(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년04월01일
(11) 등록번호 10-1249587
(24) 등록일자 2013년03월26일

(51) 국제특허분류(Int. Cl.)
G06K 19/07 (2006.01) *G06K 9/46* (2006.01)
(21) 출원번호 10-2011-0091803
(22) 출원일자 2011년09월09일
심사청구일자 2011년09월09일
(65) 공개번호 10-2013-0028327
(43) 공개일자 2013년03월19일
(56) 선행기술조사문헌
KR1020110054352 A
KR1020090051147 A
KR1020070084801 A

(73) 특허권자
아이리텍 잉크
미국, 캘리포니아 95134, 산 호세, 3003 엔 퍼스트 스트리트 슈트 255
(72) 발명자
김대훈
서울특별시 강남구 삼성로 212, 18동 1012호 (대치동, 은마아파트)
최형인
서울특별시 송파구 양재대로 1109, 7동 601호 (방이동, 대림가락아파트)
(뒷면에 계속)
(74) 대리인
이상묵

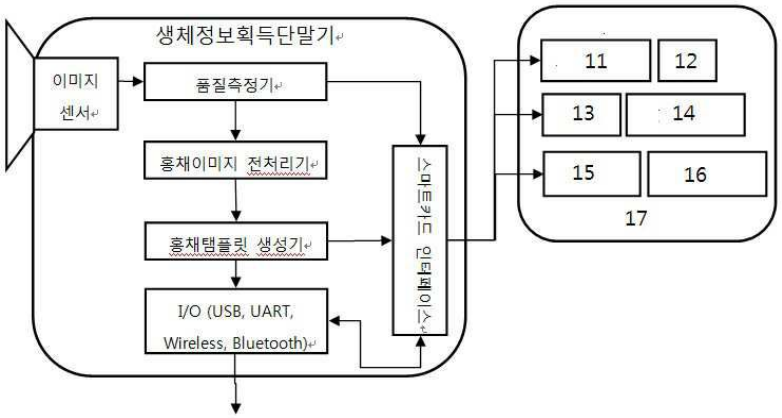
전체 청구항 수 : 총 13 항 심사관 : 성백두

(54) 발명의 명칭 **홍채이미지 정보를 포함하는 일회용 비밀번호가 탑재된 스마트카드**

(57) 요 약

본 발명은 사용자가 최초로 등록한 홍채이미지 탬플릿이 메모리에 저장되어 있고, 스마트카드 메모리에 홍채이미지 탬플릿간의 유사도를 측정하는 알고리즘이 탑재되며, 스마트카드 메모리에 저장된 홍채이미지 탬플릿과 단말기 또는 거치대에 부착 설치된 카메라로부터 획득하여 카드로 전달된 홍채이미지 탬플릿이 서로 동일 또는 유사한지 여부를 판단하기 위한 스마트카드의 매칭기를 구비하며, 매칭기에서 실소유자라고 판단되면 홍채이미지 정보가 포함된 일회용 비밀번호를 생성하여 카드리드기가 설치된 거치대 또는 단말기를 통해서 인증서버로 전송하여 자원접근 권한 획득을 위한 인증절차를 거쳐서, 자원접근 권한을 얻도록 구성된 홍채이미지 정보를 포함하는 일회용 비밀번호가 탑재된 스마트카드에 관한 것이다.

대 표 도 - 도2



(72) 발명자

뒤엔 응위엔

서울특별시 관악구 청림3라길 21, 연구공원본관 420호 (봉천동, 서울대학교)

중밤

서울특별시 관악구 청림3라길 21, 연구공원본관 420호 (봉천동, 서울대학교)

특허청구의 범위

청구항 1

홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드에 있어서,

스마트카드의 사용자가 실소유자임을 확인하기 위하여 메모리에 저장된 홍채이미지 탬플릿;

카메라와 카드리드기가 고정 설치된 단말기 또는 거치대에서, 카메라에서 촬영 획득하여 카드리드기를 통해서 전송된 인증을 위한 홍채이미지 탬플릿을 시드(seed)로 하여 일련의 해쉬 데이터를 생성하고, 생성된 해쉬 데이터를 일회용 비밀번호로 생성하는 수단;

상기 일회용 비밀번호를 생성하기 위한 프로그램을 탑재한 메모리; 및

상기 메모리에 저장된 프로그램을 실행하기 위한 마이크로프로세서가 내장된 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 2

청구항 1에 있어서,

상기 카메라에서 촬영 획득하여 카드리드기를 통해서 전송된 홍채이미지 탬플릿과 스마트카드 리드기에 등록 저장된 홍채이미지 탬플릿을 비교하여 스마트카드 사용자가 실소유자를 판단하는 수단을 구비함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 3

청구항 1에 있어서,

상기 홍채이미지 탬플릿은 사용자 각각의 홍채이미지 특징을 포함하고 있는 특정 영역에 속한 픽셀단위의 홍채이미지 데이터만을 잘라내어 일회용 비밀번호 생성 시 해쉬함수의 변수로 사용함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 4

삭제

청구항 5

청구항 1에 있어서,

상기 스마트카드는 사용자가 실소유자임을 확인할 수 있도록 사용자의 개인식별번호(PIN)를 스마트카드 메모리에 저장하고, 사용자가 입력패드를 통해서 입력하는 개인식별번호와 스마트카드 메모리에 저장된 개인식별번호를 비교하는 수단을 구비함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 6

청구항 1 내지 청구항 3 및 청구항 5 중 어느 한 항에 있어서,

상기 스마트카드는 해쉬함수의 n개의 해쉬데이터 사슬 중에서 n-1개의 해쉬데이터 사슬을 스마트카드의 메모리에 저장함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 7

청구항 1에 있어서,

상기 스마트카드에는 보안성을 높이기 위하여 일회용 비밀번호 생성 프로그램에 의하여 생성된 일회용 비밀번호를 암호화하기 위한 암호화기를 탑재하고, 일회용 비밀번호를 암호화하여 인증서버로 전송함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 8

청구항 6에 있어서,

상기 스마트카드는 보안성을 높이기 위하여 인증서버에서 인증 승인이 이루진 후 홍채이미지 데이터를 해쉬함수에 적용하여 해쉬데이터를 변형하여 대기해쉬로 보유함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 9

청구항 5에 있어서,

상기 스마트카드는 보안성을 높이기 위한 스마트카드가 가진 해쉬데이터 사슬을 갱신하며, 해쉬데이터 사슬의 갱신은 인증서버에서 인증 승인 후 대기해쉬를 기반으로 이루어지고, 대기해쉬는 인증서버와 동일한 홍채이미지 탬플릿을 기반으로 이루어짐을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 10

청구항 9에 있어서,

상기 스마트카드의 해쉬데이터 갱신은 단말기 또는 거치대에 고정 설치된 카메라에서 촬영 획득한 홍채이미지 탬플릿을 기반으로 하여 수행됨을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 11

청구항 1에 있어서,

상기 스마트카드는 스마트카드 메모리에 홍채이미지 탬플릿에 부여되는 트랜잭션 번호, 스크램블링 및 서명을 저장해 두고, 카드리드기에 스마트카드를 삽입할 때 카메라가 설치된 단말기 또는 거치대로부터 홍채이미지 탬플릿에 트랜잭션 번호, 스크램블링 및 서명 중에서 하나 이상을 부여하여 전송할 경우에 스마트카드 메모리에 저장된 것과 비교 확인하여 실제로 홍채정보획득을 위하여 카메라가 설치된 단말기 또는 거치대로부터 전송되어 온 홍채이미지 탬플릿인지를 판별하도록 구성됨을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 12

청구항 1에 있어서,

상기 스마트카드는 카드리드기에 삽입할 때 카드리드기로부터 전원을 공급받을 수 있도록 전원공급단자를 더 구비함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 13

청구항 8에 있어서,

상기 스마트카드는 인증서버와 재동기화를 수행하기 위하여 카드리드기가 설치된 단말기 또는 거치대를 통해서 인증서버와 신호를 주고받는 수단을 구비함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

청구항 14

홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드에 있어서,

스마트카드와 인증서버 간에 인증을 위해 해쉬데이터 사슬이 생성되고,

스마트카드와 인증서버가 공통으로 구비한 각 해쉬데이터 사슬의 말단 해쉬데이터를 이용하여 대기해쉬를 생성함을 특징으로 하는 홍채이미지 정보를 포함하는 일회용 비밀번호를 생성하는 스마트카드.

명 세 서

기 술 분 야

[0001] 본 발명은 사용자가 최초로 등록한 홍채이미지 탬플릿이 메모리에 저장되어 있고, 스마트카드 메모리에 홍채이미지 탬플릿간의 유사도를 측정하는 알고리즘이 탑재되며, 스마트카드 메모리에 저장된 홍채이미지 탬플릿과 단말기 또는 거치대에 부착 설치된 카메라로부터 획득하여 카드로 전달된 홍채이미지 탬플릿이 서로 동일 또는 유사한지 여부를 판단하기 위한 스마트카드의 매칭기를 구비하며, 매칭기에서 실소유자라고 판단되면 홍채이미지 정보가 포함된 일회용 비밀번호를 생성하여 카드리드기가 설치된 거치대 또는 단말기를 통해서 인증서버로 전송하여 자원접근 권한 획득을 위한 인증절차를 거쳐서, 자원접근 권한을 얻도록 구성된 홍채이미지 정보를 포함하는 일회용 비밀번호가 탑재된 스마트카드에 관한 것이다.

배 경 기 술

[0002] 통상의 스마트카드는 스마트카드의 사용자가 본인임을 확인하는 절차를 거치지 않고, 비밀번호 또는 일회용 비밀번호(OTP, one-time password)만을 확인하는 경우가 많아서 분실된 카드를 타인이 이용할 수 있어 보안성에 문제점가 있다.

[0003] 또한, 통상의 스마트카드에는 일회용 비밀번호를 생성하는 프로그램이나 암호화 알고리즘이 탑재되어 있지 아니하여 인증서버와 카드리드기가 설치된 단말기를 통해서 인증절차를 거칠 때 해커에 의하여 개인정보를 해킹 당할 가능성이 높은 문제점이 있다.

발명의 내용

해결하려는 과제

[0004] 본 발명이 해결하려는 과제는 생체정보와 일회용 비밀번호를 결합하여 인증을 수행하되, 카드리드기가 설치된 거치대 또는 단말기에 고정 설치된 카메라로 홍채정보를 획득하고, 획득한 홍채정보를 스마트카드의 메모리에 저장된 홍채정보와 비교하여 카드의 실제소유자임을 확인하도록 하는데 있다.

[0005] 본 발명이 해결하려는 또 다른 과제는 스마트카드에 홍채이미지 정보를 저장하고, 카드리드기 설치된 단말기 또는 거치대 전면에 설치된 카메라를 이용하여 촬영 획득한 홍채이미지 정보가 포함된 해쉬함수에 의하여 생성된 데이터를 일회용 비밀번호를 생성하는 프로그램이 탑재되어 비밀번호의 유출이나 해킹에 의한 개인정보 유출을 최소화하여 보안성을 높이는데 있다.

[0006] 본 발명이 해결하려는 또 다른 과제는 해커에 의한 해킹 시 보안성을 높이기 위하여 홍채이미지 정보를 해쉬함수의 변수로 사용하여 일회용 비밀정보를 생성하되, 해쉬함수의 해쉬데이터사슬에서 n번째 해쉬데이터인 H_n은 서버의 메모리에 저장하고, 나머지 n-1개의 해쉬데이터를 스미트카드 메모리에 저장하여 스마트카드와, 스마트카드와 연동하는 보안시스템의 보안성을 높이는데 있다.

과제의 해결 수단

[0007] 본 발명의 과제 해결 수단은 스마트카드의 메모리에 사용자가 최초로 등록한 홍채이미지 탬플릿이 저장되어 있고, 스마트카드 메모리에 홍채이미지 탬플릿간의 유사도를 측정하는 알고리즘이 탑재되며, 스마트카드 메모리에 저장된 홍채이미지 탬플릿과 단말기 또는 거치대에 부착 설치된 카메라로부터 획득하여 스마트카드로 전달된 홍채이미지 탬플릿이 서로 동일 또는 유사한지 여부를 판단하기 위한 스마트카드의 매칭기를 구비하며, 홍채이미지 정보가 포함된 일회용 비밀번호를 생성하는 프로그램이 탑재된 스마트카드를 제공하는데 있다.

[0008] 본 발명의 또 다른 과제 해결 수단은 해커에 의한 해킹 시 보안성을 높이기 위하여 홍채이미지 정보를 포함하는 해쉬함수의 변수로 사용하여 일회용 비밀정보를 생성하는 프로그램을 탑재하며, 해쉬함수의 해쉬데이터사슬에서 n번째 해쉬데이터인 H_n은 서버의 메모리에 저장하고, 나머지 n-1개의 해쉬데이터가 스마트카드 메모리에 저장된 스마트카드를 제공하는데 있다.

[0009] 본 발명의 또 다른 과제 해결 수단은 보안의 안전성과 신뢰성을 높이기 위하여 홍채이미지 정보를 해쉬함수의 변수로 하는 해쉬데이터사슬을 생성한 후, 해쉬함수의 변수로 사용된 홍채이미지를 갱신하거나 변형된 해쉬데이터로 저장하는 수단을 구비한 스마트카드를 제공하는데 있다.

[0010] 본 발명의 또 다른 과제 해결 수단은 스마트카드에서 생성된 일회용 비밀번호가 인증서버에 저장된 비밀번호와 서로 일치하여 자원접근 권한 승인이 이루어지면, 스마트카드와 인증서버에 저장된 홍채이미지 정보를 변수로

하는 해쉬데이터를 갱신하여 보안성이 높은 스마트카드를 제공하는데 있다.

발명의 효과

[0011] 본 발명은 생체정보와 일회용 비밀번호를 결합하여 인증을 수행하되, 카드리드기가 설치된 거치대 또는 단말기에 고정 설치된 카메라로 홍채이미지를 획득하고, 획득한 홍채이미지 정보를 스마트카드의 메모리에 저장된 홍채이미지 정보와 비교하여 스마트카드 실제소유자임을 확인함으로써 보안성을 크게 향상시키는데 있다.

[0012] 본 발명의 또 다른 효과는 스마트카드에 홍채이미지 정보를 저장하고, 카드리드기 설치된 카메라를 이용하여 촬영 획득 홍채이미지 또는 스마트카드 메모리에 저장된 홍채이미지 정보가 포함된 해쉬함수에 의하여 생성된 데이터를 일회용 비밀번호를 생성하는 프로그램이 탑재되어 비밀번호의 유출이나 해킹에 의한 정보 유출을 최소화하여 보안성을 높이는데 있다.

[0013] 본 발명의 또 다른 효과는 해커에 의한 해킹 시 보안성을 높이기 위하여 홍채이미지 정보를 해쉬함수의 변수로 사용하여 일회용 비밀정보를 생성하되, 해쉬함수의 해쉬데이터사슬에서 n번째 해쉬데이터인 H_n은 인증서버의 메모리에 저장하고, 나머지 n-1개의 해쉬데이터를 스미트카드 메모리에 저장하여 스마트카드와, 스마트카드와 연동하는 보안시스템의 보안성을 높이는데 있다.

[0014] 본 발명의 또 다른 효과는 스마트카드에서 생성된 일회용 비밀번호가 인증서버에 저장된 비밀번호와 서로 일치하여 자원접근권한 승인이 이루어지면 스마트카드와 인증서버에 저장된 해쉬데이터를 갱신할 수 있고, 갱신은 승인이 이루어질 때마다 수행하거나 인증서버의 부담을 고려하여 갱신 빈도수를 제어할 수 있도록 구성함으로써 스마트카드의 보안성을 높이는데 있다.

도면의 간단한 설명

[0015] 도 1은 본 발명에 따른 스마트카드를 이용한 접근 제어시스템을 도시한 것이다.

도 2는 본 발명에 따른 스마트카드와 스마트카드와 연동하는 단말기 또는 거치대가 구비한 기능 및 수단을 도시한 것이다.

도 3은 본 발명에 따른 보안성을 높이기 위하여 스마트카드와 인증서버에 각각 서로 다른 해쉬데이터가 저장됨을 도시한 것이다.

<도면부호의 간단한 설명>

11; 일회용 비밀번호 생성기　　12; 일회용 비밀번호

13; 매칭기　　14; 홍채이미지 탬플릿

15; 암호화기 및 복호화기　　16; 암호화된 데이터

발명을 실시하기 위한 구체적인 내용

[0016] 본 발명의 실시를 위한 구체적인 내용에 대하여 살펴본다.

[0017] 본 발명에 따른 스마트카드는 스마트카드의 메모리에 사용자가 최초로 등록한 홍채이미지 탬플릿이 저장되어 있고, 스마트카드 메모리에 홍채이미지 탬플릿간의 유사도를 측정하는 알고리즘이 탑재되며, 스마트카드 메모리에 저장된 홍채이미지 탬플릿과 단말기 또는 거치대에 부착 설치된 카메라로부터 촬영 획득하여 스마트카드로 전달된 홍채이미지 탬플릿이 서로 동일 또는 유사한지 여부를 판단하기 위한 스마트카드의 매칭기를 구비하며, 홍채이미지 정보가 포함된 일회용 비밀번호를 생성하는 프로그램이 탑재되어 있다.

[0018] 또한, 본 발명은 해커에 의한 해킹 시 보안성을 높이기 위하여 홍채이미지를 포함하는 해쉬함수의 변수로 사용하여 일회용 비밀정보를 생성하는 프로그램을 탑재하며, 해쉬함수의 해쉬데이터사슬에서 n번째 해쉬데이터인 H_n은 인증서버의 메모리에 저장하고, 나머지 n-1개의 해쉬데이터를 스마트카드 메모리에 저장되어 있다. 본 발명의 구체적인 실시 예에 대하여 살펴본다.

[0019] <실시 예>

[0020] 본 발명의 구체적인 실시 예를 도면에 기초하여 살펴본다. 도 1은 본 발명에 따른 스마트카드를 이용한 접근 제어시스템을 도시한 것이다. 도 2는 본 발명에 따른 스마트카드와, 스마트카드와 연동하는 단말기 또는 거치대가

구비한 기능 및 수단을 도시한 것이다.

[0021] 도 1은 본 발명에 따른 스마트카드가 사용될 전체적인 보안시스템을 개략적으로 도시한 것이며, 기본적으로 스마트카드, 생체정보획득을 위한 카메라가 설치된 단말기 또는 거치대, 인증을 위한 인증서버의 세 개체(entity)로 이루어진다.

[0022] 생체정보획득을 위한 단말기 또는 거치대는 사용자의 스마트카드 사용자의 홍채이미지를 카메라로 홍채이미지를 촬영 획득하여 홍채이미지 탬플릿을 만든 후에 스마트카드로 전달하도록 구성되어 있다.

[0023] 본 발명에 따른 스마트카드는 카드리드기가 설치된 단말기 또는 거치대에서 스마트카드로 전달된 홍채이미지 탬플릿을 바탕으로 스미트카드에 저장된 홍채이미지 탬플릿과 비교하여 사용자가 스마트카드의 실소유자인지를 스마트카드에 저장된 프로그램인 매칭기에 의하여 판단하는 수단을 구비하고, 실소유자라고 판단할 때 활성화되도록 구성되어 있다.

[0024] 카드리드기는 본 발명에 따른 스마트카드를 읽을 수 있는 것을 의미하며, 생체정보는 사용자의 특징을 나타내는 지문, 홍채, 얼굴 형상 등이 될 수 있으며, 본 발명에서는 홍채이미지에 구체적으로 대하여 기술한다.

[0025] 홍채이미지의 획득은 카메라로 주로 이루어지나, 홍채이미지의 특징부를 획득할 수 있는 것이면 족하다.

[0026] 스마트카드는 단말기 또는 거치대에 고정 설치된 카메라로부터 획득한 홍채이미지 정보를 해쉬함수의 변수로 사용하여 일회용 비밀번호를 생성하고, 암호화하는 등의 소정의 프로그램을 저장하고, 이를 수행하기 위하여 메모리와 마이크로프로세서를 내장하고 있다.

[0027] 사용자가 스마트카드의 실소유자임으로 판단 결정되면, 스마트카드는 단말기 또는 거치대에 고정 설치된 카메라에서 획득한 홍채이미지를 포함하는 해쉬함수의 변수로 사용하여 일회용 비밀정보를 생성하는 수단을 구비하고, 생성된 일회용 비밀번호를 단말기 또는 거치대를 통해서 인증서버로 전송하는 수단을 구비하며, 전송된 일회용 비밀번호를 이용하여 자원 접근 권한 획득을 위한 인증 절차를 거치도록 구성되어 있다.

[0028] 인증서버로부터 인증결과 사용 승인이 이루어지면 사용자는 자원접근권한을 얻도록 구성되어 있다.

[0029] 도1에서, 호스트 PC 또는 제어프로그램을 실행하기 위한 마이크로프로세서는 스마트카드와 생체정보획득을 위한 카메라와 카드리드기가 설치된 단말기 또는 거치대간의 중계와 스마트카드와 인증서버간의 중계 역할을 담당한다.

[0030] 특별한 언급이 없다면 개체간의 신호를 주고받기 위하여 메모리에 저장된 프로그램을 실행하기 위한 마이크로프로세스 또는 호스트 PC가 중계를 하여 진행된다고 간주하면 된다.

[0031] 본 명세서에서는 더 이상의 마이크로프로세스 또는 호스트 PC에 대한 언급이나 설명을 기술하지 아니한다.

[0032] 마이크로프로세스 또는 호스트 PC는 카드리드기가 설치된 단말기 또는 거치대에 위치하거나 별도의 위치에 설치할 수 있다.

[0033] 본 발명에 따른 스마트카드는 카메라와 카드리드기가 고정 설치된 사용자 단말기 또는 거치대와, 단말기 또는 거치대와 인증서버를 연결하는 네트워크 및 단말기 또는 거치대로부터 전송되어온 홍채이미지 정보를 이용하여 인증을 수행하는 서버로 구성되어 있다.

[0034] 홍채이미지 탬플릿은 홍채 이미지 간에 동일 여부를 판단하기 위하여 홍채이미지 매칭을 수행할 때 사용되는 메모리에 저장되는 홍채이미지 포맷으로서, 개인의 고유한 생체특성은 담고 있으나, 이를 기억하기 위한 메모리의 크기는 원본 이미지에 비해 상대적으로 작은 홍채이미지 포맷을 말한다.

[0035] 홍채이미지 탬플릿은 인증 시 처리속도를 높이고 저장시 메모리 용량을 줄이기 위하여 홍채이미지를 푸리에 변환 또는 웨이블릿 변환 등으로 가공한 것이다.

[0036] 본 발명에 따라 제작된 스마트카드는 높은 보안성이 필요한 은행, 공항, 회사의 출입구 등 보안이 필요한 다양한 장소에 접근 권한을 얻기 위하여 사용할 수 있다.

[0037] 카메라와 카드리드기가 고정 설치된 단말기 또는 거치대에는 사용자가 스마트카드의 소유자임을 증명하기 위하여 생체정보획득 단말기 또는 거치대에 설치된 카메라로 홍채를 촬영한다. 이때 충분히 좋은 품질의 홍채이미지를 획득하기 위하여 생체정보획득 단말기 또는 거치대에 탑재된 품질측정기에서 촬영된 홍채이미지 품질을 측정할 수 있다.

[0038] 홍채이미지 품질을 측정하는 품질측정기는 촬영 시 홍채이미지의 가림정도 및 선명도 등을 점검하여 촬영된 홍채이미지의 품질을 측정할 수 있도록 소프트웨어로 설계 제작되어 메모리에 탑재되어 있다.

[0039] 품질측정기에 의하여 충분히 좋은 품질의 홍채이미지가 촬영되었다고 판단되면, 이 홍채이미지는 생체정보획득 단말기 또는 거치대에 탑재된 전처리기를 통하여 홍채이미지 탬플릿을 생성하기 위한 전처리과정을 거친다.

[0040] 전처리기는 인증의 정확성을 떨어뜨리지 아니하는 범위 내에서 데이터의 신속한 처리를 위하여 논리를 설정하고, 설정된 논리를 적용한 후 홍채이미지 탬플릿을 스마트카드로 전송하는 것이며, 보다 구체적으로 비교영역을 한정하는 등의 조건을 소프트웨어적으로 설계 제작하여 탑재할 수 있다.

[0041] 상기 품질측정기와 전처리기는 선택적으로 채용 적용할 수 있다.

[0042] 단말기 또는 거치대의 홍채이미지 탬플릿 생성기는 촬영한 홍채이미지에 대한 홍채이미지 탬플릿을 생성한다. 생성된 홍채이미지 탬플릿은 단말기 또는 거치대에 장착된 스마트카드 인터페이스를 통하여 스마트카드로 전송되도록 구성되어 있다.

[0043] 스마트카드에는 사용자가 최초로 등록한 홍채이미지 탬플릿이 저장되어 있다. 스미트카드에 저장된 홍채이미지 탬플릿은 스마트카드 외부에서 읽어내는 것이 가능하지 않도록 하드웨어 및/또는 소프트웨어적으로 구성하는 것이 바람직하다.

[0044] 개인의 홍채이미지 탬플릿은 그 개인에 대한 고유한 정보이므로 이것이 외부로 유출이 되지 않도록 하여야 한다.

[0045] 스마트카드에 최초로 등록한 홍채이미지 탬플릿은 사용자가 스마트카드의 실소유자임을 판단할 때 사용되며, 인증서버에도 이와 동일한 홍채이미지 템플릿이 등록 저장되어 있다.

[0046] 스마트카드의 매칭기(matcher)는 전달된 홍채이미지 탬플릿이 스마트카드에 등록 저장된 홍채이미지 탬플릿과 동일 또는 유사한지를 비교 판단한다. 이를 위하여 매칭기는 두 홍채이미지 탬플릿 사이의 유사도를 측정한다.

[0047] 홍채이미지 탬플릿간의 유사도를 측정하는 알고리즘은 스마트카드 내부의 메모리에 저장된 매칭기에 구현되어 있다.

[0048] 상기 유사도 판단 알고리즘은 스마트카드의 외부의 단말기 또는 거치대 등의 다른 장치에 구현되어 연동하도록 구성할 수도 있으나, 그런 경우에는 스마트카드의 메모리에 등록 저장된 홍채이미지 탬플릿이 그 장치로 전달되어야 하므로 이런 과정에서 등록된 홍채이미지 탬플릿이 외부로 유출될 수가 있다. 이를 방지하기 위하여 상기와 같은 홍채이미지 탬플릿간의 유사도를 측정하는 알고리즘은 스마트카드 내부에 구현되어 있도록 하는 것이 바람직하다.

[0049] 한편, 홍채이미지 탬플릿간의 유사도를 측정하는 알고리즘은 기존에 널리 알려진 어떤 것을 사용하여도 무방하다.

[0050] 하나의 예로, 홍채이미지의 유사도는 홍채이미지(홍채 텍스쳐)의 전체 또는 일부 영역에 대하여 푸리에 변환 또는 웨이블릿 변환 등을 수행하여 얻은 계수 열(coefficient sequence) 간의 유클리드 거리로 정의할 수 있다.

[0051] 단말기 또는 거치대에 고정 설치된 카메라에서 획득한 홍채이미지 탬플릿와 스마트카드에 저장된 홍채이미지 탬플릿간의 유사도가 메모리에 설정 저장된 기준 값 이상이면 사용자가 스마트카드의 실소유자라고 판단하고, 유사도가 미리 정한 기준 값 미만이면 사용자는 스마트카드의 실소유자가 아니라고 판단한다.

[0052] 사용자가 스마트카드의 실소유자로 판단되면 스마트카드는 활성화된다.

[0053] 스마트카드에 등록 저장된 홍채이미지 탬플릿은 사용자가 스마트카드의 실사용자임을 판단할 때만 사용하도록 구성하는 것이 바람직하다.

[0054] 추가적으로, 사용자가 실소유자임을 확인할 수 있도록 사용자의 개인식별번호(PIN, personal identification number)를 스마트카드 메모리에 저장하고, 사용자가 입력패드를 통하여 입력하는 개인식별번호와 메모리에 저장된 개인식별번호를 비교하는 수단을 구비하여 입력된 PIN과 스마트카드에 저장되어 있는 PIN과의 비교가 스마트카드 내부에서 이루어지도록 구성할 수 있다.

[0055] 이 경우 개인식별번호와 홍채이미지 탬플릿 두 개 모두 스마트카드의 소유자임을 증명하는데 사용된다. 사용자가 잘못된 PIN을 입력할 수 있는데, 만약 연속으로 미리 정한 최대 허용 입력 횟수(보통 3)보다 더 많이 잘못된

PIN을 입력할 경우 스마트카드를 잠근다.

[0056] 처음에는 잘못된 PIN을 입력하더라도 최대 허용 입력 횟수 이내에서 맞는 PIN을 입력하는 경우, 제대로 PIN을 입력한 것으로 간주한다.

[0057] 스마트카드에는 마이크로프로세서와 전원공급이 필요한 소자에 전원을 공급받기 위한 전원공급단자를 구비하고 있으며, 카드리드기는 전원공급단자를 통해서 스마트카드에 전원을 공급하도록 구성되어 있다.

[0058] 스마트카드의 메모리에 등록 저장된 홍채이미지 탬플릿은 스마트카드의 특성상 자체 전원을 구비하고 있지 아니하여 카드리드기를 통해서 읽혀지도록 구성된 스마트카드의 하드웨어적 구성에 의하여 외부인이 쉽게 읽어낼 수 없으나, 홍채정보획득 단말기 또는 거치대에 설치된 카메라에 의하여 촬영되어 이로부터 생성된 홍채이미지 탬플릿은 스마트카드로 보내지는 과정에서 정보 유출이 일어날 수 있다.

[0059] 홍채정보획득을 위하여 카메라가 설치된 단말기 또는 거치대에서 사용자 인증을 위해 촬영된 사용자의 홍채이미지 탬플릿은 스마트카드와 인증을 위한 인증서버로 각각 전송되어진다.

[0060] 본 발명은 해커에 의한 해킹 시 보안성을 높이기 위하여 홍채이미지 탬플릿을 해쉬함수의 변수로 사용하여 일회용 비밀정보를 생성하는 프로그램을 탑재하고, 단말기 또는 거치대에 설치된 카메라로 촬영 획득한 홍채이미지 탬플릿을 해쉬함수의 변수로 사용하여 일회용 비밀정보를 생성한다.

[0061] 보다 구체적으로, 본 발명에 따른 스마트카드에 탑재되는 일회용 비밀번호의 생성에 대하여 살펴본다.

[0062] 기본적으로, 단말기 또는 거치대에 설치된 카메라로 촬영 획득한 홍채이미지 탬플릿이 카드리드기를 통해서 스마트카드와 인증서버로 전송되고, 스마트카드로 전송된 홍채이미지 템플릿을 스마트카드의 일회용 비밀번호를 생성하기 위한 시드(seed)로 사용한다.

[0063] 상기 시드와 해쉬함수를 사용하여 일련의 해쉬데이터 사슬을 만든다. 즉, 시드로 사용되는 홍채이미지 데이터 또는 그의 파생물을 M, 해쉬함수를 h 라 하면 아래의 함수(1)과 같이 n개의 해쉬데이터 사슬(chain)을 생성할 수 있다.

[0064] 본 발명에 따른 스마트카드에 탑재될 해쉬데이터 사슬(chain)에서, 해쉬함수 h의 변수를 개인의 고유한 특징을 가진 홍채이미지 데이터 또는 그의 파생물인 M으로 해쉬데이터사슬을 구성함으로써 생성된 일회용 비밀번호의 보안의 안전성 및 신뢰도를 크게 향상시킬 수 있다.

[0065] $$h(M) \rightarrow h(h(M)) \rightarrow h(h(h(M))) \rightarrow \cdots \rightarrow h(h(\cdots h(M)\cdots) \quad (1)$$

[0066] 여기서, 각 해쉬데이터는 바로 왼쪽의 해쉬데이터에 해쉬함수를 적용하여 만든 데이터이다. 해쉬데이터 앞에서부터 차례대로 H_1, H_2, …, H_n 이라고 한다. 스마트카드 사용자가 스마트카드를 사용할 때마다 사용자 스마트카드에는 일회용 비밀번호 생성프로그램에 의하여 해쉬데이터 사슬이 생성되도록 구성되어 있다.

[0067] 사용자 홍채이미지 데이터는 단말기 또는 거치대에 설치된 카메라로부터 획득한 사용자 고유정보가 담긴 홍채이미지 템플릿으로 얻은 데이터이다.

[0068] 해쉬함수는 MD5, SHA1, SHA2 등과 같이 일반적으로 알려진 어떠한 것을 사용하여도 무방하다. 여기서 해쉬함수가 가져야 할 분명한 성질은 원본 데이터에서 해쉬데이터를 생성하는 것은 쉬우나, 반대로 해쉬데이터에서 원본 데이터를 추측하는 것이 계산적으로 거의 불가능(computationally infeasible)해야 한다는 것이다.

[0069] 도 3는 본 발명에 따른 홍채이미지를 변수로 하는 해쉬함수의 생성 흐름을 도시한 것이다.

[0070] 도 3에 도시된 해쉬데이터사슬에서 H_2에서 H_1을 역으로 추측하는 것은 거의 불가능하며, H_3에서 H_2와 H_1을 역으로 추측하는 것도 거의 불가능하다.

[0071] 또한, 홍채와 같은 생체 이미지정보를 사용하여 인증을 받기 위하여 일회용 비밀번호를 형성함에 있어서 인증시 처리속도 향상을 위하여 시드의 선택이 중요하다.

[0072] 홍채이미지 탬플릿은 사용자 각각의 특징적인 정보가 담긴 홍채이미지 탬플릿이면 족하다.

[0073] 본 발명에서 보안성을 높이기 위하여 사용되는 해쉬함수의 해쉬데이터사슬에서 n번째 해쉬데이터(해쉬 사슬의

말단 해쉬데이터)인 H_n은 인증서버의 메모리에 저장하고, 나머지 n-1개의 해쉬데이터를 생성 저장하고 있는 스마트카드에 일회용 비밀번호를 생성하여 인증서버로 전송하여 자원 접근 권한 획득을 위한 인증 절차를 거친다. 인증이 완료되면 사용자는 자원 접근 권한을 얻게 된다.

[0074] 상기 인증서버에서 인증을 위하여 사용하는 홍채이미지 탬플릿은 단말기 또는 거치대에 설치된 카메라에서 촬영 획득하여 전송된 것을 사용한다.

[0075] 인증서버의 메모리에 최초로 등록 저장된 홍채이미지 탬플릿은 보다 높은 보안성을 위하여 한 번 더 인증절차를 거칠 때 사용할 수 있다.

[0076] 상기 스마트카드에는 스마트카드에서 생성한 일회용 비밀번호를 인증을 위하여 인증서버로 전송할 때 보안성을 높이기 위하여 암호화하기 위한 암호화기와 복호화기를 탑재하는 것이 바람직하다.

[0077] 암호화기와 복호화기는 소프트웨어로 이루어지며, 통상의 암호화 또는 복호화 알고리즘을 이용하여 설계 제작된 암호화 또는 복호화프로그램을 탑재하여도 무방하다.

[0078] 보안성을 높이기 위하여 생체정보획득을 위하여 카메라가 설치된 단말기 또는 거치대는 스마트카드로부터 트랜잭션 번호를 얻은 다음 생성된 홍채이미지 탬플릿에 스마트카드로부터 얻은 트랜잭션 번호를 삽입한 후 적당한 스크램블링(scrambling) 및/또는 서명 등을 적용하여 스마트카드에 전달할 수 있다.

[0079] 상기 스마트카드는 스마트카드 메모리에 홍채이미지 탬플릿에 부여되는 트랜잭션 번호, 스크램블링 및 서명을 저장해 두고, 카드리드기에 스마트카드를 삽입할 때 카메라가 설치된 단말기 또는 거치대로부터 홍채이미지 탬플릿에 트랜잭션 번호, 스크램블링 및 서명 중에서 적어도 하나 이상을 부여하여 전송할 경우에 상기 스마트카드 메모리에 저장된 것과 비교 확인하여 실제로 홍채정보획득을 위하여 카메라가 설치된 단말기 또는 거치대로부터 전송되어온 홍채이미지 탬플릿인지를 판별하도록 구성할 수 있다. 여기에서 사용되는 스크램블링 및/또는 서명 기법은 기존의 알려진 어떠한 방법을 선택 사용하여도 무방하다.

[0080] 동기화에 대하여 살펴본다. 동기화란 스마트카드와 인증서버 사이의 해쉬데이터 사슬의 동기화를 의미한다. 스마트카드나 인증서버 간에 여러 번의 트랙잭션이 일어난 후에 어느 일측의 판단에 의하여 스마트카드에서 홍채이미지 템플릿을 변수로 사용하여 생성한 일회용 비밀번호에 사용된 홍채이미지 탬플릿을 갱신 또는 교체할 필요가 생긴다.

[0081] 인증을 위해 일회용 비밀번호가 사용되므로, 스마트카드와 인증서버는 동일한 데이터를 기반으로 하여 동시에 일회용 비밀번호에 사용된 홍채이미지 탬플릿을 갱신 또는 교체해야 한다. 해쉬데이터 사슬의 갱신은 해쉬데이터 사슬에서 해쉬함수의 변수로 사용되고 있는 홍채이미지 데이터를 갱신하는 것을 의미한다.

[0082] 동기화를 하기 위해서는 스마트카드와 인증서버 중 어느 일측이 해쉬데이터 사슬 갱신을 위한 신호를 다른 일측에 보내야 하고, 신호를 받은 일측에서는 이를 승인하는 신호를 보낸 측으로 전송하여야 한다. 그러나 서로 신호를 주고 받는 과정에서 네트워크가 갑자기 끊어지거나 신호 전송을 담당하는 부분의 고장 등의 이유로 인하여 승인하는 신호를 보내는 측에서는 승인을 했다고 생각하고 해쉬 사슬 갱신을 완료를 했으나, 승인 신호를 받지 못한 측에서는 여전히 해쉬데이터 사슬 갱신을 하지 않은 상태에 있을 수가 있다. 이러한 경우에는 인증이 불가능해질 수 있다.

[0083] 상기와 같이 네트워크가 끊어지거나 기타 원인에 의하여 해쉬데이터 사슬 갱신 여부를 확인하여야할 상황이 발생한 경우에 이를 해결하기 위하여 지속적으로 갱신완료 여부를 해쉬데이터 사슬을 체크하고, 이루어지지 않았을 경우에 재시도를 하여 데이터 사슬 갱신이 이루어지도록 구성되어 있다.

[0084] 또한, 해쉬데이터 사슬 갱신에 대해 양측이 동의를 하더라도 성공적인 동기화를 위해서는 양측이 해쉬데이터 사슬을 생성하기 위한 공통된 시드 데이터를 양측이 각각 보유하고 있어야 한다.

[0085] 생체정보획득을 위한 카메라가 고정 설치된 단말기 또는 거치대에서 인증을 위해 촬영된 사용자의 홍채이미지 탬플릿은 스마트카드와 인증서버로 각각 보내진다. 바로 이 홍채이미지 탬플릿이 스마트카드와 인증서버 양측이 공유하게 되는 데이터이다. 이 홍채이미지 탬플릿은 기존의 해쉬데이터 사슬을 만들 때 사용했던 홍채이미지 탬플릿(J0)과 다른 새로운 것이다. 물론 사용자의 고유한 홍채 특징을 포함하고 있다는 점에서는 두 홍채이미지 탬플릿은 유사하지만 바이트대 바이트(byte to byte) 비교를 하면 서로 다르다.

[0086] 인증서버에서 인증을 완료하면 홍채이미지 탬플릿이 해커에 의해 유출되지 않도록 폐기되거나 원래 홍채이미지 탬플릿을 추론할 수 없도록 다른 형태로 변형되어야 한다.

[0087] 홍채이미지 탬플릿은 새로운 해쉬데이터 사슬을 생성하는데 사용될 수 있도록 대기하고 있어야 하므로, 인증 후 곧바로 폐기되지는 않는다.

[0088] 인증서버에서 인증이 승인된 후, 스마트카드와 인증서버 양쪽이 공유하고 있는 해쉬함수를 양측에서 각각 홍채이미지 탬플릿을 해쉬함수에 적용하여 해쉬데이터 형태로 변형하여 보유하도록 구성하는 것이 바람직하다.

[0089] 인증서버와 스마트카드 각각이 변형 보유한 해쉬데이터를 대기해쉬(hash-in-wait, 스마트카드의 대기해쉬는 H_{w_SC}로 인증서버의 대기해쉬는 H_{w_SV}로 표기)로 부르기로 한다.

[0090] 양측에서 각각 대기해쉬를 생성할 때, 홍채이미지 탬플릿을 해쉬함수에 적용하여 해쉬데이터 형태로 변형하여 보유하도록 구성하는 것이 바람직하기는 하나, 홍채이미지 탬플릿만을 기반으로 구성될 필요는 없다.

[0091] 양측이 공통으로 가지고 있는 어떤 형태의 데이터라도 대기해쉬를 만드는데 쓰일 수 있다. 예를 들면 최근에 OTP를 생성하는데 이용된 해쉬 사슬은 양측이 공통으로 가지고 있는 데이터라고 볼 수 있다. 스마트카드와 인증서버 간에 인증을 위해 여러 번의 해쉬데이터 사슬이 생성되었었다면 각 해쉬데이터 사슬의 말단 해쉬데이터(H_n)는 스마트카드와 인증서버 양측이 공통으로 가지고 있는 데이터이다.

[0092] 이 경우 스마트카드와 인증서버에서는 최근에 생성된 말단 해쉬데이터들을 저장해두어야 한다. 이 말단 해쉬데이터들을 결합하여 하나의 데이터로 만든 후에 이를 기반으로 대기해쉬를 생성하여도 된다.

[0093] 이와 같이 보안성을 높이기 위한 상기 해쉬데이터 사슬의 갱신은 스마트카드와 인증서버 양측이 각각 가지고 있는 대기해쉬를 기반으로 만들어지게 된다. 이 대기해쉬는 반드시 스마트카드와 인증서버 양측 모두 동일한 홍채이미지 탬플릿을 기반으로 이루어져야 한다.

[0094] 스마트카드와 인증서버에서 동일한 홍채이미지 탬플릿을 기반으로 대기해쉬를 가지고 있더라도, 양측이 완전히 동일한 대기해쉬를 가지고 있을 필요는 없다. 예를 들면 스마트카드에서는 홍채이미지 탬플릿에 한번의 해쉬 함수를 적용하여 나온 해쉬데이터를 가지고 있고, 인증서버에서는 동일한 해쉬 함수를 미리 정한 수만큼 반복적으로 적용하여 나온 해쉬데이터를 가지고 있도록 구성할 수 있다.

[0095] 본 발명에서 제시하는 재동기화(resynchronization)는 인증이 성공된 후에 곧바로 동기화(즉 해쉬데이터 사슬을 갱신)하는 것이 아니라, 그 다음 트랜잭션에 동기화를 수행하는 지연된 동기화(delayed synchronization)에 관한 것이다.

[0096] 사용자가 인증서버로부터 최종적으로 인증 승인이 이루어져 자원 접근에 대한 권한을 얻게 되었다하더라도, 스마트카드에서는 직전의 사용자에 대한 인증이 인증서버에 의해 최종적으로 완료되었음에 대한 기록이 없을 수 있다.

[0097] 즉, 스마트카드는 직전의 최종 인증 결과는 모르고 최근에 인증을 위해 촬영된 홍채 데이터에 대한 해쉬 데이터가 스마트카드에 존재할 수 있다.

[0098] 이러한 문제를 해결하기 위하여, 인증서버에서는 최근까지 스마트카드측과의 트랜잭션에 대한 정보를 데이터베이스(이하 '트랜잭션 데이터베이스'라 한다)에 저장한다.

[0099] 트랜잭션 데이터베이스에는 스마트카드와의 트랜잭션에 대한 트랜잭션 번호, 트랜잭션 시간, 인증 성공 여부, 연속된 인증 실패 횟수 등이 기록되어 있다.

[0100] 한편, 스마트카드는 인증서버의 대기해쉬 요청 유무와 무관하게, 가장 최근에 촬영되어 생성된 홍채 탬플릿으로부터 대기해쉬(H_{w_SC})를 만들어 스마트카드 내에 저장해둔다.

[0101] 재동기화의 절차는 다음과 같다.

[0102] 스마트카드에는 인증서버와 재동기화를 수행하기 위하여 가장 최근의 홍채이미지 탬플릿을 바탕으로 대기해쉬(H_{w_SC})를 갱신했음을 알리는 신호를 인증서버에 전송하는 수단을 구비하고, 이를 인증서버로 전송한다.

[0103] 인증서버에서는 트랜잭션 데이터베이스를 검색하여 바로 직전의 트랜잭션에서 인증에 성공했는지를 알아본다.

[0104] 만약, 바로 직전의 트랜잭션에서 인증에 성공했었다면, 인증서버는 이전 트랜잭션에서 스마트카드로부터 받은 홍채이미지 탬플릿에서 대기해쉬(H_{w_SV})를 생성한다. 그리고 스마트카드로 신호를 보내는데 이 신호에는 해쉬데이터 사슬을 생성하라는 내용이 포함된다.

[0105] 스마트카드는 이 신호를 받고 대기해쉬(H_{w_SC})로부터 해쉬데이터 사슬을 생성하고, 향후 해쉬데이터 사슬의 각 해쉬데이터를 OTP로 사용한다.

[0106] 만약, 직전의 트랜잭션에서 인증에 성공하지 못했다면 인증서버는 자신의 대기해쉬를 생성하지 않는다. 그리고 스마트카드로 신호를 보내는데 이 신호에는 스마트카드에서 이미 갱신했던 대기해쉬(H_{w_SC})를 제거하고 이로부터 해쉬데이터 사슬을 생성하지 말라는 내용이 포함된다.

[0107] 앞서 설명한 대기해쉬는 인증서버와 스마트카드에 저장되는 해쉬데이터 갱신을 위한 재동기화를 위하여 필요한 것이다.

[0108] 상기 인증서버는 단말기 또는 거치대에서 전송한 생체이미지 탬플릿, 해쉬함수로 구성된 일회용 비밀번호 및 단말기 또는 거치대 ID를 이용하여 인증을 수행할 수 있다.

[0109] 카메라에 의하여 획득한 홍채이미지 자체는 저장을 위한 메모리 용량의 크기가 클 수 있기 때문에 스마트카드 또는 인증서버가 해쉬데이터 사슬을 만들려면 시간이 많이 걸릴 수 있다.

[0110] 특히, 이를 처리하기 위한 마이크로프로세서의 연산성능이 떨어지는 경우에는 단말기가 홍채 이미지를 변수로 하는 해쉬데이터 사슬을 만드는데 걸리는 시간과 메모리가 많이 소요될 수 있다.

[0111] 이를 해결하기 위하여,

[0112] 첫째, 단말기 또는 거치대에 설치된 카메라로 획득한 홍채이미지의 특징을 포함하고 있는 특정 영역에 속한 픽셀단위의 홍채이미지 데이터만을 잘라낸 데이터를 시드로 사용할 수 있다. 예를 들면 홍채이미지 중에서 사용자의 특징을 포함하고 있는 홍채이미지를 4등분하여 그 중에 하나를 시드로 사용하거나 사용자의 특징을 포함하고 있는 홍채 이미지를 다수의 행이나 열로 구분한 후에 특정 행과 특정 열에 속한 픽셀단위의 이미지 데이터만을 선택하여 시드로 사용할 수 있다.

[0113] 둘째, 홍채이미지 중에서 홍채이미지 탬플릿을 시드로 이용할 수 있다. 홍채 이미지 탬플릿은 홍채 이미지 간에 동일 여부를 판단하기 위하여 이미지 매칭을 수행할 때 사용되는 메모리에 저장되는 홍채이미지 포맷으로서, 개인의 고유한 생체 특성은 담고 있으나, 이를 기억하기 위한 메모리의 크기는 원본 이미지에 비해 상대적으로 작은 홍채이미지 포맷이다.

[0114] 예를 들어, 홍채이미지가 차지하는 메모리가 약 100KByte라면, 이에 해당하는 홍채이미지 탬플릿은 약 10KByte 정도의 메모리 크기로 원본 이미지 데이터의 약 1/10 정도이다.

[0115] 이는 홍채이미지 탬플릿은 원본 이미지 데이터 보다 상당히 줄어든다는 의미이다.

[0116] 본 발명에 따른 인증은 크게 두 개의 단계로 이루어져 있다. 일차적으로 사용자가 실제 스마트카드 소유자임을 판별하기 위하여 스마트카드와 카드리드기와 카메라가 설치된 단말기 또는 거치대에서 이루어지며, 최종 인증은 인증서버에 의해 이루어지도록 구성되어 있다.

[0117] 본 발명에 따른 스마트카드에는 등록 저장 시에 메모리에 저장되어 있던 해당 사용자의 홍채이미지 탬플릿을 변수로 하는 n-1개의 해쉬데이터 H_1, H_2, … H_n-1 중에서 무작위로 또는 스마트카드에 탑재된 프로그램의 실행에 의하여 미리 정해진 순서에 의하여 어느 하나의 해쉬데이터를 선택하도록 구성되어 있다.

[0118] 선택된 해쉬데이터는 일회 사용되는 사용자의 일회용 비밀번호가 된다. 만약 i번째 해쉬데이터 H_i 가 일회용 비밀번호로 서버로 전송되면, H_i 뒤의 해쉬데이터 즉 H_j(j >i)는 더 이상 사용되지 않는다. 왜냐하면 제 삼자가 H_i 를 가로챘다면, H_i로부터 H_j를 알아낼 수 있기 때문이다.

[0119] 따라서, H_i를 비밀번호로 사용하였다면, 다음에는 H_i 앞의 해쉬데이터 H_k (k < i)가 비밀번호로 사용될 수 있다. 이것은 S/Key 방식으로 본 발명에서는 인증시 보안의 안전성과 신뢰성을 높이기 위하여 홍채이미지 탬플릿을 해쉬 이미지 함수의 변수로 사용하여 구성한 것이다.

[0120] 인증서버로부터 사용승인을 받기 위하여, 홍채이미지 탬플릿과 해쉬함수에 의하여 생성된 해쉬데이터(H_i) 및 단말기 또는 거치대 ID 세가지 중에서 해쉬데이터를 포함하는 적어도 하나 이상으로 혼합 구성하여 일회용 비밀번호를 생성하여 스마트카드에서 단말기 또는 거치대를 거쳐서 인증서버로 전송하도록 구성되어 있다.

[0121] 상기 일회용 비밀번호를 생성 시에는 사용자의 개인식별번호(PIN)을 포함시켜 생성할 수도 있다.

[0122] 인증서버는 스마트카드에서 단말기 또는 거치대를 통해서 보낸 암호화된 일회용 비밀번호와 암호화된 대칭키를

복호기를 이용하여 암호를 해독을 한다.

[0123] 상기 인증서버는 해독된 해쉬데이터 H_i가 사용자의 일회용 비밀번호가 맞는지를 판별하기 위하여 H_i에 서버에 저장되어 있던 해쉬함수 h를 적용하도록 구성되어 있다.

[0124] 적어도 한번 이상 적용시켜 인증서버에 저장되어 있던 H_n과 동일한 해쉬데이터를 얻으면 H_i를 사용자 일회용 비밀번호가 맞다고 판단하여 접근을 승인한다.

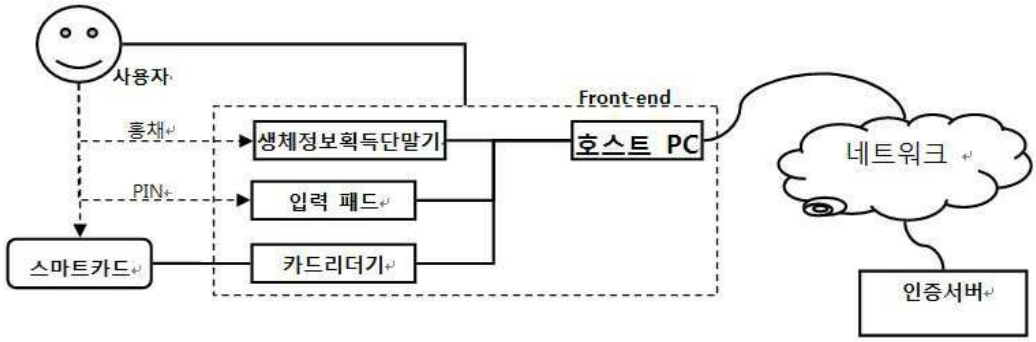
[0125] 그러나 홍채를 포함하는 생체이미지를 변수로 하는 해쉬함수를 정해진 횟수 범위내에서 적용을 시켜도 인증서버에 저장되어 있던 H_n과 일치하는 것이 나오지 않으면, H_i가 현시점에서의 사용자 일회용 비밀번호가 아니라고 판단하여 자원 접근을 거부하도록 구성되어 있다.

산업상 이용가능성

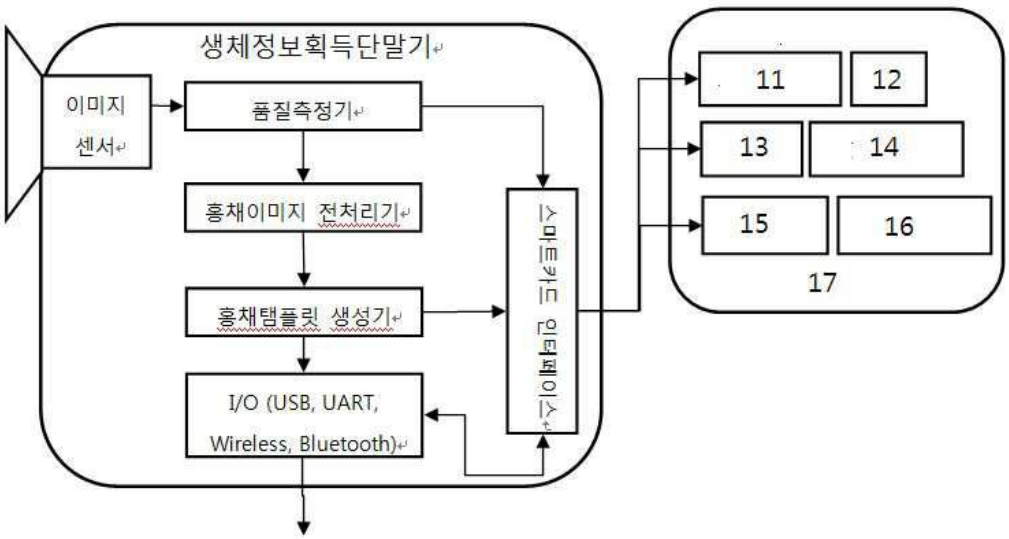
[0126] 본 발명은 사용자가 최초로 등록한 홍채이미지 탬플릿이 메모리에 저장되어 있고, 스마트카드 메모리에 홍채이미지 탬플릿간의 유사도를 측정하는 알고리즘이 탑재되며, 스마트카드 메모리에 저장된 홍채이미지 탬플릿과 단말기 또는 거치대에 부착 설치된 카메라로부터 획득하여 카드로 전달된 홍채이미지 탬플릿이 서로 동일 또는 유사한지 여부를 판단하기 위한 스마트카드의 매칭기를 구비하며, 매칭기에서 실소유자라고 판단되면 홍채이미지 정보가 포함된 일회용 비밀번호를 생성하여 카드리드기가 설치된 거치대 또는 단말기를 통해서 인증서버로 전송하여 자원접근 권한 획득을 위한 인증절차를 거쳐서, 자원접근 권한을 얻도록 구성된 홍채이미지 정보를 포함하는 일회용 비밀번호가 탑재된 스마트카드를 제공하여 보안성과 신뢰성을 크게 향상시키므로 산업상 이용가능성이 매우 높다.

도면

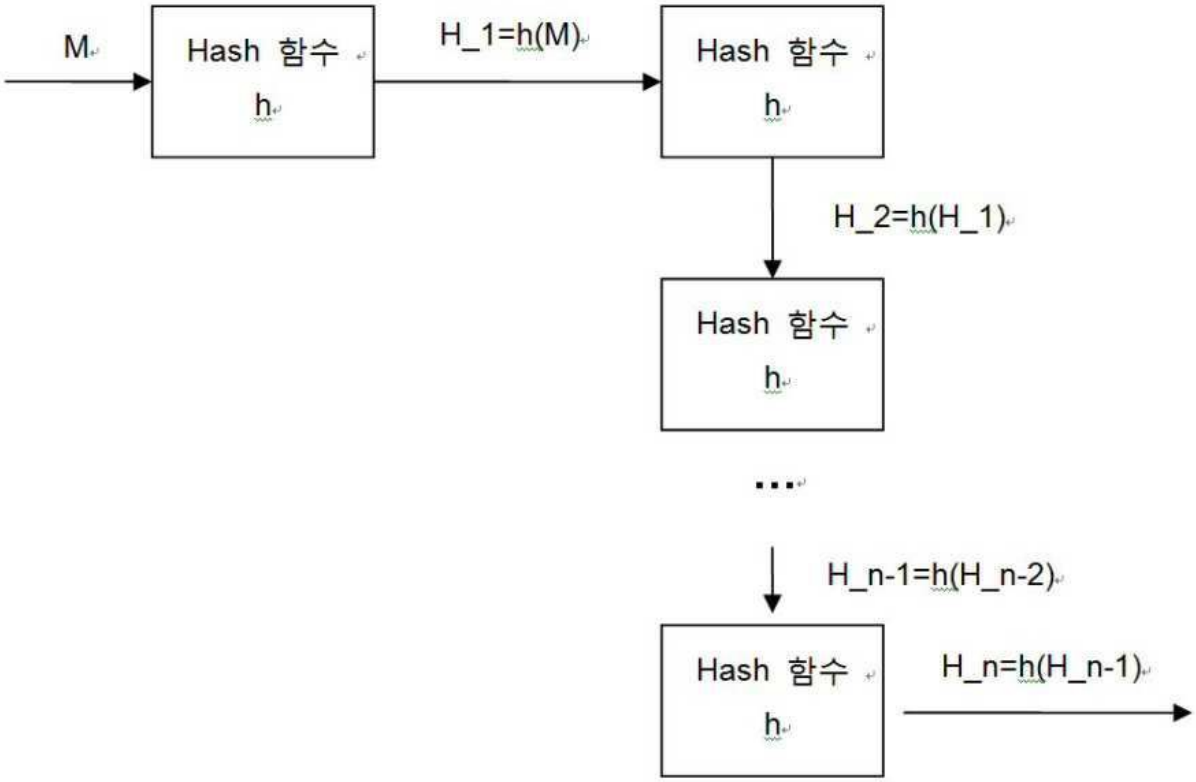
도면1



도면2



도면3


M
Hash 함수
h
H_1=h(M)
Hash 함수
h
H_2=h(H_1)
Hash 함수
h
...
H_n-1=h(H_n-2)
Hash 함수
h
H_n=h(H_n-1)