체 특징량 및 그 생체 특징량이 등록에 적합한지의 기준을 나타내는 특성 데이터를 추출하는 특징량 추출 수단과,

추출된 생체 특징량을 암호화하기 위한 암호화 수단과,

본인 확인을 위한 인증용 기준 데이터로서 암호화된 생체 특징량을, 생체 인증 장치에 접속된 제어 컴퓨터를 통하지 않고서 직접 IC 카드에 출력하는 수단

을 포함하는 것을 특징으로 하는 생체 인증 장치.

청구항 3.

개인의 생체 정보를 이용하여 본인 확인을 행하기 위한 생체 인증 장치로서,

생체 정보를 취득하는 센서와,

취득한 센서 정보로부터 인증을 행하기 위한 생체 특징량을 추출하는 특징량 추출 수단과,

인증용 기준 데이터로 되는 생체 특징량을 암호화된 형태로 생체 인증 장치 외부로부터 입력하는 수단과,

상기 인증용 기준 데이터로 되는 암호화된 생체 특징량을 복호하는 복호 수단과,

상기 특징량 추출 수단으로부터 출력된 생체 특징량과, 상기 복호된 인증용 기준 데이터로 되는 생체 특징량을 대조하는 생체 특징량 대조 수단과,

상기 생체 특징량 대조 수단의 출력을 암호화하는 암호화 수단과,

상기 암호화된 생체 특징량 대조 수단의 출력을 장치 외부에 출력하는 수단

을 포함하는 것을 특징으로 하는 생체 인증 장치.

청구항 4.

개인의 생체 정보를 이용하여 본인 확인을 행하기 위한 생체 인증 장치로서,

생체 정보를 취득하는 센서와,

취득한 센서 정보로부터 인증을 행하기 위한 생체 특징량을 추출하는 특징량 추출 수단과,

IC 카드에 저장된 인증용 기준 데이터로 되는 암호화된 생체 특징량을, 생체 인증 장치에 접속된 제어 컴퓨터를 통하지 않고서, 직접 IC 카드로부터 입력하는 수단과,

상기 인증용 기준 데이터로 되는 암호화된 생체 특징량을 복호하는 복호 수단과,

상기 특징량 추출 수단으로부터 출력된 생체 특징량과, 상기 복호된 인증용 기준 데이터로 되는 생체 특징량을 대조하는 생체 특징량 대조 수단과,

상기 생체 특징량 대조 수단의 출력을 암호화하는 암호화 수단과,

상기 암호화된 생체 특징량 대조 수단의 출력을 장치 외부에 출력하는 수단

을 포함하는 것을 특징으로 하는 생체 인증 장치.

청구항 5.

제2항 내지 제4항 중 어느 한 항에 있어서,

특징량 추출 수단과 생체 특징량 대조 수단은, 생체 인증 장치가 기동되기 전에는 암호화된 형태로 장치 내에 저장되고, 생체 인증 장치가 기동된 후에 복호되어 동작 가능한 상태로 되는 것을 특징으로 하는 생체 인증 장치.

청구항 6.

제2항 내지 제4항 중 어느 한 항에 있어서,

특징량 추출 수단과 생체 특징량 대조 수단은, 생체 인증 장치가 기동하기 전에는, 생체 인증 장치에 접속된 제어 컴퓨터와 생체 인증 장치 각각에 분할하여 저장되고, 생체 인증 장치가 기동된 후에 결합 복호되어 동작 가능한 상태로 되는 것을 특징으로 하는 생체 인증 장치.

청구항 7.

제2항 내지 제4항 중 어느 한 항에 있어서,

생체 인증 처리가 종료할 때마다 장치 내부에 저장되어 있는 생체 특징량과 상기 생체 특징량 대조 수단의 출력을 소거하는 것을 특징으로 하는 생체 인증 장치.

청구항 8.

개인의 인증에 이용되는 단말 장치에 있어서,

IC 카드에 정보를 기입하는 기입 수단과 생체 정보를 취득하는 취득 수단이 일체로 된 생체 인증 장치를 갖고,

상기 취득 수단은, 취득된 생체 정보가 등록에 적합한지의 기준을 나타내는 특성 데이터를 함께 취득하고,

상기 생체 인증 장치는, 상기 단말 장치와 별개로 구성하고 또한 상기 특성 데이터를 참조하여 등록해야할 생체 정보를 선택하고, 선택된 생체 정보를 상기 기입 수단에 의해서 상기 IC 카드에 등록하는 것을 특징으로 하는 단말 장치.

청구항 9.

개인의 인증에 이용되는 단말 장치에 있어서,

IC 카드에 정보를 기입하는 기입 수단과 생체 정보를 취득하는 취득 수단이 일체로 된 생체 인증 장치를 갖고,

상기 생체 인증 장치는, 상기 단말 장치와 별개로 구성하고 또한 취득한 생체 정보를 상기 기입 수단에 의해서 상기 IC 카드에 등록하고, 또한

암호키를 기억하는 기억 수단을 갖고,

상기 생체 인증 장치는, 생체 정보를 인증하는 인증 프로그램을 암호화하여 기억하는 기억부와, 상기 기억 수단으로부터 상기 암호키를 판독하고, 그 암호키에 의해서 암호화된 상기 인증 프로그램을 복호하는 복호부를 갖는 것을 특징으로 하는 단말 장치.

청구항 10.

제9항에 있어서,

상기 복호부에 의해서 복호된 상기 인증 프로그램에 의해, 상기 취득 수단에 의한 생체 정보의 추출을 제어하는 것을 특징으로 하는 단말 장치.

청구항 11.

개인의 인증에 이용되는 단말 장치에 있어서,

IC 카드에 정보를 기입하는 기입 수단과 생체 정보를 취득하는 취득 수단이 일체로 된 생체 인증 장치를 갖고,

상기 생체 인증 장치는, 상기 단말 장치와 별개로 구성하고 또한 취득한 생체 정보를 상기 기입 수단에 의해서 상기 IC 카드에 등록하고, 또한

암호키를 기억하는 기억 수단을 갖고,

상기 생체 인증 장치는, 상기 취득 수단에 의해서 취득한 생체 정보를 기억하는 기억부와, 상기 기억 수단으로부터 상기 암호키를 판독하고, 상기 기억부의 생체 정보를 암호화하여 상기 기입 수단에 의해서 상기 IC 카드에 기입하는 것을 특징으로 하는 단말 장치.

청구항 12.

제11항에 있어서,

상기 생체 인증 장치는, 상기 암호화한 생체 정보를 IC 카드에 기입하기 전에, 상기 기억부의 생체 정보를 삭제하는 삭제부를 갖는 것을 특징으로 하는 단말 장치.

청구항 13.

제8항에 있어서,

상기 생체 인증 장치는, 상기 취득 수단을 제어하는 암호화된 암호화 인증 프로그램을 기억하는 불휘발성 기억부와, 상기 암호화 인증 프로그램을 암호키에 의해서 복호화한 인증 프로그램을 기억하는 휘발성 기억부를 갖고,

상기 휘발성 기억부의 상기 인증 프로그램에 의해서 상기 취득 수단에 의해 생체 정보를 취득하는 것을 특징으로 하는 단말 장치.

청구항 14.

여러 가지 거래를 실행하는 자동 거래 장치에 있어서,

IC 카드의 데이터를 판독하는 IC 카드 장치와,

생체 정보를 취득하여 인증하는 생체 인증 장치와,

암호키를 기억하는 기억 수단과,

상기 IC 카드 장치에 의해서 상기 IC 카드에 기억되고, 암호화된 등록 생체 정보를 판독하여 상기 생체 인증 장치에 송신함과 함께 상기 기억 수단의 상기 암호키를 상기 생체 인증 장치에 송신하는 제어 수단을 갖고,

상기 생체 인증 장치는, 수신한 상기 암호키에 의해서 상기 암호화된 등록 생체 정보를 복호하는 복호부와, 그 복호부에 의해서 복호한 상기 등록 생체 정보와 상기 취득한 생체 정보와의 대조를 행하는 대조부를 갖고, 또한,

상기 생체 인증 장치는, 상기 대조부에 의해 얻은 대조 결과를 상기 암호키에 의해 암호화하여 상기 자동 거래 장치에 송신하는 것을 특징으로 하는 자동 거래 장치.

청구항 15.

제14항에 있어서,

상기 생체 인증 장치는, 암호화된 암호화 인증 프로그램을 기억하는 제1 기억부와, 수신한 상기 암호키에 의해서 상기 암호화 인증 프로그램을 복호하고 복호화한 인증 프로그램으로서 기억하는 제2 기억부를 갖고,

상기 제2 기억부의 상기 복호화한 인증 프로그램은, 상기 복호부 및 상기 대조부를 제어하는 것을 특징으로 하는 자동 거래 장치.

청구항 16.

제15항에 있어서,

상기 제1 기억부는 불휘발성 메모리로, 상기 제2 기억부는 휘발성 메모리로 구성하는 것을 특징으로 하는 자동 거래 장치.

청구항 17.

삭제

청구항 18.

제14항에 있어서,

상기 제어 수단은, 상기 생체 인증 장치로부터 수신하는 데이터에 포함되는 상태 코드에 의해서, 생체 인증에서의 여러 가지의 가이던스를 표시부에 표시하는 것을 특징으로 하는 자동 거래 장치.

청구항 19.

여러 가지 거래를 실행하는 자동 거래 장치에 있어서,

IC 카드의 데이터를 판독하는 IC 카드 장치와,

생체 정보를 취득하여 인증하는 생체 인증 장치와,

암호키를 기억하는 기억 수단과,

상기 IC 카드 장치에 의해서 상기 IC 카드에 기억되고, 암호화된 등록 생체 정보를 판독하여 상기 생체 인증 장치에 송신함과 함께 상기 기억 수단의 상기 암호키를 상기 생체 인증 장치에 송신하는 제어 수단을 갖고,

상기 생체 인증 장치는, 수신한 상기 암호키에 의해서 상기 암호화된 등록 생체 정보를 복호하는 복호부와, 그 복호부에 의해서 복호한 상기 등록 생체 정보와 상기 취득한 생체 정보와의 대조를 행하는 대조부를 갖고, 또한,

상기 생체 인증 장치는, 상기 대조부에 의한 대조 결과를 얻은 후로부터, 다음의 거래 개시까지 상기 복호부에 의해서 복호한 상기 등록 생체 정보를 삭제하는 삭제부를 갖는 것을 특징으로 하는 자동 거래 장치.

청구항 20.

제14항에 있어서,

비밀 번호 입력 화면을 표시하는 표시 수단과,

상기 표시 수단에 입력되는 비밀 번호에 의한 비밀 번호 인증 처리를, 상기 생체 인증 장치에 의한 생체 인증 처리와 별도로 실행하는 것을 특징으로 하는 자동 거래 장치.

청구항 21.

여러 가지 거래를 실행하는 자동 거래 장치에 있어서,

IC 카드의 데이터를 판독하는 IC 카드 장치와,

생체 정보를 취득하여 인증하는 생체 인증 장치와,

암호키를 기억하는 기억 수단과,

상기 IC 카드 장치에 의해서 상기 IC 카드에 기억되고, 암호화된 등록 생체 정보를 판독하여 상기 생체 인증 장치에 송신함과 함께 상기 기억 수단의 상기 암호키를 상기 생체 인증 장치에 송신하는 제어 수단을 갖고,

상기 생체 인증 장치는, 수신한 상기 암호키에 의해서 상기 암호화된 등록 생체 정보를 복호하는 복호부와, 그 복호부에 의해서 복호한 상기 등록 생체 정보와 상기 취득한 생체 정보와의 대조를 행하는 대조부를 갖고, 또한,

비밀번호 입력 화면을 표시하는 표시 수단과,

상기 표시 수단에 입력되는 비밀 번호에 의한 비밀 번호 인증 처리를, 상기 생체 인증 장치에 의한 생체 인증 처리와 별도로 실행함과 함께,

상기 제어 수단은, 상기 생체 인증 처리 후에 상기 비밀 번호 인증 처리를 실행할 때, 상기 생체 인증 장치로부터 송신되는 대조 결과가 올바른 것에 기초하여 상기 표시 수단에 상기 비밀 번호 입력 화면을 표시하는 것을 특징으로 하는 자동 거래 장치.

청구항 22.

삭제

명세서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 생체 정보, 예를 들면 지문이나 정맥 패턴 등을 이용한 본인 확인을 위한 생체 인증 장치, 및 그 생체 인증 방법에 관한 것이다. 특히, 인증 장치에서 취득한 생체 정보가 장치 밖으로 유출되어 제3자에게 악용되는 것을 방지하기 위해서, 생체 정보의 취득 처리, 및 인증 처리를 인증 장치 내부에서 실행하는 장치, 방법에 관한 것이다.

금융 기관에서의 예금의 인출이나 인터넷을 이용한 전자 상거래에서는, 타인의 가장을 방지하기 위해서 본인 확인을 위한 생체 인증이 매우 중요하다. 일반적인 인증 방법으로서, 자기 스트라이프를 갖는 카드와 비밀 번호 입력에 의한 인증이나, 카드 이면의 서명과 상품 구입 시의 서명을 대조함에 의한 인증이 널리 행해지고 있다.

그러나, 이러한 종래의 개인 인증 방법에는 시큐러티에 관한 문제점이 지적되고 있다. 자기 스트라이프를 갖는 캐쉬 카드와 비밀 번호 입력의 조합의 경우, 자기 정보와 비밀 번호가 제3자에게 도난되면 용이하게 예금을 인출하는 것이 가능하게 된다. 혹은, 서명인 경우에는 제3자가 서명을 모방하는 것으로 도용되는 경우도 있을 수 있다.

그런 문제점의 대책으로서, 자기 스트라이프를 갖는 카드 대신에 IC 카드의 도입이 제안되고 있다. IC 카드는, 자기 스트라이프 카드에 비해 카드의 복제가 곤란해짐과 함께, 내부 정보가 용이하게 도난되지 않는다고 하는 안전성도 확보할 수 있게 된다. 덧붙여, 카드 내부에 저장할 수 있는 정보량을 비약적으로 증대할 수 있는 것에 주목하여, 지문이나 정맥 패턴 등의 생체 정보를 IC 카드에 유지하고, 그 대조에 의한 생체 인증 기술로, 특허 문헌 1이나 특허 문헌 2의 공보가 있다.

발명이 이루고자 하는 기술적 과제

전술한 관련 기술에 따르면, 예를 들면 인증하는 장치로부터 생체 정보가 외부에 유출되면, 악의를 가진 제3자에 의해 도난되어 악용될 가능성이 있다. 생체 정보에 의한 개인 인증은, 비밀 번호나 서명에 의한 인증에 비하여 안전성이 높아지는 한편, 한번 유출하게 되면 용이하게는 변경할 수 없다고 하는 마이너스적인 측면도 있다. 그 때문에, 생체 정보가 제3자에게 용이하게 이용 가능한 형태로 외부로 유출되지 않도록 하는 장치가 특히 중요하게 된다.

덧붙여, 생체 정보로 되는 생체 특징량의 추출, 대조하는 생체 인증 프로그램에 대한 시큐러티 확보도 불가결하다. 프로그램 내부를 제3자에 의한 해석, 개변을 방지하지 않으면, 생체 인증 장치로서의 효과를 잃게 될 우려가 있다. 그 의미에서, 생체 인증 장치가 접속되어 있는 제어 장치, 예를 들면 퍼스널 컴퓨터 상에 생체 인증 프로그램이 해석 가능한 상태로 존재하면, 제3자에게 처리 수순을 해석, 도난당할 가능성이 높아진다. 가령 퍼스널 컴퓨터가 아닌 생체 인증 장치 내에 생체 인증 프로그램이 존재하였다고 하여도, 외부로부터 용이하게 해석 가능한 상태로 존재하고 있으면, 역시 악의를 가진 제3자에게 그 정보를 도난당할 가능성이 있다.

또한, 생체 인증 장치로부터 출력되는 생체 인증 결과가 제3자에게 누설되는 것도 방지할 필요가 있다. 생체 인증 장치가 인증 승인된 신호를 제3자가 위조하면, 장치에 의한 인증 거절인 경우에도 인증 장치가 접속된 제어 장치에 인증 승인의 신호가 전해져서, 부정한 거래가 행해질 가능성이 있다.

본 발명은 상기 과제 중 적어도 일부를 해결하기 위해 이루어진 것이다. 본 발명의 제1 목적은 개인의 생체 정보가 생체 인증 장치로부터 제3자가 용이하게 이용 가능한 형태로 외부로 유출하는 것을 방지하는 것이다. 본 발명의 제2 목적은, 생체 특징량을 추출하거나 대조하거나 하는 생체 인증 프로그램을 제3자가 도난, 개변하는 것을 방지하는 것이다. 본 발명의 제3 목적은, 생체 인증 장치가 출력하는 생체 인증 결과의 외부의 누설을 방지하는 것에 있다.

상기 목적을 달성하기 위해, 개인의 생체 정보를 이용하여 본인 확인을 행하는 생체 인증 장치는, 생체 정보를 취득하고, 취득된 센서 정보로부터 인증을 행하기 위한 생체 특징량을 추출하고, 추출된 생체 특징량을 암호화하고, 암호화된 생체 특징량을 본인 확인을 위한 인증용 기준 데이터로서 생체 인증 장치 외부로 출력한다.

또한, 다른 바람직한 예에서는, 개인의 생체 정보를 이용하여 본인 확인을 행하기 위한 생체 인증 장치로서, 센서는 생체 정보를 취득하고, 생체 인증 장치는, 취득된 센서 정보로부터 인증을 행하기 위한 생체 특징량을 추출하고, 추출된 생체 특징량을 암호화하여, 본인 확인을 위한 인증용 기준 데이터로서 암호화된 생체 특징량을, 생체 인증 장치에 접속된 제어 컴퓨터를 통하지 않고서 직접 IC 카드에 출력한다.

또한, 다른 바람직한 예에서는, 개인의 생체 정보를 이용하여 본인 확인을 행하기 위한 생체 인증 장치는, 센서에 의해서 생체 정보를 취득하고, 취득된 센서 정보로부터 인증을 행하기 위한 생체 특징량을 추출하고, 인증용 기준 데이터로 되는 생체 특징량을 암호화된 형태로 생체 인증 장치 외부로부터 입력하고, 상기 인증용 기준 데이터로 되는 암호화된 생체 특징량을 복호하고, 상기 입력된 생체 특징량과, 상기 복호된 인증용 기준 데이터로 되는 생체 특징량을 대조하여, 상기 대조 결과의 출력을 암호화하고, 상기 암호화된 생체 특징량 대조 결과의 출력을 장치 외부에 출력한다.

또한, 다른 바람직한 예에서는, 개인의 생체 정보를 이용하여 본인 확인을 행하기 위한 생체 인증 장치로서, 생체 정보를 취득하고, 취득된 센서 정보로부터 인증을 행하기 위한 생체 특징량을 추출하고, IC 카드에 저장된 인증용 기준 데이터로 되는 암호화된 생체 특징량을, 생체 인증 장치에 접속된 제어 컴퓨터를 통하지 않고서, 직접 IC 카드로부터 입력하고, 상기 인증용 기준 데이터로 되는 암호화된 생체 특징량을 복호하고, 상기 출력된 생체 특징량과, 상기 복호된 인증용 기준 데이터로 되는 생체 특징량을 대조하고, 상기 생체 특징량 대조 결과의 출력을 암호화하고, 상기 암호화된 대조 결과의 출력을 장치 외부에 출력한다.

또한, 다른 바람직한 예에서는, 생체 인증 장치는, 상기 특징량 추출 처리를 행하는 프로그램과 상기 생체 특징량 대조를 행하는 프로그램을, 생체 인증 장치를 기동하기 전에는 암호화된 형태로 장치 내에 저장하고, 장치가 기동된 후에 복호한다.

또한, 다른 바람직한 예에서는, 생체 인증 장치는, 상기 특징량 추출 처리를 행하는 프로그램과 상기 생체 특징량 대조 처리를 행하는 프로그램을, 생체 인증 장치가 기동하기 전에는, 생체 인증 장치에 접속된 제어 컴퓨터와 생체 인증 장치 각각에 분할하여 저장하고, 생체 인증 장치가 기동된 후에 결합 복호하여 동작 가능한 상태로 한다.

발명의 구성

이하, 본 발명의 바람직한 실시 형태에 대하여 도면을 참조하여 상세히 설명한다. 또한, 이에 따라 본 발명이 한정되는 것은 아니다.

본 실시 형태에서는, IC 카드를 통한 금융 영업점에서의 영업점 창구 단말기에서의 생체 정보 등록 처리와 ATM(현금 자동 예불기)에서의 생체 정보 인증 처리에 대하여 설명한다. 여기서 생체 정보란, 개인을 특정하기 위해 유효한 생체 특징량이라고 상정한다.

영업점 창구 단말기에서의 생체 특징량의 등록 처리에서는, 창구 단말기에서 IC 카드에 개인 인증용 암호화된 생체 특징량을 등록한다. 창구 단말기에는 IC 카드 장치 부착 생체 인증 장치가 접속되어 있고, 등록용 생체 특징량이 암호화되어, 창구 단말기를 경유하지 않고서 생체 인증 장치로부터 IC 카드에 직접 전송된다. 한편, ATM(현금 자동 예불기)에서는, IC 카드로부터 암호화된 생체 특징량이 판독되어, ATM에 접속된 생체 인증 장치에 전송되어 장치 내부에서 인증 처리를 행한다. 또한, IC 카드에 한하지 않고 RFID 태그 등, 휴대 가능한 전자적 매체이면, 임의의 매체로 된다.

도 1은 전체 시스템의 구성예이다. 참조 부호 101은 금융 영업점이고, 계정계 호스트 컴퓨터(109)가 설치되어 있는 데이터 센터(103)와는, 광역 네트워크(102)를 통하여 접속되어 있다. 금융 영업점(101)에서는, 영업점 창구 단말기(105)나 ATM(107)이 영업점 내의 LAN(108)으로 접속되어 있다. 영업점 창구 단말기(105)에는 IC 카드 장치 부착 생체 인증 장치(104)를 접속한다. 마찬가지로 ATM(107)에는 생체 인증 장치(106)를 접속하고, IC 카드 장치는 ATM 내부에 조립하고 있다.

우선, 도 2, 도 3, 도 4를 이용하여 영업점 창구 단말기(105)에서의 생체 특징량의 등록 처리에 대하여 설명한다. 도 2는 IC 카드 장치 부착 생체 인증 장치(104)의 구성예를 도시하는 도면이다. CPU(201)는 장치의 데이터 처리를 담당하는 프로세서로, 후술하는 각종 프로그램, 데이터의 제어, 처리를 담당한다. 주변 장치 I/O 디바이스(202)는, 생체 인증 장치(104)와 영업점 창구 단말기(105)를 접속하기 위한 인터페이스이다. 참조 부호 203은 생체 화상을 취득하기 위한 조명 LED로, 예를 들면 손가락 정맥 인증이면 손가락의 정맥 패턴의 취득에 적합한 근적외 광 LED를 이용한다. 화상 센서(204)는 생체 화상을 취득하기 위한 센서로, CCD 등의 디바이스를 예로 들 수 있고, LED(203)에 의해서 조사된 손가락의 정맥 패턴을 취득한다. IC 카드 장치(205)는 암호화된 등록용 생체 특징량을 IC 카드에 기입하기 위한 장치이다.

주기억 장치(207)는 휘발성 메모리(DRAM 등)으로 구성되어 있고, 인증 장치의 전원이 차단되면 저장되어 있는 데이터가 소멸한다. 여기에는 장치를 동작시키기 위한 각종 프로그램이나 데이터 영역이 확보되어 있다. 주기억 장치(207)에 기억되는 프로그램, 데이터는 후술하는 플래시 메모리(217)로부터 판독하여 기억하는 기억부, 기억 수단이다. 장치 전체 제어 프로그램(208)은 IC 카드 장치(205)의 제어도 포함시켜 인증 장치(104) 전체를 제어하는 프로그램이다. 주변 장치 I/O 제어 프로그램(209)은 주변 장치 I/O 디바이스(202)를 제어한다.

암호/복호 프로그램(210)은 2개의 처리를 행한다. 하나는 플래시 메모리(이하, 불휘발성 메모리라고 함)(217)에 저장된 암호화 인증 프로그램(219)을 복호하고, 참조 부호 211의 영역에 인증 프로그램으로서 저장하는 것이다. 다른 하나는, 인증 프로그램(211)이 생성한 등록용 생체 특징량을 IC 카드에 기입하기 전에 암호화하는 것이다. IC 카드 장치 제어 프로그램(212)은 IC 카드 장치(205)를 제어하는 프로그램이다.

이와 같이, 프로그램은 각종 기능을 갖고, 또한 여러 가지의 처리를 행하여, 전술한 바와 같이, CPU(201)의 하드 구성에 의해서 제어된다. 본 발명에서는 프로그램을 중심으로 하여 설명하지만, 이들 각 프로그램의 여러 가지 기능, 예를 들면 제어 수단, 암호화 수단, 인증 수단, 등록 수단, 대조 수단 등이라고도 할 수 있고, 각 수단을 각 부라고도 표현할 수 있는 것은 물론이다.

화상 버퍼(213)는 화상 센서(204)에서 취득한 생체 화상 데이터(생 데이터)를 저장하기 위한 영역이다. 생체 특징량(214)은, 화상 버퍼(213)에 저장된 생체 화상 데이터로부터 인증 프로그램(211)에 의해서 예를 들면, 정맥 패턴만을 추출하여 생성된 생체 특징량을 저장하기 위한 영역이다. 암호화 생체 특징량(215)은, 생체 특징량(214)의 데이터를 암호/복호 프로그램(210)에 의해서 암호화된 데이터를 저장하는 영역이다. 참조 부호 215의 데이터(암호화 상태의 생체 특징량)는 IC 카드 장치(205)를 통하여 IC 카드에 생체 등록 특징량으로서 저장된다. 또한, IC 카드 장치(205)와 인증 장치 사이에 영업점 창구 단말기(105)를 접속, 개재시키는 경우에도, 인증 장치에서 취득한 암호화 상태의 생체 특징량을 창구 단말기(105)에 기억시키지 않고서(남기지 않고서), IC 카드 장치(205)에 의해서 IC 카드 내에 등록한다. 암호키(216)는 암호/복호 프로그램(210)이 데이터를 암호화하거나, 복호하거나 할 때에 필요한 키 데이터이다. 본 키 데이터는 생체 인증 장치가 접속되어 있는 영업점 창구 단말기(105)나 ATM(107)으로부터 주변 I/O 디바이스를 통하여 취득하는 것도 특징 중 하나이다. 참조 부호 206은 인증 장치 내의 프로세서나 각 디바이스를 접속하는 버스이다. 참조 부호 217은 인증 장치의 전원을 차단하여도 내용이 소거되지 않는 불휘발성 메모리로, 그 내부에 암호화된 인증 프로그램(218)이 저장되어 있다. 인증 장치가 기동되면, 암호/복호 프로그램(210)이 암호키(216)를 이용하여 암호화 인증 프로그램(218)을 복호하여, 참조 부호 211의 영역에 저장한다.

도 3은 영업점 창구 단말기(105)의 구성예를 도시하는 도면이다. 창구 단말기(105)는 금융 기관의 카운터에 설치되어, 오퍼레이터가 입금, 출금, 약속 어음 등의 처리 업무를 행하는 컴퓨터로서, 덧붙여 생체 인증의 등록 처리도 행하는 단말 장치이다.

CPU(301)는 단말기의 데이터 처리, 각종 제어를 담당하는 프로세서이다. LAN 디바이스(302)는 영업점 내의 LAN(108)과 단말기를 접속하기 위한 디바이스이고, LAN(108)을 통하여 계정계 호스트 컴퓨터(109)에 접속되어 있다. 주변 장치 I/O 디바이스(303)는, IC 카드 장치 부착 생체 인증 장치(104)를 접속하기 위한 인터페이스이다. 표시 장치(304)는 생체 특징량의 등록 결과(성공인지, 실패인지의 스테이터스로서, 생체 특징량은 포함하지 않고)나, 고객의 거래 정보, 거래에 필요한 항목 등을, 창구 단말기를 조작하는 오퍼레이터에 표시하는 모니터로, 키 입력 장치(305)는 오퍼레이터의 키 입력 장치이다. 현금 처리 장치(306)는 단말기에서의 현금 처리를 행하기 위한 장치이다. 주기억 장치(308)에는, 각종 프로그램이나 데이터가 저장되어 있다. 참조 부호 309는 창구 단말기 전체를 제어하는 전체 제어 프로그램이고, 참조 부호 310에는 창구에서 행하는 업무에 관한 업무 어플리케이션 프로그램이 저장되어 있다. 주변 장치 I/O 제어 프로그램(311)은 주변 장치 I/O 디바이스(303)를 제어한다. 생체 인증 장치 제어 프로그램(312)은, 주변 장치 I/O 디바이스(303)를 통하여 접속되어 있는 IC 카드 장치 부착 생체 인증 장치(104)를 제어하는 프로그램이다. 암호키(313)는 IC 카드 장치 부착 생체 인증 장치(104)를 기동하거나, IC 카드에 등록하는 생체 특징량을 암호화하기 위해 사용된다. 참조 부호 307은 단말기 내의 각 장치를 연결하는 버스이다.

도 4를 이용하여 IC 카드 장치 부착 생체 인증 장치(104), 및 영업점 창구 단말기(105)의 동작을 설명한다. 스텝 401, 406, 407, 408은, 영업점 창구 단말기(105)가 출력하는 지시에 기초하여 IC 카드 장치 부착 생체 인증 장치(104)가 처리하는 내용이다.

창구 단말기(105)의 표시 장치(304)에 표시하는 생체 인증 등록의 항목을 입력 장치(305)에서 선택하면, 전체 제어 프로그램(309)이 생체 인증에 관한 기능을 생체 인증 장치(104)에 전개한다. 스텝 401에서는, 영업점 창구 단말기(105)에 저장된 생체 인증 장치 제어 프로그램(312)이 생체 특징량 등록 처리의 기동 신호, 및 암호키(313)를 IC 카드 장치 부착 생체 인증 장치(104)에 송신한다. 생체 인증 장치(104)에서는, 수신한 기동 신호에 의해 CPU(201)를 중심으로 하여 기동하고, 수신한 암호키(313)를 장치 전체 제어 프로그램(208)이 참조 부호 216의 영역에 저장된다. 그 후, 장치 전체 제어 프로그램(208)은 암호/복호 프로그램(210)을 기동하고, 암호키(216)를 이용하여 불휘발성 메모리(217) 내의 암호화 인증 프로그램(218)을 복호하여, 참조 부호 211에 저장하여 프로그램을 기동한다. 그 때문에 다음과 같은 내 탬퍼성을 갖고 있다.

전술한 바와 같이, 불휘발성 메모리(217) 내에 암호화된 상태에서 인증 프로그램(218)을 저장하고, 기동 시에 주기억 장치(207) 내의 참조 부호 211에 전개하고 있다. 생체 인증 장치에 전원이 들어와 정상적으로 동작하고 있는 경우에는, 장치 외부와의 통신은 암호키(216)를 이용하여 암호화되어 있기 때문에, 정규로 접속된 단말기가 아니면 생체 인증 장치의 내부를 참조할 수는 없다. 그 때문에, 인증 프로그램(211)이 주기억 장치(207)에 해석 가능한 상태로 저장되어 있어도, 외부로부터의 부정 액세스로부터 보호되어 있다. 한편, 생체 인증 장치에 전원이 들어가 있지 않는 상태에서는, 불휘발성 메모리(217)에만 암호화된 인증 프로그램(218)이 저장되어 있다. 이와 같이, 프로그램을 암호화함으로써 제3자가 장치를 분해하여 불휘발성 메모리(217)를 해석, 그 위조, 개찬이 곤란해진다는 효과가 있다.

전술한 예에서는 불휘발성 메모리(217)에 암호화 인증 프로그램을, 휘발성 메모리(207)에 복호하여 전개한 인증 프로그램을 저장, 기억하는 방식 1에 대하여 설명하였다.

그 외에, 암호화 인증 프로그램을 휘발성 메모리(217)에 기억하는 방식 2와, 불휘발성 메모리(217) 내에서 암호화 인증 프로그램(218)을 전개하여 인증 프로그램을 기억하는 방식 3이라고 생각된다. 단, 방식 2에서는 인증 장치의 전원 차단에 의해 암호화 인증 프로그램이 소거되게 되기 때문에 현실적이지 않다. 또한 방식 3에서는 인증 장치가 불휘발성 메모리(217) 내의 복호된 인증 프로그램을 소거하기 전에 인증 장치의 전원을 차단하면, 그대로 불휘발성 메모리(217) 내에 복호되게 된 인증 프로그램이 잔존한다. 그렇기 때문에, 시큐러티의 면에서 적절하지 않다.

이상으로부터 방식 1은 다른 방식 2, 3에 비하여 현실적이며, 안정성이 높은 것이다. 또한, 본 실시예에서는, 인증 장치가 기동하였을 때에 불휘발성 메모리(217)의 암호화 인증 프로그램이 주기억 장치(207)에 복호되고, 이후 인증 장치가 전원을 차단할 때까지 주기억 장치(207)에 복호된 인증 프로그램이 계속 존재한다. 더욱 바람직한 예로서는, 생체 특징량을 추출/인증할 때마다, 암호화된 프로그램을 복호하여 주기억 장치에 전개하고, 처리가 끝나면 주기억 장치 상의 인증 프로그램을 소거하는 예가 있다. 이 경우, 장치 내에서 인증 프로그램이 해석 가능(실행 가능)한 상태로 존재하는 시간이 보다 짧아지기 때문에, 안전성을 더욱 높이는 것을 기대할 수 있다.

계속해서, 주기억 장치(207)에 올바르게 인증 프로그램(211)이 복호되어 기동하면, 영업점 창구 단말기(105), 및 IC 카드 장치 부착 생체 인증 장치(104)는 암호키를 통하여 서로 기기 인증을 확립한다. 제3자가 생체 인증 장치를 도난하여 부정한 제어 컴퓨터에 접속하였다고 하여도, 인증 프로그램이 기동하지 않기 때문에 인증 장치를 동작시키는 것이 불가능하다. 또한, 인증 프로그램은 전술한 바와 같이, 불휘발성 메모리(217)에 의해 암호화되므로, 제3자가 인증 장치를 분해하여 해석하였다고 하여도 인증 프로그램의 내용을 아는 것은 매우 곤란하다. 이와 같이 기동에 대하여 설명하였지만, 창구 단말기(105)의 셧 다운, 전원 차단 등에 기초한 인증 장치(104)의 종료에서는, 참조 부호 211에 저장한 복호화된 인증 프로그램을 클리어(또는 불활성화)함으로써 프로그램의 해석을 곤란한 것으로 할 수 있다.

인증 프로그램(211)은, 조명 LED(203), 및 화상 센서(204)를 제어하여 생체 화상의 특징량을 취득하여 화상 버퍼(213)에 저장한다(402). 그 후, 인증 프로그램(211)은 화상 버퍼(213)에 저장된 생체 화상을 판독하고, 화상으로부터 IC 카드에 등록하기 위한 생체 특징량, 및 등록 특징량을 선택하기 위한 특성 데이터를 추출하여 결과를 생체 특징량(214)에 저장한다(403). 또한, 등록 특징량의 선택은 후술하는 스텝 406에서 반복 등록되는 데이터로부터 선택하는 것을 말한다. 여기서, 특성 데이터는 예를 들면 손가락 정맥 인증의 경우, 손가락의 기울기 등 등록에 적합한 생체 특징량을 선택하기 위한 기준으로 되는 데이터이다. 또한, 생체 특징량은 단순히 생체 정보라고도 하여, 생체 인증 장치는 생체 정보를 취득하는 취득 수단, 취득부를 갖고 있다.

장치 전체 제어 프로그램(208)은 암호/복호 프로그램(210)을 재차 기동한다. 즉, 전술에서는 인증 프로그램의 기동, 복호화(활성화)의 기능을 갖고 있지만, 다음의 설명에서는 취득한 생체 특징량의 암호화의 기능에 이용하기 위해서 재기동한다. 프로그램(210)의 재기동에 의해서, 암호키(216)에 의해 생체 특징량(214)을 암호화하여, 결과를 암호화 생체 특징량(215)에 저장한다(404). 그 후, 데이터가 유출하는 것을 방지하기 위해서, 화상 버퍼(213), 생체 특징량(214)의 영역을 메모리 클리어한다(405).

영업점 창구 단말기(105)는 규정 횟수에 도달할 때까지 스텝 402 내지 405의 처리를 IC 카드 장치 부착 생체 인증 장치(104)에 반복하여 실행시키고, 결과를 암호화 생체 특징량(215)에 저장한다(406). 그리고, 영업점 창구 단말기(105)로부터의 지시로, 인증 프로그램(211)은 스텝 403에서 추출한 특성 데이터(기준 데이터)에 기초하여, IC 카드에 등록할 암호화 등록 특징량을 215의 데이터 중에서 선택한다(407).

장치 전체 제어 프로그램(208)은, 창구 단말기(105)로부터의 지시 하에, IC 카드 장치 제어 프로그램(212)을 통하여, 선택된 암호화 등록 특징량을 IC 카드 장치(205)에 기입한다(408). 그 후, 장치 내에 암호화 등록 특징량이 잔존하는 것을 방지하기 위해서, 암호화 생체 특징량(215)의 영역을 메모리 클리어한다(409). 또한, 전술에서는 창구 단말기(105)의 지시에 의해서 각 종 처리가 행해지는 예를 설명하였지만, 인증 장치 내부만으로 이들의 처리를 자동적으로 행하여도 된다. 또한, S409의 클리어 시에 S405의 클리어를 동시에 하는 예도 있지만, 전술한 406의 반복 처리 전에 행하는 것이 좋다. 즉, 반복 실행에 의해서 그 데이터 사이즈가 커지고, 결국, 화상 버퍼(213)의 사이즈도 크게 할 필요가 있기 때문이다. 또한 S409의 암호화 데이터의 클리어에 비교하여, S405의 데이터는 암호화되어 있지 않은 데이터를 위해 사용 후에는 가능한 한 빠르게 클리어한 쪽이 시큐러티 향상으로 되기 때문이다.

이상의 스텝 401 내지 409의 처리에 의해, 영업점 창구 단말기(105)에 생체 특징량이 출력되지 않고, 생체 인증 장치 내부에서 암호화되어 IC 카드에 저장된다.

다음으로, 도 5, 도 6, 도 7, 도 8을 이용하여 IC 카드 내에 저장된 생체 특징량을 이용하여 ATM에서의 인증 처리에 대하여 설명한다. ATM은 금융 기관에 설치되어, 최종 사용자에 의해서 입금, 출금, 불입 처리 등을 자동적으로 행하고, 현금 자동 거래 장치라고도 한다. ATM의 예로써 설명하지만, 이용자의 개인 인증에 이용되는 단말기, 컴퓨터에 응용 가능하여, 자동 거래 장치로도 칭한다.

도 5는 ATM(107)의 구성예를 도시하는 도면이다. CPU(501)는 ATM의 데이터 처리를 담당하는, 각종 프로그램의 제어나 커맨드의 발생 등 여러 가지의 처리, 제어를 행하는 프로세서이다. LAN 디바이스(502)는 영업점 내의 LAN(108)과 단말기를 접속하기 위한 디바이스이고, LAN(108)을 통하여 계정계 호스트 컴퓨터(109)에 접속되어 있다. 주변 장치 I/O 디바이스(503)는, 생체 인증 장치(106)를 접속하기 위한 인터페이스이다. IC 카드 장치(504)는 ATM의 카드 삽입구에 조립되어 있고, ATM에서는 본인 확인에 이용하는 생체 인증 장치(106)와 분리되어 있다. 표시 장치(505)는 거래 정보나 생체 인증 결과를 이용자에게 표시하는 모니터이고, 키 입력 장치(506)는 이용자가 거래 메뉴나 비밀 번호를 키 입력하기 위한 장치이다. 현금 처리 장치(507)는 ATM에서의 현금 처리를 행하기 위한 장치이다. 주기억 장치(509)에는, 각종 프로그램이나 데이터가 저장되어 있다.

참조 부호 510은 ATM 전체를 제어하는 전체 제어 프로그램이고, 참조 부호 511에는 ATM 거래에서 행하는 업무에 관한 업무 어플리케이션 프로그램이 저장되어 있다. 주변 장치 I/O 제어 프로그램(512)은 주변 장치 I/O 디바이스(503)를 제어한다. 생체 인증 장치 제어 프로그램(513)은, 주변 장치 I/O 디바이스(503)를 통하여 접속되어 있는 생체 인증 장치(106)를 제어하는 프로그램이다. 암호/복호 프로그램(515)은 암호키(516)를 이용하여, 생체 인증 장치(106)로부터 송신되는 암호화된 인증 결과(생체 특징량은 포함하지 않음)를 복호한다. 참조 부호 517은 생체 인증 장치(106)로부터 송신되는 암호화된 인증 결과를 저장하는 영역이고, 참조 부호 518은 암호키(516)를 이용하여 그것을 복호한 결과를 저장하는 영역이다.

ATM에 접속되어 있는 인증용 생체 인증 장치(106)의 구성예를 도 6에 도시한다. 참조 부호 601 내지 604는 각각 도 2에서의 참조 부호 201 내지 204와 마찬가지의 기능을 갖기 때문에 설명을 생략한다. 주기억 장치(605)에는 장치를 동작시키기 위한 각종 프로그램이나 데이터 영역이 확보되어 있다. 장치 전체 제어 프로그램(607)은 생체 인증 장치 전체를 제어하는 프로그램이다. 참조 부호 608 내지 612는, 각각 도 2에서의 참조 부호 209 내지 211, 및 213, 214와 마찬가지로 설명을 생략한다. 참조 부호 613은 주변 장치 I/O 디바이스(602)를 통하여 생체 인증 장치가 IC 카드에 등록된 암호화 생체 등록 특징량을 ATM으로부터 수신하여 저장하기 위한 영역이다. 생체 등록 특징량(614)은 참조 부호 613의 암호화 특징량을 암호/복호 프로그램(609)이 암호키(617)를 이용하여 복호하여 저장하는 영역이다. 대조 결과(615)는 생체 특징량(612)과 생체 등록 특징량(614)을 인증 프로그램(610)이 대조한 결과를 저장하는 영역이다. 암호화 대조 결과(616)는, 암호/복호 프로그램(609)이 암호키(617)를 이용하여 대조 결과(615)를 암호화하여 저장하는 영역이다. 암호키(617)는 생체 인증 장치가 접속되어 있는 ATM(107)으로부터 취득한다. 참조 부호 606은 프로세서나 각 디바이스를 접속하는 버스이다. 참조 부호 618, 619는 각각 도 2의 참조 부호 217, 218과 마찬가지이다.

여기서는, ATM이 전원 ON, 또는 기동하였을 때에 생체 인증 장치(106)도 동시에 기동된다고 가정한다. 구체적으로는, 인증 장치(106)는 기동 시에 ATM(107)로부터 암호키를 수신하여 참조 부호 617에 저장한다. 그것과 동시에, 불휘발성 메모리(618)에 저장된 암호화 인증 프로그램(619)을, 암호키(617)를 이용하여 복호하여 주기억 장치(605)의 참조 부호 610에 저장되어 있는 것을 상정하고 있다. 또한, ATM의 정상 폐국 또는 이상 시의 셧 다운, 전원 차단에 의해서 인증 장치(106)도 종료하지만, 그 종료와 함께 인증 프로그램(610)은 클리어된다. 이들의 인증 프로그램의 복호화에 의한 ATM의 제어부와 생체 인증 장치와의 확립 처리 등이나, 불휘발성 메모리(618)와 주기억 장치(휘발성 메모리)(605)와의 구성으로 한 이유에 대해서는 전술한 영업점 시스템의 예에서 설명하였기 때문에 생략한다.

도 7을 이용하여 ATM(107) 및 생체 인증 장치(106)의 동작에 대하여 설명한다. ATM은 CPU(제어 수단부)(501)의 지시로, 표시 장치(505)에 초기 화면으로서 예입, 지불, 불입 등의 각종 항목(메뉴)을 표시한다. ATM의 이용자는 표시 장치(505)에 표시되어 있는 거래 메뉴로부터, 키 입력 장치(506)를 이용하여 거래 항목을 선택한다(701). 또한, 표시 장치(505)와 키 입력 장치(506)는 터치 패널로, 단순히 표시 장치(수단, 부)라고도 한다. 예를 들면, 여기서는 예금의 지불 거래를 선택하였다고 가정한다. 그 후, 표시 장치(505)에 표시되는 「카드를 삽입하여 주세요」라는 가이던스에 따라, 이용자는 IC 카드를 ATM의 카드 삽입구에 삽입하면, 삽입된 IC 카드는 IC 카드 장치(504)에 취득되어 내용을 판독한다(702). 계속해서, 표시부(505)에는 텐키와 함께 비밀 번호 입력의 가이던스를 표시하고, 이용자는 가이던스에 따라 키 입력 장치(506)를 이용하여 비밀 번호를 입력한다(703). 입력된 비밀 번호는 호스트(109)에 송신되어, 호스트에서 대조된 결과(정부)를 수신한다. 비밀 번호의 송신에서, 암호키(516)에 의해 데이터를 암호화하는 것이 바람직하다. 비밀 번호 입력에 의한 대조 결과가 잘못되었으면, 표시 장치(505)에 「다시 한번 입력하여 주세요」라는 가이던스를 표시하여, 비밀 번호의 재입력을 재촉한다.

한편, 대조 결과가 올바르면, IC 카드 내의 등록된 생체 정보를 판독하거나 또는 「생체 장치에 손가락을 대 주세요」 등의 가이던스를 표시 장치(505)에 표시한다. 그것과 같이, ATM 내의 생체 인증 장치 제어 프로그램(513)의 제어, 처리가 생체 인증 장치(106)의 장치 전체 제어 프로그램(607)으로 이행되어, 생체 인증 처리를 실행한다(704). 이와 같이, 비밀 인증 처리는 ATM 측에서 실행되어, 생체 인증 처리는 다음에 나타내는 생체 인증 장치측에서 실행하는 것도 시큐러티 향상 중 하나의 특징이기도 하다.

스텝 704의 생체 인증 처리의 상세에 대하여 도 8, 및 도 6을 이용하여 설명한다. 우선, ATM(107)이 IC 카드 내에 저장되어 있는 암호화된 생체 등록 특징량을, IC 카드 장치(504)에 의해서 판독(판독 처리)하여, 다이렉트로 생체 인증 장치(106)에 송신한다. 즉, 암호화된 생체 정보의 암호 상태를 유지한 채, 생체 인증 장치로 송신하는 처리를 ATM(제어부)가 실행한다. 이와 같이, ATM(107)에도 암호키(516)를 갖고 있지만, IC 카드로부터 판독한 암호화 생체 등록 특징량을 복호하지 않는다. 인증 장치(106)는 그 암호화된 특징량을 수신하여, 도 6에서의 암호화 생체 등록 특징량(613)에 저장한다(801). 다음으로, 장치 전체 제어 프로그램(607)은 암호/복호 프로그램(609)을 기동하고, 암호키(617)를 이용하여 참조 부호 613에 저장된 암호 데이터를 복호한(복호 처리, 복호부) 후, 그 결과를 생체 등록 특징량(614)에 저장한다(802).

ATM의 표시 장치(505)에 표시되는 가이던스에 따라, 이용자는 생체 인증 장치(106) 위에 예를 들면 손가락을 놓아두면, 장치(106) 내의 인증 프로그램(610)은, 조명 LED(603), 및 화상 센서(604)를 제어하여 생체 화상을 취득하여 화상 버퍼(611)에 저장한다(803). 인증 프로그램(610)은 화상 버퍼(611)에 저장된 생체 화상을 판독하고, 화상으로부터 인증용 생체 특징량을 추출하여 결과를 생체 특징량(612)에 저장한다(804). 이와 같이, 이용자의 생체 화상, 정보, 특징량을 취득하는 기능을 단순히 취득 처리(수단, 부)라고도 한다.

다음으로, 인증 프로그램(610)은 생체 특징량(612)과 생체 등록 특징량(614)을 판독하여 이들 사이의 거리값을 계산하여(매칭, 대조 처리, 부), 거리값이 임계값 미만이면 대조 승인하고, 임계값 이상이면 대조 거절로서 결과를 615에 저장한다. 또한, 615에는 승인이나 거절 등과 같은 대조 결과에 부수하여 상태 코드를 맞추어서 저장한다(805). 예를 들면, 대조 거절인 경우, 생체를 장치에 놓는 위치가 나쁜 것인지, 생체를 압박하는 힘이 극단적으로 강하여 생체 정보를 취득할 수 없었는지, 등을 나타내는 코드를 첨부한다. 인증 장치는 이 코드를 ATM(107)에 송신하고, ATM(107)이 본 코드를 이용함으로써, 예를 들면 대조 거절인 경우, 코드에 맞춘 생체의 놓는 방향 등의 가이던스를 ATM 이용자에 대하여 표시하는 것이 가능하게 된다. 이 결과, 생체 인증의 방식에 관한 정확한 가이던스를 할 수 있기 때문에, 이용자가 필요 이상으로 생체 인증을 반복한다고 하는 번거로움을 저감하는 것이 가능하게 된다.

암호/복호 프로그램(609)은, 615에 저장한 대조 결과에 대하여 암호키(617)를 이용하여 암호화하고 결과를 616에 저장한다(806). 그 후, 외부에 데이터가 유출할 가능성을 없애기 위해서, 장치 전체 제어 프로그램(607)은 611로부터 617에 저장되어 있는 데이터를 클리어한다 (807). 이에 의해, ATM은 생체 인증 장치(106) 내에 잔존하고 있는 생체 특징량을 삭제할 필요가 없어짐과 함께, 장치 내에 잔존하는 생체 특징량이 외부로 누설하는 것을 방지하는 것이 가능하게 된다. 마지막으로, 220에 저장된 암호화 대조 결과를 ATM에 대하여 송신함과 함께(생체 정보 자신은 포함하지 않음과 함께) 장치 내에 존재하는 암호화 대조 결과를 소거한다(808). 가령, 인증 결과가 거절인 경우, ATM은 규정 횟수에 도달할 때까지 스텝 801로부터 808의 처리를 반복한다. 이상 설명한 도 7의 처리에 의해 스텝 704의 생체 인증 처리가 완료된다. 여기서, 스텝 808에서 대조 결과를 암호화한 것을 ATM에 송신하고 있는데, 그 이유는 이하와 같다.

인증 장치는 기본적으로 ATM에 대하여 인증 승인인지, 인증 거절인지의 데이터를 송신하면 된다. 그러나, 그 데이터 포맷이 제3자에게 누설되면, 정규 생체 인증 장치를 벗어나, 인증 승인의 데이터를 항상 송신하는 부정한 기기를, ATM에 접속할 가능성이 생긴다. 이 경우, 생체 인증을 행하지 않아도 인증 승인의 데이터를 ATM은 수취하기 때문에, 생체 인증 장치의 부정 방지 효과를 잃게 될 우려가 있기 때문이다.

스텝 704의 생체 인증의 결과, 인증 승인으로 OK이면 스텝 706으로 진행하고, NG이면 스텝 710의 거래 중지로 진행한다(705).

이용자는 키 입력 장치(506)를 이용하여 반환 금액을 ATM(107)에 입력하고(706), ATM(107)은 입력된 금액에 기초하여 계정계 호스트 컴퓨터(109)와 통신 계정 처리를 행한다(707). 그 후, ATM은 IC 카드를 IC 카드 삽입구로부터 배출함과 함께, 거래 결과를 기재한 명세서를 인쇄한다(708). 마지막으로 ATM은 현금 처리 장치(507)로부터 입력된 금액분의 지폐가 출금되고, 현금 취출구로부터 현금을 배출하여 일련의 처리를 종료한다(709).

이상의 스텝 701로부터 709의 처리에 의해, 생체 인증 장치(106)로부터 생체 특징량이 외부에 출력되지 않고 인증 처리가 완료된다. 또한, IC 카드 장치(504)와 생체 인증 장치(106)를 별개의 부재로 구성하는 예를 설명하였지만, 도 2와 같이 일체로 형성된 것이어도 된다. 이 경우, IC 카드로부터 판독하는 등록, 암호화된 생체 정보는 ATM 내를 일체 통하지 않고, 더욱 시큐러티의 안전을 확보할 수 있다.

상기 실시예에서는 영업점 창구 단말기로 생체 특징량을 IC 카드에 등록하고, ATM에서 생체 인증을 행하는 방식에 대하여 설명하였지만, 생체 특징량의 등록도 ATM에 접속되어 있는 생체 인증 장치에서 행하여도 되고, 영업점 단말기로 생체 인증을 행하여도 되고, 전술과 마찬가지로 등록 생체 정보는 영업점 단말기를 통할 필요가 없다. 또한, 등록과 인증을 1대의 생체 인증 장치에서 겸용하는 경우에는, 도 6에서의 613으로부터 616의 데이터를 도 2의 주기억 장치(207)에 추가하면 가능하게 된다.

또한, 상기 실시예에서는 암호화를 위한 암호키를 1 종류밖에 갖게 하지 않았지만, 인증 프로그램을 복호하기 위한 암호키와 인증 결과를 암호화/복호하기 위한 암호키를 나누어도 되고, 암호화 방식은 임의의 방법을 이용하여도 된다.

또한, 상기 실시예에서는 생체 인증 장치 내의 인증 프로그램은 장치가 기동되어 있지 않을 때에는 암호화된 상태로 불휘발성 메모리에 저장되어, 장치의 기동 시에 복호되는 방식에 대하여 설명하였다. 이 암호화에 의한 인증 프로그램의 시큐

러티 확보 이외에도, 인증 프로그램을 분할하고, 프로그램의 일부를 장치 밖으로 저장하고, 잔여를 생체 인증 장치 내의 불휘발성 메모리에 저장하는 방법도 유효하다. 즉, 인증 장치의 기동 시에 장치 외부에 저장된 인증 프로그램의 일부와, 장치 내의 불휘발성 메모리에 저장된 인증 프로그램의 일부를 결합하고, 원래의 인증 프로그램에 복원할 수 있다. 혹은, 인증 프로그램의 암호화와 분할을 조합하는 것도 가능하다.

또한, ATM에서의 인증에서, 비밀 번호에 의한 인증 처리 후에, 생체 인증 처리를 실행하는 예로 설명하였다. 비밀 번호를 먼저 입력하는 방식의 이점으로서 이하의 점을 들 수 있다. 생체 인증을 이용하지 않는 거래로서는 「거래 메뉴 선택」, 「캐쉬 카드 삽입」, 「비밀 번호 입력」의 형태로 처리가 진행한다. 그 때문에, ATM 이용자는 이러한 순서의 수순에 익숙해지고 있고, 생체 인증이 후이면 그 수순은 변하지 않기 때문에 조작의 당황이 없다. 한편, 생체 인증 처리 후에 비밀 번호 인증 처리를 행하는 예는, 비밀 번호 입력후의 호스트와의 전문 타이밍, 표시하는 화면의 천이등 일절 변경할 필요가 없는 점에서 유리하다. 이 때, 생체 인증 장치로부터 송신되는 대조 결과가 OK일 때에 처음으로 비밀 번호의 입력 화면을 표시하고, 비밀 번호 인증 처리에 이행함으로써 이용자에 대하여 2중 시큐러티를 확보할 수 있다.

상기 실시예에서는, 창구 단말기나 ATM에 암호키가 존재하여, 그 키를 이용하여 생체 특징량을 암호화하여 IC 카드에 등록하였다. 생체 특징량을 암호화하는 키는 반드시 창구 단말기나 ATM에 존재할 필요는 없고, 생체 인증 장치 내에만 존재하여도 된다. 이 경우, 창구 단말기나 ATM 경유로 IC 카드 생체 인증 장치 사이에서 암호화된 생체 특징량을 기입 및 판독할 때에는, 키가 창구 단말기나 ATM에 존재하지 않기 때문에 암호화 생체 특징량을 해독하는 것이 원리적으로 곤란하게 되고, 시큐러티를 향상시키는 것이 가능하게 된다.

상기 실시예에 따르면, 악의를 가진 제3자가 생체 정보 또는 생체 특징량을 훔쳐내는 것을 방지할 수 있다. 또한, 생체 인증에 관한 생체 특징량 추출 처리,생체 특징량의 대조 처리를 행하는 프로그램의 해석, 개찬, 취득 등을 방지할 수 있다. 또한, 만약 장치를 분해하여, 해석하여도 개찬을 방지할 수 있다.

발명의 효과

본 발명에 따르면, 개인의 생체 정보가 생체 인증 장치로부터 제3자가 용이하게 이용 가능한 형태로 외부로 유출하는 것을 방지할 수 있다. 또한, 생체 특징량을 추출하거나 대조하거나 하는 생체 인증 프로그램을 제3자가 도난, 개변하는 것을 방지하고, 또한 생체 인증 장치가 출력하는 생체 인증 결과의 외부의 누설을 방지할 수 있게 된다.

도면의 간단한 설명

도 1은 생체 인증을 이용한 금융 영업점 시스템의 전체 구성예를 도시하는 도면.

도 2는 영업점 창구 단말기에 접속되는 IC 카드 장치 부착 생체 인증 장치의 구성예를 도시하는 도면.

도 3은 영업점 창구 단말기의 구성예를 도시하는 도면.

도 4는 영업점 창구 단말기와 IC 카드 장치 부착 생체 인증 장치를 이용하여 생체 인증용 특징량을 IC 카드에 등록하는 처리 플로우를 도시하는 도면.

도 5는 ATM(자동 현금 예불기)의 구성예를 도시하는 도면.

도 6은 ATM에 접속되는 생체 인증 장치의 구성예를 도시하는 도면.

도 7은 ATM에서 생체 인증 처리를 포함하는 거래 업무 플로우를 도시하는 도면.

도 8은 ATM에 접속되는 생체 인증 장치의 처리 플로우를 도시하는 도면.

<도면의 주요 부분에 대한 부호의 설명>

101 : 금융 영업점

102 : 광역 네트워크

103 : 데이터 센터

104 : IC 카드 장치 부착 생체 인증 장치

105 : 영업점 창구 단말기

106 : 생체 인증 장치

107 : ATM

108 : LAN

109 : 계정계 호스트 컴퓨터

201 : CPU

202 : 주변 장치 I/O 디바이스

203 : 조명 LED

204 : 화상 센서

205 : IC 카드 장치

207 : 주기억 장치

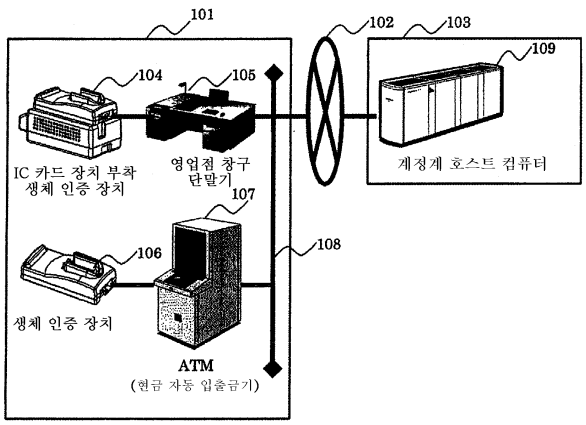
208 : 장치 전체 제어 프로그램

209 : 주변 장치 I/O 제어 프로그램

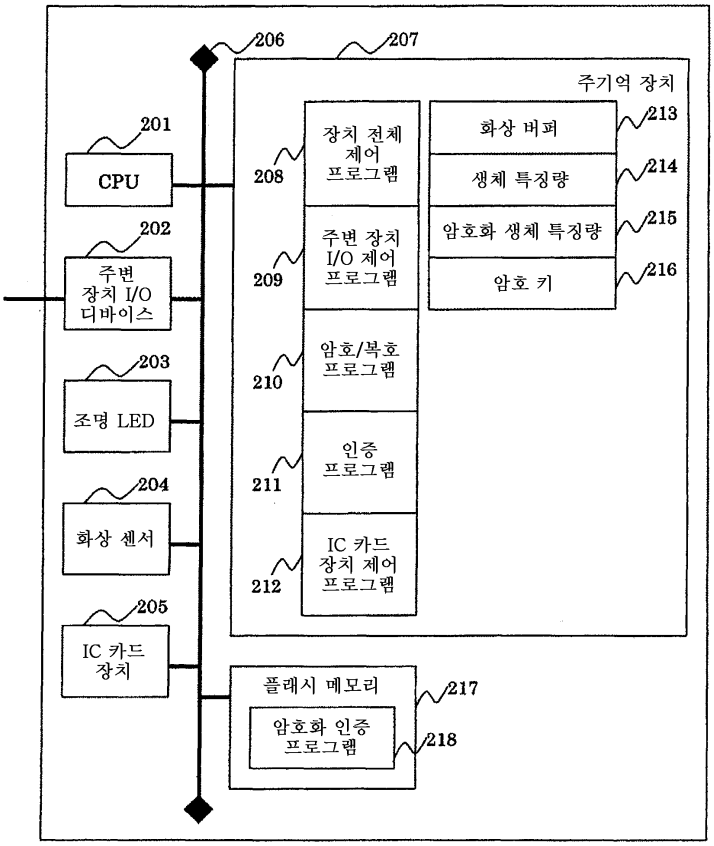
217 : 플래시 메모리

도면

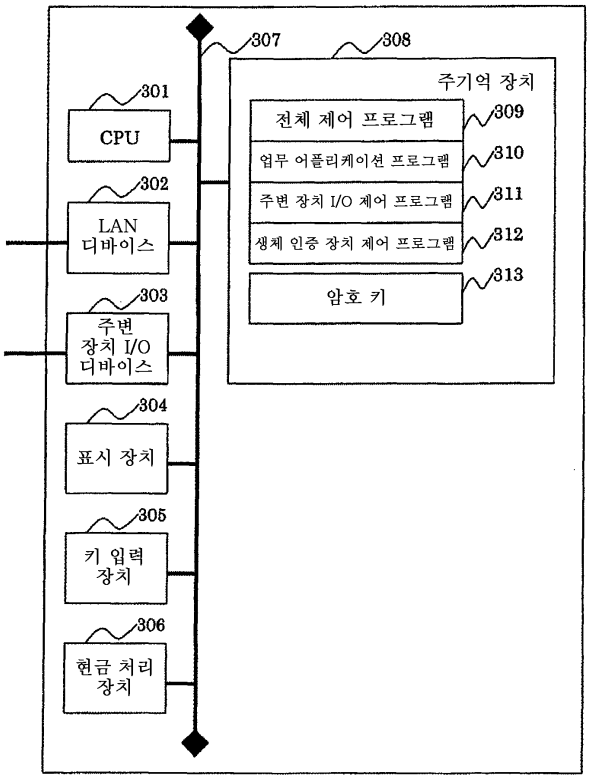
도면1



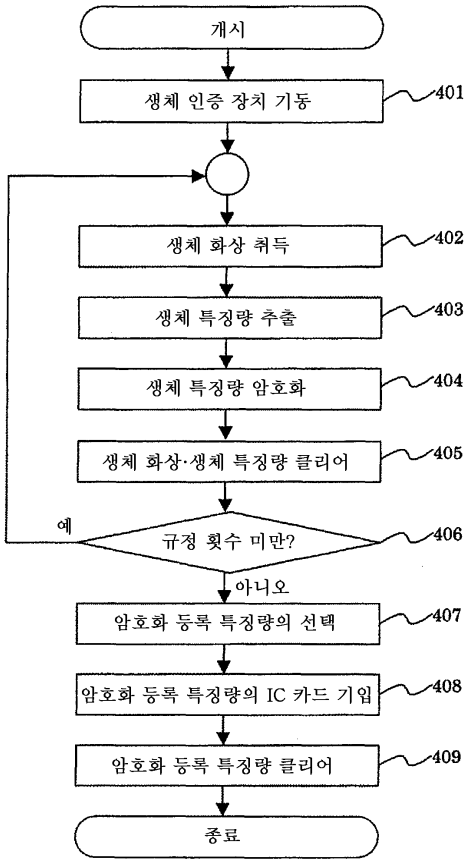
도면2


206
207
주기억 장치
201
CPU
208
장치 전체 제어 프로그램
화상 버퍼
213
생체 특징량
214
202
주변 장치 I/O 디바이스
209
주변 장치 I/O 제어 프로그램
암호화 생체 특징량
215
암호 키
216
203
조명 LED
210
암호/복호 프로그램
204
화상 센서
211
인증 프로그램
205
IC 카드 장치
212
IC 카드 장치 제어 프로그램
플래시 메모리
217
암호화 인증 프로그램
218

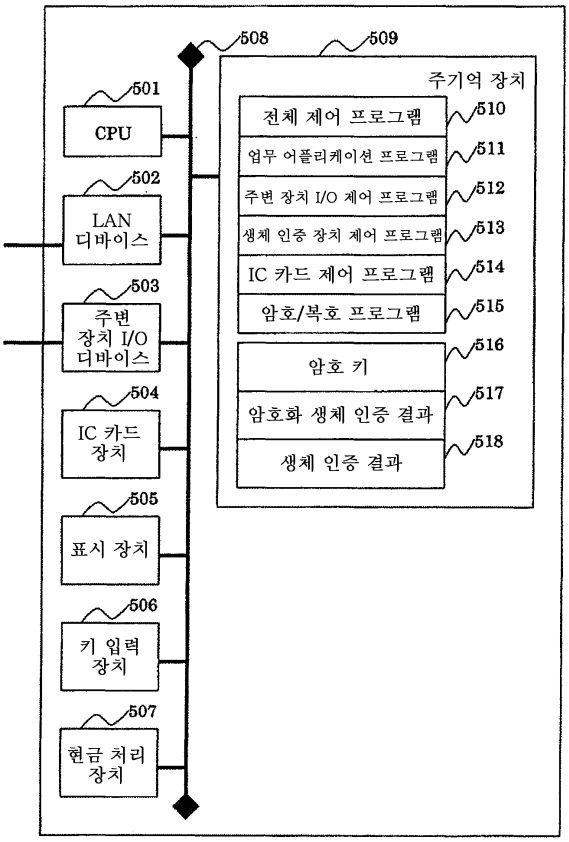
도면3


307
308
주기억 장치
301
CPU
전체 제어 프로그램
309
업무 어플리케이션 프로그램
310
302
LAN 디바이스
주변 장치 I/O 제어 프로그램
311
생체 인증 장치 제어 프로그램
312
303
주변 장치 I/O 디바이스
암호 키
313
304
표시 장치
305
키 입력 장치
306
현금 처리 장치

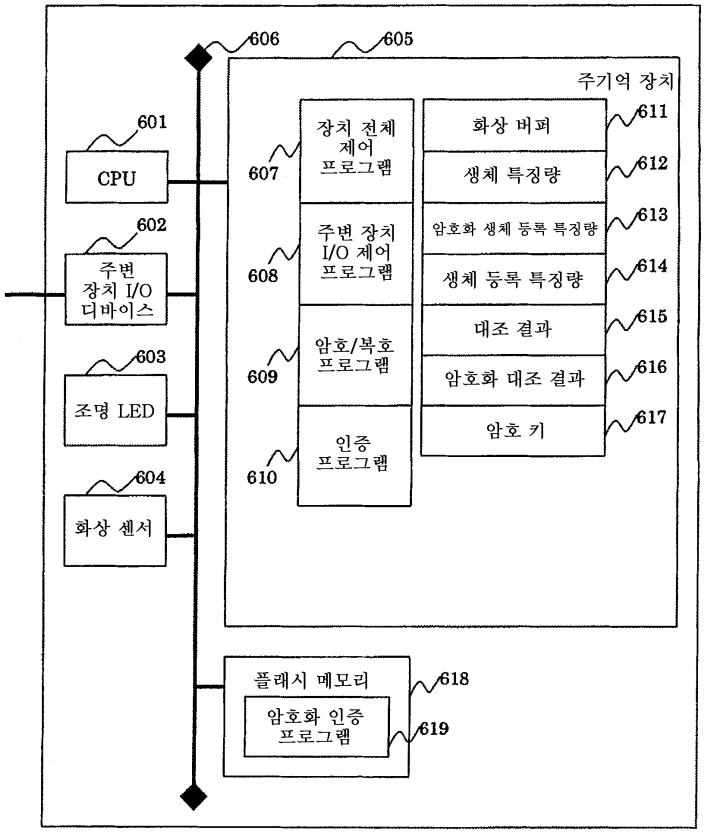
도면4


개시
생체 인증 장치 기동
401
생체 화상 취득
402
생체 특징량 추출
403
생체 특징량 암호화
404
생체 화상·생체 특징량 클리어
405
예
규정 횟수 미만?
406
아니오
암호화 등록 특징량의 선택
407
암호화 등록 특징량의 IC 카드 기입
408
암호화 등록 특징량 클리어
409
종료

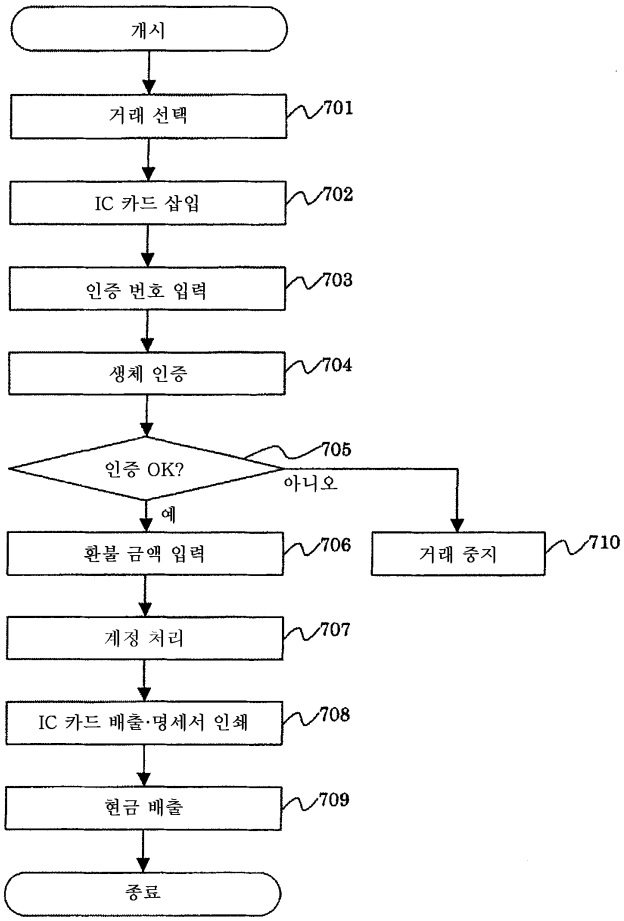
도면5


508
509
주기억 장치
501
CPU
502
LAN 디바이스
503
주변 장치 I/O 디바이스
504
IC 카드 장치
505
표시 장치
506
키 입력 장치
507
현금 처리 장치
전체 제어 프로그램
510
업무 어플리케이션 프로그램
511
주변 장치 I/O 제어 프로그램
512
생체 인증 장치 제어 프로그램
513
IC 카드 제어 프로그램
514
암호/복호 프로그램
515
암호 키
516
암호화 생체 인증 결과
517
생체 인증 결과
518

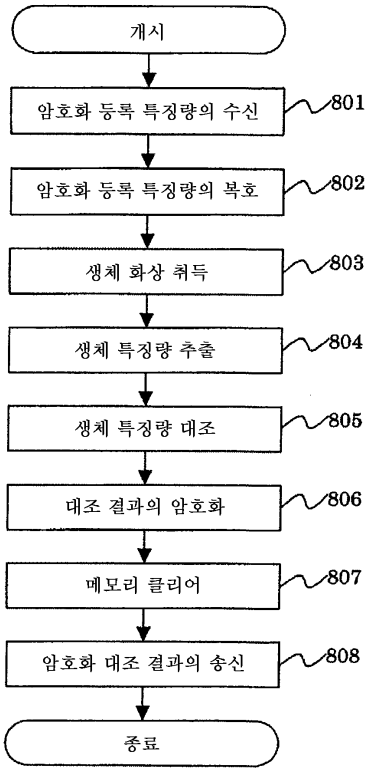
도면6


606
605
주기억 장치
601
CPU
602
주변
장치 I/O
디바이스
603
조명 LED
604
화상 센서
607
장치 전체
제어
프로그램
608
주변 장치
I/O 제어
프로그램
609
암호/복호
프로그램
610
인증
프로그램
화상 버퍼
611
생체 특징량
612
암호화 생체 등록 특징량
613
생체 등록 특징량
614
대조 결과
615
암호화 대조 결과
616
암호 키
617
플래시 메모리
618
암호화 인증
프로그램
619

도면7


개시
거래 선택
701
IC 카드 삽입
702
인증 번호 입력
703
생체 인증
704
인증 OK?
705
아니오
예
환불 금액 입력
706
거래 중지
710
계정 처리
707
IC 카드 배출·명세서 인쇄
708
현금 배출
709
종료

도면8


개시
암호화 등록 특징량의 수신
801
암호화 등록 특징량의 복호
802
생체 화상 취득
803
생체 특징량 추출
804
생체 특징량 대조
805
대조 결과의 암호화
806
메모리 클리어
807
암호화 대조 결과의 송신
808
종료