(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2016-0035523
(43) 공개일자 2016년03월31일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06K 19/06* (2006.01)
(21) 출원번호 10-2014-0160163
(22) 출원일자 2014년11월17일
심사청구일자 2014년11월17일
(30) 우선권주장
1020140125433 2014년09월22일 대한민국(KR)

(71) 출원인
한국과학기술원
대전광역시 유성구 대학로 291(구성동)
(72) 발명자
김찬우
대전 유성구 대학로 291
(74) 대리인
양성보

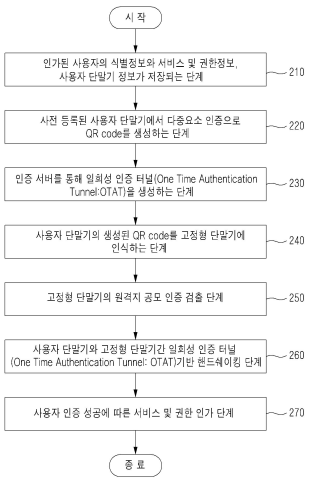
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **동적 상호작용 큐알 코드를 기반으로 한 다중요소 인증 방법 및 시스템**

(57) 요 약

동적 상호작용 큐알 코드를 기반으로 한 다중요소 인증 방법 및 시스템이 개시된다. 인증 방법에 있어서, 인증 대상인 사용자 단말기와 상기 사용자 단말기의 접근 여부를 결정하는 고정형 단말기 간의 인증을 위한 일회성 인증 터널(One Time Authentication Tunnel)을 생성하는 단계; 상기 사용자 단말기와 상기 고정형 단말기의 순차적인 요청에 따라 다차원 코드를 생성하는 단계; 및 상기 사용자 단말기와 상기 고정형 단말기 간의 상기 다차원 코드를 이용한 핸드쉐이킹(handshaking)을 통한 상기 일회성 인증 터널의 통과 여부에 따라 상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 단계를 포함할 수 있다.

대 표 도 - 도2



명 세 서

청구범위

청구항 1

컴퓨터로 구현되는 인증 방법에 있어서,

인증 대상인 사용자 단말기와 상기 사용자 단말기의 접근 여부를 결정하는 고정형 단말기 간의 인증을 위한 일회성 인증 터널(One Time Authentication Tunnel)을 생성하는 단계;

상기 사용자 단말기와 상기 고정형 단말기의 순차적인 요청에 따라 다차원 코드를 생성하는 단계; 및

상기 사용자 단말기와 상기 고정형 단말기 간의 상기 다차원 코드를 이용한 핸드쉐이킹(handshaking)을 통한 상기 일회성 인증 터널의 통과 여부에 따라 상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 단계

를 포함하는 인증 방법.

청구항 2

제1항에 있어서,

상기 다차원 코드를 생성하는 단계는,

인증 임계 값(Authentication Threshold Value) 이내에서 유효한 소멸성 QR(Quick Response) 코드를 생성하는 것

을 특징으로 하는 인증 방법.

청구항 3

제1항에 있어서,

상기 일회성 인증 터널을 생성하는 단계는,

상기 사용자 단말기와 상기 고정형 단말기 간에 수행되는 핸드쉐이킹 횟수에 따른 임의 순열을 포함하는 상기 일회성 인증 터널을 생성하는 것

을 특징으로 하는 인증 방법.

청구항 4

제3항에 있어서,

상기 일회성 인증 터널을 생성하는 단계는,

상기 사용자 단말기와 상기 고정형 단말기 간의 인증을 위한 고유 세션 키(session key)와 함께 상기 일회성 인증 터널을 생성하는 것

을 특징으로 하는 인증 방법.

청구항 5

제3항에 있어서,

상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 단계는,

상기 사용자 단말기와 상기 고정형 단말기가 상기 다차원 코드를 이용한 핸드쉐이킹을 통해 상기 임의 순열을 순차적으로 통과하는 경우 상기 사용자 단말기와 상기 고정형 단말기를 인증 통과 처리하는 것

을 특징으로 하는 인증 방법.

청구항 6

적어도 하나의 프로그램이 로딩된 메모리; 및

적어도 하나의 프로세서

를 포함하고,

상기 적어도 하나의 프로세서는, 상기 프로그램의 제어에 따라,

인증 대상인 사용자 단말기와 상기 사용자 단말기의 접근 여부를 결정하는 고정형 단말기 간의 인증을 위한 일회성 인증 터널(One Time Authentication Tunnel)을 생성하는 과정;

상기 사용자 단말기와 상기 고정형 단말기의 순차적인 요청에 따라 다차원 코드를 생성하는 과정; 및

상기 사용자 단말기와 상기 고정형 단말기 간의 상기 다차원 코드를 이용한 핸드쉐이킹(handshaking)을 통한 상기 일회성 인증 터널의 통과 여부에 따라 상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 과정

을 처리하는 인증 서버.

청구항 7

인증 대상인 사용자 단말기;

상기 사용자 단말기의 접근 여부를 결정하는 고정형 단말기; 및

상기 사용자 단말기와 상기 고정형 단말기 간의 인증을 위한 다차원 코드 및 일회성 인증 터널(One Time Authentication Tunnel)을 생성하는 인증 서버

를 포함하고,

상기 인증 서버는,

상기 사용자 단말기와 상기 고정형 단말기 간의 상기 다차원 코드를 이용한 핸드쉐이킹(handshaking)을 통한 상기 일회성 인증 터널의 통과 여부에 따라 상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 것

을 특징으로 하는 인증 시스템.

청구항 8

제7항에 있어서,

상기 인증 서버는,

상기 사용자 단말기의 인증 요청에 따라 임의 순열을 포함하는 상기 일회성 인증 터널을 생성한 후 상기 임의 순열에 따라 상기 다차원 코드를 순차적으로 생성하고,

상기 사용자 단말기와 상기 고정형 단말기는,

상기 다차원 코드에 대한 표출과 인식을 교차적으로 수행하는 핸드쉐이킹으로 상기 일회성 인증 터널을 통과하는 것

을 특징으로 하는 인증 시스템.

청구항 9

제7항에 있어서,

상기 인증 서버는,

인증 임계 값(Authentication Threshold Value) 이내에서 유효한 소멸성 QR(Quick Response) 코드를 생성하는 것

을 특징으로 하는 인증 시스템.

청구항 10

제7항에 있어서,

상기 인증 서버는,

상기 사용자 단말기와 상기 고정형 단말기 간의 인증을 위한 고유 세션 키(session key)와 함께 상기 일회성 인증 터널을 생성하는 것

을 특징으로 하는 인증 시스템.

청구항 11

제7항에 있어서,

상기 고정형 단말기는,

상기 인증 서버에서 정해진 회전 방향과 회전 속도 및 회전 각도 중 적어도 하나의 회전 패턴 튜플로 상기 사용자 단말기를 회전하도록 요구한 후 카메라에서 획득한 동영상을 분석하여 상기 사용자 단말기를 검증하는 것

을 특징으로 하는 인증 시스템.

청구항 12

제7항에 있어서,

상기 사용자 단말기와 관련된 인증 정보와 상기 고정형 단말기와 관련된 인증 정보를 관리하는 저장소; 및

상기 저장소를 이용하여 적법하지 않은 형태의 상기 일회성 인증 터널의 접근을 차단하는 접근 통제 센터

를 더 포함하는 인증 시스템.

청구항 13

제7항에 있어서,

사용자 별 인가된 서비스와 접근 권한을 포함하는 사전 등록 정보를 관리하는 저장소; 및

상기 사용자 단말기와 상기 고정형 단말기의 인증이 완료되면 상기 고정형 단말기로 상기 사용자 단말기에 대응되는 사전 등록 정보를 전달하는 인가 서버

를 더 포함하는 인증 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명의 실시예들은 QR(Quick Response) 코드를 이용한 인증 기술에 관한 것이다.

배 경 기 술

[0002] 인증은 주체의 식별(identification)을 통해 적법한 권한을 인가하기 위한 중요한 수단으로 활용된다. 인증 기술의 일 예로, 한국공개특허 제10-2006-0114079호(공개일 2006년 11월 06일)에는 이동통신단말기에 저장되어 있는 공인인증서를 이용하여 네트워크 사용자의 인증 절차를 수행하는 기술이 제안된 바 있다.

[0003] 인증은 식별 매체에 따라 3가지로 구분할 수 있다.

[0004] TYPE 1 인증은 암호, 개인식별번호, 어머니 이름, 자물쇠 번호, 전화번호와 같이 본인이 알고 있는 정보(Something You Know)를 활용한 방법으로 유추 및 재사용이 용이한 단점을 가진다.

[0005] TYPE 2 인증은 열쇠, 스와이프 카드(swipe card), 액세스 카드, 공인인증서와 같이 본인이 가지고 있는 것(Something You Have)으로 분실, 도난, 탈취 등에 의한 제3자에 의한 사칭이 가능하고 쉽게 복제될 수 있는 단점을 가진다.

[0006] TYPE 3 인증은 홍채, 망막, 지문, 얼굴, 음성과 같은 생체정보를 인식하는 것으로 본인 그 자체(Something You Are)를 인증매체로 하며, 지문 등 일부 생체정보는 복제 및 재사용이 가능하거나 신체 접촉에 의한 거부감을 유발하고 있으며, 생체정보 최초 추출시점과 유사한 임계구간의 인식 환경특성을 만족해야 허가된 사용자의 접근을 거부하는 비율(False Rejection Rate: FRR) 및 거부해야 할 사용자의 접근을 허용하는 비율(False

Acceptance Rate: FAR)을 일정 수준 이하로 유지할 수 있다는 단점을 가진다.

[0007] 보안강도는 TYPE 3 인증, TYPE 2 인증, TYPE 1 인증 순으로 높으나, TYPE 1~3의 인증 중 2가지 이상을 결합한 다중요소 인증(2-factor 인증, 3-factor 인증)의 강도는 TYPE 3 보다 강력하다.

[0008] 한편, QR 코드는 종횡으로 2차원 형태로 구성하여 더 많은 정보를 가질 수 있으며, 숫자 외에 알파벳과 한자, 일본어 등 다국어 문자 데이터를 저장할 수 있어 기존 1차원 형태의 일반 바코드(bar code)를 데이터의 표현 범위 및 양에서 개선된 것이며, QR 코드는 일반적으로 인쇄매체에 정적으로 인쇄되거나 웹사이트 화면 또는 스마트폰 등 이동단말기에 생성될 수 있다.

[0009] QR 코드 리더기(reader)는 하드웨어 또는 스마트폰 등 이동 단말의 어플리케이션으로 구현되어 QR 코드를 읽어들여 특정 URL로 사용자의 접속을 유도하는 방식으로 인터넷 서비스와 결합되어 사용되고 있다.

[0010] QR 코드를 사용하여 국내 및 해외 은행업계에서 모바일용 공인인증서 다운로드 URL 접근에 활용하거나 신용카드 모바일 결재 수단으로 온라인 상점에서 생성한 QR 코드를 모바일 신용카드 앱(App)에서 판독하여 결재를 하는 등 인증초기 수단으로 생성되고 있다.

[0011] QR 코드는 인증 수단으로 RFID(Radio-frequency identification) 보다 저렴하고 일반 인쇄방식이나 모바일 단말, 웹 브라우저를 포함하는 각 종 어플리케이션에서 생성할 수 있어 그 사용범위가 급격히 확대되고 있다.

[0012] 그러나, 인증수단으로서 QR 코드는 쉽게 복제할 수 있고 임의로 생성하거나 위조하기 쉬운 취약성을 지니고 있어 뛰어난 비용효율성에도 불구하고 출입제어 등 민감한 영역에서 활용될 수 없는 보안 장애요소를 지니고 있다.

[0013] 최근 국내에서 일부 기업에서 QR 코드를 동적으로 생성하여 인증에 사용하고 있으나, 30초 정도로 통상 주어지는 인증 가능한 임계 시간 이내에 스마트 폰 카메라를 통해 멀티미디어 메시지 서비스(Multimedia Message Service: MMS) 및 화상통화를 통해 원격지에서 생성 QR 코드를 전송 받아 비 인가된 자가 인증을 통과할 수 있는 보안 취약점이 존재한다.

[0014] QR 코드는 기존 RFID 기반의 출입제어, 교통카드 등 다양한 분야의 대체 기술로 활용될 수 있는 경제성 및 편리성, 유지보수성을 가지고 있으나 복제, 위조 등 보안취약성으로 기술적용의 한계점을 지니고 있다.

발명의 내용

해결하려는 과제

[0015] 기존 인증 기술의 한계점을 극복하기 위하여 QR 코드를 대체 인증수단으로 적용하여 시스템 구축 및 유지 관리 측면에서 경제성, 편리성, 휴대 용이성, 보안성을 보장할 수 있는 인증 방법 및 시스템을 제공한다.

[0016] QR 코드를 이용하여 동적 상호작용 방식인 핸드쉐이킹(handshaking) 방식의 인증 환경을 제공할 수 있는 인증 방법 및 시스템을 제공한다.

[0017] 화상 통화를 사용한 원격지의 비인가 접근을 효과적으로 차단할 수 있는 QR 코드를 이용한 인증 방법 및 시스템을 제공한다.

과제의 해결 수단

[0018] 컴퓨터로 구현되는 인증 방법에 있어서, 인증 대상인 사용자 단말기와 상기 사용자 단말기의 접근 여부를 결정하는 고정형 단말기 간의 인증을 위한 일회성 인증 터널(One Time Authentication Tunnel)을 생성하는 단계; 상기 사용자 단말기와 상기 고정형 단말기의 순차적인 요청에 따라 다차원 코드를 생성하는 단계; 및 상기 사용자 단말기와 상기 고정형 단말기 간의 상기 다차원 코드를 이용한 핸드쉐이킹(handshaking)을 통한 상기 일회성 인증 터널의 통과 여부에 따라 상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 단계를 포함하는 인증 방법을 제공한다.

[0019] 일 측면에 따르면, 상기 다차원 코드를 생성하는 단계는, 인증 임계 값(Authentication Threshold Value) 이내에서 유효한 소멸성 QR(Quick Response) 코드를 생성할 수 있다.

[0020] 다른 측면에 따르면, 상기 일회성 인증 터널을 생성하는 단계는, 상기 사용자 단말기와 상기 고정형 단말기 간에 수행되는 핸드쉐이킹 횟수에 따른 임의 순열을 포함하는 상기 일회성 인증 터널을 생성할 수 있다.

[0021] 또 다른 측면에 따르면, 상기 일회성 인증 터널을 생성하는 단계는, 상기 사용자 단말기와 상기 고정형 단말기 간의 인증을 위한 고유 세션 키(session key)와 함께 상기 일회성 인증 터널을 생성할 수 있다.

[0022] 또 다른 측면에 따르면, 상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 단계는, 상기 사용자 단말기와 상기 고정형 단말기가 상기 다차원 코드를 이용한 핸드쉐이킹을 통해 상기 임의 순열을 순차적으로 통과하는 경우 상기 사용자 단말기와 상기 고정형 단말기를 인증 통과 처리할 수 있다.

[0023] 적어도 하나의 프로그램이 로딩된 메모리; 및 적어도 하나의 프로세서를 포함하고, 상기 적어도 하나의 프로세서는, 상기 프로그램의 제어에 따라, 인증 대상인 사용자 단말기와 상기 사용자 단말기의 접근 여부를 결정하는 고정형 단말기 간의 인증을 위한 일회성 인증 터널(One Time Authentication Tunnel)을 생성하는 과정; 상기 사용자 단말기와 상기 고정형 단말기의 순차적인 요청에 따라 다차원 코드를 생성하는 과정; 및 상기 사용자 단말기와 상기 고정형 단말기 간의 상기 다차원 코드를 이용한 핸드쉐이킹(handshaking)을 통한 상기 일회성 인증 터널의 통과 여부에 따라 상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 과정을 처리하는 인증 서버를 제공한다.

[0024] 인증 대상인 사용자 단말기; 상기 사용자 단말기의 접근 여부를 결정하는 고정형 단말기; 및 상기 사용자 단말기와 상기 고정형 단말기 간의 인증을 위한 다차원 코드 및 일회성 인증 터널(One Time Authentication Tunnel)을 생성하는 인증 서버를 포함하고, 상기 인증 서버는, 상기 사용자 단말기와 상기 고정형 단말기 간의 상기 다차원 코드를 이용한 핸드쉐이킹(handshaking)을 통한 상기 일회성 인증 터널의 통과 여부에 따라 상기 사용자 단말기와 상기 고정형 단말기를 인증 처리하는 것을 특징으로 하는 인증 시스템을 제공한다.

[0025] 일 측면에 따르면, 상기 인증 서버는, 상기 사용자 단말기의 인증 요청에 따라 임의 순열을 포함하는 상기 일회성 인증 터널을 생성한 후 상기 임의 순열에 따라 상기 다차원 코드를 순차적으로 생성하고, 상기 사용자 단말기와 상기 고정형 단말기는, 상기 다차원 코드에 대한 표출과 인식을 교차적으로 수행하는 핸드쉐이킹으로 상기 일회성 인증 터널을 통과할 수 있다.

[0026] 다른 측면에 따르면, 상기 인증 서버는, 인증 임계 값(Authentication Threshold Value) 이내에서 유효한 소멸성 QR(Quick Response) 코드를 생성할 수 있다.

[0027] 또 다른 측면에 따르면, 상기 인증 서버는, 상기 사용자 단말기와 상기 고정형 단말기 간의 인증을 위한 고유 세션 키(session key)와 함께 상기 일회성 인증 터널을 생성할 수 있다.

[0028] 또 다른 측면에 따르면, 상기 고정형 단말기는, 상기 인증 서버에서 정해진 회전 방향과 회전 속도 및 회전 각도 중 적어도 하나의 회전 패턴 튜플로 상기 사용자 단말기를 회전하도록 요구한 후 카메라에서 획득한 동영상을 분석하여 상기 사용자 단말기를 검증할 수 있다.

[0029] 또 다른 측면에 따르면, 인증 시스템은, 상기 사용자 단말기와 관련된 인증 정보와 상기 고정형 단말기와 관련된 인증 정보를 관리하는 저장소; 및 상기 저장소를 이용하여 적법하지 않은 형태의 상기 일회성 인증 터널의 접근을 차단하는 접근 통제 센터를 더 포함할 수 있다.

[0030] 또 다른 측면에 따르면, 인증 시스템은, 사용자 별 인가된 서비스와 접근 권한을 포함하는 사전 등록 정보를 관리하는 저장소; 및 상기 사용자 단말기와 상기 고정형 단말기의 인증이 완료되면 상기 고정형 단말기로 상기 사용자 단말기에 대응되는 사전 등록 정보를 전달하는 인가 서버를 더 포함할 수 있다.

발명의 효과

[0031] 본 발명의 실시예에 따르면, QR 코드를 이용하여 다중요소 인증을 구현함으로써 기존 인증 기술의 한계점을 극복할 수 있고 QR 코드를 대체 인증수단으로 적용하여 시스템 구축 및 유지 관리 측면에서 경제성, 편리성, 휴대용이성, 보안성을 보장할 수 있다.

[0032] 본 발명의 실시예에 따르면, QR 코드를 기반으로 다중요소 인증 환경을 제공함으로써 QR 코드를 강력한 보안인증 수단으로 향상시킬 수 있으며 복잡한 기존 인증수단을 대체할 수 있다.

[0033] 본 발명의 실시예에 따르면, QR 코드를 이용하여 핸드쉐이킹의 동적 상호작용 방식을 구현함으로써 원격지 인가자 공모방식의 비인가자 인증을 효과적으로 차단할 수 있다.

[0034] 본 발명의 실시예에 따르면, 핸드쉐이킹의 안전성과 보안성을 확보하기 위해 일회성 인증 터널을 제공할 수 있으며, 임의로 유추 불가한 일회성 인증 터널을 침해의 목적으로 접근할 경우 이를 차단하고 검출하는 보호 장벽

을 구현할 수 있다.

도면의 간단한 설명

[0035] 도 1은 본 발명의 일 실시예에 있어서, QR 코드를 이용한 인증 시스템을 도시한 것이다.

도 2는 본 발명의 일 실시예에 있어서, QR 코드를 이용한 인증 방법을 도시한 순서도이다.

도 3은 본 발명의 일 실시예에 있어서, 고정형 단말기를 통한 원격지 공모 인증 검출 과정을 설명하기 위한 흐름도이다.

도 4는 본 발명의 일 실시예에 있어서, 일회성 인증 터널(OTAT)을 사용한 인증 과정을 설명하기 위한 구조도이다.

도 5는 본 발명의 일 실시예에 있어서, OTAT에 대한 보호 장벽인 접근 통제 센터를 설명하기 위한 구조도이다.

도 6은 본 발명의 일 실시예에 있어서, 컴퓨터 시스템의 내부 구성의 일례를 설명하기 위한 블록도이다.

발명을 실시하기 위한 구체적인 내용

[0036] 이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

[0037] 본 실시예들은 QR 코드를 동적 상호작용 방식으로 적용한 다중요소 인증 기술에 관한 것으로, 출입 통제나 도어락 등과 관련된 인증 분야에 적용될 수 있으며, 더 나아가 휴대폰 인증 및 결제 시장 등 인증이 요구되는 다양한 산업 분야로 확대 적용 가능하다.

[0038] 본 명세서에서는 인증수단으로 QR 코드를 적용하는 것으로 설명하고 있으나, 이에 한정되는 것은 아니며 QR 코드 이외에도 데이터 매트릭스(Data Matrix), 맥시 코드(Maxicode) 등 모든 종류의 다차원 코드를 적용할 수 있음은 물론이다.

[0039] 이하에서는 'QR 코드'를 다차원 코드의 대표적인 예로서 설명하기로 한다. 일 예로, QR 코드로는 JIS(Japanese Industrial Standards) 규격 및 ISO(International Organization for Standardization) 규격의 코드를 활용할 수 있다.

[0040] 도 1은 본 발명의 일 실시예에 있어서, QR 코드를 이용한 인증 시스템을 도시한 것이다.

[0041] 도 1을 참조하면, 본 발명에 따른 인증 시스템은 사용자 단말기(102), 고정형 단말기(104), 접근 통제 센터(108), 인증 서버(Authentication Server)(112), 저장소(Repository)(114), 인가 서버(Authorization Server)(116)를 포함할 수 있다.

[0042] 사용자 단말기(102)는 스마트폰(smart phone), 태블릿(tablet), 웨어러블 컴퓨터(wearable computer) 등 이동성을 가진 단말 형태로, 카메라와 디스플레이를 탑재한 단말을 의미할 수 있다. 사용자 단말기(102)는 인증 시스템과 관련된 웹/모바일 사이트의 접속 또는 서비스 전용 어플리케이션의 설치 및 실행이 가능한 모든 단말 장치를 의미할 수 있다. 이때, 사용자 단말기(102)는 웹/모바일 사이트 또는 전용 어플리케이션의 제어 하에 서비스 화면 구성, 데이터 입력, 데이터 송수신, 데이터 저장 등 서비스 전반의 동작을 수행할 수 있다.

[0043] 인증 대상인 사용자가 사용자 단말기(102)를 통해 일차 인증을 통과한 경우 인증 서버(112)는 사전 정책에서 지정된 인증 임계 값(Authentication Threshold Value: ATV) 이내에만 유효한 소멸성 QR 코드를 생성할 수 있다. 이때, 사용자 단말기(102)는 인증 서버(112)에서 생성된 QR 코드를 디스플레이를 통해 표출할 수 있고, 이에 사용자는 ATV에 지정된 시간 이내에 고정형 단말기(104)에 디스플레이에 표출된 QR 코드의 인식을 요청할 수 있다.

[0044] 사용자 단말기(102)의 일차 인증은 암호, 개인식별번호, 전화번호 등을 이용한 지식 기반 TYPE 1 인증과, 열쇠, 스와이프 카드, 액세스 카드, 공인인증서 등 매개물을 이용한 TYPE 2 인증과, 홍채, 망막, 지문, 얼굴, 음성 등 생체 정보를 이용한 TYPE 3 인증 중 어느 하나를 이용한 단일요소 인증 방식 또는 둘 이상을 조합한 다중요소 인증 방식을 적용할 수 있다. 이때, 다중요소 인증 방식으로는 TYPE 1 + TYPE 2, TYPE 1 + TYPE 3, TYPE 2 + TYPE 3, TYPE 1 + TYPE 2 + TYPE 3의 형태 중 어느 하나가 될 수 있다.

[0045] 저장소(114)는 인증 및 인가를 위한 정보와 처리 결과를 저장하고 있는 기술적/물리적/관리적 보안의 적용을 받

는 서버이며, 관리 대상 정보로 사용자 식별 정보, 고정형 단말기(104)의 식별 정보, 고정형 단말기(104)의 물리적 설치 위치, 설치 위치 또는 구역별 접근 가능한 사용자 정보, 사용자 단말기(102)의 식별 정보, 사용자 별 인가된 서비스와 접근 권한, 인증 기록, 인가 기록 등 주체 및 자원의 인증/인가를 위한 사전 정보와 처리결과를 관리할 수 있다.

[0046] 인증 서버(112)는 최초 QR 코드를 생성하는 시점에 인증을 위한 통신 터널인 일회성 인증 터널(One Time Authentication Tunnel: OTAT)(110)을 생성하는 역할을 한다. OTAT는 사용자 단말기(102)와 고정형 단말기(104) 사이에 수행되는 핸드쉐이킹 횟수(n=1)에 따른 임의의 순열(permutation)로 구성되어 해당 인증 건의 고유 세션 키(session key)와 함께 생성된다. 본 실시예에서는 OTAT의 구성을 위해 순열 외 순서가 있는 임의 문자열의 사용을 포함할 수 있으며, 편의 상 순열로 표현하고자 한다. 인증 서버(112)는 사용자 단말기(102)와 고정형 단말기(104)가 순차적으로 QR 코드를 통해 순열을 통과할 경우에 최종 인증 통과 처리를 수행하게 되며, QR 코드에 대응하는 URL이 인증 서버(112) 상의 HTTPS 등 공개키(public key) 기반의 암호화 통신 환경 위에서 동작하는 게이트웨이(Gateway) 어플리케이션으로 세션키와 OTAT의 순열의 기대 값, 인증 요청 단말 정보를 입력받아 해당 세션의 순열과 인가 서버(116)의 인증 처리를 수행한다. 생성된 순열과 세션키를 보호하기 위해 일방향 함수를 적용할 수 있다.

[0047] 접근 통제 센터(108)는 OTAT에 대한 보호 장벽으로서 저장소(114)에 등재되지 않은 단말기나 비 인가된 단말기, 존재하지 않는 세션키, 올바르지 않은 요청 순열 등 적법하지 않은 형태로 OTAT에 접근하는 모든 경우를 차단하고, 일정 수준 이상의 침해 시도가 계속될 경우 관리자에게 경보를 발생할 수 있다.

[0048] 인가 서버(116)는 인증된 사용자에 대해 저장소(114)의 사전 등록 정보에 기초하여 사용자가 접근 가능한 고정형 단말기(104)와 인가된 서비스 및 권한을 고정형 단말기(104)에 전달한다.

[0049] 고정형 단말기(104)는 고정형 단말 형태로 사용자 단말기(102)와의 동적 상호작용 방식으로 사용자 단말기(102)에 대한 접근 가능 여부를 확인하는 역할은 한다. 이를 위하여, 고정형 단말기(104)는 3단계로 동작하며, 1단계로 QR 코드 검증, 2단계로 원격지 공모 인증 검출, 3단계로 핸드쉐이킹을 수행한다. 본 실시예에서는 3단계에 대한 순서의 재배치를 포함할 수 있으며, 3개의 단계를 1회 이상 재배치하여 보안 강도를 상승시킬 수 있다.

[0050] QR 코드 검증 단계에서 고정형 단말기(104)는 사용자 단말기(102)에 표출된 QR 코드를 카메라를 통해 1차 검증을 수행하며, ATV 만료 등 검증 오류가 있는 경우 사용자에게 QR 코드의 재생성을 요청할 수 있다. 그리고, 고정형 단말기(104)는 인가 서버(116)에 사용자가 물리적 위치 또는 구역에 접근 가능한지 질의를 요청하여 접근 가능한 경우에 정상 처리를 하고 접근 불가한 경우는 처리를 중단하고 저장소(114)에 비인가 접근을 기록하고 사용자에게 비인가 접근에 대한 안내를 디스플레이 또는 스피커를 통해 출력한다.

[0051] 원격지 공모 인증 검출 단계는 사용자 단말기(102)에 표출된 QR 코드가 검증을 정상적으로 통과한 경우, 화상통화 및 방송 장비 등 실시간 동화상으로 비인가 사용자가 원격지 상의 인가된 사용자의 공모를 통해 인증을 시도하는 경우를 차단하기 위한 방법이다. 인증 서버(112)에서 인증 요청 시점마다 임의(random) 함수로 회전 패턴 튜플(회전 방향, 회전각도, 회전속도)를 정하여 고정형 단말기(104)의 디스플레이를 통한 안내를 따라 사용자 단말기(102)를 회전하도록 요구하여 고정형 단말기(104)의 카메라에서 촬영된 회전 동화상을 분석하여 지시를 따른 사용자 단말기 회전 여부 및 검증된 QR 코드의 유지 여부, 사용자 단말기(102) 화면 상의 어플리케이션 경계 유지 여부 등 검증한다. 본 발명의 ATV는 원격지의 인가된 사용자의 공모 시 기간 이내에 사전에 동화상을 제작할 수 없는 한계 기간으로 설정되며, 본 발명은 사용자 단말기(102) 회전의 궤적 요청을 불규칙하게 구성하여 원격지의 인가 사용자가 고정형 단말기(104)의 회전 지시 화면을 볼 수 없는 상태에서 정확한 회전 방향과 속도를 현장의 공모자와 정확하게 동기화할 수 없어 발생하는 동화상의 논리적 오류를 검출하여 원격지 공모 인증을 효과적으로 방어할 수 있다.

[0052] 고정형 단말기(104)의 핸드쉐이킹 단계는 인증 서버(112)에서 일회성 인증 터널(OTAT)(110)을 기반으로 사용자 단말기(102)의 카메라에서 인식할 수 있는 일회성 QR 코드를 생성하여 사전 설정된 핸드쉐이킹 횟수에 따라 OTAT를 정상적으로 통과하는 시점까지 사용자 단말기(102)와 상호 작용을 한다. OTAT를 정상 통과하지 못한 경우 이를 보안 침해로 검출하여 고정형 단말기(104)에 나타난 사용자의 촬영 정보 및 요청 QR 코드의 이미지, 기타 정보를 로깅(logging)하여 인증 서버(112)에 저장을 요청한다.

[0053] 인가 서버(112)는 인증이 완료된 사용자에게 고정형 단말기(104)에서 인가된 서비스나 권한을 사용자에게 제공하는 것으로, 출입 통제 측면의 출입문 개방, 서비스에서 물품의 구매 의사 표현, 인사 근태 관리의 출퇴근, 전

자상거래의 대금 결제 등 다양한 서비스와 권한으로 연계 구성할 수 있으며, 사용자 단말기(102) 상의 연계 서비스에 대한 인가를 포함할 수 있다.

[0054] 사용자 단말기(102)에 대해 TYPE 1 + TYPE 2 (2-factor) 인증 방식과 5-way 핸드쉐이킹을 적용하는 경우를 가정하여 구체적인 인증 과정을 설명하면 다음과 같다.

[0055] 사용자 단말기(102)로서 이미 등록된 스마트폰을 활용한다면 TYPE 2 인증을 만족하게 되며 스마트폰에 본인의 생년월일이나 로그인 ID와 암호와 같은 TYPE 1 인증을 결합하여 인증 서버(112)에 요청하면 일차 인증의 TYPE 1 + TYPE 2 (2-factor)인 다중요소 인증 요건을 만족한다.

[0056] 인증 서버(112)에서 정상적인 인증 통과를 할 경우에 한하여 5개의 임의의 순열이 생성되고, 첫 번째 숫자와 유일한 세션키, 사용자 단말기(102)의 식별 정보가 결합된 첫 번째 QR 코드가 사용자 단말기(102)에 디스플레이에서 표출되며 순열을 보호하기 위해 일방향 함수를 적용하는 것을 포함할 수 있다. 사용자는 인증 임계 값(ATV)에 지정된 시간 이내에 고정형 단말기(104)로 사용자 단말기(102)에 표출된 QR 코드의 인식을 요청한다.

[0057] 고정형 단말기(104)는 사용자 단말기(102)에 표출된 QR 코드의 인식 단계를 수행하고 물리적 위치 또는 구역에 접근가능 여부를 점검한다. 고정형 단말기(104)의 원격지 공모 인증 검출 단계는 이전 단계의 정상 통과를 확인한 후 진행되며, 인증 서버(112)에서 매번 임의로 지정된 방향과 회전 속도로 사용자 단말기(102)를 회전하도록 한다. 예를 들어, 임의 함수의 결과가 (반시계 방향, 30도, 빠르게)와 (시계 방향, 45도, 느리게)라고 한다면, 고정형 단말기(104)의 디스플레이를 통해 사용자 안내와 함께 사용자 단말기(102)가 요구한 최초 위치로부터 반시계 방향으로 30도 회전 이동 후 보다 빠른 속도로 시계 방향으로 45도 회전이동을 요구한다. 회전 동작의 특성 상 원격지 공모가 있는 경우, 사용자 단말기(102)의 디스플레이는 원격지의 단말기를 화상 통화 또는 방송 장비로 중계하는 과정에서 회전각의 불일치가 발생하게 되며 임의의 방향과 속도로 요구되는 회전동작을 일치하기 어렵게 되어 용이하게 검출할 수 있다. 고정형 단말기(104)의 핸드쉐이킹 단계는 이전 단계의 정상 통과를 확인한 후 진행되며, 인증 서버(112)에서 일회성 인증 터널(110)을 기반으로 사용자 단말기(102)의 카메라에서 인식할 수 있는 일회성 QR 코드를 생성하여 사전 설정된 핸드쉐이킹 횟수 5회에 따라 일회성 인증 터널(OTAT)(110)을 정상적으로 통과하는 시점까지 사용자 단말기(102)와 상호 작용을 정상적으로 진행한다. 고정형 단말기(104)의 인가 단계는 이전 단계의 정상통과를 확인한 후 진행되며, 인증이 완료된 사용자에게 고정형 단말기(104)에서 인가된 서비스 및 권한을 사용자에게 제공하는 것으로 예를 들어 근태관리 시스템의 출근을 확인하는 등 실제 서비스에 연결될 수 있다.

[0058] 도 2는 본 발명의 일 실시예에 있어서, QR 코드를 이용한 인증 방법을 도시한 흐름도이다. 일 실시예에 따른 인증 방법은 도 1을 통해 설명한 인증 시스템에 의해 각각의 단계가 수행될 수 있다.

[0059] 단계(210)에서, 인증을 위한 정보로서 사전에 인가된 사용자의 식별 정보와 접근 가능한 서비스 및 권한 정보, 사용자 단말기 정보 등을 저장소(114)에 등록할 수 있다.

[0060] 단계(220)에서, 저장소(114)에 사전 등록된 사용자 단말기 여부를 점검하고 등록된 경우 사용자가 일차 인증(지식 기반 TYPE 1, 매개물을 이용한 TYPE 2, 생체 정보를 이용한 TYPE 3 중 적어도 하나에 따른 인증)을 통과하면 QR 코드를 생성한다. 이때, 일차 인증은 TYPE 1, TYPE 2, TYPE 3 중 하나의 인증 방식이 적용되거나 둘 이상의 인증 방식이 조합된 다중요소 인증으로 동작할 수 있으며, 다중요소 인증 시 모든 인증의 정상처리 후 QR 코드를 생성한다.

[0061] 단계(230)에서, 인증 서버(112)는 사전 지정된 핸드쉐이크 횟수만큼의 순열을 임의 함수로 생성하고 세션 키를 부여하고, 단계(220)에서 인증을 요청한 사용자 단말기의 식별 번호를 세션 키에 맵핑하여 일회성 인증 터널(OTAT)을 생성하고, 사용자 단말기(102)로 순열의 첫 번째 값을 전달하여 사용자 단말기(102)가 첫 번째 QR 코드를 만들 수 있도록 한다.

[0062] 단계(240)에서, 사용자는 인증 임계 값(ATV) 시간 이내에 사용자 단말기(102)에 생성된 QR 코드를 고정형 단말기(104)에 인식해야 하며, ATV 시간을 초과할 경우 생성된 QR 코드는 자동 소멸된다. ATV는 조절될 수 있으나 원격지에서 생성하여 촬영 후 전송할 수 있는 시간보다 짧아야 한다.

[0063] 단계(250)에서, 단계(240)에서 전달된 QR 코드가 일회성 인증 터널(OTAT)의 첫 번째 순열 값으로 만들어진 것인지 인증 서버(112)에 검증을 요청하며, 검증 시 고정형 단말기(104)의 식별 정보가 함께 전달되고 OTAT에 상호 인증을 위한 고정형 단말기(104)의 식별 번호가 맵핑(mapping)된다. 이미 OTAT에 고정형 단말기(104)의 식별 번호가 맵핑이 될 경우, 인증 서버(112)는 오류 처리를 하고 해당 OTAT를 폐기 처리하고 비인가 접근으로 저장소(114)에 로깅하며 관리자에게 경고를 보낼 수 있다. 인증 서버(112)에 정상적으로 상호 인증을 위한 고정형

단말기(104)의 식별 번호가 맵핑된 경우 다음 단계로 임의 함수로 회전 패턴 튜플(회전 방향, 회전각도, 회전속도)를 정하여 고정형 단말기(104)의 디스플레이를 통한 안내를 따라 사용자 단말기(102)를 회전하도록 요구하여 고정형 단말기(104)의 카메라 모듈에서 촬영된 회전 동화상을 분석 및 공모여부를 검증한다. 원격지에 있는 인가된 사용자가 고정형 단말기(104)의 회전 지시 화면을 볼 수 없는 상태에서 정확한 회전 방향과 속도를 현장의 공모자와 정확하게 동기화할 수 없어 발생하는 동화상의 논리적 오류를 검출할 수 있으며, 구체적인 검출 방법으로 지시에 따른 사용자 단말기 회전여부 및 검증된 QR 코드 유지여부, 사용자 단말기 화면 상의 어플리케이션 경계선 유지 여부, 플래쉬(Flash) 모듈을 구동할 경우 깜빡임의 감지 등 다양한 검증 방법을 포함할 수 있다.

[0064] 단계(260)에서, 사용자 단말기(102)와 고정형 단말기(104) 사이에 핸드쉐이킹 지정 횟수만큼 상호 QR code를 발생 시키고 인식하는 방법으로 일회성 인증 터널(OTAT)을 통과 함으로써 인증을 처리한다.

[0065] 단계(270)에서, 인가서버(116)는 인증을 정상적으로 마친 사용자의 정보를 저장소(114)에서 가져와 사용자의 접근 가능 서비스 및 서비스별 권한을 부여할 수 있다.

[0066] 도 3은 본 발명의 일 실시예에 있어서, 고정형 단말기를 통한 원격지 공모 인증 검출 과정을 설명하기 위한 흐름도이다.

[0067] 단계(310)에서, 인증 서버(112)에서 임의 함수로 회전 패턴 튜플(회전 방향, 회전각도, 회전속도)을 최소 2개 이상 생성하며, 회전 방향은 시계 방향 또는 반시계 방향이며 회전 각도는 사람이 회전하기 적합한 범위에서 최소 값 이상 최대 값 이하의 난수를 발생하여 정한다. 회전 속도는 사람이 디스플레이를 따라 회전할 수 있는 범위에서 최소 값 이상 최대 값 이하를 정하여 여러 개의 구간 값으로 구분한 후 난수를 발생하여 정한다.

[0068] 단계(320)에서, 고정형 단말기(104)에서 결정된 이동 패턴 튜플(회전 방향, 회전각도, 회전속도)에 따라 사용자 단말기(102)에 회전 요청을 전달하여 동화상을 촬영할 수 있다.

[0069] 단계(330)에서, 고정형 단말기(104)가 촬영된 동화상으로 구분 이미지를 추출할 수 있다. 구분 이미지의 추출은 관심 영역 기반의 영상 처리 기술 등을 이용할 수 있다.

[0070] 단계(340)에서, 추출된 이미지들로부터 회전지시 이행여부, 검증된 QR 코드 유지여부, 사용자 단말기 화면 상의 어플리케이션 경계 유지 여부 등 원격지 공모 인증을 검증할 수 있다.

[0071] 도 4는 본 발명의 일 실시예에 있어서, 일회성 인증 터널(OTAT)을 사용한 인증 과정을 설명하기 위한 구조도이다.

[0072] 도 4를 참조하면, 일회성 인증 터널(OTAT)이 세션키, 사용자 단말기 식별자, 고정형 단말기 식별자, N차의 순열 값으로 구성됨을 볼 수 있다.

[0073] 사용자 단말기(102)의 인증 요청에 의해 일회성 인증 터널(OTAT)이 생성되며, 사용자 단말기(102)에서 첫 번째 순열 값과 세션키 등 정보를 조합하여 QR 코드로 생성되어 고정형 단말기(104)에 인식된다. 고정형 단말기(104)가 첫 번째 QR 코드를 인식하여 인증 서버(112)를 통해서 정상 검증을 확인한 경우, 고정형 단말기(104)는 두 번째 순열 값과 세션키, 고정형 단말기 식별번호 등 정보를 조합하여 두 번째 QR 코드를 고정형 단말기(104)의 디스플레이에 표출한다. 사용자 단말기(102)에 대기 중인 인증 어플리케이션은 고정형 단말기(104)에 표출된 두 번째 QR 코드를 카메라 모듈로 인식하고 인증 서버(112)를 통해서 정상 검증을 확인한 경우, 인증 서버(112)로부터 세 번째 순열 값을 수신하고 세션키, 사용자 단말기 식별번호 등 정보를 결합하여 세 번째 QR 코드를 생성하여 사용자 단말기(102)의 디스플레이에 표출하면 고정형 단말기(104)의 카메라 모듈이 세 번째 QR 코드를 인식하고 인증 서버(112)를 통해서 정상 검증을 확인한다.

[0074] 이와 같이 QR 코드의 생성과 인증 과정이 3번을 수행하면 3-way 핸드쉐이크라고 부르며, 수초 이내에 이 과정은 종결된다. 본 발명은 n-way 핸드쉐이크를 제시하고 있으며, 요구되는 보안 강도에 따라 n의 값을 지정할 수 있다.

[0075] 도 5는 본 발명의 일 실시예에 있어서, OTAT에 대한 보호 장벽인 접근 통제 센터를 설명하기 위한 구조도이다.

[0076] 본 발명은 접근 통제 센터(108)에 의해 일회성 인증 터널(OTAT)이 보호되는 구조를 제시할 수 있다. 도 5를 참조하면, 접근 통제 센터(108)는 올바른 세션키 및 사용자 단말기 식별자, 고정형 단말기 식별자로 접근하지 않는 모든 경우 인증 접근을 차단하고, 저장소(114)에 로깅을 하고, 관리자에게 경고를 보낼 수 있다. 또한, N차의 순열 값이 순서대로 호출되지 않는 경우에도 인증 접근을 차단하고 저장소(114)에 로깅을 하고, 관리자에게 경고를 보낼 수 있다.

[0077] 도 6는 본 발명의 일 실시예에 있어서, 컴퓨터 시스템의 내부 구성의 일례를 설명하기 위한 블록도이다. 컴퓨터 시스템(600)은 적어도 하나의 프로세서(processor)(610), 메모리(memory)(620), 주변장치 인터페이스(peripheral interface)(630), 입/출력 서브시스템(I/O subsystem)(640), 전력 회로(650) 및 통신 회로(660)를 적어도 포함할 수 있다. 이때, 컴퓨터 시스템(600)은 도 1 내지 도 5를 통해 설명한 인증 시스템에 포함된 구성 요소 각각에 해당될 수 있다.

[0078] 메모리(620)는, 일례로 고속 랜덤 액세스 메모리(high-speed random access memory), 자기 디스크, 에스램(SRAM), 디램(DRAM), 롬(ROM), 플래시 메모리 또는 비휘발성 메모리를 포함할 수 있다. 메모리(620)는 컴퓨터 시스템(600)의 동작에 필요한 소프트웨어 모듈, 명령어 집합 또는 그밖에 다양한 데이터를 포함할 수 있다. 이때, 프로세서(610)나 주변장치 인터페이스(630) 등의 다른 컴포넌트에서 메모리(620)에 액세스하는 것은 프로세서(610)에 의해 제어될 수 있다.

[0079] 주변장치 인터페이스(630)는 컴퓨터 시스템(600)의 입력 및/또는 출력 주변장치를 프로세서(610) 및 메모리(620)에 결합시킬 수 있다. 프로세서(610)는 메모리(620)에 저장된 소프트웨어 모듈 또는 명령어 집합을 실행하여 컴퓨터 시스템(600)을 위한 다양한 기능을 수행하고 데이터를 처리할 수 있다.

[0080] 입/출력 서브시스템(640)은 다양한 입/출력 주변장치들을 주변장치 인터페이스(630)에 결합시킬 수 있다. 예를 들어, 입/출력 서브시스템(640)은 모니터나 키보드, 마우스, 프린터 또는 필요에 따라 터치스크린이나 센서 등의 주변장치를 주변장치 인터페이스(630)에 결합시키기 위한 컨트롤러를 포함할 수 있다. 다른 측면에 따르면, 입/출력 주변장치들은 입/출력 서브시스템(640)을 거치지 않고 주변장치 인터페이스(630)에 결합될 수도 있다.

[0081] 전력 회로(650)는 단말기의 컴포넌트의 전부 또는 일부로 전력을 공급할 수 있다. 예를 들어 전력 회로(650)는 전력 관리 시스템, 배터리나 교류(AC) 등과 같은 하나 이상의 전원, 충전 시스템, 전력 실패 감지 회로(power failure detection circuit), 전력 변환기나 인버터, 전력 상태 표시자 또는 전력 생성, 관리, 분배를 위한 임의의 다른 컴포넌트들을 포함할 수 있다.

[0082] 통신 회로(660)는 적어도 하나의 외부 포트를 이용하여 다른 컴퓨터 시스템과 통신을 가능하게 할 수 있다. 또는 상술한 바와 같이 필요에 따라 통신 회로(660)는 RF 회로를 포함하여 전자기 신호(electromagnetic signal)라고도 알려진 RF 신호를 송수신함으로써, 다른 컴퓨터 시스템과 통신을 가능하게 할 수도 있다.

[0083] 이러한 도 6의 실시예는, 컴퓨터 시스템(600)의 일례일 뿐이고, 컴퓨터 시스템(600)은 도 6에 도시된 일부 컴포넌트가 생략되거나, 도 6에 도시되지 않은 추가의 컴포넌트를 더 구비하거나, 2개 이상의 컴포넌트를 결합시키는 구성 또는 배치를 가질 수 있다. 예를 들어, 모바일 환경의 통신 단말을 위한 컴퓨터 시스템은 도 6에 도시된 컴포넌트들 외에도, 터치스크린이나 센서 등을 더 포함할 수도 있으며, 통신 회로(660)에 다양한 통신 방식(WiFi, 3G, LTE, Bluetooth, NFC, Zigbee 등)의 RF 통신을 위한 회로가 포함될 수도 있다. 컴퓨터 시스템(600)에 포함 가능한 컴포넌트들은 하나 이상의 신호 처리 또는 어플리케이션에 특화된 집적 회로를 포함하는 하드웨어, 소프트웨어, 또는 하드웨어 및 소프트웨어 양자의 조합으로 구현될 수 있다.

[0084] 본 발명의 실시예에 따른 방법들은 다양한 컴퓨터 시스템을 통하여 수행될 수 있는 프로그램 명령(instruction) 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다.

[0085] 본 실시예에 따른 프로그램은 PC 기반의 프로그램 또는 모바일 단말 전용의 어플리케이션으로 구성될 수 있다. 본 실시예에서의 QR 코드를 이용한 인증 어플리케이션은 독립적으로 동작하는 프로그램 형태로 구현되거나, 혹은 특정 어플리케이션의 인-앱(in-app) 형태로 구성되어 상기 특정 어플리케이션 상에서 동작이 가능하도록 구현될 수 있다.

[0086] 이와 같이, 본 발명의 실시예에 따르면, QR 코드를 이용한 인증 모델을 구현함으로써 기존 인증 기술의 한계점을 극복할 수 있고 QR 코드를 대체 인증수단으로 적용하여 시스템 구축 및 유지 관리 측면에서 경제성, 편리성, 휴대 용이성, 보안성을 보장할 수 있다. 그리고, 본 발명의 실시예에 따르면, QR 코드를 이용하여 핸드쉐이킹의 동적 상호작용 방식을 구현함으로써 QR 코드를 강력한 보안인증 수단으로 향상시킬 수 있으며 복잡한 기존 인증수단을 대체할 수 있으며, 더욱이 원격지 인가자 공모방식의 비인가자 인증을 효과적으로 차단할 수 있다.

[0087] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령

(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제 상에서 수행되는 하나 이상의 소프트웨어 애플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.

[0088] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상 장치(virtual equipment), 컴퓨터 저장 매체 또는 장치, 또는 전송되는 신호 파(signal wave)에 영구적으로, 또는 일시적으로 구체화(embody)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨터 시스템 상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.

[0089] 실시예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0090] 이상과 같이 실시예들이 비록 한정된 실시예와 도면에 의해 설명되었으나, 해당 기술분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다.

[0091] 그러므로, 다른 구현들, 다른 실시예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

부호의 설명

[0092] 102: 사용자 단말기

104: 고정형 단말기

108: 접근 통제 센터

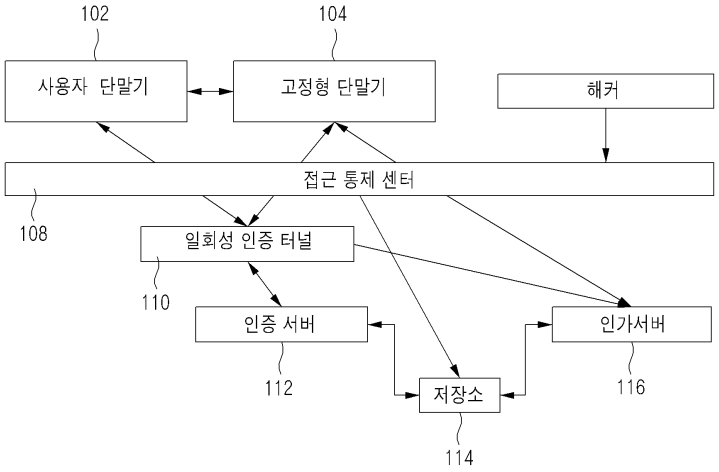
112: 인증 서버

114: 저장소

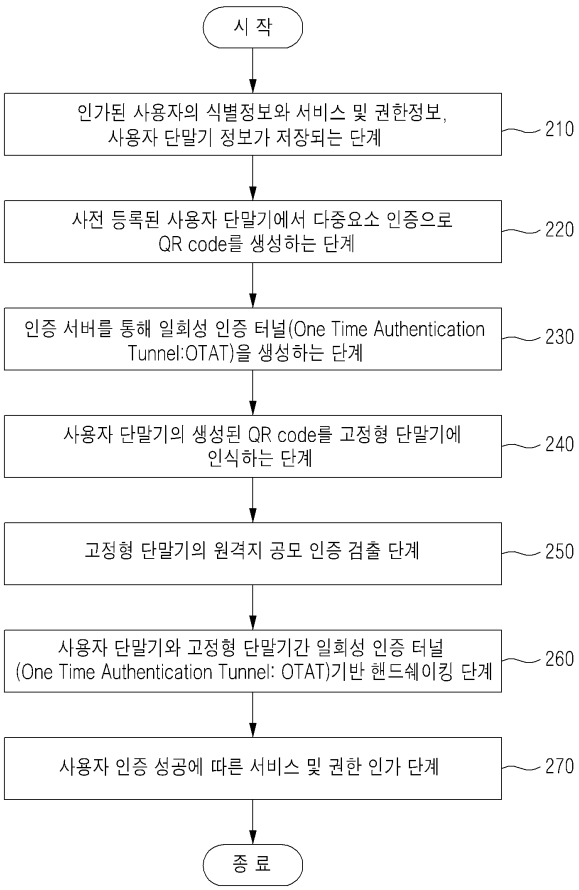
116: 인가 서버

도면

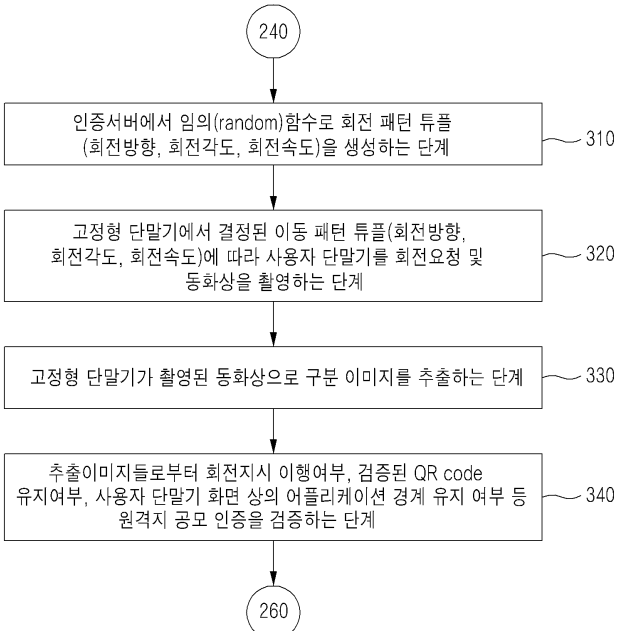
도면1


102
104
사용자 단말기
고정형 단말기
해커
접근 통제 센터
108
일회성 인증 터널
110
인증 서버
112
저장소
114
인가서버
116

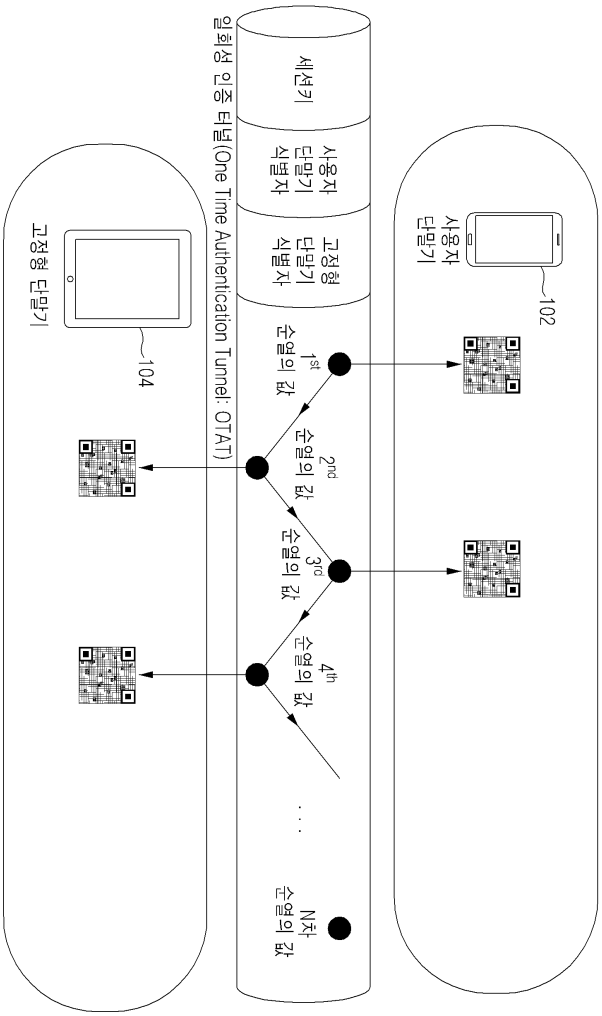
도면2


시 작
인가된 사용자의 식별정보와 서비스 및 권한정보, 사용자 단말기 정보가 저장되는 단계
210
사전 등록된 사용자 단말기에서 다중요소 인증으로 QR code를 생성하는 단계
220
인증 서버를 통해 일회성 인증 터널(One Time Authentication Tunnel:OTAT)을 생성하는 단계
230
사용자 단말기의 생성된 QR code를 고정형 단말기에 인식하는 단계
240
고정형 단말기의 원격지 공모 인증 검출 단계
250
사용자 단말기와 고정형 단말기간 일회성 인증 터널 (One Time Authentication Tunnel: OTAT)기반 핸드쉐이킹 단계
260
사용자 인증 성공에 따른 서비스 및 권한 인가 단계
270
종 료

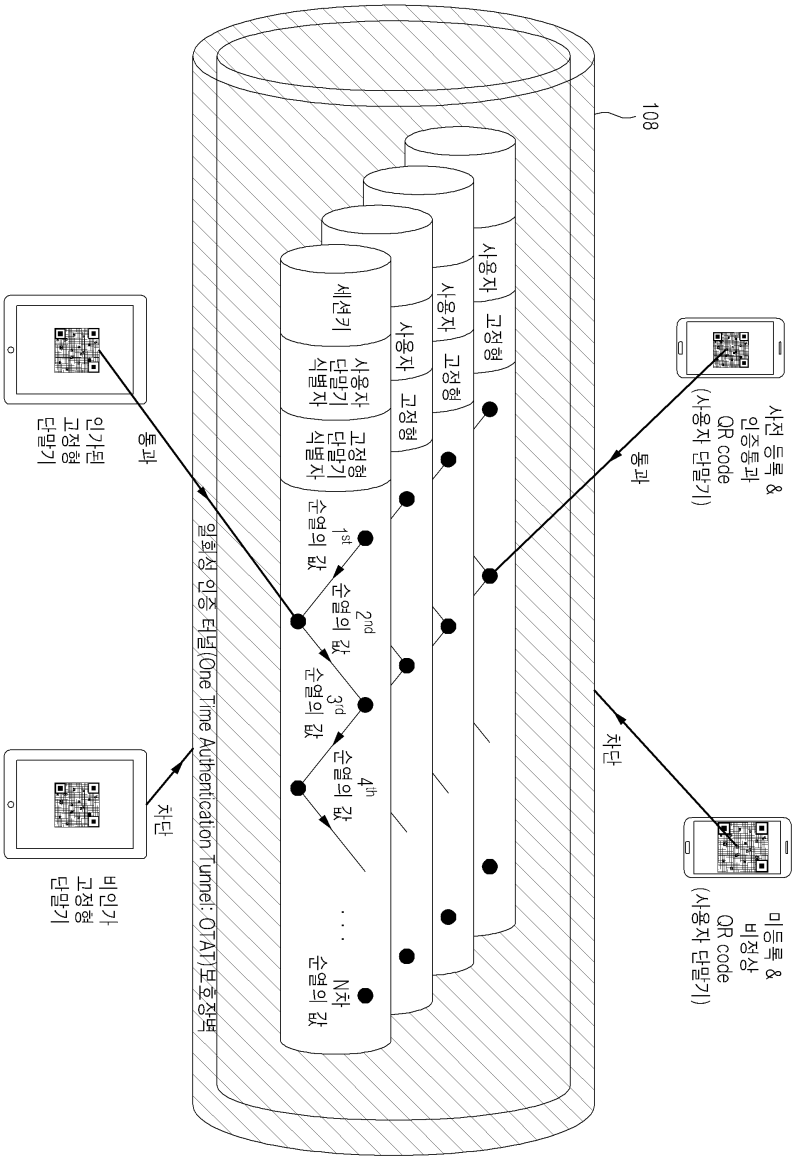
도면3


240
인증서버에서 임의(random)함수로 회전 패턴 튜플 (회전방향, 회전각도, 회전속도)을 생성하는 단계
310
고정형 단말기에서 결정된 이동 패턴 튜플(회전방향, 회전각도, 회전속도)에 따라 사용자 단말기를 회전요청 및 동화상을 촬영하는 단계
320
고정형 단말기가 촬영된 동화상으로 구분 이미지를 추출하는 단계
330
추출이미지들로부터 회전지시 이행여부, 검증된 QR code 유지여부, 사용자 단말기 화면 상의 어플리케이션 경계 유지 여부 등 원격지 공모 인증을 검증하는 단계
340
260

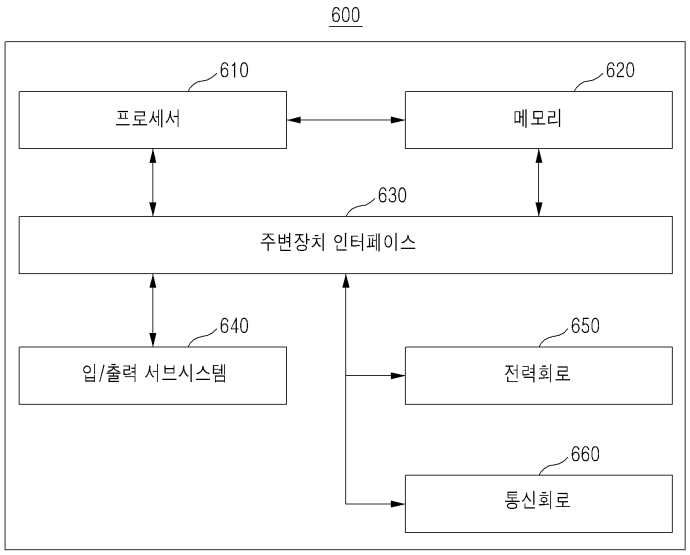
도면4


일회성 인증 터널(One Time Authentication Tunnel: OTAT)
세션키
사용자 단말기 식별자
고정형 단말기 식별자
1st 순열의 값
2nd 순열의 값
3rd 순열의 값
4th 순열의 값
N차 순열의 값
사용자 단말기
102
고정형 단말기
104

도면5


108
사용자 고정형
사용자 고정형
사용자 고정형
세션키
사용자 단말기 식별자
고정형 단말기 식별자
1st 순열의 값
2nd 순열의 값
3rd 순열의 값
4th 순열의 값
N차 순열의 값
일회성 인증 터널(One Time Authentication Tunnel: OTAT)보호장벽
사전 등록 & 인증통과 QR code (사용자 단말기)
통과
인가된 고정형 단말기
통과
차단
비인가 고정형 단말기
차단
미등록 & 비정상 QR code (사용자 단말기)

도면6


600
610
프로세서
620
메모리
630
주변장치 인터페이스
640
입/출력 서브시스템
650
전력회로
660
통신회로