(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2008년06월16일
(11) 등록번호 10-0838488
(24) 등록일자 2008년06월09일

(51) Int. Cl.
G06F 15/00 (2006.01)
(21) 출원번호 10-2007-0007270
(22) 출원일자 2007년01월24일
심사청구일자 2007년01월24일
(56) 선행기술조사문헌
1020040094379 A
1020050039542 A

(73) 특허권자
현대중공업 주식회사
울산광역시 동구 전하동 1번지
(주)지인소프트
서울특별시 서초구 양재2동 314-12
(72) 발명자
김용안
울산 동구 전하동 한마음아파트 1306호
안영택
경기 과천시 문원동 115-377
(74) 대리인
장순부, 최영규

전체 청구항 수 : 총 2 항 심사관 : 박성웅

(54) 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한정보 보안 방법 및 장치

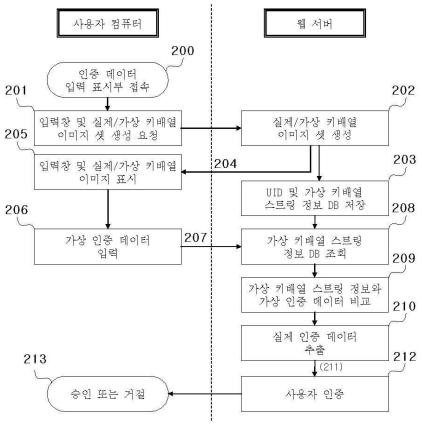
(57) 요 약

본 발명은 사용자 컴퓨터에 키스트로크 해킹 보안 방법 및 장치에 있어서, 인증을 위한 인증 데이터를 입력할 때 변조된 가상의 키보드 이미지를 생성하고 생성된 이미지에 의해 인증 데이터를 입력함으로서 키스트로크 해킹 보안 프로그램 설치가 필요 없이 변조된 일회성 키보드 이미지를 사용하여 키스트로크 보안을 할 수 있도록 하는 정보 보안 방법 및 장치에 관한 것이다.

상기 목적 달성을 위한 본 발명은 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법 및 장치에 있어서, 네트워크를 통해 제공되는 각종 사이트 중 사용자가 원하는 사이트로 사용자 컴퓨터(100)를 접속시켜주는 웹 서버(101)와, 접속된 사이트에서 사용자의 인증을 위한 인증 데이터를 입력하는 인증 데이터 입력 표시부(103)와, 접속된 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋이 생성되는 웹 서버(101)의 실제/가상 키배열(Key-array) 이미지 셋(Set) 생성부(104)와, 상기 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 실제/가상 키배열 이미지 셋 중 가상 키배열 스트링 정보 및 가상 키배열 스트링의 UID(Unique IDentifier; 단일 식별자) 정보를 저장하는 데이터베이스 저장부(105)와, 사용자의 실제 인증 데이터 스트링의 각 문자(숫자, 특수기호 포함)와 매칭된 가상 인증 데이터 스트링을 입력할 수 있는 입력 인터페이스(102)와, 사용자 컴퓨터(100)로부터 전송받은 가상 인증 데이터 스트링과 가상인증 데이터 스트링의 UID 정보를 데이터베이스 저장부(105)에 저장된 가상 키배열 스트링 정보 및 가상 키배열 스트링의 UID 정보와 비교하여 실제 인증 데이터 스트링을 추출하는는 웹 서버(101)의 가상 인증 데이터 비교부(106)와, 웹 서버(101)의 가상 인증 데이터 비교부(106)에서 추출된 실제 인증 데이터 스트링을 전송받아 사용자 인증을 하는 웹 서버(101)의 사용자 인증부(107)로 구성되어, 웹 서버(101)로부터 네트워크를 통해 제공되는 각종 사이트 중 사용자가 원하는 사이트의 인증 데이터 입력 표시부(103)에 사용자 컴퓨터(100)를 통해 접속하는 단계(200, 201, 300, 301); 웹 서버(101)의 실제/가상 키배열(Key-array) 이미지 셋(Set) 생성부(104)에서 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋이 생성되는 단계(202); 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 실제/가상 키배열 이미지 셋 중 가상 키배열 스트링 정보와 가상 키배열 스트링의 UID(Unique IDentifier; 단일 식별자)정보를 데이터베이스 저장부(105)에 저장하는 단계(203); 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋 중 실제/가상 키배열 이미지(400)와 실제/가상 키배열 이미지의 UID 정보를 사용자 컴퓨터(100)의 인증 데이터 입력 표시부(103)에 전송하는 단계(204); 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋 중 실제/가상 키배열 이미지(400)를 사용자 컴퓨터(100)를 통해 인증 데이터 입력 표시부(103)에 표시하는 단계(205, 302); 사용자의 실제 인증 데이터 스트링의 각 문자(숫자, 특수기호 포함)와 매칭된 가상 인증 데이터 스트링을 사용자로부터 사용자 컴퓨터(100)의 입력 인터페이스(102)를 통해 입력받는 단계(206, 304); 사용자로부터 입력받은 가상 인증 데이터 스트링과 가상 인증 데이터 UID 정보를 웹 서버(101)의 가상 인증 데이터 비교부(106)로 전송하는 단계(207); 웹 서버(101)의 가상 인증 데이터 비교부(106)에서 사용자 컴퓨터(100)로부터 전송받은 가상 인증 데이터 스트링과 가상 인증 데이터 스트링의 UID 정보를 데이터베이스 저장부(105)에 저장된 가상 키배열 스트링 정보 및 UID 정보와 비교하여 실제 인증 데이터 스트링을 추출하는 단계(208, 209, 210, 306);

웹 서버(101)의 가상 인증 데이터 비교부(106)에서 추출된 실제 인증 데이터 스트링을 웹 서버(101)의 사용자 인증부(107)로 전송하는 단계(211)로 이루어져 있는 것을 특징으로 하는 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법 및 장치.

대표도 - 도2



특허청구의 범위

청구항 1

사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 장치에 있어서,

네트워크를 통해 제공되는 각종 사이트 중 사용자가 원하는 사이트로 사용자 컴퓨터(100)를 접속시켜주는 웹 서버(101)와,

접속된 사이트의 사용자 인증을 위한 인증 데이터를 입력하는 인증 데이터 입력 표시부(103)와,

접속된 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋이 생성되는 웹 서버(101)의 실제/가상 키배열(Key-array) 이미지 셋(Set) 생성부(104)와,

상기 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 실제/가상 키배열 이미지 셋 중 가상 키배열 스트링 정보와 가상 키배열 스트링 UID(Unique IDentifier; 단일 식별자)정보를 저장하는 데이터베이스 저장부(105)와,

사용자의 실제 인증 데이터 스트링의 각 문자(숫자, 특수기호 포함)와 매칭된 가상 인증 데이터 스트링을 입력할 수 있는 입력 인터페이스(102)와,

사용자 컴퓨터(100)로부터 전송받은 가상 인증 데이터 스트링과 가상 인증 데이터 스트링 UID 정보를 데이터베이스 저장부(105)에 저장된 가상 키배열 스트링 정보 및 가상 키배열 스트링 UID 정보와 비교하여 실제 인증 데이터 스트링을 추출하는는 웹 서버(101)의 가상 인증 데이터 비교부(106)와,

웹 서버(101)의 가상 인증 데이터 비교부(106)에서 추출된 실제 인증 데이터 스트링을 전속받아 사용자 인증을 하는 웹 서버(101)의 사용자 인증부(107)로 구성되어 있는 것을 특징으로 하는 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 장치.

청구항 2

사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법에 있어서,

웹 서버(101)로부터 네트워크를 통해 제공되는 각종 사이트 중 사용자가 원하는 사이트의 인증 데이터 입력 표시부(103)에 사용자 컴퓨터(100)를 통해 접속하는 단계(200, 201, 300, 301);

웹 서버(101)의 실제/가상 키배열(Key-array) 이미지 셋(Set) 생성부(104)에서 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋이 생성되는 단계(202);

웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 실제/가상 키배열 이미지 셋 중 가상 키배열 스트링 정보와 가상 키배열 스트링 UID(Unique IDentifier; 단일 식별자) 정보를 데이터베이스 저장부(105)에 저장하는 단계(203);

웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋 중 실제/가상 키배열 이미지(400)와 실제/가상 키배열 이미지 UID 정보를 사용자 컴퓨터(100)의 인증 데이터 입력 표시부(103)에 전송하는 단계(204);

웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋 중 실제/가상 키배열 이미지(400)를 사용자 컴퓨터(100)를 통해 인증 데이터 입력 표시부(103)에 표시하는 단계(205, 302);

사용자의 실제 인증 데이터 스트링의 각 문자(숫자, 특수기호 포함)와 매칭된 가상 인증 데이터 스트링을 사용자로부터 사용자 컴퓨터(100)의 입력 인터페이스(102)를 통해 입력받는 단계(206, 304);

사용자로부터 입력받은 가상 인증 데이터 스트링과 상 인증 데이터 스트링 UID 정보를 웹 서버(101)의 가상 인증 데이터 비교부(106)로 전송하는 단계(207);

웹 서버(101)의 가상 인증 데이터 비교부(106)에서 사용자 컴퓨터(100)로부터 전송받은 가상 인증 데이터 스트링과 가상 인증 데이터 스트링 UID 정보를 데이터베이스 저장부(105)에 저장된 가상 키배열 스트링 정보 및 가

상 키배열 스트링 UID 정보와 비교하여 실제 인증 데이터 스트링을 추출하는 단계(208, 209, 210, 306);

웹 서버(101)의 가상 인증 데이터 비교부(106)에서 추출된 실제 인증 데이터 스트링을 웹 서버(101)의 사용자 인증부(107)로 전송하는 단계(211)로 이루어져 있는 것을 특징으로 하는 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<11> 본 발명은 사용자 컴퓨터에 키스트로크 해킹 보안 방법 및 장치에 있어서, 인증을 위한 인증 데이터를 입력할 때 변조된 가상의 키보드 이미지를 생성하고 생성된 이미지에 의해 인증 데이터를 입력함으로서 키스트로크 해킹 보안 프로그램 설치가 필요 없이 변조된 일회성 키보드 이미지를 사용하여 키스트로크 보안을 할 수 있도록 하는 정보 보안 방법 및 장치에 관한 것이다.

<12> 오늘날 컴퓨터 사용자는 인터넷쇼핑몰이나 오픈마켓 등의 전자상거래 사이트에서부터, 인터넷뱅킹이나 주식거래 등의 금융거래 사이트, 음악이나 영화, 게임 등의 엔터테인먼트 사이트, 강의나 진료, 여행 등의 각종 편의 서비스 사이트, 커뮤니티 포털과 메신저, 이메일, 특정 인트라넷 사이트에 까지 네트워크 상의 수많은 웹 기반 서비스와 솔루션, 그리고 애플리케이션이 제공되는 웹 사이트에서 사용자 식별을 필요로 하는 인증 과정을 거치게 된다.

<13> 그런데, 하루에도 몇 번씩은 보통 거치게 되는 이런 사용자 인증은, 본질적으로 인증 보안이라는 핵심 요소가 역할을 다해줘야만 제 가치를 발휘한다. 또한, 현재의 IT환경 패러다임이 점차 유비쿼터스 환경으로 변모해감에 따라, 정보 공유와 협업의 중요성은 날로 증대되고 있어 사용자 식별을 위한 인증 과정의 필요성과 인증 보안의 중요성은 당연히 따로 언급할 필요가 없다고 하겠다.

<14> 그리고, 최근 컴퓨터 기술의 발전과 더불어 키로깅(Keylogging), 스니핑(Sniffing), 피싱(Phishing) 등 점차 고도화되어가고 있는 해킹 기술로 인해 키스트로크(Keystroke) 해킹 보안 프로그램이나 방화벽, 침입탐지시스템과 같은 네트워크 보안 제품의 개별적 사용으로는 인증 정보 유출 위험을 제거하는 것은 쉽지 않으며, 인증 정보는 물론, 인증 정보 외의 개인 정보가 유출되어 많은 경제적, 사회적 피해가 발생하고 있다. 인증 정보는 개인 정보 유출의 키(Key)와 같은 것으로 보안에 있어 가장 기본이 되며 매우 중요한 존재이다.

<15> 일반적으로 인증 데이터 정보를 보호하기 위해 여러 가지 방법을 적용하고 있다.

<16> 첫째로, 입력 인터페이스를 통해 인증 데이터 정보를 사용자가 직접 입력하고 인증 데이터 정보를 가공하지 않은 상태로 인증 서버로 전송하여 처리하는 것이 가장 일반적인 형태다. 그러나, 이러한 방법은 사용자 컴퓨터상에서 키스트로크 해킹이나 네트워크 전송 중에 인증 데이터 정보가 고스란히 노출되어 정보 유출의 위험을 가지고 있다.

<17> 둘째로, 입력 인터페이스를 통해 인증 데이터 정보를 사용자가 직접 입력하면 암호화를 하여 인증 서버로 전송 처리하는 방법이다. 그러나, 이러한 방법도 사용자 컴퓨터상에서의 키스트로크 해킹의 위험은 존재하며, 네트워크 전송 중에도 암호화 수준과 방식에 따라 유출 위험도 없다고 볼 수는 없다.

<18> 셋째로, 사용자 컴퓨터상에 키스트로크 해킹 보안 프로그램을 설치하고, 암호화를 하여 인증 서버로 전송 처리하는 방법이다. 키스트로크 해킹 보안 프로그램으로 사용자 컴퓨터상에서의 입력 인터페이스와 관련된 인증 데이터 정보의 유출을 방지하고 네트워크 전송 중에서는 암호화 기법을 이용하여 보다 나은 정보 유출 방지할 수 있다. 하지만, 사이트마다 다르게 제공되는 각각의 해킹 보안 프로그램을 사용자 컴퓨터에 적어도 한 번씩은 설치해야하고, 보안을 위해서 당해 사이트를 이용하고자 하면 사용자의 불편함을 감수해야하는 단점을 안고 있다. 게다가, 해킹 보안 프로그램 자체나 사용자 컴퓨터상에 설치하는 과정에서도 무결성(Integrity)이 추가로 보장되어야 한다.

<19> 넷째로, 상기한 종래의 기술과 병행하여 사용자 이용 측면에서 볼 때, 인증 데이터의 문자, 숫자, 특수기호 등의 조합, 일정 수 이상의 자리수 제한, 한 번 등록한 인증 데이터 정보의 사용 제한 등 좀 더 복잡한 인증 데이

터 정보를 요구하기도 한다. 이것은 인증 보안성을 다소 높일 수는 있으나 사용자 편의성은 상대적으로 떨어뜨리는 결과를 가져온다. 일반적으로 사용자의 성향은 대부분 보안성에 대한 만족은 유지하면서 특정 의미가 부여되거나 간단하고 기억하기 쉬운 인증 데이터 정보를 사용하길 원한다.

발명이 이루고자 하는 기술적 과제

<20> 본 발명은 상기와 같은 종래의 문제점을 해결하기 위하여 창출된 것으로, 종래의 기술에서 해킹 보안 프로그램이 인증 데이터 정보의 유출 방지에 초점이 맞추어진 것과는 달리, 네트워크 상의 수많은 웹 기반 서비스와 솔루션, 그리고 웹 애플리케이션, 특히 인터넷 웹 사이트에서의 로그인 인증이나 전자결제 인증과 같은 사용자 인증을 필요로 하는 곳에서 키스트로크 해킹을 당하거나 네트워크 전송 중에 인증 데이터 정보가 고스란히 노출되어도 정확한 인증 데이터 정보를 알아채지 못하도록 하기 위하여 사용자 인증 화면이 리로딩(Reloading)이 될 경우에 매번 변경되는 인증 데이터를 생성하고, 사용자 컴퓨터상에 키스트로크 해킹 보안을 위하여 프로그램을 설치하지 않아도 되며, 기억하기 쉽고 간단한 인증 데이터 정보를 사용하여도 보안성을 떨어뜨리지 않도록 하기 위해, 인증 보안성과 사용자 편의성을 동시에 고려할 수 있는 변조된 일회성 인증 데이터 생성 방식을 이용한 인증 데이터 정보 보안 방법 및 장치를 제공함을 목적으로 한다.

발명의 구성 및 작용

<21> 상기 목적을 달성하기 위하여, 첨부된 도면에 의거 본 발명의 일 실시예를 설명하면 다음과 같다.

<22> 도 1 은 본 발명인 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 장치의 구성도를 나타낸 것이다.

<23> 도면에서 보는 바와 같이 상기 목적 달성을 위한 본 발명은 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 장치에 있어서, 네트워크를 통해 제공되는 각종 사이트 중 사용자가 원하는 사이트로 사용자 컴퓨터(100)를 접속시켜주는 웹 서버(101)와, 접속된 사이트의 사용자 인증을 위한 인증 데이터를 입력하는 인증 데이터 입력 표시부(103)와, 접속된 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋이 생성되는 웹 서버(101)의 실제/가상 키배열(Key-array) 이미지 셋(Set) 생성부(104)와, 상기 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 실제/가상 키배열 이미지 셋 중 가상 키배열 스트링 정보와 가상 키배열 스트링 UID(Unique IDentifier; 단일 식별자)정보를 저장하는 데이터베이스 저장부(105)와, 사용자의 실제 인증 데이터 스트링의 각 문자(숫자, 특수기호 포함)와 매칭된 가상 인증 데이터 스트링을 입력할 수 있는 입력 인터페이스(102)와, 사용자 컴퓨터(100)로부터 전송받은 가상 인증 데이터 스트링과 가상 인증 데이터 스트링 UID 정보를 데이터베이스 저장부(105)에 저장된 가상 키배열 스트링 정보 및 가상 키배열 스트링 UID 정보와 비교하여 실제 인증 데이터 스트링을 추출하는는 웹 서버(101)의 가상 인증 데이터 비교부(106)와, 웹 서버(101)의 가상 인증 데이터 비교부(106)에서 추출된 실제 인증 데이터 스트링을 전속받아 사용자 인증을 하는 웹 서버(101)의 사용자 인증부(107)로 구성되어 있다.

<24> 한편, 도 2 는 본 발명인 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법을 사용한 사용자 컴퓨터와 웹 서버간의 동작 흐름을 나타낸 흐름도이고, 도 3 은 본 발명의 일 실시예에 따른 사용자 인증 과정을 나타낸 순서도로, 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법에 있어서,

<25> 웹 서버(101)로부터 네트워크를 통해 제공되는 각종 사이트 중 사용자가 원하는 사이트의 인증 데이터 입력 표시부(103)에 사용자 컴퓨터(100)를 통해 접속하는 단계(200, 201, 300, 301);

<26> 웹 서버(101)의 실제/가상 키배열(Key-array) 이미지 셋(Set) 생성부(104)에서 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋이 생성되는 단계(202);

<27> 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 실제/가상 키배열 이미지 셋 중 가상 키배열 스트링 정보와 가상 키배열 스트링UID(Unique IDentifier; 단일 식별자) 정보를 데이터베이스 저장부(105)에 저장하는 단계(203);

<28> 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋 중 실제/가상 키배열 이미지(400)와 실제/가상 키배열 이미지의 UID 정보를 사용자 컴퓨터(100)의 인증 데이터 입력 표시부(103)에 전송하는 단계(204);

<29> 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋 중 실제/가상 키배열 이미지(400)를 사용자 컴퓨터(100)를 통해 인증 데이터 입력 표시부(103)에 표시하는 단계(205, 302);

<30> 사용자의 실제 인증 데이터 스트링의 각 문자(숫자, 특수기호 포함)와 매칭된 가상 인증 데이터 스트링을 사용자로부터 사용자 컴퓨터(100)의 입력 인터페이스(102)를 통해 입력받는 단계(206, 304);

<31> 사용자로부터 입력받은 가상 인증 데이터 스트링과 가상 인증 데이터 스트링 UID 정보를 웹 서버(101)의 가상 인증 데이터 비교부(106)로 전송하는 단계(207);

<32> 웹 서버(101)의 가상 인증 데이터 비교부(106)에서 사용자 컴퓨터(100)로부터 전송받은 가상 인증 데이터 스트링과 가상 인증 데이터 스트링 UID 정보를 데이터베이스 저장부(105)에 저장된 가상 키배열 스트링 정보 및 가상 키배열 스트링 UID 정보와 비교하여 실제 인증 데이터 스트링을 추출하는 단계(208, 209, 210, 306);

<33> 웹 서버(101)의 가상 인증 데이터 비교부(106)에서 추출된 실제 인증 데이터 스트링을 웹 서버(101)의 사용자 인증부(107)로 전송하는 단계(211)가 제공된다.

<34> 상기 웹 서버(101)로부터 네트워크를 통해 제공되는 각종 사이트 중 사용자가 원하는 사이트의 인증 데이터 입력 표시부(103)에 사용자 컴퓨터(100)를 통해 접속하는 단계(200, 201, 300, 301)에서, 당해 사이트의 인증 데이터 입력 표시부(103)는 웹 페이지 또는 웹 기반의 서비스, 솔루션, 애플리케이션으로 구현된 다양한 방식의 인증 데이터 입력창(예를 들면, 로그인 인증창, 전자 결제 인증창 등)을 포함하는 것이 바람직 하며, 여기서, 당해 사이트의 인증 데이터 입력 표시부(103)에 접속하면 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에 인증 데이터 입력창과 실제/가상 키배열 이미지 셋 생성을 요청(201, 301)하는 것을 특징으로 한다.

<35> 상기 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋이 생성되는 단계(202)에서, 실제/가상 키배열 이미지 셋은 실제/가상 키배열 이미지(400)와 실제/가상 키배열 이미지의 UID 정보, 가상 키배열 스트링 정보로 구성되는 것이 바람직 하며, 여기서, 실제/가상 키배열 이미지(400)는 본 발명에 따른 일 실시예를 나타내는 것으로 가상 키배열이 랜덤하게 셔플링(Shuffling)되어 실제 키배열과 1:1 매칭된 이미지로 생성되는 것을 특징으로 한다.

<36> 또한, 본 발명에 따른 다른 실시예에 따라 실제/가상 키배열 이미지(400)는 당해 사이트의 인증 데이터 유효 조건(예를 들면, 숫자만 유효, 문자만 유효, 특수기호 제외 등)에 따라 생성 조건을 제한(예를 들면, 숫자만 생성, 문자만 생성, 문자·숫자 혼합 생성 등)할 수 있다.

<37> 또한, 실제/가상 키배열 이미지의 UID는 생성된 실제/가상 키배열 이미지(400)의 고유 식별자로서 실제/가상 키배열 이미지(400)와 1:1 매칭되는 것을 특징으로 한다.

<38> 또한, 가상 키배열 스트링 정보는 실제/가상 키배열 이미지(400)에서 실제 키배열과 1:1 매칭된 가상 키배열을 나타내는 정보로, 사용자로부터 입력받은 가상 인증 데이터 스트링으로 실제 인증 데이터 스트링을 추출하기 위해 필요한 정보이다.

<39> 또한, 본 발명에 따른 다른 실시예에 따라 실제/가상 키배열 이미지 셋에는 시간 정보(예를 들면, 생성시각, 입력제한시각, 유효시간 등)를 포함할 수 있는데, 시간 정보는 당해 사이트의 입력 시간 제한이 필요한 인증 데이터 입력 표시부(103)의 자동 갱신 타이머(Timer) 기능을 위해 추가적으로 생성될 수 있으며, 자동 갱신이 되면 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 실제/가상 키배열 이미지 셋이 재생성되어 사용자 컴퓨터(100)를 통해 인증 데이터 입력 표시부(103)에 표시된다.(305)

<40> 또한, 사용자 또는 시스템에 의한 당해 사이트의 인증 데이터 입력 표시부(103) 재접속(예를 들면, 갱신 또는 다시 열기, 새로 열기, 통신 장애로 인한 재연결 등) 로딩(Loading)이 이루어질 경우에도 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 실제/가상 키배열 이미지 셋이 재생성되어 사용자 컴퓨터(100)를 통해 인증 데이터 입력 표시부(103)에 표시된다.(303)

<41> 상기 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 실제/가상 키배열 이미지 셋 중 가상 키배열 스트링 정보와 UID 정보를 데이터베이스 저장부(105)에 저장하는 단계(203)에서, 실제/가상 키배열 이미지 셋에 시간 정보가 포함된 경우에는 시간 정보도 데이터베이스 저장부(105)에 저장하는 것을 특징으로 한다.

<42> 상기 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋을 사용자 컴퓨터(100)의 인증 데이터 입력 표시부(103)에 전송하는 단계(204)에서,

실제/가상 키배열 이미지(400)와 그것의 실제/가상 키배열 이미지의 UID 정보는 전송 중에 노출되어도 인증 정보 유출에는 무방하나, 당해 사이트의 네트워크 전송 암/복호화 보안 방법이 이용되고 있다면 이를 적용하여 보안성을 높일 수도 있다.

<43> 상기 웹 서버(101)의 실제/가상 키배열 이미지 셋 생성부(104)에서 생성된 당해 사이트의 인증 데이터 입력창과 실제/가상 키배열 이미지 셋 중 실제/가상 키배열 이미지(400)를 사용자 컴퓨터(100)를 통해 인증 데이터 입력 표시부(103)에 표시하는 단계(205, 302)에서, 인증 데이터 입력 표시부(103)는 웹 페이지 안에 포함된 고정식 외에도 본 발명에 따른 다른 실시예에 따라 자유롭게 이동이 가능한 이동식, 팝업창식의 입력창 형태도 포함하는 것을 특징으로 한다.

<44> 상기 사용자의 실제 인증 데이터 스트링의 각 문자(숫자, 특수기호 포함)와 매칭된 가상 인증 데이터 스트링을 사용자로부터 사용자 컴퓨터(100)의 입력 인터페이스(102)를 통해 입력받는 단계(206, 304)에서, 사용자는 실제/가상 키배열 이미지(400)를 보고서 인증 데이터 입력창에 실제 인증 데이터 스트링과 매칭된 가상 인증 데이터 스트링을 순서대로 입력을 하게 된다.

<45> 여기서, 실제 인증 데이터는 당해 사이트에 등록된 인증 데이터(예를 들면, 로그인 패스워드, 전자결제 인증 패스워드 등)로 사용자가 기억하고 있는 정보이다.

<46> 또한, 사용자가 입력한 가상 인증 데이터 스트링은 키스트로크 해킹 프로그램에 의한 키로깅 노출되어도 실제 인증 데이터 스트링이 아닌 변조된 인증 데이터 스트링이므로 실제 인증 데이터 스트링을 파악하기 어렵다.

<47> 또한, 사용자 컴퓨터(100)의 입력 인터페이스(102)는 키보드 뿐만 아니라, 본 발명에 따른 다른 실시예에 따라 마우스, 키패드 등의 인터페이스도 포함되며, 비단 컴퓨터 시스템에 국한된 것이 아니라, PDA나 휴대폰과 같은 휴대 단말기에서의 입력 인터페이스(102)도 포함하는 것을 특징으로 한다.

<48> 상기 사용자로부터 입력받은 가상 인증 데이터 스트링과 가상 인증 데이터 스트링의 UID 정보를 웹 서버(101)의 가상 인증 데이터 비교부(106)로 전송하는 단계(207)에서, 가상 인증 데이터 스트링과 가상 인증 데이터 스트링 UID 정보는 전송 중에 노출되어도 인증 정보 유출에는 무방하나, 당해 사이트의 네트워크 전송 암/복호화 보안 방법이 이용되고 있다면 이를 적용하여 보안성을 높일 수도 있다.

<49> 상기 웹 서버(101)의 가상 인증 데이터 비교부(106)에서 사용자 컴퓨터(100)로부터 전송받은 가상 인증 데이터 스트링과 가상 인증 데이터 스트링 UID 정보를 데이터베이스 저장부(105)에 저장된 가상 키배열 스트링 정보 및 가상 키배열 스트링 UID 정보와 비교하여 실제 인증 데이터 스트링을 추출하는 단계(208, 209, 210, 306)에서, 사용자 컴퓨터(100)로부터 전송받은 가상 인증 데이터 스트링 UID 정보와 동일한 UID를 데이터베이스 저장부(105)에서 조회(208)하여 해당하는 가상 키배열 스트링 정보를 가져오며, 가상 인증 데이터 스트링을 가상 키배열 스트링 정보와 비교(209)한 후 가상 인증 데이터 스트링의 각 문자(숫자, 특수기호 포함)와 1:1 매칭되는 실제 인증 데이터 스트링을 추출하는 것을 특징으로 한다.

<50> 상기 웹 서버(101)의 가상 인증 데이터 비교부(106)에서 추출된 실제 인증 데이터 스트링을 웹 서버(101)의 사용자 인증부(107)로 전송하는 단계(211)에서, 추출된 실제 인증 데이터 스트링은 사용자 인증(예를 들면, 로그인 승인 또는 거절을 위한 인증, 전자결제 승인 또는 거절을 위한 인증 등)(212, 213, 307, 308)을 위해 사용자 인증부(107)로 전송하는 것을 특징으로 한다.

<51> 여기서, 사용자 인증부(107)는 이미 당해 사이트에서 제공하고 있는 사용자 인증부(107)를 이용하는 것 외에도 본 발명에 따른 다른 실시예에 따라 사용자 인증부(107)를 함께 새로이 구성할 수도 있는 것을 특징으로 한다.

<52> 상기 목적을 달성하기 위하여, 이상의 본 발명의 일 실시예를 적용함에 있어서 변조된 인증 데이터 생성 방식을 다음과 같이 함수(Function)로 정의 표현할 수 있다.

<53> y=x

<54> 즉, 실제 인증 데이터 스트링 x는 가상 인증 데이터 스트링 y와 1:1 매칭되어 변조된다.

<55> 또한, 본 발명에 따른 다른 함수의 적용에 의한 실시예에 따라 다음과 같이 함수로 정의 표현할 수 있다.

<56> y=shift(x, +1)

<57> y=shift(x, -1)

<58> 즉, 가상 인증 데이터 스트링 y는 실제 인증 데이터 스트링 x에서 1:1 매칭되어 변조될 때 배열변경(shift)의

적용에 의해 +1 또는 -1 변경되어 적용된다.

<59> 본 발명은 상술한 특정의 바람직한 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 고안이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 범위 내에 있게 된다.

발명의 효과

<60> 상기와 같은 구성 및 작용에 의해 기대할 수 있는 본 발명의 효과는 다음과 같다.

<61> 종래의 키스트로크 해킹 보안 프로그램이 키스트로크 해킹으로 인한 인증 데이터 정보의 유출을 막는 것에 초점이 맞추어진 것과 달리, 키스트로크 해킹을 당하거나 네트워크 전송 중에 인증 데이터 정보가 고스란히 노출되어도 변조된 인증 데이터 생성 방식을 이용하여 정확한 인증 데이터 정보를 알아채지 못하도록 가상의 인증 데이터 정보로 변조하여 입력 및 전송하므로 키스트로크 해킹 보안 및 네트워크 전송 중 정보 유출 방지 효과를 제공한다.

<62> 또한, 본 발명은, 사용자 인증 화면이 리로딩(Reloading)이 될 경우에 매번 변경되는 일회성 인증 데이터를 생성 방식을 적용하고 있어서 보다 효과적인 보안성을 제공한다.

<63> 또한, 본 발명은, 종래의 키스트로크 해킹 보안 프로그램이 사용자 컴퓨터상에 설치를 해야만 해킹 보안 효과를 얻으며, 이 또한 해킹 보안 프로그램 자체나 사용자 컴퓨터상에 설치하는 과정에서 무결성을 보장받지 못하는 경우도 발생하는 것과는 달리, 사용자 컴퓨터상에 키스트로크 해킹 보안을 위하여 프로그램을 설치하지 않아도 되므로 이와 같은 위험성을 배제하면서 정보 유출 방지 효과를 제공하며, 게다가 이용하는 사이트마다 다른 해킹 보안 프로그램 설치를 하는 것에 회의적인 사용자라면 더욱 사용자 편의성 효과도 제공한다.

<64> 또한, 본 발명은, 기억하기 쉽고 간단하거나 특정 의미가 부여된 인증 데이터 정보를 사용하고자 하는 일반적인 사용자 성향을 고려하여 간단한 인증 데이터를 사용하더라도 가상 인증 데이터가 생성 및 전송되므로 보안성을 떨어뜨리지 않도록 하는 효과도 제공한다.

<65> 이상과 같이, 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법 및 장치의 적용을 통하여 인증 보안성과 사용자 편의성을 동시에 고려할 수 있어 효과가 매우 크다.

도면의 간단한 설명

<1> 도 1 은 본 발명인 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 장치의 구성도,

<2> 도 2 는 본 발명인 사용자 컴퓨터에 키스트로크 해킹 보안 프로그램 설치가 필요 없는 변조된 일회성 인증 데이터 생성 방식을 이용한 정보 보안 방법을 사용한 사용자 컴퓨터와 웹 서버간의 동작 흐름을 나타낸 흐름도,

<3> 도 3 은 본 발명의 일 실시예에 따른 사용자 인증 과정을 나타낸 순서도,

<4> 도 4 는 본 발명의 일 실시예에 따른 실제/가상 키배열 이미지.

<5> <도면의 주요부분에 대한 부호의 설명>

<6> (100): 사용자 컴퓨터 (101): 웹 서버

<7> (102): 입력 인터페이스 (103) 인증 데이터 입력 포시부

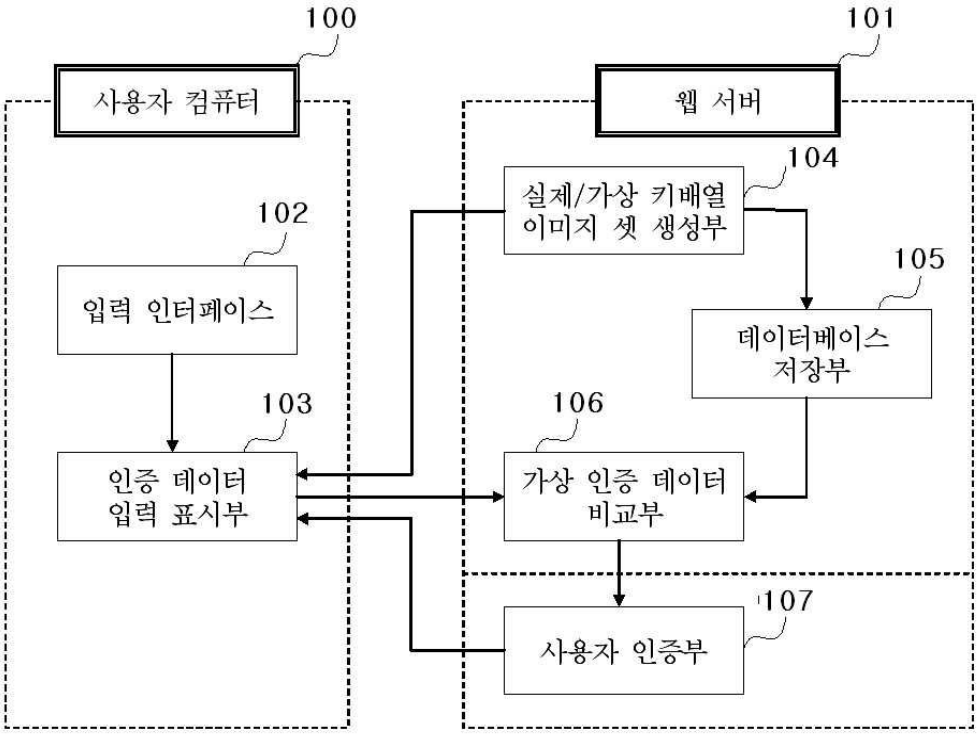
<8> (104): 실제/가상 키배열 이미지 셋 생성부

<9> (105): 데이터베이스 저장부 (106): 가상 인증 데이터 비교부

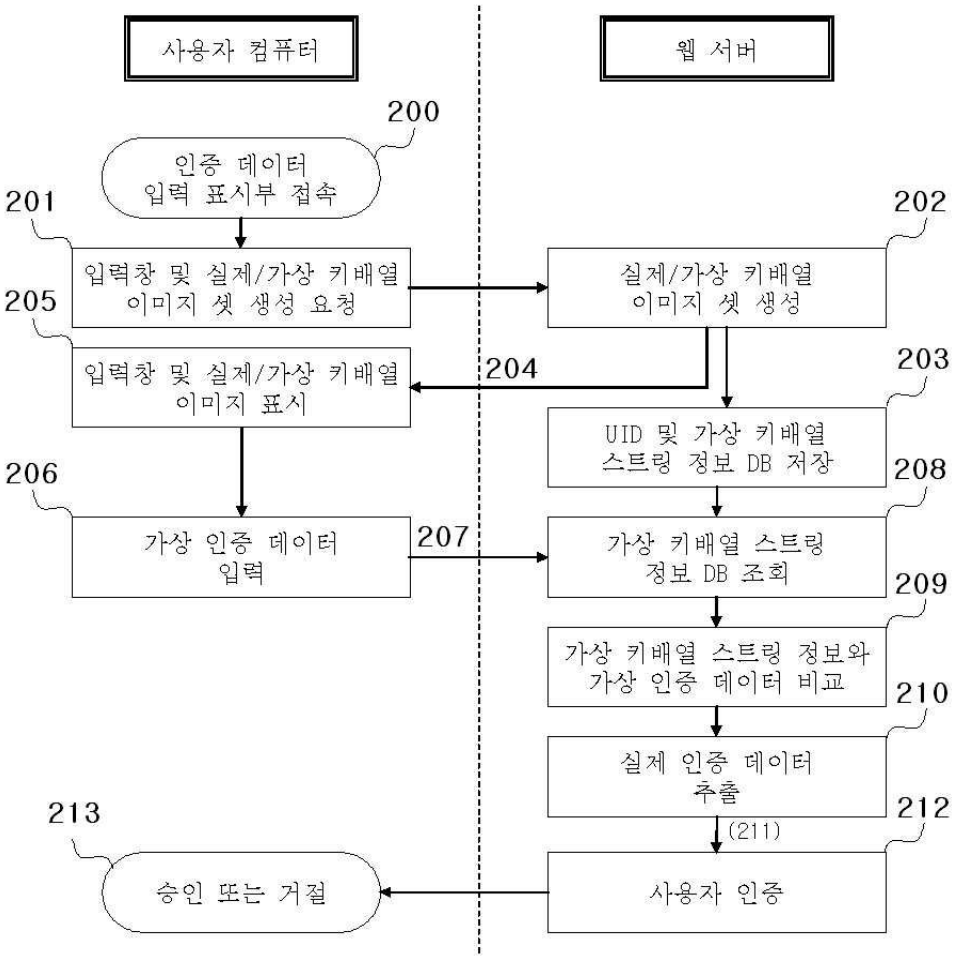
<10> (107): 사용자 인증부 (400): 실제/가상 키배열 이미지

도면

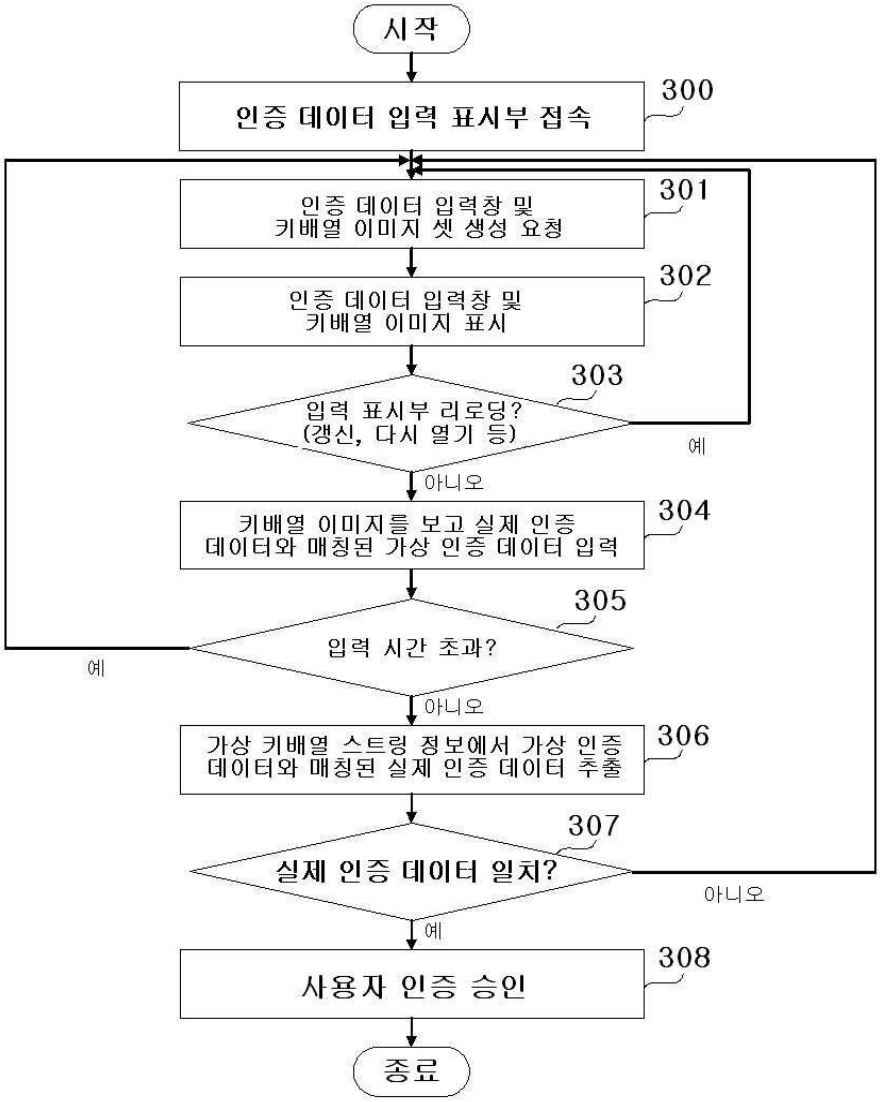
도면1


100
사용자 컴퓨터
101
웹 서버
104
실제/가상 키배열
이미지 셋 생성부
102
입력 인터페이스
105
데이터베이스
저장부
103
인증 데이터
입력 표시부
106
가상 인증 데이터
비교부
107
사용자 인증부

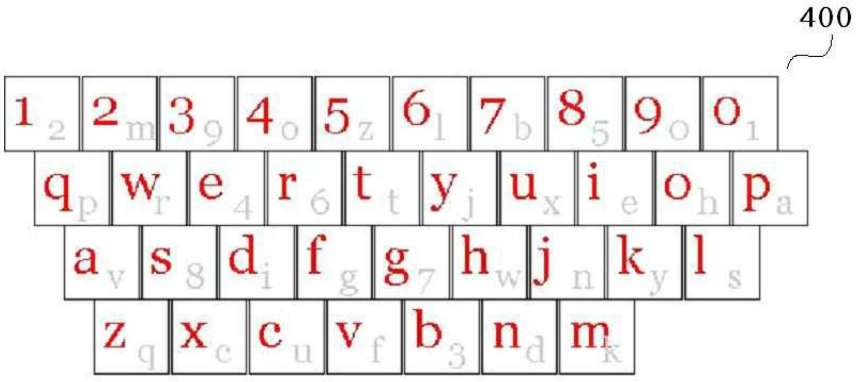
도면2


사용자 컴퓨터
웹 서버
200
인증 데이터
입력 표시부 접속
201
입력창 및 실제/가상 키배열
이미지 셋 생성 요청
202
실제/가상 키배열
이미지 셋 생성
205
입력창 및 실제/가상 키배열
이미지 표시
204
203
UID 및 가상 키배열
스트링 정보 DB 저장
206
가상 인증 데이터
입력
207
208
가상 키배열 스트링
정보 DB 조회
209
가상 키배열 스트링 정보와
가상 인증 데이터 비교
210
실제 인증 데이터
추출
(211)
212
213
승인 또는 거절
사용자 인증

도면3


시작
인증 데이터 입력 표시부 접속
300
인증 데이터 입력창 및
키배열 이미지 셋 생성 요청
301
인증 데이터 입력창 및
키배열 이미지 표시
302
입력 표시부 리로딩?
(갱신, 다시 열기 등)
303
예
아니오
키배열 이미지를 보고 실제 인증
데이터와 매칭된 가상 인증 데이터 입력
304
입력 시간 초과?
305
예
아니오
가상 키배열 스트링 정보에서 가상 인증
데이터와 매칭된 실제 인증 데이터 추출
306
실제 인증 데이터 일치?
307
아니오
예
사용자 인증 승인
308
종료

도면4


400
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
z x c v b n m