

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2012년 9월 27일 (27.09.2012)



(10) 국제공개번호
WO 2012/128478 A2

- (51) 국제특허분류:
H04L 9/32 (2006.01) G06K 9/18 (2006.01)
H04W 12/06 (2009.01)
- (21) 국제출원번호: PCT/KR2012/001249
- (22) 국제출원일: 2012년 2월 20일 (20.02.2012)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2011-0024704 2011년 3월 21일 (21.03.2011) KR

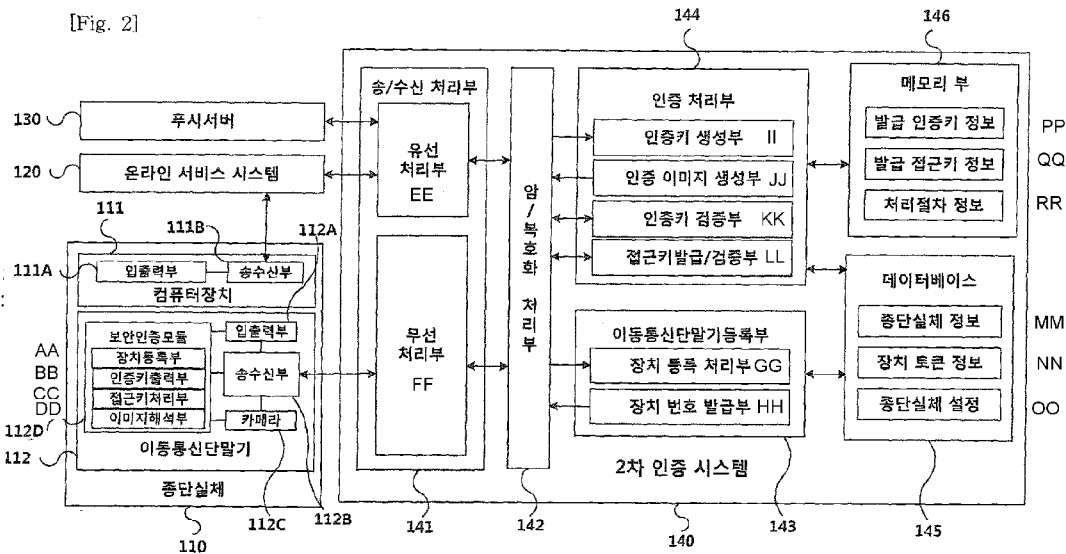
- (71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): (주) 잉카인터넷 (INCA INTERNET CO., LTD.) [KR/KR]; 서울특별시 구로구 구로3동 235-2 에이스하이엔드타워 1201호, 152-740 Seoul (KR).
- (72) 발명자; 겸
- (75) 발명자/출원인 (US 에 한하여): 정영석 (JUNG, Young Suk) [KR/KR]; 경기도 안양시 만안구 박달2동 대림한숲타운 105동 102호, 430-702 Gyeonggi-do (KR). 한형덕 (HAN, Hyung-Deok) [KR/KR]; 경기도 광명시 소하1동 소하휴먼시아 5단지 503동 1002호, 423-051 Gyeonggi-do (KR). 황재연 (HWANG, Jae Yeon) [KR/KR]; 서울특별시 동작구 상도동 509-11번지, 156-030 Seoul (KR).

[다음 쪽 계속]

(54) Title: SYSTEM AND METHOD FOR IMAGE-BASED AUTHENTICATION

(54) 발명의 명칭 : 이미지 기반 인증시스템 및 방법

[Fig. 2]



- 110 ... End entity
111 ... Computer device
111A, 112A ... Input/output unit
111B, 112B ... Transceiver unit
112 ... Mobile communication terminal
112C ... Camera
112D ... Security authentication module
AA ... Device registration unit
BB ... Authentication key display unit
CC ... Access key processing unit
DD ... Image analysis unit
120 ... Online service system
130 ... Push server
140 ... Second authentication system
141 ... Transmitting/receiving processing unit

- EE ... Wired processing unit
FF ... Wireless processing unit
142 ... Encoding/decoding processing unit
143 ... Unit for registering a mobile communication terminal
GG ... Device registration processing unit
HH ... Device number issuing unit
144 ... Authentication processing unit
II ... Authentication key generating unit
JJ ... Authentication image generating unit
KK ... Authentication key verification unit
LL ... Access key issuing/verification unit
145 ... Database
MM ... End entity information
NN ... Device token information
OO ... End entity setting
146 ... Memory unit
PP ... Issue authentication key information
QQ ... Issue access key information
RR ... Processing procedure information



(74) **대리인: 특허법인 우인 (WOON PATENT & LAW FIRM);** 서울특별시 강남구 역삼동 648-15 신원빌딩 3층, 135-911 Seoul (KR).

(81) **지정국** (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) **지정국** (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

(57) **Abstract:** The present invention relates to a system and method for image-based authentication, wherein user authentication is performed by the preregistered mobile communication terminal of a user transmitting, to an authentication server, an authentication key corresponding to an authentication image. In the image-based authentication system according to the present invention, a system for authenticating an end entity comprises a computer device for performing a first authentication through communication with an online service system and a mobile communication terminal for performing a second authentication, and includes: a unit for registering a mobile communication terminal, which registers the end entity information needed for the second authentication, and a mobile communication terminal matching the end entity information; a unit for generating an authentication key, which generates a second authentication key issued to the end entity in which the first authentication is completed; a unit for generating an authentication image, which generates an authentication image corresponding to the generated second authentication key and provides the authentication image for display on the computer device of the end entity in which the first authentication is completed through the online service system; and a unit for verifying authentication, which verifies the second authentication key received from the activated mobile communication terminal after activating the mobile communication terminal registered in the end entity in which the first authentication is completed.

(57) **요약서:** 이 발명은 사용자의 기등록된 이동통신단말기가 인증용 이미지에 대응하는 인증키를 인증서버에게 전송함으로써 사용자 인증이 이루어지도록 하는 이미지 기반 인증 시스템 및 방법에 관한 것이다. 이 발명에 따른 이미지 기반 인증 시스템은, 온라인 서비스 시스템과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 중단실체를 인증하는 시스템에 있어서, 2차 인증에 필요한 중단실체 정보와 상기 중단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록부와; 1차 인증 완료된 중단실체에 발급할 2차인증키를 생성하는 인증키생성부와; 상기 생성된 2차인증키에 대응하는 인증 이미지를 생성하고 상기 온라인 서비스 시스템을 통해 상기 1차 인증 완료된 중단실체의 컴퓨터장치에 표시되도록 제공하는 인증 이미지 생성부와; 상기 1차 인증 완료된 중단실체에 등록된 이동통신단말기를 활성화시킨 후 상기 활성화된 이동통신단말기로부터 수신되는 2차인증키를 검증하는 인증키검증부를 포함한다.

명세서

발명의 명칭: 이미지 기반 인증시스템 및 방법

기술분야

- [1] 이 발명은 인증시스템 및 방법에 관한 것으로서, 보다 상세하게는 사용자의 기등록된 이동통신단말기가 인증용 이미지에 대응하는 인증키를 인증서버에게 전송함으로써 사용자 인증이 이루어지도록 하는 이미지 기반 인증시스템 및 방법에 관한 것이다.

배경기술

- [2] 오늘날 인터넷의 발달에 힘입어 다양한 종류의 온라인 서비스가 제공되고 있다. 대부분의 온라인 서비스 시스템들은 인터넷을 통해 해당 시스템에 접근하는 클라이언트 컴퓨터장치가 해당 온라인 서비스를 이용할 자격을 가지는지 여부를 인증하고 있다.
- [3] 가장 보편적으로 사용되는 사용자 인증방법은 사용자 아이디와 비밀번호를 이용한 인증방법으로서, 사용자가 온라인 서비스 시스템에 회원으로 가입할 때 사용자 아이디와 비밀번호를 등록하고, 추후 해당 사용자가 해당 시스템에 접속하고자 할 때 기등록한 사용자 아이디와 비밀번호를 입력받아 그 사용자의 본인 여부를 검증한다.
- [4] 그러나, 이러한 아이디와 비밀번호를 이용한 인증방법은 인증 정보(사용자 아이디와 비밀번호)가 도용되거나 해킹되기 쉬우며, 인증 정보가 노출될 경우 악의적인 접근 시도를 차단할 수 없는 문제점이 있다.
- [5] 온라인 서비스 시스템에는 다양한 개인 정보들이 관리되고 있고, 최근 온라인 서비스 시스템을 통한 무형의 자산(예컨대, 온라인 게임에서의 아이템, 사이버머니 등)이 증가함에 따라, 보다 강력한 본인 인증방법들이 요구되고 있다.
- [6] 이러한 요구에 따라 상술한 사용자 아이디와 비밀번호에 의한 1차 인증 후의 다양한 2차 인증방식들이 시도되고 있는데, 특히 사용자의 이동통신단말기를 이용한 일회용 인증키 기반 2차 인증방식이 널리 사용되고 있다. 이 일회용 인증키 기반 인증방식은 통상 다음과 같은 절차로 진행된다. 먼저, 온라인 서비스 시스템은 1차 인증 절차(예컨대, 사용자 아이디와 비밀번호 확인)를 진행하고, 1차 인증 후, 2차인증서버에게 2차 인증을 요청한다. 2차인증서버는 사용자의 이동통신단말기에 일회용 인증키가 포함된 문자메시지(SMS)를 발송한다. 온라인 서비스 시스템은 사용자의 컴퓨터장치를 통해 그 일회용 인증키를 입력받아 2차인증서버에게 전달한다. 그러면 2차인증서버는 사용자의 이동통신단말기에게 발송한 일회용 인증키와 온라인 서비스 시스템을 통해 입력받은 일회용 인증키가 동일한 지를 검증함으로써,
- [7] 이러한 일회용 인증키 기반 2차인증방식은 본인 인증 보안 강도를 어느 정도 강화시킬 수는 있으나, 아래와 같은 원거리 해킹이나 근거리 해킹에 의한

취약점이 여전히 존재한다.

- [8] 즉, 원거리 해킹 기법으로서, 사용자가 일회용 인증키를 온라인 서비스 시스템으로 전송할 때 해커가 네트워크 스누핑을 통해 일회용 인증키를 가로채거나, 해커가 사용자의 컴퓨터장치에 미리 키로거를 설치하고 원격에서 사용자의 컴퓨터장치에 입력되는 일회용 인증키를 모니터링하여 빼내거나, 사용자가 온라인 서비스 시스템이 아닌 피싱사이트에 접속하도록 유도하여 피싱사이트로 입력되는 일회용 인증키를 갈취하는 방법 등을 통해 인증키가 갈취될 수 있다. 예로서, 2006년 7월 미국의 한 은행에서 원거리 해킹 기법인 피싱사이트를 통해 갈취한 인증키로 은행 계좌에 침투한 사례가 있다.
- [9] 또한, 근거리 해킹 기법으로서, 사용자 근처에서 숄더서핑(shoulder surfing)이나 사회공학(social engineering) 등의 기법을 통해 사용자의 이동통신단말기에 전송된 일회용 인증키를 알아내어 도용하기도 한다.
- [10] 따라서, 일회용 인증키를 이용한 2차 인증방식으로서, 원거리 해킹 기법이나 근거리 해킹 기법 등에 의해 해커에게 일회용 인증키가 갈취되더라도, 이에 저항할 수 있는 보다 강력한 본인 인증기술이 필요하다.

발명의 상세한 설명

기술적 과제

- [11] 상술한 종래기술의 필요성을 충족시키기 위하여 안출된 이 발명의 목적은, 1차인증이 완료된 컴퓨터장치에 대응되어 기등록된 이동통신단말기로부터 이미지 기반 인증키를 입력받아 기등록된 인증키와 비교하여 사용자 인증을 함으로써, 원거리 해킹 기법 또는 근거리 해킹 기법을 통한 일회용 인증키 갈취에 저항할 수 있는 이미지 기반 인증시스템 및 방법을 제공하기 위한 것이다.

과제 해결 수단

- [12] 상술한 목적을 달성하기 위한 이 발명의 제1실시예에 따른 이미지 기반 인증 시스템은, 온라인 서비스 시스템과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 종단실체를 인증하는 시스템에 있어서, 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록부와; 1차 인증 완료된 종단실체에 발급할 2차인증키를 생성하는 인증키생성부와; 상기 생성된 2차인증키에 대응하는 인증 이미지를 생성하고 상기 온라인 서비스 시스템을 통해 상기 1차 인증 완료된 종단실체의 컴퓨터장치에 표시되도록 제공하는 인증 이미지 생성부와; 상기 1차 인증 완료된 종단실체에 등록된 이동통신단말기를 활성화시킨 후 상기 활성화된 이동통신단말기로부터 수신되는 2차인증키를 검증하는 인증키검증부를 포함한 것을 특징으로 한다.
- [13] 또한, 이 발명의 제1실시예에 따른 이미지 기반 인증 방법은, 온라인 서비스

시스템과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 종단실체를 인증하는 방법에 있어서, 2차인증시스템이 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록단계와; 상기 온라인 서비스 시스템으로부터 상기 종단실체의 2차 인증이 요청되면, 상기 2차인증시스템이 1차 인증 완료된 종단실체에 발급할 2차인증키를 생성하는 인증키생성단계와; 상기 2차인증시스템이 상기 생성된 2차인증키에 대응하는 인증 이미지를 생성하고 상기 온라인 서비스 시스템을 통해 상기 1차 인증 완료된 종단실체의 컴퓨터장치에 표시되도록 제공하는 인증 이미지 생성단계와; 상기 2차인증시스템이 상기 인증 이미지 생성단계 후 상기 1차 인증 완료된 종단실체에 등록된 이동통신단말기를 활성화시키고 상기 활성화된 이동통신단말기로부터 수신되는 2차인증키를 검증하는 인증키검증단계를 포함한 것을 특징으로 한다.

- [14] 또한, 이 발명의 제2실시예에 따른 이미지 기반 인증 시스템은, 온라인 서비스 시스템과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 종단실체를 인증하는 시스템에 있어서, 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록부와; 상기 이동통신단말기등록부에 등록된 상기 이동통신단말기를 통해 인증이미지를 수신하는 인증이미지수신부와; 상기 수신된 인증이미지로부터 2차인증키를 생성하여 저장하고 상기 이동통신단말기에게 발급하여 저장되도록 하는 인증키생성발급부와; 1차 인증 완료된 종단실체에 등록된 이동통신단말기를 활성화시킨 후 상기 활성화된 이동통신단말기로부터 기저장된 2차인증키를 수신하여 검증하는 인증키검증부를 포함한 것을 특징으로 한다.

- [15] 또한, 이 발명의 제2실시예에 따른 이미지 기반 인증 방법은, 온라인 서비스 시스템과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 종단실체를 인증하는 방법에 있어서, 2차인증시스템이 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록단계와; 상기 2차인증시스템이 상기 이동통신단말기등록부에 등록된 상기 이동통신단말기를 통해 인증이미지를 수신하는 인증이미지수신단계와; 상기 2차인증시스템이 상기 수신된 인증이미지로부터 2차인증키를 생성하여 저장하고 상기 이동통신단말기에게 발급하여 저장되도록 하는 인증키생성발급단계와; 상기 온라인 서비스 시스템으로부터 상기 종단실체의 2차 인증이 요청되면, 상기 2차인증시스템이 1차 인증 완료된 종단실체에 등록된 이동통신단말기를 활성화시키고 상기 활성화된 이동통신단말기로부터 기저장된 2차인증키를 수신하여 검증하는 인증키검증단계를 포함한 것을 특징으로 한다.

발명의 효과

- [16] 이상과 같이 이 발명에 따르면 1차 인증이 완료된 컴퓨터장치와 매칭되어 등록된 이동통신단말기로부터 이미지 기반 인증키를 입력받아 사용자에게 대한 2차 인증을 하기 때문에, 인증 보안이 더욱 강화되는 효과가 있다.

도면의 간단한 설명

- [17] 도 1은 이 발명에 따른 이미지 기반 인증시스템의 개략적인 구성 블록도이다.
 [18] 도 2는 이 발명의 제1실시예에 따른 이미지 기반 인증시스템의 상세 구성 블록도이다.
 [19] 도 3은 이 발명의 제1실시예에 따른 이미지 기반 인증시스템의 이동통신단말기의 동작을 도시한 동작 흐름도이다.
 [20] 도 4는 이 발명의 제1실시예에 따른 이미지 기반 인증시스템의 2차인증시스템의 동작을 도시한 동작 흐름도이다.
 [21] 도 5는 이 발명의 제2실시예에 따른 이미지 기반 인증시스템의 상세 구성 블록도이다.
 [22] 도 6은 이 발명의 제2실시예에 따른 이미지 기반 인증시스템 이동통신단말기에서의 등록 및 2차인증키 발급 과정을 도시한 동작 흐름도이다.
 [23] 도 7은 이 발명의 제2실시예에 따른 이미지 기반 인증시스템 2차인증시스템에서의 등록 및 2차인증키 발급 과정을 도시한 동작 흐름도이다.
 [24] 도 8은 이 발명의 제2실시예에 따른 이미지 기반 인증시스템 이동통신단말기에서의 2차 인증 과정을 도시한 동작 흐름도이다.
 [25] 도 9는 이 발명의 제2실시예에 따른 이미지 기반 인증시스템 2차인증시스템에서의 2차 인증 과정을 도시한 동작 흐름도이다.
 [26] [부호의 설명]
 [27] 110 : 종단실체 111 : 컴퓨터장치
 [28] 112 : 이동통신단말기 120 : 온라인 서비스 시스템
 [29] 130 : 푸시서버 140 : 2차인증시스템
 [30] 141 : 송수신처리부 142 : 암호호화 처리부
 [31] 143 : 이동통신단말기등록부 144 : 인증처리부
 [32] 145 : 데이터베이스 146 : 메모리부

발명의 실시를 위한 최선의 형태

- [33] 이하, 첨부된 도면을 참조하여 이 발명에 따른 이미지 기반 인증시스템 및 방법을 보다 상세하게 설명한다.
 [34] 도 1은 이 발명에 따른 이미지 기반 인증시스템의 개략적인 구성 블록도이다.
 [35] 종단실체(110)는 이 발명을 통한 인증 절차를 이용하는 최종 사용자이다. 이 종단실체(110)는 통신망(100)을 통해 온라인 서비스 시스템(120)에서 온라인 서비스를 제공받기 위해 이 발명에 따른 인증 절차를 이용한다. 종단실체(110)는 온라인 서비스 시스템(120)의 온라인 서비스를 제공받고 온라인 서비스

시스템(120)과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치(111)와, 이 발명에 따른 2차 인증을 수행하기 위한 이동통신단말기(112)를 포함한다. 컴퓨터장치(111)는 데스크탑, 노트북과 같은 다양한 컴퓨터 환경을 포함한다. 이동통신단말기(112)는 운영체제(OS)를 탑재하고 다양한 어플리케이션(응용프로그램)의 설치 및 구동이 가능한 스마트폰인 것이 바람직하다. 이 발명을 구현하기 위한 컴퓨터장치(111)와 이동통신단말기(112)의 내부 상세 구성은 후술하기로 한다.

[36] 온라인 서비스 시스템(120)은 통신망(100)을 통해 다수의 사용자들에게 온라인 서비스를 제공하는 웹 상의 시스템으로서, 종단실체(110)에 대한 1차 인증을 수행한다. 통상적으로 온라인 서비스 시스템(120)은 로그인 처리 시스템(121)을 구비하고, 이 로그인 처리 시스템(121)에서 종단실체(110)에 대한 1차 인증을 수행한다. 1차 인증은 지식기반인증, 소유기반인증, 존재(신체)기반인증 등의 모든 단일요소인증(Single Factor Authentication) 형태를 포함한다.

[37] 푸시(PUSH)서버(130)는 종단실체(110)의 이동통신단말기(112)의 제조업체에서 제공하는 서비스이다. 이동통신단말기(112)는 임의의 어플리케이션에 대해 푸시서비스를 제공받고자 할 경우, 먼저 푸시서버(130)로부터 해당 어플리케이션에 대응하는 장치토큰을 발급받는다. 그러면, 푸시서버(130)는 이동통신단말기(112)에 푸시메시지를 전송하여 이동통신단말기(112)를 깨우고(wakeup), 해당 토큰장치에 대응되는 어플리케이션(이 발명에서는 보안인증모듈)을 활성화시키는 역할을 수행한다. 이동통신단말기(112)가 푸시(PUSH)서버로부터 장치토큰을 발급받는 것에 대한 상세한 설명은 후술하기로 한다. 푸시서버(130)의 예로서, iOS 계열은 애플사에서 제공하는 APNs(Apple Push Notification Service)를 푸시서버로 사용하고, 안드로이드 계열은 구글사에서 제공하는 C2DM(Cloud To Device Messaging)을 푸시서버로 사용한다.

[38] 2차인증시스템(140)은 1차 인증이 완료된 종단실체(110)에 대해 온라인 서비스 시스템(120)으로부터 2차 인증이 요청되면, 종단실체(110)의 장치토큰을 이용하여 기등록된 이동통신단말기(112)를 깨우면서 이동통신단말기(112)에 설치된 보안인증모듈을 활성화시키고, 그 이동통신단말기(112)로부터 2차인증키를 입력받아 2차 인증 절차를 수행한다. 이 발명의 명세서에서는 2차 인증 절차로서, 2가지 실시예를 제안한다.

[39] 제1실시예에 따른 2차 인증 절차를 간략하게 설명하면, 2차인증시스템(140)은 1차 인증 정보에 대응하는 종단실체(110)의 이동통신단말기(112)를 등록한다. 온라인 서비스 시스템(120)으로부터 2차 인증이 요청되면, 2차인증시스템(140)은 2차인증키를 발급하고 그 발급된 2차인증키에 대응하는 인증 이미지를 생성하여 종단실체(110)의 컴퓨터장치(111)에 표시되도록 하며 기등록된 이동통신단말기(112)를 통해 상기 인증 이미지에 기반한 2차인증키를 입력받는다. 2차인증시스템(140)은 이동통신단말기(112)를 통해 입력되는

- 2차인증키와 기발급된 2차인증키를 비교하여 사용자 인증을 수행한다.
- [40] 도 2는 이 발명의 제1실시예에 따른 이미지 기반 인증시스템의 상세 구성 블록도이다.
- [41] 이 발명에 따른 종단실체(110)의 컴퓨터장치(111)는 입출력부(111A)와, 송수신부(111B)를 포함한다. 입출력부(111A)는 통상적인 키보드, 마우스, 모니터 등으로서, 사용자와의 인터페이스를 수행한다. 송수신부(111B)는 유선 통신망을 통해 온라인 서비스 시스템(120)과 접속한다. 컴퓨터장치(111)는 2차인증시스템(140)으로부터 인증 이미지를 입력받아 입출력부(111A)의 화면에 출력한다.
- [42] 이 발명에 따른 종단실체(110)의 이동통신단말기(112)는 입출력부(112A)와, 송수신부(112B)와, 카메라(112C)와, 보안인증모듈(112D)을 포함한다. 입출력부(112A)는 통상적인 터치패드 등으로서, 사용자와의 인터페이스를 수행한다. 송수신부(112B)는 이동 통신망을 통해 푸시서버(130) 및 2차인증시스템(140)과 접속한다. 카메라(112C)는 이동통신단말기 사용자의 조작에 따라 영상(이미지)을 촬영하여 이미지 데이터를 획득한다.
- [43] 보안인증모듈(112D)은 푸시서버(130)로부터 2차인증시스템(140)과의 통신을 위한 장치토큰을 발급받고 그 발급된 장치토큰을 2차인증시스템(140)에 등록하는 장치등록부와, 푸시서버(130)로부터 전달된 푸시메시지에 의해 실행되어 상기 컴퓨터장치(111)의 화면에 표시된 인증 이미지를 기반한 2차인증키를 2차인증시스템(140)에게 전송하는 인증키출력부를 포함한다.
- [44] 또한, 보안인증모듈(112D)은 푸시서버(130)로부터 푸시메시지와 함께 전달되는 접근키를 이용하여 상기 2차인증시스템(140)에 접근하는 접근키처리부를 더 포함할 수 있으며, 이 접근키처리부는 암호화된 접근키를 복호화하는 기능을 추가적으로 포함할 수도 있다. 즉, 2차인증시스템(140)은 이동통신단말기(112)에게 푸시메시지와 함께 접근키를 암호화하여 전송하고, 접근키처리부는 암호화된 접근키를 복호화하여 복호화된 접근키를 이용하여 2차인증시스템(140)에 접근한다. 2차인증시스템(140)은 이동통신단말기(112)로부터 입력되는 접근키를 이용하여 해당 접근을 시도하는 이동통신단말기(112)의 접근 권한을 검증한다.
- [45] 보안인증모듈(112D)의 인증키출력부는 입출력부(112A)를 통해 직접 입력되는 2차인증키를 2차인증시스템(140)에게 출력할 수 있다. 즉, 인증 이미지는 그림, 숫자, 문자를 포함한 이미지이고, 사용자가 입출력부(112A)를 이용하여 해당 인증 이미지에 포함된 그림의 이름(예컨대, 코끼리, 해바라기, 우산 등과 같은 동,식물 또는 사물의 이름)이나, 인증 이미지에 포함된 숫자와 문자를 직접 입력하도록 할 수 있다.
- [46] 또한, 보안인증모듈(112D)은 카메라(112C)를 통해 입력되는 인증 이미지 데이터를 해석하여 자동으로 2차인증키를 추출하는 이미지해석부를 더 포함할 수 있다. 즉, 이 인증 이미지는 이차원 바코드이고, 이미지해석부는 바코드

해석부일 수 있다. 이차원 바코드는 QR 코드(Quick Response Code), PDF417, 데이터 매트릭스(Data Matrix), 맥시 코드(Maxi code) 등이 포함된다.

- [47] 이 발명에 따른 온라인 서비스 시스템(120)은 종단실체(110)의 1차 인증에 필요한 정보를 저장하고, 1차 인증이 완료된 종단실체(110)에 대해 2차인증시스템(140)에게 2차 인증을 요청하고, 2차인증시스템(140)으로부터 인증 이미지를 입력받아 그 인증 이미지가 포함된 웹페이지를 종단실체(110)의 컴퓨터장치(111)에게 제공한다.
- [48] 이 발명에 따른 2차인증시스템(140)은 종단실체(110)와 온라인 서비스 시스템(120)과 푸시서버(130)와의 데이터 송수신을 위한 송수신처리부(141)와, 송수신되는 데이터를 암호화 또는 복호화하는 암호화 처리부(142)와, 종단실체(110) 정보와 이동통신단말기(112)의 장치토큰을 매칭하여 등록하는 이동통신단말기등록부(143)와, 1차 인증 완료된 종단실체(110)에 발급할 2차인증키를 생성하고 2차인증키에 대응하는 인증 이미지를 생성하여 온라인 서비스 시스템(120)을 통해 종단실체(110)의 컴퓨터장치(111)에게 제공하고 1차 인증 완료된 종단실체(110)의 이동통신단말기(112)로부터 상기 인증 이미지에 대응하는 2차인증키를 입력받아 검증하는 인증 처리부(144)와, 종단실체 정보와 장치토큰 정보와 각 종단실체별 설정사항을 저장하는 데이터베이스(145)와, 인증 처리부(144)에서 발급된 2차인증키 정보와 처리절차 정보 등을 저장한 메모리부(146)를 포함한다.
- [49] 여기서, 송수신처리부(141)는 유선 통신망을 통해 온라인 서비스 시스템(120) 및 푸시서버(130)와 통신하는 유선처리부와, 무선 통신망을 통해 이동통신단말기(112)와 통신하는 무선처리부를 포함한다.
- [50] 이동통신단말기등록부(143)는 각 이동통신단말기(112)에 대해 장치 등록을 처리하는 장치등록처리부와, 등록된 이동통신단말기에 대해 번호를 발급하는 장치번호발급기를 포함한다.
- [51] 인증 처리부(144)는 1차 인증 완료된 종단실체(110)에게 발급할 2차인증키를 생성하는 인증키생성부와, 상기 2차인증키에 대응하는 인증 이미지를 생성하여 온라인 서비스 시스템(120)에게 제공하여 상기 1차 인증 완료된 종단실체(110)의 컴퓨터장치(111)에 표시되도록 하는 인증 이미지 생성부와, 상기 1차 인증 완료된 종단실체(110)의 기등록된 이동통신단말기(112)로부터 입력되는 2차인증키와 상기 인증키생성부에서 생성된 2차인증키를 비교하여 검증하는 인증키검증부를 포함한다. 또한, 인증 처리부(144)는 상기 1차 인증 완료된 종단실체(110)의 기등록된 이동통신단말기(112)에 접근키를 발급하고 상기 이동통신단말기(112)로부터 입력되는 접근키와 발급한 접근키를 비교하여 이동통신단말기(112)를 검증하는 접근키 발급/검증부를 더 포함하고, 상기 메모리부(146)는 이동통신단말기(112)에게 발급된 발급 접근키 정보를 더 저장한다.

[52]

- [53] 도 3은 이 발명의 제1실시예에 따른 이미지 기반 인증시스템의 이동통신단말기의 동작을 도시한 동작 흐름도이다.
- [54] 이동통신단말기(112)의 보안인증모듈(112D)은 이동통신단말기(112)에 탑재된 운영체제를 기반으로 제작되어, 이 발명에 따른 인증 절차를 수행하는 응용프로그램(어플리케이션)이다.
- [55] 먼저, 종단실체의 이동통신단말기(112)에 보안인증모듈(112D)을 설치한다(S301). 이 보안인증모듈(112D)은 인증 수행을 위한 종단실체 정보(온라인 서비스 시스템에 접속하기 위한 사용자 아이디, 이동통신단말기의 시스템 정보 등)를 2차인증시스템(140)에게 전송하고, 이로써 2차인증시스템(140)은 이동통신단말기(112)를 통해 종단실체 정보를 수집한다(S302).
- [56] 2차인증시스템(140)은 수집된 종단실체 정보를 확인하고, 이동통신단말기 자체에 대한 실명인증 및 본인인증을 수행하고, 그 결과를 이동통신단말기(112)에게 전송한다. 2차인증시스템(140)으로부터 실명인증 및 본인인증 실패 결과가 수신되면(S303), 이동통신단말기의 보안인증모듈(112D)은 장치 등록 실패로 인식하고 종료한다(S304).
- [57] 한편, 2차인증시스템(140)으로부터 이동통신단말기(112)에 대한 실명인증 및 본인인증 성공 결과가 수신되면(S303), 이동통신단말기의 보안인증모듈(112D)은 푸시서버(130)에 접속하여 보안인증모듈의 인증서와 이동통신단말기 고유정보를 푸시서버에게 전송하면서 장치토큰 발급을 요청한다(S305).
- [58] 이동통신단말기의 보안인증모듈(112D)은 푸시서버(130)로부터 장치토큰이 발급되면(S306), 그 발급된 장치토큰을 2차인증시스템에게 전달한다(S307). 그러면 2차인증시스템(140)은 해당 종단실체 정보와 함께 이동통신단말기(112)의 장치토큰을 데이터베이스에 등록한다.
- [59] 이러한 환경에서, 푸시서버로부터 푸시메시지가 수신되면(S308), 이동통신단말기는 깨어나서 보안인증모듈(112D)을 활성화시킨다(S309). 그리고, 암호화된 접근키가 수신되면(S310), 이동통신단말기의 보안인증모듈(112D)은 암호화된 접근키를 복호화한다(S311). 사용자로부터 2차인증정보가 입력되면(S312), 보안인증모듈(112D)은 2차인증정보로부터 2차인증키를 추출하고(S313), 단계 S311에서 복호화한 접근키로 2차인증시스템에 접근하여 2차인증시스템에게 2차인증키를 전송한다(S314).
- [60] 상기 2차인증정보는 종단실체의 컴퓨터장치의 화면에 표시된 인증 이미지를 촬영한 인증 이미지 데이터일 수 있으며, 보안인증모듈(112D)은 인증 이미지 데이터를 해석하여 2차인증키를 추출한다. 특히, 인증 이미지는 이차원 바코드이다. 또는, 2차인증정보는 이동통신단말기의 입출력부를 통해 직접 입력되는 값이며, 보안인증모듈(112D)은 입력값에서 2차인증키를 추출한다.
- [61]

- [62] 도 4는 이 발명의 제1실시예에 따른 이미지 기반 인증시스템의 2차인증시스템의 동작을 도시한 동작 흐름도이다.
- [63] 먼저, 보안인증모듈이 설치된 이동통신단말기가 도 3의 단계 S302를 수행하면, 2차인증시스템은 2차 인증에 필요한 종단실체 정보(예컨대, 온라인 서비스 시스템에 접속하기 위한 사용자 아이디와 이동통신단말기의 시스템 정보 등)를 수집하고 수집된 종단실체 정보를 확인하며 이동통신단말기 자체에 대해 실명인증 및 본인인증을 수행하고, 그 결과(인증 성공/실패)를 이동통신단말기에게 전송하고, 인증 성공한 이동통신단말기로부터 그의 장치토큰을 입력받아 등록한다.
- [64] 이러한 환경에서, 종단실체 컴퓨터장치가 온라인 서비스 시스템에 접근하면, 온라인 서비스 시스템은 이 종단실체 컴퓨터장치에 대해 1차 인증을 수행한다. 이때, 컴퓨터장치는 인증에 필요한 종단실체 정보를 온라인 서비스 시스템에게 전송한다. 1차 인증에 성공하면, 온라인 서비스 시스템은 종단실체 정보를 2차인증시스템에게 전달하며 2차 인증을 요청한다.
- [65] 2차인증시스템은 온라인 서비스 시스템으로부터 종단실체 정보가 입력되면서 2차 인증이 요청되면(S401), 수신된 종단실체 정보에 대응하여 이동통신단말기가 등록되어 있는지를 확인한다(S402).
- [66] 이동통신단말기가 등록되어 있으면(S403), 2차인증시스템은 2차인증키를 생성하여 저장하고, 생성된 2차인증키에 대응하는 인증 이미지를 생성하여 온라인 서비스 시스템을 통해 1차 인증이 완료된 종단실체 컴퓨터장치에 표시한다(S404). 이때, 2차인증키에 대응하는 인증 이미지는 2차인증키 정보를 포함한 이차원 바코드 이미지일 수 있다. 2차인증키는 중복 발급을 방지하기 위해, 협정시계시(Universal Time Clock, UTC)를 기반으로 타임스탬프를 생성하고 그 타임스탬프와 종단실체 정보를 시드값으로 하여 생성한다.
- [67] 2차인증시스템은 접근키를 생성하고 저장하며 암호화한다(S405).
- [68] 2차인증시스템은 1차 인증에 성공한 종단실체에 기등록된 이동통신단말기의 장치토큰을 이용하여 이동통신단말기의 보안인증모듈(112D)을 활성화시키고 암호화된 접근키를 이동통신단말기에게 발급하기 위한 메시지를 푸시서버에게 전달한다(S406).
- [69] 이 푸시서버는 2차인증시스템으로부터 전달받은 장치토큰으로부터 메시지를 전달할 이동통신단말기를 파악하고, 해당 이동통신단말기에 푸시 메시지를 전달하여 보안인증모듈을 활성화시키고, 암호화된 접근키를 보안인증모듈에게 전달한다.
- [70] 그러면, 이동통신단말기는 암호화된 접근키를 복호화하고 사용자로부터 2차인증정보를 입력받을 준비를 하며, 사용자로부터 2차인증정보를 입력받고 이로부터 2차인증키를 추출하여, 복호화된 접근키와 2차인증키를 2차인증시스템에게 전송한다. 이로써, 2차인증시스템은 이동통신단말기로부터 접근키와 2차인증키를 수신한다(S407). 2차인증시스템은 단계 S407에서 수신한

접근키와 단계 S405에서 생성하여 이동통신단말기에게 발급한 접근키를 비교한다(S408). 단계 S408의 비교 결과 두 접근키가 일치하면, 2차인증시스템은 단계 S407에서 수신한 2차인증키와 단계 S404에서 저장한 2차인증키를 비교한다(S409). 단계 S409의 비교 결과 두 2차인증키가 일치하면, 2차인증시스템은 인증을 승인 처리하고(S410), 온라인 서비스 시스템에게 그 결과를 전송한다(S411).

- [71] 한편, 단계 S408의 비교 결과 두 접근키가 일치하지 않거나, 단계 S409의 비교 결과 두 2차인증키가 일치하지 않으면, 2차인증시스템은 인증을 실패 처리하고(S412), 온라인 서비스 시스템에게 그 결과를 전송한다(S411). 한편, 단계 S403에서 이동통신단말기가 등록되어 있지 않으면 미등록 이동통신단말로 처리하고(S413), 그 처리 결과를 온라인 서비스 시스템에 통보한다(S411).

[72]

발명의 실시를 위한 형태

- [73] 제2실시예에 따른 2차 인증 절차를 간략하게 설명하면, 2차인증시스템(140)은 1차 인증 정보에 대응하는 종단실체(110)의 이동통신단말기(112)를 등록하는데, 이때 이동통신단말기(112)로부터 입력되는 임의의 이미지로부터 2차인증키를 생성하여 저장하고, 이동통신단말기(112)에게 발급한다. 이동통신단말기(112)는 사용자로부터 인증키저장비밀번호(핀번호)를 입력받아 2차인증시스템(140)으로부터 발급된 2차인증키를 암호화한 후 저장한다. 이 후, 온라인 서비스 시스템(120)으로부터 2차 인증이 요청되면 이동통신단말기(112)는 사용자로부터 인증키저장비밀번호를 입력받아 암호화되어 저장된 2차인증키를 복호화한 후 2차인증시스템(140)에게 전송하고, 2차인증시스템(140)은 2차 인증 요청시 이동통신단말기(112)로부터 입력되는 2차인증키와 기저장된 2차인증키를 비교하여 사용자 인증을 수행한다.

- [74] 도 5는 이 발명의 제2실시예에 따른 이미지 기반 인증시스템의 상세 구성 블록도이다.

- [75] 제2실시예에 따른 이미지 기반 인증시스템을 구성하는 종단실체의 컴퓨터장치와 온라인 서비스 시스템 및 푸시서버는 제1실시예에 따른 이미지 기반 인증시스템을 구성하는 종단실체의 컴퓨터장치와 온라인 서비스 시스템 및 푸시서버와 각각 동일하다. 다만, 이 제1실시예의 온라인 서비스 시스템은 2차인증시스템에게 종단실체에 대한 2차인증을 요청한 후, 2차인증시스템으로부터 인증이미지를 수신받아 종단실체의 컴퓨터장치에 표시되도록 하였지만, 제2실시예에서는 이러한 과정이 생략된다. 또한, 제1실시예의 2차인증시스템에서 발급되는 2차인증키는 일회용 인증키의 성질이 강하기 때문에 메모리부에 저장되지만, 제2실시예의 2차인증시스템에서 발급되는 2차인증키는 지속적으로 사용가능한 인증키이므로 데이터베이스의 종단실체정보의 한 항목으로서 저장되는 것이 바람직하다. 제1실시예에 따른

이미지 기반 인증시스템과 제2실시에 따른 이미지 기반 인증시스템은 종단실체의 이동통신단말기의 보안인증모듈과, 2차인증시스템의 인증처리부의 내부 구성상 차이점이 있다. 그 차이점을 중심으로 설명한다.

- [76] 제2실시에 따른 이동통신단말기는 통상적인 입출력부와 송수신부와 카메라와 저장부와 이 발명에 따른 이미지 기반 인증을 수행하기 위한 보안인증모듈(510)을 포함한다. 저장부는 이동통신단말기에 통상적으로 장착되는 USIM 카드(universal subscriber identity module card) 또는 내부 메모리일 수 있다.
- [77] 보안인증모듈(510)은 푸시서버로부터 2차인증시스템과의 통신을 위한 장치토큰을 발급받고 그 발급된 장치토큰을 2차인증시스템에 등록하고 카메라에서 촬영된 임의의 인증 이미지를 2차인증시스템에 전송한 후 상기 2차인증시스템으로부터 상기 인증 이미지에 대응하는 2차인증키를 발급받는 장치등록부(511)와, 상기 장치등록부(511)에서 발급받은 2차인증키를 사용자로부터 입력되는 인증키저장비밀번호로 암호화하여 그 암호화된 2차인증키를 저장부에 저장하고 푸시서버로부터 전달된 푸시메시지에 의해 실행되어 상기 저장부로부터 상기 암호화된 2차인증키를 읽어 사용자로부터 입력되는 인증키저장비밀번호로 복호화하여 상기 2차인증시스템에게 전송하는 인증키처리부(512)를 포함한다.
- [78] 또한, 보안인증모듈(510)은 푸시서버로부터 푸시메시지와 함께 전달되는 접근키를 이용하여 상기 2차인증시스템에 접근하는 접근키처리부(513)를 더 포함할 수 있으며, 이 접근키처리부(513)는 암호화된 접근키를 복호화하는 기능을 추가적으로 포함할 수도 있다. 즉, 2차인증시스템은 암호화된 접근키를 이동통신단말기에게 발급하며, 접근키처리부(513)는 이 암호화된 접근키를 복호화한 후 복호화된 접근키를 이용하여 2차인증시스템에 접근한다.
- [79] 이 발명의 제2실시에 따른 2차인증시스템의 인증처리부(520)는 이동통신단말기로부터 인증이미지를 수신하는 인증이미지수신부(521)와, 상기 수신된 인증이미지로부터 2차인증키를 생성하여 저장하고 이동통신단말기에게 발급하는 인증키생성발급부(522)와, 1차 인증 완료된 종단실체의 기등록된 이동통신단말기로부터 입력되는 2차인증키와 상기 이동통신단말기에게 발급한 2차인증키를 비교하여 검증하는 인증키검증부(523)를 포함한다. 또한, 인증처리부(520)는 상기 1차 인증 완료된 종단실체의 기등록된 이동통신단말기에 암호화된 접근키를 발급하고 상기 이동통신단말기로부터 입력되는 접근키와 발급한 접근키를 비교하여 이동통신단말기를 검증하는 접근키 발급/검증부(524)를 더 포함한다.
- [80] 즉, 제2실시에 따른 인증 기술은, 2차인증시스템이 이동통신단말기를 등록하는 과정에서, 사용자가 이동통신단말기의 카메라를 이용하여 촬영한 인증 이미지 데이터로부터 2차인증키를 생성하여 저장하고 이동통신단말기에게 발급한다. 이동통신단말기는 사용자로부터

인증키저장비밀번호를 입력받아 그 입력된 인증키저장비밀번호로 2차인증키를 암호화하고 그 암호화된 2차인증키를 저장부에 저장한다. 그 후, 사용자가 온라인 서비스 시스템을 이용하기 위해 2차인증을 할 때마다 이동통신단말기는 사용자로부터 인증키저장비밀번호를 다시 입력받아 암호화된 2차인증키를 복호화한 후 2차인증시스템에게 제공한다.

- [81] 이러한 제2실시에 따르면 사용자가 촬영한 인증 이미지 데이터로부터 2차인증키를 생성하여 발급하기 때문에, 2차인증키의 중복 발급을 원천적으로 방지할 수 있다. 또한, 2차 인증을 할 때마다 온라인 서비스 시스템이나 이동통신단말기에게 일회용 2차 인증키를 발급할 필요가 없다.
- [82]
- [83] 도 6은 이 발명의 제2실시에 따른 이미지 기반 인증시스템 이동통신단말기에서의 등록 및 2차인증키 발급 과정을 도시한 동작 흐름도이고, 도 7은 이 발명의 제2실시에 따른 이미지 기반 인증시스템 2차인증시스템에서의 등록 및 2차인증키 발급 과정을 도시한 동작 흐름도이다.
- [84] 도 6과 도 7을 참조하면서 이동통신단말기와 2차인증시스템을 통한 장치 등록 및 2차인증키 발급 과정을 살펴본다.
- [85] 먼저, 종단실체의 이동통신단말기에 보안인증모듈(510)을 설치한다(S601). 이 보안인증모듈(510)은 인증 수행을 위한 종단실체 정보(온라인 서비스 시스템에 접속하기 위한 사용자 아이디, 이동통신단말기의 시스템 정보 등)를 2차인증시스템에게 전송한다(S602).
- [86] 2차인증시스템은 이동통신단말기로부터 인증 수행을 위한 종단실체 정보(온라인 서비스 시스템에 접속하기 위한 사용자 아이디, 이동통신단말기의 시스템 정보 등)이 수신되면(S701), 해당 이동통신단말기 자체에 대한 실명인증 및 본인인증을 수행하고(S702), 그 결과를 이동통신단말기에게 전송한다(S703).
- [87] 이동통신단말기는 2차인증시스템으로부터 실명인증 및 본인인증 실패 결과가 수신되면(S603), 장치 등록 실패로 인식하고 종료한다(S604).
- [88] 2차인증시스템으로부터 이동통신단말기에 대한 실명인증 및 본인인증 성공 결과가 수신되면(S603), 이동통신단말기의 보안인증모듈은 푸시서버에 접속하여 보안인증모듈의 인증서와 이동통신단말기 고유정보를 푸시서버에게 전송하면서 장치토큰 발급을 요청한다(S605).
- [89] 이동통신단말기의 보안인증모듈(510)은 푸시서버로부터 장치토큰이 발급되면(S606), 그 발급된 장치토큰을 2차인증시스템에게 전달한다(S607). 2차인증시스템은 이동통신단말기로부터 장치토큰이 수신되면(S704), 해당 종단실체 정보와 함께 이동통신단말기의 장치토큰을 데이터베이스에 등록한다(S705).
- [90] 장치토큰 등록 후, 이동통신단말기의 보안인증모듈(510)은 사용자에게 인증이미지 촬영 요청을 하고(S608), 인증이미지 데이터가 입력되면(S609) 그 인증이미지 데이터를 2차인증시스템에게 전송한다(S610). 2차인증시스템은

장치토큰이 등록된 이동통신단말기로부터 인증 이미지가 수신되면(S706), 그 수신된 인증 이미지로부터 2차인증키를 생성하여 저장하고(S707), 생성된 2차인증키를 해당 이동통신단말기에 발급한다(S708).

- [91] 이동통신단말기는 2차인증시스템으로부터 2차인증키가 발급되면(S611), 사용자에게 인증키저장비밀번호 입력을 요청한다(S612). 인증키저장비밀번호가 입력되면(S613), 보안인증모듈(510)은 단계 S611 단계에서 발급된 2차인증키를 단계 S612에서 입력된 인증키저장비밀번호로 암호화한 후 저장부에 저장한다(S614).
- [92]
- [93] 도 8은 이 발명의 제2실시예에 따른 이미지 기반 인증시스템 이동통신단말기에서의 2차 인증 과정을 도시한 동작 흐름도이고, 도 9는 이 발명의 제2실시예에 따른 이미지 기반 인증시스템 2차인증시스템에서의 2차 인증 과정을 도시한 동작 흐름도이다.
- [94] 도 8과 도 9를 참조하면서 이동통신단말기와 2차인증시스템을 통한 2차 인증 과정을 살펴본다.
- [95] 2차인증시스템은 온라인 서비스 시스템으로부터 종단실체 정보가 입력되면서 2차 인증이 요청되면(S901), 수신된 종단실체 정보에 대응하여 이동통신단말기가 등록되어 있는지를 확인한다(S902).
- [96] 이동통신단말기가 등록되어 있으면(S903), 2차인증시스템은 접근키를 생성하고 저장하며 암호화한다(S904). 그리고, 2차인증시스템은 1차 인증에 성공한 종단실체에 기등록된 이동통신단말기의 장치토큰을 이용하여 이동통신단말기의 보안인증모듈을 활성화시키고 암호화된 접근키를 이동통신단말기에게 발급하기 위한 메시지를 푸시서버에게 전달한다.
- [97] 이 푸시서버는 2차인증시스템으로부터 전달받은 장치토큰으로부터 메시지를 전달할 이동통신단말기를 파악하고, 해당 이동통신단말기에 푸시메시지를 전달하여 보안인증모듈을 활성화시키고, 암호화된 접근키를 보안인증모듈에게 전달한다.
- [98] 푸시서버로부터 푸시메시지가 수신되면(S801), 이동통신단말기는 깨어나서 보안인증모듈을 활성화시킨다(S802). 그리고, 암호화된 접근키가 수신되면(S803), 이동통신단말기의 보안인증모듈은 암호화된 접근키를 복호화하고(S804), 사용자에게 인증키저장비밀번호 입력을 요청한다(S805). 사용자로부터 인증키저장비밀번호가 입력되면(S806), 보안인증모듈은 저장부에 저장되어 있는 암호화된 2차인증키를 인증키저장비밀번호로 복호화한다(S807). 그리고, 보안인증모듈은 단계 S804에서 복호화한 접근키로 2차인증시스템에 접근하여 단계 S807에서 복호화한 2차인증키를 전송한다(S808). 이로써, 2차인증시스템은 이동통신단말기로부터 접근키와 2차인증키를 수신한다(S906). 2차인증시스템은 단계 S906에서 수신한 접근키와 단계 S905에서 발급한 접근키를 비교한다(S907). 단계 S907의 비교 결과 두

접근키가 일치하면, 2차인증시스템은 단계 S906에서 수신한 2차인증키와 기저장된 2차인증키를 비교한다(S908). 단계 S908의 비교 결과 두 2차인증키가 일치하면, 2차 인증시스템은 인증을 승인 처리하고(S909), 온라인 서비스 시스템에게 그 결과를 전송한다(S910).

- [99] 한편, 단계 S907의 비교 결과 두 접근키가 일치하지 않거나, 단계 S908의 비교 결과 두 2차인증키가 일치하지 않으면, 2차 인증시스템은 인증을 실패 처리하고(S911), 온라인 서비스 시스템에게 그 결과를 전송한다(S910). 한편, 단계 S903에서 이동통신단말기가 등록되어 있지 않으면 미등록 이동통신단말로 처리하고(S912), 그 처리 결과를 온라인 서비스 시스템에 통보한다(S910).

[100]

청구범위

- [청구항 1] 온라인 서비스 시스템과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 종단실체를 인증하는 시스템에 있어서, 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록부와; 1차 인증 완료된 종단실체에 발급할 2차인증키를 생성하는 인증키생성부와; 상기 생성된 2차인증키에 대응하는 인증 이미지를 생성하고 상기 온라인 서비스 시스템을 통해 상기 1차 인증 완료된 종단실체의 컴퓨터장치에 표시되도록 제공하는 인증 이미지 생성부와; 상기 1차 인증 완료된 종단실체에 등록된 이동통신단말기를 활성화시킨 후 상기 활성화된 이동통신단말기로부터 수신되는 2차인증키를 검증하는 인증키검증부를 포함한 것을 특징으로 하는 이미지 기반 인증 시스템.
- [청구항 2] 제 1 항에 있어서, 상기 이동통신단말기등록부는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 등록하고, 상기 인증키검증부는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 이용하여 푸시서버를 통해 상기 이동통신단말기를 활성화시킨 후 상기 이동통신단말기와 통신하여 상기 이동통신단말기로부터 상기 2차인증키를 수신하는 것을 특징으로 하는 이미지 기반 인증 시스템.
- [청구항 3] 제 1 항에 있어서, 상기 인증 이미지는 이차원 바코드인 것을 특징으로 하는 이미지 기반 인증 시스템.
- [청구항 4] 제 1 항에 있어서, 상기 인증 이미지는 상기 2차원인증키에 대응하는 그림, 문자, 숫자 중 적어도 하나를 포함한 이미지인 것을 특징으로 하는 이미지 기반 인증 시스템.
- [청구항 5] 제 1 항에 있어서, 상기 1차 인증 완료된 종단실체에 등록된 이동통신단말기에 접근키를 발급하고 상기 이동통신단말기로부터 수신되는 접근키와 발급한 접근키를 비교하여 상기 이동통신단말기를 검증하는 접근키 발급/검증부를 더 포함한 것을 특징으로 하는 이미지 기반 인증 시스템.
- [청구항 6] 제 5 항에 있어서, 상기 접근키 발급/검증부는 상기 접근키를 암호화하여 상기 이동통신단말기에게 발급하고, 상기 이동통신단말기로부터 복호화된 접근키를 수신하는 것을 특징으로 하는 이미지 기반 인증 시스템.
- [청구항 7] 온라인 서비스 시스템과의 통신을 통해 1차 인증을 수행하는

컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 종단실체를 인증하는 방법에 있어서,
 2차인증시스템이 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록단계와;
 상기 온라인 서비스 시스템으로부터 상기 종단실체의 2차 인증이 요청되면, 상기 2차인증시스템이 1차 인증 완료된 종단실체에 발급할 2차인증키를 생성하는 인증키생성단계와;
 상기 2차인증시스템이 상기 생성된 2차인증키에 대응하는 인증 이미지를 생성하고 상기 온라인 서비스 시스템을 통해 상기 1차 인증 완료된 종단실체의 컴퓨터장치에 표시되도록 제공하는 인증 이미지 생성단계와;
 상기 2차인증시스템이 상기 인증 이미지 생성단계 후 상기 1차 인증 완료된 종단실체에 등록된 이동통신단말기를 활성화시키고 상기 활성화된 이동통신단말기로부터 수신되는 2차인증키를 검증하는 인증키검증단계를 포함한 것을 특징으로 하는 이미지 기반 인증 방법.

[청구항 8]

제 7 항에 있어서, 상기 이동통신단말기등록단계는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 등록하는 단계이고, 상기 인증키검증단계는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 이용하여 푸시서버를 통해 상기 이동통신단말기를 활성화시키고 상기 이동통신단말기와 통신하여 상기 이동통신단말기로부터 상기 2차인증키를 수신하는 단계인 것을 특징으로 하는 이미지 기반 인증 방법.

[청구항 9]

제 7 항에 있어서, 상기 인증 이미지는 이차원 바코드인 것을 특징으로 하는 이미지 기반 인증 방법.

[청구항 10]

제 7 항에 있어서, 상기 인증 이미지는 상기 2차원인증키에 대응하는 그림, 문자 또는 숫자 중 적어도 하나를 포함한 이미지인 것을 특징으로 하는 이미지 기반 인증 방법.

[청구항 11]

제 7 항에 있어서, 상기 2차인증시스템이 상기 인증키생성단계 내지 상기 인증키검증단계를 진행하는 동안에 상기 1차 인증 완료된 종단실체에 등록된 이동통신단말기에 접근키를 발급하고 상기 이동통신단말기로부터 수신되는 접근키와 발급한 접근키를 비교하여 상기 이동통신단말기를 검증하는 접근키 발급/검증단계를 더 포함한 것을 특징으로 하는 이미지 기반 인증 방법.

[청구항 12]

제 11 항에 있어서, 상기 접근키 발급/검증단계는 상기 접근키를 암호화하여 상기 이동통신단말기에게 발급하고, 상기

[청구항 13]

이동통신단말기로부터 복호화된 접근키를 수신하는 것을 특징으로 하는 이미지 기반 인증 방법.

온라인 서비스 시스템과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 종단실체를 인증하는 시스템에 있어서,

2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록부와;

상기 이동통신단말기등록부에 등록된 상기 이동통신단말기를 통해 인증이미지를 수신하는 인증이미지수신부와;

상기 수신된 인증이미지로부터 2차인증키를 생성하여 저장하고 상기 이동통신단말기에게 발급하여 저장되도록 하는 인증키생성발급부와;

1차 인증 완료된 종단실체에 등록된 이동통신단말기를 활성화시킨 후 상기 활성화된 이동통신단말기로부터 기저장된 2차인증키를 수신하여 검증하는 인증키검증부를 포함한 것을 특징으로 하는 이미지 기반 인증 시스템.

[청구항 14]

제 13 항에 있어서, 상기 이동통신단말기등록부는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 등록하고, 상기 인증키검증부는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 이용하여 푸시서버를 통해 상기 이동통신단말기를 활성화시킨 후 상기 이동통신단말기와 통신하여 상기 이동통신단말기로부터 상기 2차인증키를 입력받는 것을 특징으로 하는 이미지 기반 인증 시스템.

[청구항 15]

제 13 항에 있어서, 상기 1차 인증 완료된 종단실체에 등록된 이동통신단말기에 접근키를 발급하고 상기 이동통신단말기로부터 수신되는 접근키와 발급한 접근키를 비교하여 상기 이동통신단말기를 검증하는 접근키 발급/검증부를 더 포함한 것을 특징으로 하는 이미지 기반 인증 시스템.

[청구항 16]

제 15 항에 있어서, 상기 접근키 발급/검증부는 상기 접근키를 암호화하여 상기 이동통신단말기에게 발급하고, 상기 이동통신단말기로부터 복호화된 접근키를 수신하는 것을 특징으로 하는 이미지 기반 인증 시스템.

[청구항 17]

온라인 서비스 시스템과의 통신을 통해 1차 인증을 수행하는 컴퓨터장치와, 2차 인증을 수행하기 위한 이동통신단말기를 포함하는 종단실체를 인증하는 방법에 있어서,

2차인증시스템이 2차 인증에 필요한 종단실체 정보와 상기 종단실체 정보와 매칭되는 이동통신단말기를 등록하는 이동통신단말기등록단계와;

상기 2차인증시스템이 상기 이동통신단말기등록부에 등록된 상기 이동통신단말기를 통해 인증이미지를 수신하는 인증이미지수신단계와;
 상기 2차인증시스템이 상기 수신된 인증이미지로부터 2차인증키를 생성하여 저장하고 상기 이동통신단말기에게 발급하여 저장되도록 하는 인증키생성발급단계와;
 상기 온라인 서비스 시스템으로부터 상기 종단실체의 2차 인증이 요청되면, 상기 2차인증시스템이 1차 인증 완료된 종단실체에 등록된 이동통신단말기를 활성화시키고 상기 활성화된 이동통신단말기로부터 기저장된 2차인증키를 수신하여 검증하는 인증키검증단계를 포함한 것을 특징으로 하는 이미지 기반 인증 방법.

[청구항 18]

제 17 항에 있어서, 상기 이동통신단말기등록단계는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 등록하고, 상기 인증키검증단계는 상기 종단실체 정보와 매칭되는 이동통신단말기의 장치토큰을 이용하여 푸시서버를 통해 상기 이동통신단말기를 활성화시킨 후 상기 이동통신단말기와 통신하여 상기 이동통신단말기로부터 상기 2차인증키를 입력받는 것을 특징으로 하는 이미지 기반 인증 방법.

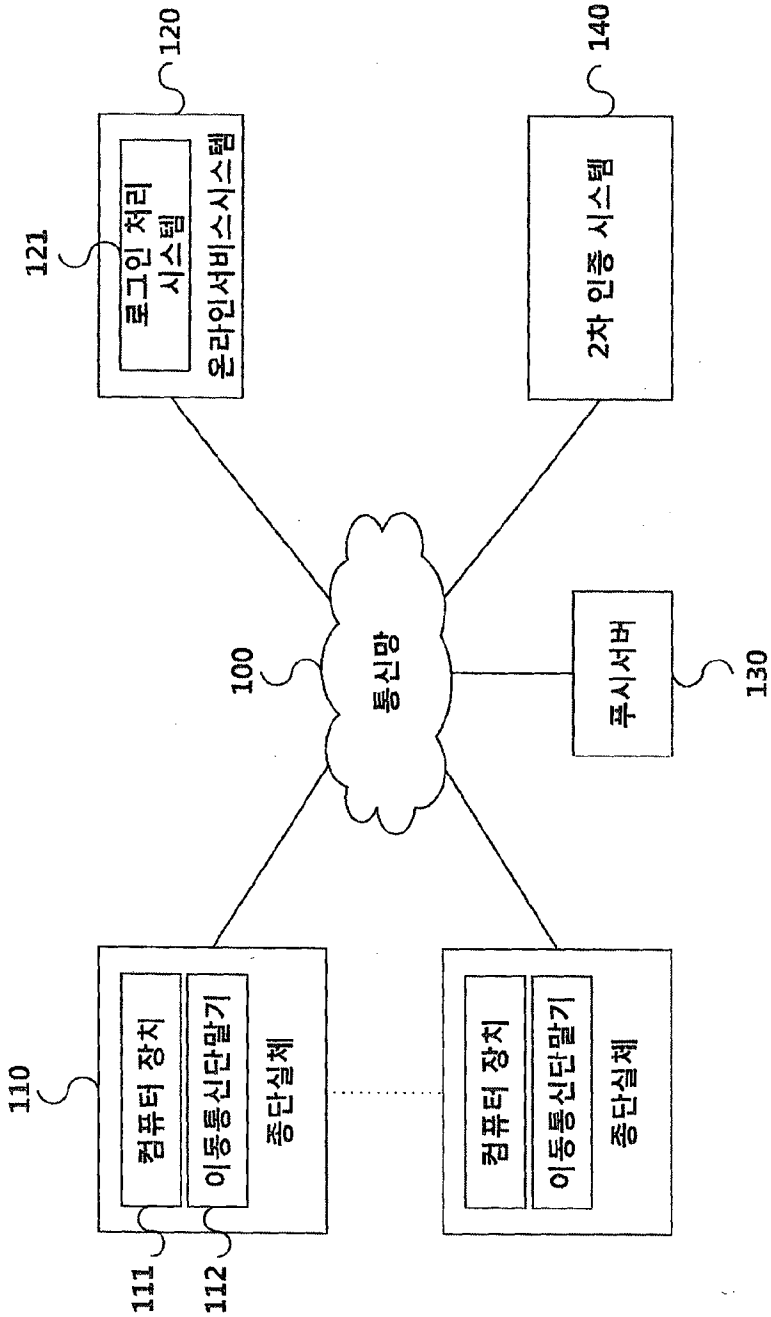
[청구항 19]

제 17 항에 있어서, 상기 2차인증시스템이 상기 인증키검증단계를 진행하는 동안에 상기 1차 인증 완료된 종단실체에 등록된 이동통신단말기에 접근키를 발급하고 상기 이동통신단말기로부터 수신되는 접근키와 발급한 접근키를 비교하여 상기 이동통신단말기를 검증하는 접근키 발급/검증단계를 더 포함한 것을 특징으로 하는 이미지 기반 인증 방법.

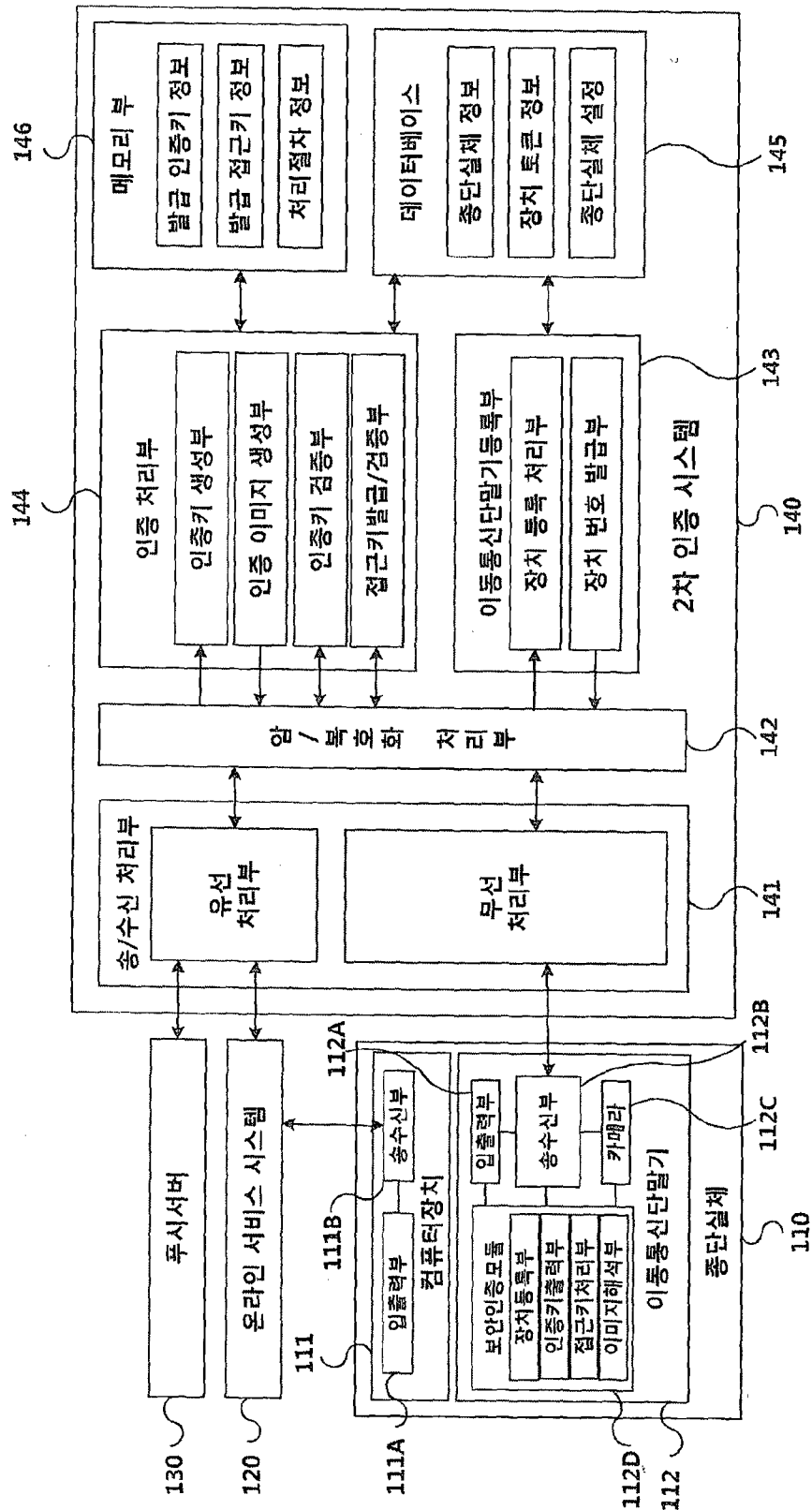
[청구항 20]

제 19 항에 있어서, 상기 접근키 발급/검증단계는 상기 접근키를 암호화하여 상기 이동통신단말기에게 발급하고, 상기 이동통신단말기로부터 복호화된 접근키를 수신하는 것을 특징으로 하는 이미지 기반 인증 방법.

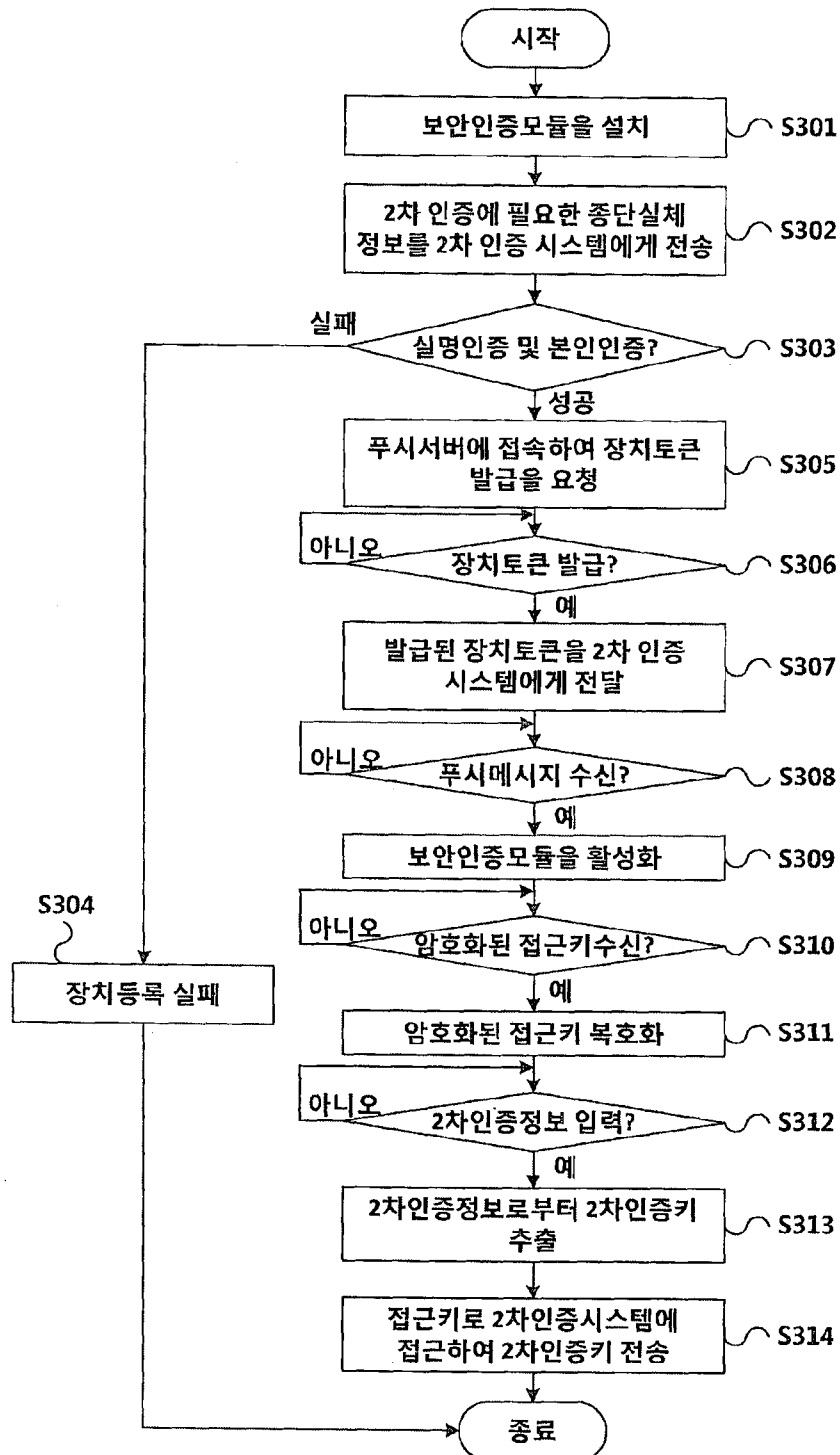
[Fig. 1]



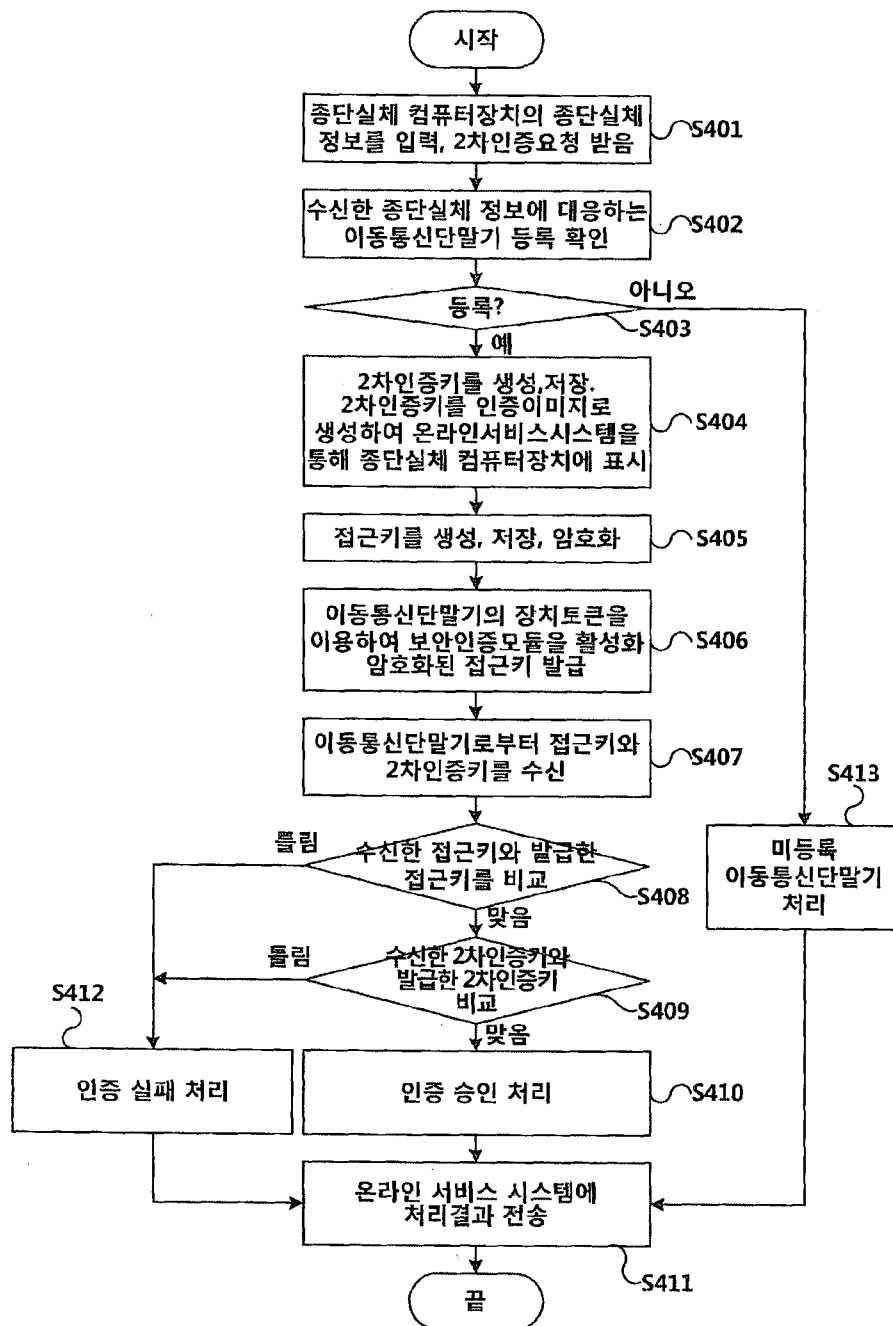
[Fig. 2]



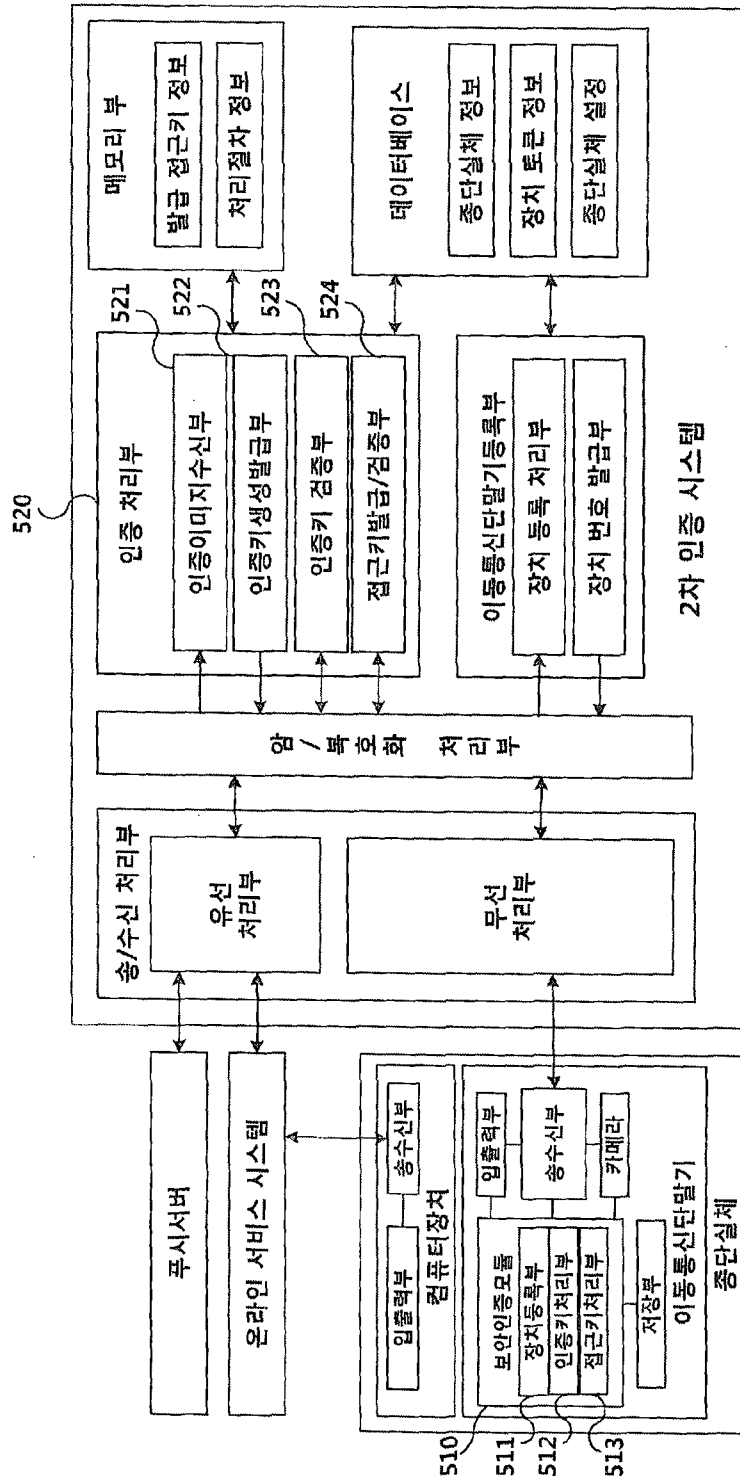
[Fig. 3]



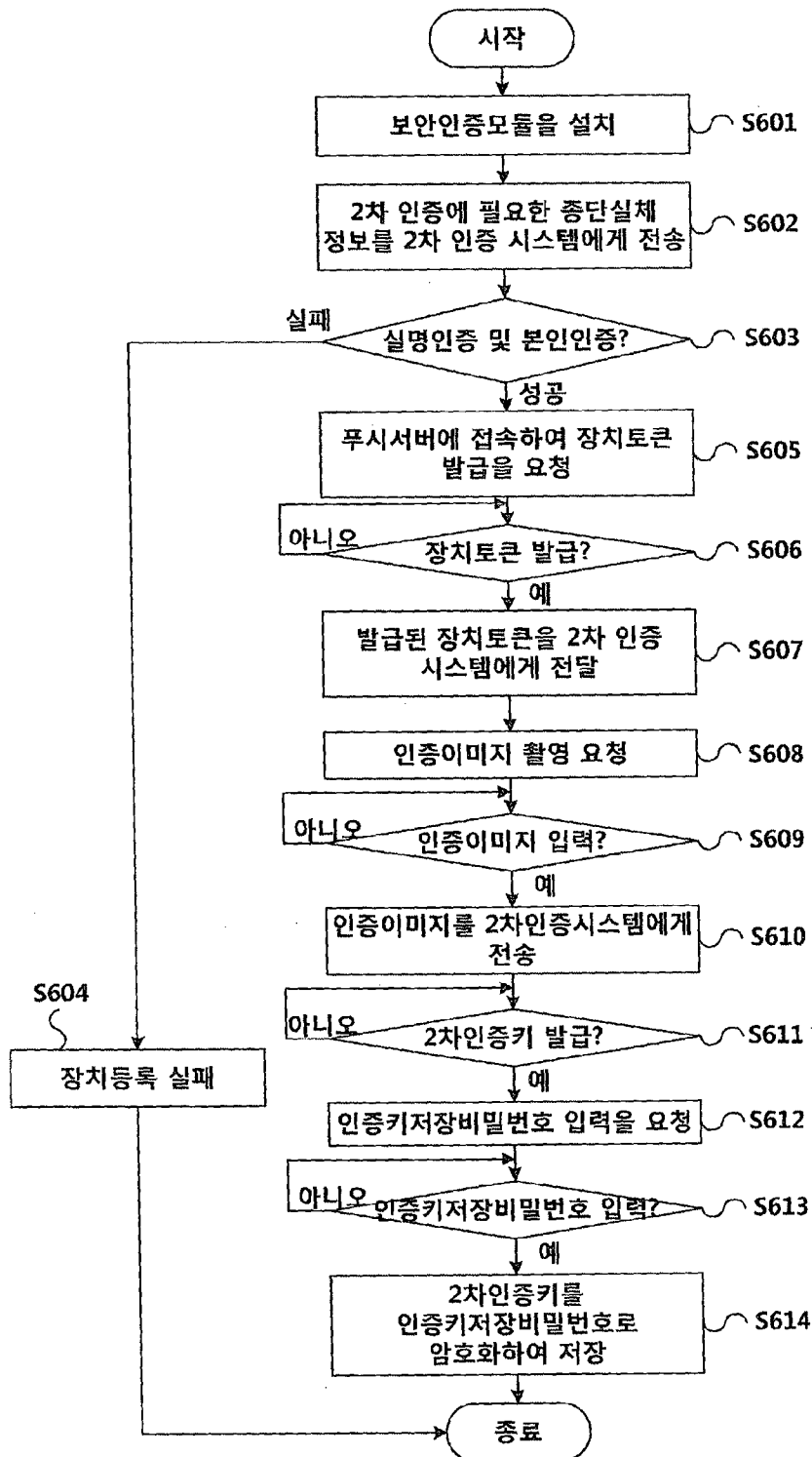
[Fig. 4]



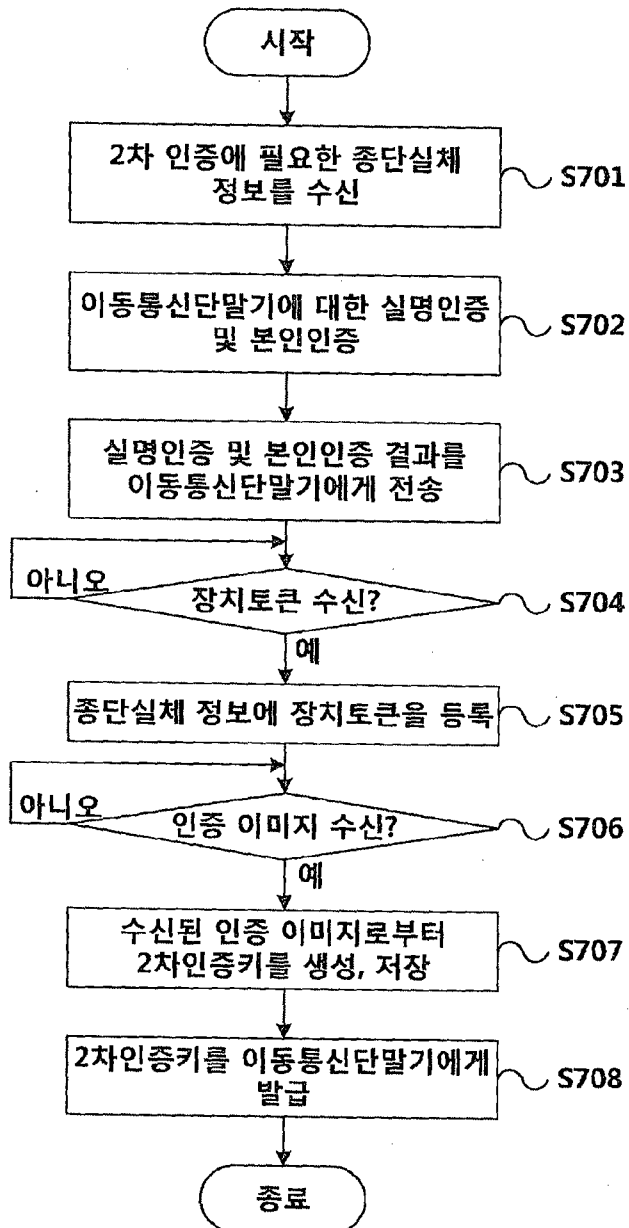
[Fig. 5]



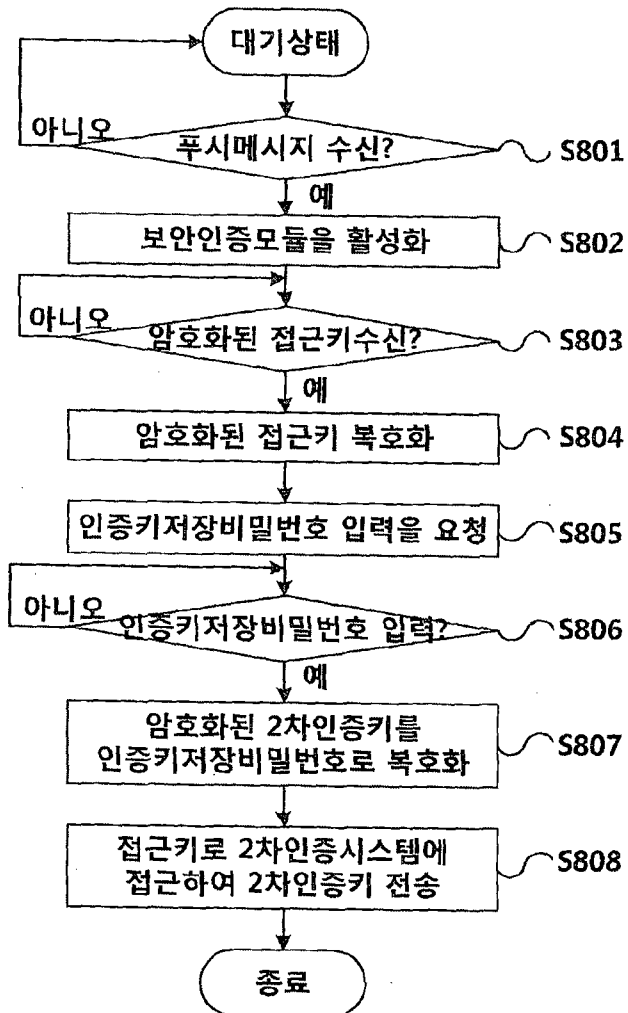
[Fig. 6]



[Fig. 7]



[Fig. 8]



[Fig. 9]

