(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2018년05월02일
(11) 등록번호 10-1853266
(24) 등록일자 2018년04월24일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01)
(52) CPC특허분류
H04L 9/3234 (2013.01)
G06K 9/00013 (2013.01)
(21) 출원번호 10-2015-0022976
(22) 출원일자 2015년02월15일
심사청구일자 2016년08월02일
(65) 공개번호 10-2016-0101248
(43) 공개일자 2016년08월25일
(56) 선행기술조사문헌
KR1020050099106 A*
KR100606393 B1*
KR1020060060236 A*
이남일 외 2명, 지문인식 센서 알고리즘 기술 동향, 정보보호학회지 제12권 제2호 (2002.04.)
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
에코스솔루션(주)
서울특별시 구로구 구로중앙로 207, 12층 1224호 (구로동, 구로동복합건물OPUS1)
(72) 발명자
나경필
서울특별시 구로구 구로중앙로 207 1224호 1, 12층 (구로동,오피스)
길용석
서울특별시 구로구 구로중앙로 207 1224호 1, 12층 (구로동,오피스)
(뒷면에 계속)
(74) 대리인
민혜정

전체 청구항 수 : 총 5 항 심사관 : 양종필

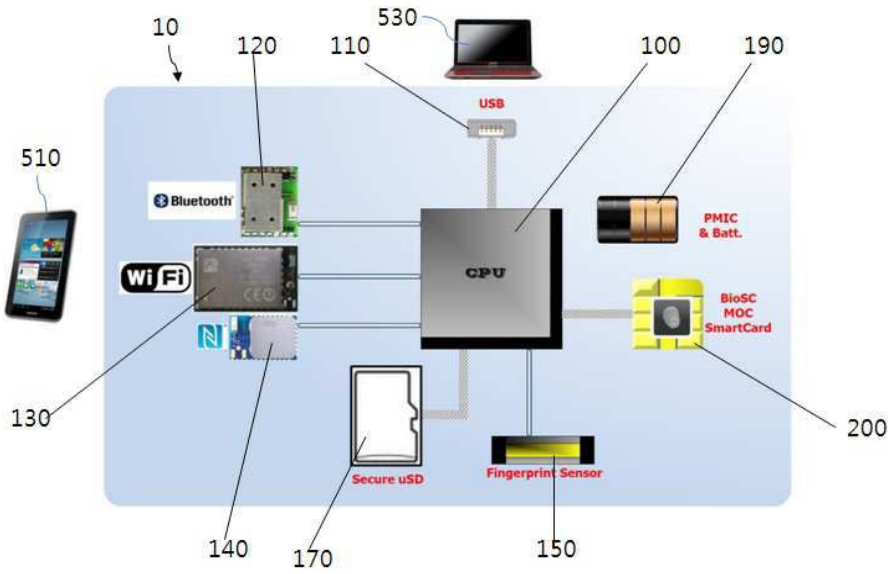
(54) 발명의 명칭 **지문인식방법을 채용한 휴대용 보안인증기**

(57) 요 약

본 발명은 지문인식방법을 채용한 휴대용 보안인증기에 관한 것으로, 보다 상세히는, 지문인식부와 MOC(On-Card Match) 스마트카드를 내장하며, 지문 센서를 통해 지문 이미지를 받아들여, 특징정보를 추출하여, MOC 스마트카드에서, 기 저장된 사용자 정보와 비교하여 사용자 인증을 수행하고, 사용자 인증이 성공하면 메모리에 저장된

(뒷면에 계속)

대 표 도 - 도3



데이터의 접근을 허용하여, 소정의 데이터를 유무선 통신 인터페이스를 통해 모바일 단말기로 전송하여, 인증하여, 모바일 단말기로 필요한 작업을 수행하게 하는, 지문인식방법을 채용한 휴대용 보안인증기에 관한 것이다.

본 발명은, 지문센서를 구비하되, 상기 지문센서가 보안인증장치의 하우징부에 밖으로 노출되도록 장착되어지는, 지문센서부; 암호로된 사용자 지문정보를 저장하고 있으며, 연산처리부로부터 수신된 지문의 특징정보를, 바이오인식 매칭 프로그램(Bio matching algorithm)을 이용하여, 상기 사용자 지문정보와 비교하여 사용자 인증을 수행하는, MOC 스마트카드; 지문센서로부터 수신된 지문영상으로부터 특징점을 추출하여, MOC 스마트카드로 전송하고, MOC 스마트카드에서 사용자 인증결과를 수신하여, 사용자 인증이 성공하였다면, 메모리부에 저장된 데이터에의 접근을 허용하게 하는, 연산처리부;를 포함하여 이루어진 것을 특징으로 한다.

MOC 스마트카드는 OTP 애플렛, PKCS 애플렛, eID 애플렛, HPTP 애플렛, 지불(Payment) 애플렛, 전자화폐(E-Cash) 애플렛을 포함하고 있으며, 지문센서는 스윕(SWIPE) 센서이다.

(52) CPC특허분류
G06K 9/00067 (2013.01)
H04L 9/3231 (2013.01)
H04W 12/06 (2013.01)

(72) 발명자
김문철
서울특별시 구로구 구로중앙로 207 1224호 1, 12층 (구로동,오퍼스)
김명하
서울특별시 구로구 구로중앙로 207 1224호 1, 12층 (구로동,오퍼스)

명 세 서

청구범위

청구항 1

지문센서를 구비하되, 상기 지문센서가 보안인증장치의 하우징부에 밖으로 노출되도록 장착되어지는, 지문센서부;

암호로된 사용자 지문정보를 저장하고 있으며, 연산처리부로부터 수신된 지문의 특징정보를, 바이오인식 매칭 프로그램(Bio matching algorithm)을 이용하여, 상기 사용자 지문정보와 비교하여 사용자 인증을 수행하는, MOC 스마트카드;

지문센서로부터 수신된 지문 이미지로부터 특징점을 추출하여, MOC 스마트카드로 전송하고, MOC 스마트카드에서 사용자 인증결과를 수신하여, 사용자 인증이 성공하였다면, 메모리부에 저장된 데이터에의 접근을 허용하게 하는, 연산처리부;

를 포함하며,

MOC 스마트카드는 OTP 애플렛, PKCS 애플렛, eID 애플렛, HPTP 애플렛, 지불(Payment) 애플렛, 전자화폐(E-Cash) 애플렛을 포함하며,

연산처리부는, 지문 이미지를 세선화하고, 세선화 이미지로부터 융선의 흐름에 변화가 발생하는 단점과 분기점 정보를 추출하여 후보 특징점을 추출하고, 추출된 후보 특징점 중 의사 특징점을 제거하여, 지문의 특징점을 검출하며,

MOC 스마트카드는 추출된 지문의 특징점 정보와, 기저장된 사용자 지문정보을 이용하여 두 지문 이미지 간의 유사도를 결정하되,

MOC 스마트카드는 연산처리부로부터 수신된 지문의 특징정보와 기저장된 사용자 지문정보의 두 지문 이미지의 특징점이 최대로 많이 겹쳐지는 회전, 천이량을 산출하여 이미지의 정렬 기준점을 선정하고, 정렬 기준점에 맞추어지도록 특징점의 좌표를 변환한 후 대응되는 특징점 쌍을 결정하고, 결정된 대응 특징점 쌍의 좌표, 종류, 각도정보를 이용하여 유사도(Measure Vector)를 계산하고, 대응 특징점 쌍의 유사도로부터 두 지문 이미지의 일치하는 정도를 기 설정된 규칙데이터에 따라, 점수로서 연산처리부로 출력하며,

메모리부에는 외부의 모바일 단말기, POS 단말기, 컴퓨터의 단말기 중 어느 하나의 비밀번호가 저장되어 있는 것을 특징으로 하는, 휴대용 보안인증기.

청구항 2

삭제

청구항 3

제1항에 있어서,

지문센서는 스윕(SWIPE) 센서인 것을 특징으로 하는, 휴대용 보안인증기.

청구항 4

제1항에 있어서,

블루투수 통신부, WiFi 통신부, NFC 통신부, USB 커넥터부를 더 포함하여 이루어진 것을 특징으로 하는, 휴대용 보안인증기.

청구항 5

삭제

청구항 6

제1항에 있어서,

연산처리부는 MOC 스마트카드에서 사용자 인증결과를 수신하여, 사용자 인증이 성공하였다면, MOC 스마트카드의 OTP 애플렛, PKCS 애플렛, eID 애플렛, HPTP 애플렛, 지불(Payment) 애플렛, 전자화폐(E-Cash) 애플렛 중 하나를 구동하도록 하는 것을 특징으로 하는, 휴대용 보안인증기.

청구항 7

제1항에 있어서,

지문의 특징점은, 분기점과 단점 중 어느 하나를 나타내는 특징점의 종류, 지문 이미지내에서의 위치, 특징점이 위치한 융선의 방향에 대한 정보를 포함하는 것을 특징으로 하는, 휴대용 보안인증기.

청구항 8

삭제

청구항 9

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 지문인식방법을 채용한 휴대용 보안인증기에 관한 것으로, 보다 상세히는, 지문인식부와 MOC(On-Card Match) 스마트카드를 내장하며, 지문 센서를 통해 지문 이미지를 받아들여, 특징정보를 추출하여, MOC 스마트카드에서, 기 저장된 사용자 정보와 비교하여 사용자 인증을 수행하고, 사용자 인증이 성공하면 메모리에 저장된 데이터의 접근을 허용하여, 소정의 데이터를 유무선 통신 인터페이스를 통해 모바일 단말기로 전송하여, 인증하여, 모바일 단말기로 필요한 작업을 수행하게 하는, 지문인식방법을 채용한 휴대용 보안인증기에 관한 것이다.

배 경 기 술

[0002] 기존의 바이오인식 기술이 적용되는 시장은 출입이나 근태관리 등 물리적인근제어가 가장 큰 비중을 차지하고, 그 외 디바이스나 시스템의 접근제어를 위한 논리적 접근제어나 신분 확인 등의 공공부분에서 주로 사용된다. 그러나 최근에는 모바일 기기에 바이오인식 기술이 적용되어 그 적용영역이 확대되고 있다.

[0003] 지문 바이오인식은 실험실 등의 높은 보안 수준을 요구하는 장소에서 접근제어를 위해 널리 채택되었다. 모바일 기기에 지문 스캐너를 장착함으로써 휴대전화 관련 보안을 위해 활용될 수 있다. 휴대전화의 경우 기본으로 탑재된 입력장치로는 정밀한 지문 이미지를 획득할 수 없어 별도의 지문 이미지 스캐너가 필요하다.

[0004] 최근들어, 컴퓨터, 인터넷, 휴대폰과 같은 정보통신 인프라의 급속한 발달에 따라 개인정보 및 기업정보의 보안에 대한 필요성이 절실히 요구되고 있는 추세이며, 인터넷이나 휴대폰을 통한 인터넷뱅킹, 신용카드 결제, 모바일 결제 등의 신용 거래가 활발하게 이루어짐에 따라 개인에 대한 고유의 인증 수단이 요구되고 있다.

[0005] 따라서, 개인이 휴대하면서 편리하게 사용할 수 있는 지문인식 기반의 보안 인증기기가 요망되며, 특히, 지문정보를 이용하여 보다 안전한 개인 정보 보안 관리를 위해, On-Card Match(MOC)를 활용한 바이오 인증 기반의 휴대용 보안인증 기기가 요망된다.

[0006] 일반적으로, 바이오인식 시스템은 기본적으로는 사용자를 등록하는 과정(registration/enrollment)과 사용자를 확인받는 인증(verification, 1:1), 데이터베이스에서 사용자를 찾아내는 인식(identification, 1:N)으로 구분된다. 인증과 인식은 응용영역에 따라 선택적으로 이용되어지며, 이에 따른 시스템의 구성도 서로 상이하다. 등록과 인증/인식을 수행하는 바이오인식 시스템의 5대 구성요소는 Capture, Storage, Processing, Matching, Decision이다.

[0007] 본 발명의, 지문인식방법을 채용한 휴대용 보안인증기는 지문인식, 스마트카드 및 MoC기반의 기술을 활용한 시

스템이다.

[0008] 종래 기술로서, USB 저장장치에 암호화 기술을 임베디드하여 데이터를 암호화함으로써 저장장치 분실 시 저장되어 있는 정보의 유출을 차단하는 방법은, 보안 USB 사용시 로그온 패스워드 입력 방식을 적용하는데 이때 사용하는 패스워드를 고의적으로 유출시키거나 해킹에 의한 패스워드 누출발생 시 USB 저장장치에 저장되어 있는 정보가 유출될 수 있는 상황이 발생하게 되는 데, 이에 따라서, 패스워드 방식이 아닌 사용자를 고유하게 인식할 수 있는 바이오인증방식이 필요하다.

[0009] 일반적으로, Bio 보안토큰 및 보안 USB메모리를 위해서는, 암·복호화 기술, 사용자 인증 및 식별 기능, 저장된 데이터의 임의복제 방지 기능, 분실 도난 시 데이터 보호를 위한 삭제 기능 등이 필요하다.

[0010] USB 메모리로 데이터 전송시 데이터를 암호화하고, USB 메모리의 데이터 확인시 자동으로 복호화 해 주는 기술로서, 암·복호화 기술은 하드웨어 방식과 소프트웨어 방식으로 구분이 되며 전용 보안 칩 형태로 제공하는 형태의 제품들이 제공되고 있다.

[0011] 사용자 인증 및 식별 기능에 있어서, 사용자의 메모리 영역에 비밀번호 설정 기능 혹은 지문인식 기능을 탑재하는 보안 기능으로써, 타 기능과 연동하여 사용한다.

[0012] 저장된 데이터의 임의복제 방지 기능에 있어서, 사용자 인증 없이 저장 메모리 내 데이터의 접근 자체를 불가능하게 하여 외부로 데이터 복제를 불가능하게 하는 기능이다.

[0013] 분실 도난 시 데이터 보호를 위한 삭제 기능에 있어서, 스마트폰, 보안인증기기를 분실하였을 경우, 다른 사용자가 개인정보 영역의데이터를 접근할 수 없도록 메모리 데이터를 삭제하는 기능과 단말기 도난 시원격에서 추적하여 데이터를 삭제하는 등의 기능을 제공한다.

[0014] 지문 인증을 이용하여 사용자 인증을 하는 바이오 인증 USB 메모리의 기술에 관련하여, 기존의 방식에서는 지문센서에서 읽어들인 데이터의 특징점추출/매칭 작업시에 방대한 계산양 때문에 주로 PC S/W상에서 추출/매칭작업을 해주는 기술이 필요하다. 지문 센서에서 체취한 개인 지문 정보를 USB를 통해 PC에 전송해야 되는 데, 이때 개인의 생체 및 보안정보의 노출 등의 프라이버시 문제가 발생할 소지가있어 지문의 추출/매칭이 USB 메모리 장치 내에서 모두 이루어지는 구조로 이루어진 것이 필요하다.

[0015] 최근의 인증 처리방식은 스마트카드 내에서 지문캡처/특징점 추출/매칭의 전체 과정을 수행하는 형태(SOC, System On Card)와 인증처리 방식의 일부 과정을 단말기에서 처리하는 형태(MOC, MatchingOn Card)로 발전하였다.

[0016] SOC 스마트카드는 지문 센서 및 지문처리 알고리즘을 스마트카드내에서 처리하여야 하므로 고성능의 CPU와 대용량의 메모리를 사용하여야 하는 단점이 있다. 반면, MOC 스마트카드는 매칭 알고리즘만 처리하므로 상용 스마트카드로 처리할 수 있는 장점이 있다. 카드의 매칭에 사용되는 코드는 10kbytes이내 RAM 메모리의 크기는 5kbytes 크기 이내 정도로 구현되며, 처리속도는 5초 이내로 수행한다.

[0017] 최근 스마트폰을 이용한 모바일 금융 서비스 시장이 증대되고 있다. 공간과 시간의 제약을 크게 줄일 수 있게 되었으며 하나의 스마트폰을 통해 신용카드, 계좌 정보 등의 금융 정보뿐만 아니라 쿠폰, 포인트 등의 관련 서비스 정보까지 통합 관리할 수 있게 되었다. 그러나 모바일 기기에 개인 정보가 집중되고 개방적인 무선망을 사용함에 따라 분실이나 도난, 도청 및 감청에 의한 정보 유출과 위조 및 변조에 대한 위험성 또한 증대되었다. 이에 따라 기존의 인증수단에 비해 높은 안정성을 가지며 이용편의성을 충족시킬 수 있는 새로운 인증기술이 요구되고 있다.

[0018] 바이오인식은 해당 정보의 성격이 개인과 떨어질 수 없다는 특징으로 인해 높은 보안성과 이용편의성을 충족시킬 수 있으나, 아직까지 센서, 하드웨어 성능을 뒷받침할 수 있는 범용의 모바일 단말기가 존재하지 않고, 스마트폰도 인증에 사용될 수 있는 정확한 인식률을 충족시키지는 못하고 있다.

[0019] 선행기술로, 국내 공개특허공보 제2001-0095788호의 휴대용 보안 인증 장치 및 시스템 그리고 그의 동작 방법이 있다.

[0020] 국내 공개특허공보 제2001-0095788호는 사용자 고유로 갖는 생체적 특징의 패턴(지문 및 음성 등)을 인식하여 허여된 사용자 여부를 결정하고, 상기 결정 결과에 따라 사용자의 패스워드 안내 및 패스워드 입력 동작, 그리고 사용 및 접근하고자 하는 시스템의 개방과 상기 시스템 개방을 원격 상태에서 이룰 수 있도록 한다.

[0021] 그러나, 이 발명의 경우, 사용자 정보 DB, 사용자 지문 DB 등을 이용하여 인식하는 것으로, 컴팩트하지

못하며, 연산처리 등에 시간이 너무 많이 소요되며, 정보가 노출될 위험이 있고, 악의적인 사용자로부터 해킹을 당할 여지가 있는 등, 보안의 쉽지 않다는 단점이 있다.

발명의 내용

해결하려는 과제

[0022] 본 발명이 해결하고자 하는 과제는, 지문인식부와 MOC(On-Card Match) 스마트카드를 내장하며, 지문 센서를 통해 지문 이미지를 받아들여, 지문 이미지를 가공처리하여 추출한 특징정보를 MOC 스마트카드로 전송하여, 상기 카드내에 설치된 바이오인식 매칭 프로그램을 통해서, 카드 내에 암호로 저장된 사용자 정보와 비교하여 사용자 인증을 수행하고, 사용자 인증이 성공하면 메모리에 저장된 데이터의 접근을 허용하며, 소정의 데이터를 유무선 통신 인터페이스를 통해 모바일 단말기로 전송하여, 인증하여 모바일 단말기로 필요한 작업을 수행하게 하는, 지문인식방법을 채용한 휴대용 보안인증기를 제공하는 것이다.

[0023] 본 발명이 해결하고자 하는 다른 과제는, 지문 이미지의 특징정보를 추출하여, MOC 스마트카드에서, 기 저장된 사용자 정보와 비교하는, 사용자 인증을 통해, MOC 스마트카드에 설치되어 있는 다양한 서비스, 예로 OTP(One Time Password, 일회용비밀번호), PKCS(공개키 암호작성 시스템, Public-Key Cryptography System), eID, 지불 등에 대한 접근을 허용하게 하는, 지문인식방법을 채용한 휴대용 보안인증기를 제공하는 것이다.

[0024] 본 발명이 해결하고자 하는 다른 과제는, 바이오 등록/인증 매니저 프로그램을 통하여 사용자의 지문정보를 스마트카드의 보안 메모리 영역에 저장 관리하고, 입력된 지문정보에 대해 스마트카드의 On-Card Match 지문인식 알고리즘을 수행하여 사용자를 인증하며, 인증된 사용자에 대해 스마트폰/태블릿과 연결한 유/무선 인터페이스를 통해 개인정보 및 저장데이터를 사용할 수 있도록 접근권한을 부여하는, 지문인식방법을 채용한 휴대용 보안인증기를 제공하는 것이다.

[0025] 본 발명이 해결하고자 하는 다른 과제는, 스마트카드에 저장된 생체정보를 외부로부터 입력된 생체정보와 비교하여 인증을 수행한 후, 인증된 사용자가 핸드폰이나 각종 서비스를 이용하도록 하되, On-Card Match 기술 및 바이오 보안인증 플랫폼과 바이오인증 솔루션을 이용하여 스마트카드 내에 생체정보를 저장 한 후 사용자 인증을 스마트카드 내에서 처리하도록 이루어진, 지문인식방법을 채용한 휴대용 보안인증기를 제공하는 것이다.

본 발명이 해결하고자 하는 다른 과제는, MOC 스마트카드가 추출된 특징점 정보과, 기저장된 사용자 지문정보을 이용하여 두 지문 이미지 간의 유사도를 결정하며, 연산처리부는, 지문 이미지를 세선화하고, 세선화 이미지로부터 융선의 흐름에 변화가 발생하는 단점과 분기점 정보를 추출하여 후보 특징점을 추출하고, 추출된 후보 특징점 중 의사 특징점을 제거하여, 지문의 특징점을 검출하도록 이루어진, 지문인식방법을 채용한 휴대용 보안인증기를 제공하는 것이다.

본 발명이 해결하고자 하는 다른 과제는, MOC 스마트카드가 연산처리부로부터 수신된 지문의 특징정보와 기저장된 사용자 지문정보의 두 지문 이미지의 특징점이 최대로 많이 겹쳐지는 회전, 천이량을 산출하여 이미지의 정렬 기준점을 선정하고, 정렬 기준점에 맞추어지도록 특징점의 좌표를 변환한 후 대응되는 특징점 쌍을 결정하고, 결정된 대응 특징점 쌍의 좌표, 종류, 각도정보를 이용하여 유사도(Measure Vector)를 계산하고, 대응 특징점 쌍의 유사도로부터 두 지문 이미지의 일치하는 정도를 기 설정된 규칙데이터에 따라, 점수로서 연산처리부로 출력하도록 이루어진, 지문인식방법을 채용한 휴대용 보안인증기를 제공하는 것이다.

과제의 해결 수단

[0026] 상기 과제를 해결하기 위해, 본 발명은, 지문센서를 구비하되, 상기 지문센서가 보안인증장치의 하우징부에 밖으로 노출되도록 장착되어지는, 지문센서부; 암호로된 사용자 지문정보를 저장하고 있으며, 연산처리부로부터 수신된 지문의 특징정보를, 바이오인식 매칭 프로그램(Bio matching algorithm)을 이용하여, 상기 사용자 지문정보와 비교하여 사용자 인증을 수행하는, MOC 스마트카드; 지문센서로부터 수신된 지문영상으로부터 특징점을 추출하여, MOC 스마트카드로 전송하고, MOC 스마트카드에서 사용자 인증결과를 수신하여, 사용자 인증이 성공하였다면, 메모리부에 저장된 데이터에의 접근을 허용하게 하는, 연산처리부;를 포함하여 이루어진 것을 특징으로 한다.

[0027] MOC 스마트카드는 OTP 애플렛, PKCS 애플렛, eID 애플렛, HPTP 애플렛, 지불(Payment) 애플렛, 전자화폐(E-Cash) 애플렛을 포함하고 있다.

[0028] 지문센서는 스윕(SWIPE) 센서이다.

[0029] 블루투수 통신부, WiFi 통신부, NFC 통신부, USB 커넥터부를 더 포함하여 이루어진다.

[0030] 메모리부에는 외부의 모바일 단말기, POS 단말기, 컴퓨터의 단말기 중 어느 하나의 비밀번호가 저장되어 있을 수 있다.

[0031] 연산처리부는 MOC 스마트카드에서 사용자 인증결과를 수신하여, 사용자 인증이 성공하였다면, MOC 스마트카드의 OTP 애플렛, PKCS 애플렛, eID 애플렛, HPTP 애플렛, 지불(Payment) 애플렛, 전자화폐(E-Cash) 애플렛 중 하나를 구동하도록 한다.

[0032] MOC 스마트카드는 추출된 특징점 정보과, 기저장된 사용자 지문정보을 이용하여 두 지문 이미지 간의 유사도를 결정한다.

[0033] 연산처리부는, 지문 이미지를 세선화하고, 세선화 이미지로부터 융선의 흐름에 변화가 발생하는 단점과 분기점 정보를 추출하여 후보 특징점을 추출하고, 추출된 후보 특징점 중 의사 특징점을 제거하여, 지문의 특징점을 검출한다.

[0034] MOC 스마트카드는 연산처리부로부터 수신된 지문의 특징정보와 기저장된 사용자 지문정보의 두 지문 이미지의 특징점이 최대로 많이 겹쳐지는 회전, 천이량을 산출하여 이미지의 정렬 기준점을 선정하고, 정렬 기준점에 맞추어지도록 특징점의 좌표를 변환한 후 대응되는 특징점 쌍을 결정하고, 결정된 대응 특징점 쌍의 좌표, 종류, 각도정보를 이용하여 유사도(Measure Vector)를 계산하고, 대응 특징점 쌍의 유사도로부터 두 지문 이미지의 일치하는 정도를 기 설정된 규칙데이터에 따라, 점수로서 연산처리부로 출력하도록 이루어진다.

발명의 효과

[0035] 본 발명의 지문인식방법을 채용한 휴대용 보안인증기에 따르면, 지문인식부와 MOC(On-Card Match) 스마트카드를 내장하며, 지문 센서를 통해 지문 이미지를 받아들여, 지문 이미지를 가공처리하여 추출한 특징정보를 MOC 스마트카드로 전송하여, 상기 카드내에 설치된 바이오인식 매칭 프로그램을 통해서, 카드 내에 암호로 저장된 사용자 정보와 비교하여 사용자 인증을 수행하고, 사용자 인증이 성공하면 메모리에 저장된 데이터의 접근을 허용하며, 소정의 데이터를 유무선 통신 인터페이스를 통해 모바일 단말기로 전송하여, 인증하여 모바일 단말기로 필요한 작업을 수행하게 한다.

[0036] 또한, 본 발명은, 지문 이미지의 특징정보를 추출하여, MOC 스마트카드에서, 기 저장된 사용자 정보와 비교하는, 사용자 인증을 통해, MOC 스마트카드에 설치되어 있는 다양한 서비스, 예로 OTP(One Time Password, 일회용비밀번호), PKCS(공개키 암호작성 시스템, Public-Key Cryptography System), eID, 지불 등에 대한 접근을 허용하게 한다.

[0037] 또한, 본 발명은, 바이오 등록/인증 매니저 프로그램을 통하여 사용자의 지문정보를 스마트카드의 보안 메모리 영역에 저장 관리하고, 입력된 지문정보에 대해 스마트카드의 On-Card Match 지문인식 알고리즘을 수행하여 사용자를 인증하며, 인증된 사용자에 대해 스마트폰/태블릿과 연결한 유/무선 인터페이스를 통해 개인정보 및 저장데이터를 사용할 수 있도록 접근권한을 부여한다.

[0038] 또한, 본 발명은, 스마트카드에 저장된 생체정보를 외부로부터 입력된 생체정보와 비교하여 인증을 수행한 후, 인증된 사용자가 핸드폰이나 각종 서비스를 이용하도록 하되, On-Card Match 기술 및 바이오 보안인증 플랫폼과 바이오인증 솔루션을 이용하여 스마트카드 내에 생체정보를 저장 한 후 사용자 인증을 스마트카드 내에서 처리하도록 이루어진다.

[0039] 따라서 본 발명은, 컴팩트하고, 속도가 빠르고, 보다 정보 보안에 안정하다.

[0040] 본 발명은 임베디드 시스템으로, 제품의 소형화, 단가의 저렴화 및 유지보수가 용이하며, 자동차, POS, ATM, 휴대폰, 개인화기, 카드리더 등 다양한 응용 시스템에 적용가능하다.

또한, 본 발명은, MOC 스마트카드가 추출된 특징점 정보과, 기저장된 사용자 지문정보을 이용하여 두 지문 이미지 간의 유사도를 결정하며, 연산처리부는, 지문 이미지를 세선화하고, 세선화 이미지로부터 융선의 흐름에 변화가 발생하는 단점과 분기점 정보를 추출하여 후보 특징점을 추출하고, 추출된 후보 특징점 중 의사 특징점을 제거하여, 지문의 특징점을 검출하도록 이루어진, 지문인식방법을 채용한 휴대용 보안인증기를 제공한다.

또한, 본 발명은, MOC 스마트카드가 연산처리부로부터 수신된 지문의 특징정보와 기저장된 사용자 지문정보의

두 지문 이미지의 특징점이 최대로 많이 겹쳐지는 회전, 천이량을 산출하여 이미지의 정렬 기준점을 선정하고, 정렬 기준점에 맞추어지도록 특징점의 좌표를 변환한 후 대응되는 특징점 쌍을 결정하고, 결정된 대응 특징점 쌍의 좌표, 종류, 각도정보를 이용하여 유사도(Measure Vector)를 계산하고, 대응 특징점 쌍의 유사도로부터 두 지문 이미지의 일치하는 정도를 기 설정된 규칙데이터에 따라, 점수로서 연산처리부로 출력하도록 이루어진, 지문인식방법을 채용한 휴대용 보안인증기를 제공한다.

도면의 간단한 설명

[0041] 도 1은 본 발명의 지문인식방법을 채용한 휴대용 보안인증기의 외관의 일예이다.

도 2는 본 발명의 지문인식방법을 채용한 휴대용 보안인증기의 사용에 대한 설명을 위한 모식도이다.

도 3은 도 1의 휴대용 보안인증기의 구성을 개략적으로 설명하기 위한 구성도이다.

도 4는 MOC 스마트카드의 구성을 개략적으로 설명하는 모식도이다.

도 5는 도 3의 지문센서에서 신호검출에 대한 개념을 설명하기 위한 모식도이다.

도 6은 본 발명의 휴대용 보안인증기에서 지문인식하는 과정을 개략적으로 설명하는 흐름도이다.

도 7은 도 6의 특징추출단계의 설명하는 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0042] 이하, 본 발명에 의한 지문인식방법을 채용한 휴대용 보안인증기를 첨부한 도면을 참조하여 상세히 설명한다.

[0043] 도 1은 본 발명의 지문인식방법을 채용한 휴대용 보안인증기의 외관의 일예이고, 도 2는 본 발명의 지문인식방법을 채용한 휴대용 보안인증기의 사용에 대한 설명을 위한 모식도이고 도 3은 도 1의 휴대용 보안인증기의 구성을 개략적으로 설명하기 위한 구성도이고, 도 4는 MOC 스마트카드의 구성을 개략적으로 설명하는 모식도이다.

[0044] 도 1에서와 같이, 본 발명의 휴대용 보안인증기(10)는 보안인증기 하우징(20)의 내측에 지문센서부(150)와 MOC 스마트카드(200)를 내장하되, 보안인증기 하우징(20)의 통공(창)을 통해, 지문센서부(150)의 지문센서가 외부로 노출되도록 이루어진다. 도 1에서는 미도시되었으나 휴대용 보안인증기(10)는 작동개시 등의 스위치를 더 구비할 수 있다.

[0045] 도 2에서와 같이, 지문 센서를 통해 지문 이미지를 받아들여, 특징정보를 추출하여, MOC 스마트카드(200)에서, 기 저장된 사용자 정보와 비교하여 사용자 인증을 수행하고, 사용자 인증이 성공하면, 메모리부(170)에 저장된 데이터의 접근을 허용하여, 소정의 데이터(예를들어 인증에 필요한 데이터(비밀번호, 암호등))를 유무선 통신 인터페이스, 즉, 블루투수 통신부(120), WiFi(Wireless-Fidelity) 통신부(130), NFC(Near Field Communication, 근거리무선통신) 통신부(140), USB 커넥터부(110)을 통해, 모바일 단말기(510), POS(point of sales) 단말기, 컴퓨터의 단말기(530) 등으로 전송하여, 인증하게 하여, 모바일 단말기(510), POS 단말기, 컴퓨터의 단말기(530)에서 필요한 작업, 즉 OTP, PKCS, eID, 지불 등을 수행하게 한다.

[0046] 도 3에서와 같이, 휴대용 보안인증기(10)는 연산처리부(100), 지문센서부(150), MOC 스마트카드(200), 메모리부(170), 배터리부(190), 블루투수 통신부(120), WiFi 통신부(130), NFC 통신부(140), USB 커넥터부(110)를 포함하여 이루어진다.

[0047] 연산처리부(100)는 휴대용 보안인증기(10)의 전반적인 제어를 담당하는 수단으로, CPU로 이루어질 수 있다. 연산처리부(100)의 CPU로서, ST사의 STM32F4 시리즈 프로세서 또는 Atmel사의 SAMA5 시리즈를 사용할 수 있다.

[0048] 연산처리부(100)는 지문센서부(150)를 통해 지문 이미지를 수신하여, 지문 이미지를 가공처리하여 지문의 특징정보를 추출하여, 추출된 지문의 특징정보를 MOC 스마트카드(200)로 전송하고, MOC 스마트카드(200)에서 사용자 인증결과를 수신하여, 사용자 인증의 성공여부를 판단하고, 사용자 인증이 성공하였다면, 메모리부(170)에 저장된 데이터의 접근 등을 허용하게 한다.

[0049] 지문센서부(150)는 지문센서, 지문센서 구동부 등을 구비한다.

[0050] 지문센서는 손가락 지문의 영상 정보를 획득하는 수단으로, 지문영상을 검출하여 연산처리부(100)로 전송한다. 지문센서는 스윕(SWIPE) 센서를 사용할 수 있다. 스윕 센서로서 128×8 픽셀을 인식하는 방식의 CMOS 센서를 사용할 수 있다.

[0051] 일반적으로 지문 센서는, 한번에 전체 지문을 인식하는 평면센서와, 라인센서형태로 센서에 손가락을 움직여서 지문을 인식하는 스윕(SWIPE) 센서로 구분되며, 스윕 센서의 경우 가격이 저렴하고 면적을 적게 차지한다.

[0052] 지문센서 구동부는 연산처리부(100)의 지문센싱 요청신호에 따라 지문센서를 구동시켜, 지문영상을 검출하게 한다.

[0053] MOC 스마트카드(200)는 연산처리부(100)로부터 수신된 지문의 특징정보를 수신하여, MOC 스마트카드(200) 내에 설치된 바이오인식 매칭 프로그램(Bio matching algorithm)을 통해서, MOC 스마트카드(200) 내에 암호로 저장된 사용자 정보와 비교하여 사용자 인증을 수행하고, 그 결과를 연산처리부(100)로 전송한다.

[0054] 도 4에서와 같이, MOC 스마트카드(200)는 바이오인식 매칭 알고리즘(Bio matching algorithm)을 구비하여 사용자 인증을 행하는 바이오 보안 플랫폼(Bio security platform) 이외에, OTP, PKCS, eID, HPTP, 지불(Payment), 전자화폐(E-Cash) 등의 애플렛(applet)을 포함한다.

[0055] 메모리부(170)는 MOC 스마트카드(200)에서 사용자 인증 후, 접근되는 데이터를 저장하고 있다. 메모리부(170)는 SD 메모리, 즉, Secure uSD로 이루어져, 사용자 인증이 성공으로 이루어진 후 접근되는 메모리로, 모바일 단말기(510), POS 단말기, 컴퓨터의 단말기(530) 등에서 인증을 위한 정보 등, 예를들어, 비밀번호 등을 저장하고 있다. MOC 스마트카드(200)에서 사용자 인증이 이루어진 후, 연산처리부(100)의 요청에 따라서 소정의 정보를 연산처리부(100)로 전송한다.

[0056] 배터리부(190)는 휴대용 보안인증기(10)의 내의 전원 수단이다.

[0057] 블루투수 통신부(120)는 연산처리부(100)로부터 수신된 정보를 블루투스로 모바일 단말기(510), POS 단말기, 컴퓨터의 단말기(530) 등으로 전송한다.

[0058] WiFi 통신부(130)는 연산처리부(100)로부터 수신된 정보를 WiFi로 모바일 단말기(510), POS 단말기, 컴퓨터의 단말기(530) 등으로 전송한다.

[0059] NFC 통신부(140)는 연산처리부(100)로부터 수신된 정보를 NFC 통신으로 모바일 단말기(510) 등으로 전송한다.

[0060] USB 커넥터부(110)는 USB 커넥터와 USB 구동부로 이루어져, USB 커넥터를 통해, 연산처리부(100)와 외부의 컴퓨터의 단말기(530) 등과 데이터를 송수신하게 한다.

[0061] 도 5는 도 3의 지문센서에서 신호검출에 대한 개념을 설명하기 위한 모식도이다.

[0062] 도 5의 (a)는 지문센서로서 스윕 센서를 사용하는 방법을 설명한다. 지문센서의 상측부터 하측으로 손가락을 움직이게 하며, 이때 지문센서는 지문 영상을 획득하게 된다.

[0063] 도 5의 (b)는 도 5의 (a)와 같이, 손가락을 움직일 때 지문 영상을 획득하는 과정을 설명하는 것으로, 지문센서의 상측부터 하측으로 손가락을 움직임에 따라 각 순간의 지문영상을 다층으로 얻어지게 된다.

[0064] 본 발명은 MOC 스마트카드(200) 내에서 인증을 처리해야하기 때문에 지문정보 및 COS(Card Operating System), 애플리케이션(지문인식 알고리즘 등) 등을 MOC 스마트카드(200) 내에 저장하고 사용자 인증을 수행한다.

[0065] 도 6은 본 발명의 휴대용 보안인증기에서 지문인식하는 과정을 개략적으로 설명하는 흐름도이고, 도 7은 도 6의 특징추출단계의 설명하는 흐름도이다.

[0066] 데이터 캡쳐(Data Capture)단계(S110)로, 사용 초기에 사용자의 지문정보를 MOC 스마트카드(200) 내에 저장하는 단계로, 즉, MOC 스마트카드(200)에 사용자의 지문정보를 최초 저장 시 필요한 단계로, 지문센서의 상측부터 하측으로 손가락을 움직임에 따라, 지문센서부(150)로부터, 각 순간의 지문영상을 다층으로 수신하여 하나의 영상으로 영상 정합하고, 영상 정합된 지문영상을 MOC 스마트카드(200)에 저장한다. 경우에 따라서는, 영상 정합된 지문영상에서 특징을 추출하여 함께 저장할 수 있다.

[0067] 데이터 캡쳐 단계(S110)의 이후 단계는 사용자 인증을 수행하기 위하여 MOC 스마트카드(200) 내에서 처리된다. 데이터 캡쳐 단계(S110)의 이후 단계는 크게 지문검출 및 특징추출(feature extraction)단계(S150)와 지문정합(fingerprint matching)단계(200)의 2단계를 거치게 된다.

[0068] 지문검출 및 특징추출 단계로(S150), 지문정합 단계에서 사용할 특징점(Minutiae) 데이터 파일을 구성하는 단계로, 지문센서부(150)로부터, 각 순간의 지문영상을 다층으로 수신하여 하나의 영상으로 영상 정합하고, 하나

의 영상으로 정합된 지문영상으로부터 특징을 추출한다.

[0069] 특징추출단계는, 전처리(pre-processing)단계(S160), 특징점 추출단계(S170) 및 후처리(post-processing) 단계(S180)의 3단계로 진행된다.

[0070] 전처리 단계(S160)는 지문 이미지를 세선화하는 단계로, 이미지 개선(image enhancement)을 행하고, 이미지 개선된 지문영상을 이진화(binarization)를 행하고, 세선화(thinning)한다.

[0071] 즉, 전처리 단계(S160)는 블록 방향성 이미지, 이진화 이미지, 세선화 이미지로의 변환과정을 거치게 된다. 지문 이미지를 일정 크기의 블록으로 나누고 각 블록별로 융선의 흐름을 나타내는 방향을 결정하여 블록별 방향 이미지로 변환한다. 이렇게 구해진 블록별 융선 방향 정보는 이진화, 평활화 과정에 사용된다. 이진화 과정에서 지문 이미지는 검은색과 흰색으로만 표현되는 이진 이미지로 바뀌고, 다시 이진 이미지는 잡음을 제거하고 융선을 강조하는 평활화 처리를 거침으로써 융선의 연결성을 향상시키고 융선을 1화소 굵기의 선으로 표현하여 세선화 이미지로 변환된다,

[0072] 특징점 추출단계(S170)는 전처리 단계(S160)에서 세선화된 지문영상에서 후보 특징점을 추출하는 단계이다.

[0073] 여기서, 특징점(Minutiae)이란 단점(융선의 흐름이 끊기는 지점)과 분기점(하나의 융선이 두개로 갈라지는 지점)이라고 부르는 융선의 흐름에 변화가 발생하는 점을 말한다. 특징량(T={m1, m2, ..., mm})은 지문 화상에 존재하는 특징점(mi)의 정보들로 이루어지는데 대부분의 경우 사용되는 특징점의 정보는 분기점과 단점 중 어떤 것인지를 나타내는 특징점의 종류, 지문 이미지내에서의 위치, 특징점이 위치한 융선의 방향에 대한 정보가 있다.

[0074] 즉, 특징점 추출단계(S170)는 후보 특징점 추출과정으로, 세선화 이미지로부터 융선의 흐름에 변화가 발생하는 단점과 분기점 정보를 저장한다. 세선화 이미지의 융선 정보로부터 의사 특징점을 포함한 후보 특징점을 추출한다. 이때, 세선화 이미지의 잘못된 융선 부분으로 인해 의사 특징점이 발생될 수 있다. 의사 특징점이란 지문 획득시의 잡음으로 인해 세선화 과정 중 발생하는 가짜 특징점을 말한다. 의사 특징점은 무의미한 계산량을 증가시키고 에러를 증가시켜 시스템의 성능을 저하시키는 요인이 된다.

[0075] 후처리 단계(S180)는 특징점 추출단계(S170)에서 추출한 특징점에서 가짜 특징점을 제거하는 단계이다. 즉, 후처리 단계(S180)는 의사 특징점의 발생원인이 되는 융선 부분을 수정하여 의사 특징점을 제거하고 누락된 특징점을 추가하여 최종적인 특징점을 추출한다.

[0076] 지문정합 단계(200)는, 특징점을 이용한 지문 인식방법의 정합 알고리즘에서는 추출 알고리즘에 의해 추출된 특징점 정보로부터 정의된 특징량을 사용하여 두 지문 이미지간의 유사도를 결정한다. 정합 알고리즘은 그림 16과 같이 정렬(Image Alignment), 정합(Mnutiae Matching), Scoring 3단계로 구분된다.

[0077] 지문정합 단계(200)는, 추출된 특징점 정보로부터 정의된 특징량을 사용하여 두 지문 이미지간의 유사도를 결정하는 단계로, 정렬(Image Alignment)단계(S210), 정합(Mnutiae Matching)단계(S230), 점수획득(Scoring)단계(S250) 3단계를 포함하여 이루어진다.

[0078] 정렬단계(S210)에서는 두 지문 이미지의 특징점이 가장 많이 겹쳐지는 회전, 천이량을 산출하여 이미지의 정렬 기준점을 선정한다. 이어서 정렬 기준점에 맞추어지도록 특징점의 좌표를 변환한 후 대응되는 특징점 쌍을 결정한다. 이때, 이상적인 회전 천이량을 찾기 위해서는 가능한 많은 후보 정렬을 수행해야 한다.

[0079] 정합단계(S230)에서는 정렬단계(S210)에서 결정된 대응 특징점 쌍의 좌표, 종류, 각도정보를 이용하여 유사도(Measure Vector)를 계산한다. 대응 특징점 쌍의 유사도를 사실적으로 반영하기 위해서는 유사도 결정방법에 있어 다양한 통계적 기법으로 여러 각도에서 고려될 수 있다.

[0080] 점수획득(Scoring)단계(S250)에서는 대응 특징점 쌍의 유사도 (Measure Vector)로부터 두 지문 이미지의 일치하는 정도를 기 설정된 규칙데이터에 따라, 점수로 나타낸다.

[0081] 규칙데이터는 정합단계와 마찬가지로 이미지의 일치하는 정도를 정확히 반영하기 위해서, Score계산 규칙의 선정(Decision Making)에 통계적인 근거와 수학적인 모델링을 이용하여 사전에 정하여진 데이터이다.

[0082] 상술한 바와 같이, 본 발명은 지문정보를 이용한 바이오 인식과 안전한 개인 정보 보안 관리를 위해 On-Card Match(MOC)를 활용한 바이오 인증 기반의 휴대용 보안 인증 기술 및보안인증기기에 관한 것이다.

[0083] 본 발명의 연산처리부(100)는 우선, 휴대용 보안인증단말기의 지문 센서부(150)를 통해 지문 이미지를 받아들이

고, 입력받은 지문 이미지를 가공처리하여 지문의 특징정보를 추출하고, 추출한 지문의 특징정보를 MOC 스마트카드(200)으로 전송하여 MOC 스마트카드(200) 내에 설치된 바이오인식 매칭 알고리즘의 애플릿(applet)을 통해서 카드 내에 암호로 저장된 사용자 정보와 비교하여 최종적인 사용자 인증을 수행한다. 이렇게 사용자 인증이 성공하면 메모리부에 저장된 데이터의 접근을 허용하며 유무선 통신 인터페이스를 통해 모바일 단말기로 전송하고 인증하여 필요한 작업을 수행하게 한다. 또한 사용자 인증을 통해 MOC 스마트카드에 설치되어 있는 다양한 서비스 애플릿(OTP, PKCS, eID, 지불 등)에 대한 접근을 허용한다.

[0084] 본 발명에서는, 본 발명의 휴대용 보안인증기 로그인 매니저를 통하여 새로운 사용자 지문을 MOC 스마트카드(200) 내에 암호화하여 저장한다. 그 후, 휴대용 보안인증기를 사용하기 위해 사용자가 지문센서에 지문을 입력하고, 입력된 지문정보에 대해 MOC 스마트카드(200)의 바이오보안플랫폼이 제공하는 지문인식 알고리즘을 통해 MOC 스마트카드(200)에 저장된 지문정보와 매칭 프로세스를 통해 사용자 인증을 수행한다. 인증된 사용자에 대해서 MOC 스마트카드(200)의 바이오보안플랫폼을 통해 MOC 스마트카드(200)의 애플릿서비스를 사용할 수 있도록 접근 권한을 부여한다.

[0085] 또한, 본 발명은, 저장된 보안 데이터에 대해 암호화/복호화 알고리즘을 가동하여 저장장치의 도난이나 분실에 대비하는 기능을 제공하며, 휴대용 보안인증기 프로그램을 통해 사용자 지문 등록/인증, 애플릿 관리, 메모리 관리 기능을 제공한다.

[0086] 이상에서는, 본 발명을 특정의 바람직한 실시예에 대해서 도시하고 설명하였다. 그러나 본 발명은 상술한 실시예에만 한정되는 것은 아니며, 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자라면 이하의 청구범위에 기재된 본 발명의 기술적 사상의 요지를 벗어남이 없이 얼마든지 다양하게 변경 실시할 수 있을 것이다.

부호의 설명

[0087] 10: 휴대용 보안인증기 20: 보안인증기 하우징

100: 연산처리부 110: USB 커넥터부

120: 블루투수 통신부 130: WiFi 통신부

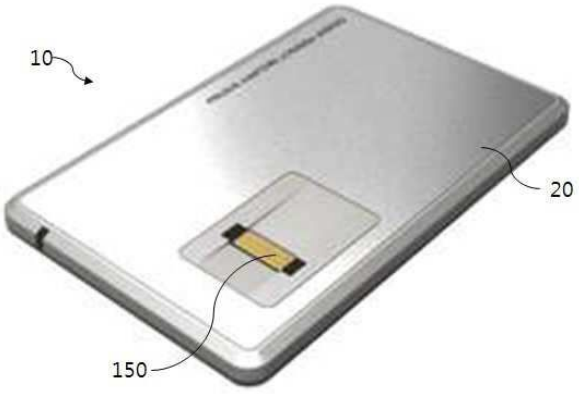
140: NFC 통신부 150: 지문센서부

170: 메모리부 190: 배터리부

200: MOC 스마트카드

도면

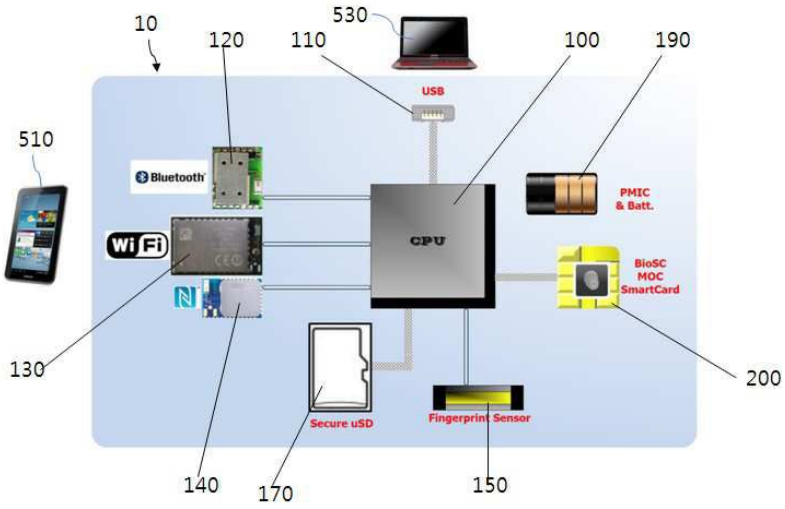
도면1



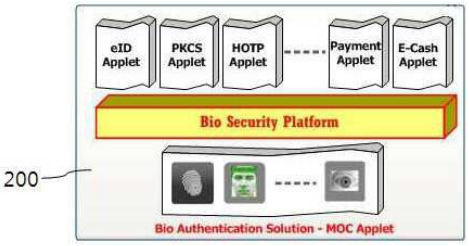
도면2


Mobile
510
POS
520
Smart BioDongle
10
Terminal
530

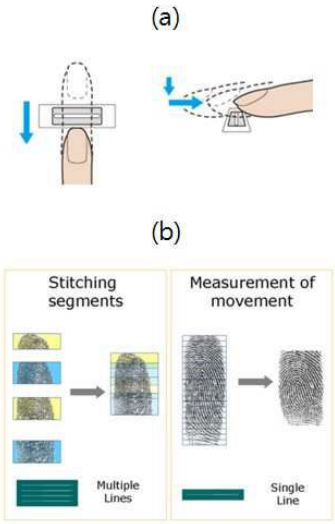
도면3


10
120
110
530
100
190
USB
510
Bluetooth
Wi Fi
CPU
PMIC
& Batt.
BioSC
MOC
SmartCard
130
200
Secure uSD
Fingerprint Sensor
140
170
150

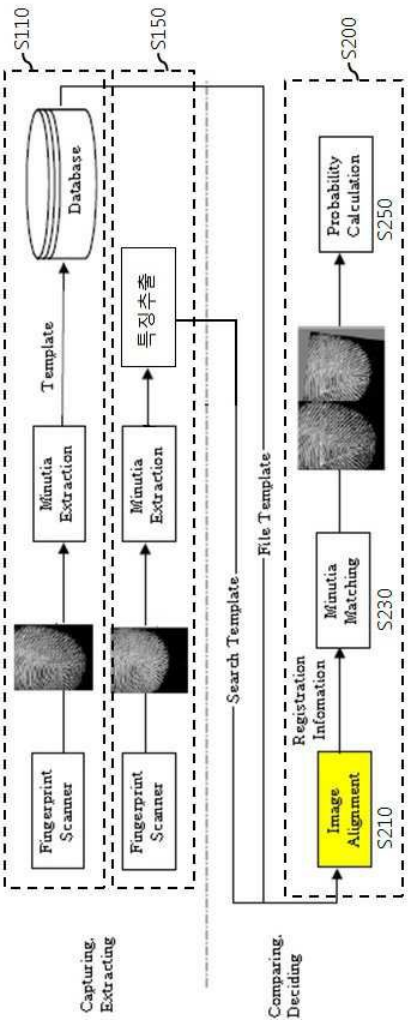
도면4


eID Applet
PKCS Applet
HOTP Applet
Payment Applet
E-Cash Applet
Bio Security Platform
200
Bio Authentication Solution - MOC Applet

도면5


(a)
(b)
Stitching segments
Measurement of movement
Multiple Lines
Single Line

도면6


S110
S150
S200
Database
Template
Minutia Extraction
Fingerprint Scanner
특징추출
Minutia Extraction
Fingerprint Scanner
Search Template
File Template
Probability Calculation
S250
Minutia Matching
S230
Registration Infomation
Image Alignment
S210
Capturing, Extracting
Comparing, Deciding

도면7