(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년01월24일
(11) 등록번호 10-1226319
(24) 등록일자 2013년01월18일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06F 21/20* (2006.01)
G06Q 20/42 (2012.01)
(21) 출원번호 10-2011-0000514
(22) 출원일자 2011년01월04일
심사청구일자 2011년01월04일
(65) 공개번호 10-2012-0046664
(43) 공개일자 2012년05월10일
(30) 우선권주장
1020100108194 2010년11월02일 대한민국(KR)
(56) 선행기술조사문헌
KR1020100108490 A
KR1020100095346 A
KR100838488 B1
KR1020040081179 A
전체 청구항 수 : 총 30 항

(73) 특허권자
인하대학교 산학협력단
인천광역시 남구 인하로 100, 인하대학교 (용현동)
(72) 발명자
양대헌
인천광역시 남구 소성로 71, 하이테크센터 317호 (용현동, 인하대학교)
(74) 대리인
특허법인무한

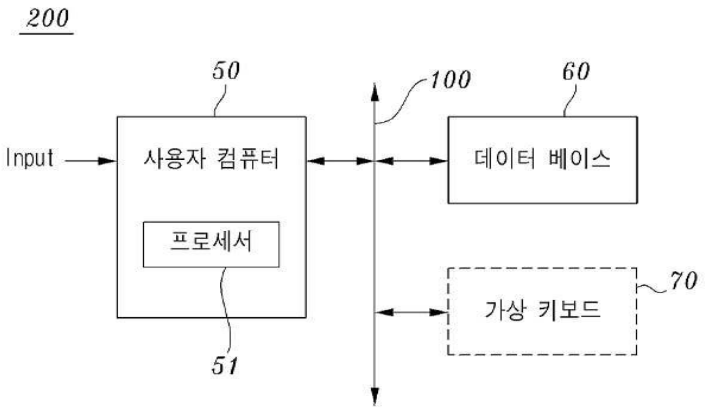
심사관 : 양종필

(54) 발명의 명칭 **신원 확인 인증 방법 및 이를 이용한 시스템**

(57) 요 약

신원 확인 인증 방법 및 이를 이용한 시스템을 개시한다. 상기 본 발명의 신원 확인 인증 시스템은 신원 확인 해독 프로그램이 설치된 컴퓨터 및 상기 컴퓨터로부터 신원 확인 요청을 수신한 후, 가상 키보드를 생성한 후, 상기 신원 확인 요청에 상응하는 데이터를 데이터 베이스로부터 추출하여 암호화시켜 상기 가상 키보드 상의 2차원 바코드 키캡으로 신원 확인 승인 여부의 2차원 바코드를 발급하는 인증 서버를 포함한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

사용자 컴퓨터로부터 신원 확인 요청을 수신한 후, 상기 신원 확인 요청에 상응하는 데이터를 데이터 베이스로부터 추출 및 암호화하여 2차원 바코드를 생성하고, 가상 키보드 상의 2차원 바코드 키캡에 신원 확인 승인 여부의 상기 2차원 바코드를 발급하는 인증 서버를 포함하는 신원 확인 인증 시스템.

청구항 2

사용자 컴퓨터로부터 신원 확인 요청을 수신한 후, 상기 사용자 컴퓨터의 화면 상에 표시하기 위한 가상 키보드를 생성하여 상기 사용자 컴퓨터로 전송하고, 상기 신원 확인 요청에 상응하는 데이터를 데이터 베이스로부터 추출하여 암호화하고, 상기 암호화된 데이터를 이용하여 생성된 워터마크 코드를 상기 가상 키보드 상에 추가하는 인증 서버를 포함하고,

상기 가상 키보드를 영상 이미지로 수신하여 상기 워터마크 코드를 해독하는 신원 확인 해독 프로그램이 프로그래밍된 카메라를 통해 상기 암호화된 데이터가 복호화되어 표시되는 것을 특징으로 하는 신원 확인 인증 시스템.

청구항 3

사용자 컴퓨터로부터 신원 확인 요청을 수신한 후, 상기 사용자 컴퓨터의 화면 상에 표시하기 위한 가상 키보드를 생성하고, 상기 신원 확인 요청에 상응하는 데이터를 데이터 베이스로부터 추출하여 암호화하고, 상기 암호화된 데이터를 이용하여 생성된 2차원 바코드를 상기 가상 키보드 상에 추가하는 인증 서버를 포함하고,

상기 가상 키보드를 영상 이미지로 수신하여 상기 2차원 바코드를 해독하는 신원 확인 해독 프로그램이 프로그래밍된 카메라를 통해 상기 암호화된 데이터가 복호화되어 표시되는 것을 특징으로 하는 신원 확인 인증 시스템.

청구항 4

제1항 또는 제3항에 있어서,

상기 2차원 바코드는,

상기 가상 키보드 상의 키캡들에 표시될 적어도 하나의 부호 및 해당 부호의 상기 가상 키보드 상에서의 위치 정보를 포함하는 상기 암호화된 데이터를 이용하여 생성되는 것을 특징으로 하는 가상 키보드를 이용한 신원 확인 인증 시스템.

청구항 5

제1항 또는 제3항에 있어서,

상기 가상 키보드의 키캡들 각각은,

빈 키캡들을 포함하거나 또는 의미 없는 무늬를 갖는 키캡들을 포함하는 것을 특징으로 하는 신원 확인 인증 시스템.

청구항 6

제1항 또는 제3항 중 어느 한 항에 있어서,

상기 2차원 바코드는,

Quic Response 코드, Aztec 코드, Data Matrix 코드, Cuecat 코드, Sema 코드, shot 코드들 중 어느 하나인 것을 특징으로 하는 신원 확인 인증 시스템.

청구항 7

제1항 내지 제3항 중 어느 한 항에 있어서,

상기 사용자 컴퓨터는,

상기 인증 서버와 유무선 접속이 가능한, 휴대용단말기, 휴대인터넷장치(Mobile Internet Device), MP3, MP4, PMP(Portable Multimedia Player), 노트북 컴퓨터, UMPC(Ultra Mobile PC), 또는 PC(personal computer), 휴대전화(cellular phone), 스마트폰, 및 PDA(personal digital assistants) 중 하나를 포함하는 전자 장치인 것을 특징으로 하는 신원 확인 인증 시스템.

청구항 8

제2항에 있어서,

상기 워터마크 코드는,

디지털 워터마킹 기술을 이용하여 생성되는 그림 또는 문자인 것을 특징으로 하는 신원 확인 인증 시스템.

청구항 9

사용자 컴퓨터로부터의 신원 확인 요청에 따라, 가상 키보드, 상기 가상 키보드의 키캡들에 표시될 적어도 하나의 부호 및 상기 적어도 하나의 부호의 상기 가상 키보드 상에서의 위치 정보를 생성하는 단계;

상기 적어도 하나의 부호 및 상기 위치 정보를 포함하는 데이터를 암호화하는 단계;

상기 암호화된 데이터를 이용하여 2차원 바코드 또는 워터마크 코드를 생성하는 단계;

상기 2차원 바코드 또는 워터마크 코드를 상기 사용자 컴퓨터로 전송하는 단계;

상기 사용자 컴퓨터에서 상기 사용자 컴퓨터의 사용자에 의해 상기 가상 키보드를 통해 입력된 정보를 수신하는 단계; 및

상기 수신된 정보를 이용하여 상기 사용자의 신원을 확인하는 단계

를 포함하는 신원 확인 인증 방법.

청구항 10

제9항에 있어서,

상기 암호화하는 단계는,

상기 사용자와 미리 공유된 비밀키 또는 상기 사용자의 공인 인증서의 공개키를 이용하여 상기 데이터를 암호화하는 단계인 것을 특징으로 하는 신원 확인 인증 방법.

청구항 11

인증 서버로 전송한 신원 확인 요청에 따라 상기 인증 서버로부터 수신된 2차원 바코드 또는 워터마크 코드를 및 가상 키보드를 화면에 표시하는 단계; 및

사용자에 의해 상기 가상 키보드를 통해 입력되는 정보를 상기 인증 서버로 전송하는 단계

를 포함하고,

상기 2차원 바코드 또는 워터마크 코드는 상기 가상 키보드의 키캡들에 표시될 적어도 하나의 부호 및 상기 적어도 하나의 부호의 상기 가상 키보드 상에서의 위치 정보를 포함하고,

상기 2차원 바코드 또는 워터마크 코드를 카메라를 통해 입력받는 휴대기기에서 상기 2차원 바코드 또는 워터마크 코드가 해석되고, 상기 적어도 하나의 부호가 상기 위치 정보에 기초하여 상기 가상 키보드의 해당 키캡에 대응하여 상기 휴대기기의 화면에 표시되는 신원 확인 인증 방법.

청구항 12

사용자 컴퓨터의 화면에 표시된 2차원 바코드 또는 워터마크 코드가 카메라를 통해 이미지 형태로 인식되는 경우, 상기 2차원 바코드 또는 워터마크 코드를 해석 및 복호화하고, 상기 사용자 컴퓨터의 화면에 더 표시된 가

상 키보드의 키캡들에 표시될 적어도 하나의 부호 및 상기 적어도 하나의 부호의 상기 가상 키보드 상에서의 위치 정보를 추출하는 단계; 및

상기 추출된 위치 정보에 기초하여 상기 적어도 하나의 부호를 상기 가상 키보드 상의 해당 키캡에 대응하여 표시하는 단계

를 포함하는 신원 확인 인증 방법.

청구항 13

사용자 컴퓨터로부터의 신원 확인 요청에 따라 생성 또는 선택된 적어도 하나의 부호를 암호화하는 단계;

상기 암호화된 부호를 이용하여 2차원 바코드 또는 워터마크 코드를 생성하는 단계;

상기 2차원 바코드 또는 워터마크 코드를 상기 사용자 컴퓨터로 전송하는 단계;

상기 사용자 컴퓨터에서 상기 사용자 컴퓨터의 사용자에 의해 입력된 부호를 수신하는 단계; 및

상기 수신된 부호와 상기 생성 또는 선택된 적어도 하나의 부호를 비교하여 상기 사용자의 신원을 확인하는 단계

를 포함하는 신원 확인 인증 방법.

청구항 14

인증 서버로부터 수신된 2차원 바코드 또는 워터마크 코드를 화면에 표시하는 단계;

사용자에 의해 입력되는 부호를 상기 인증 서버로 전송하는 단계

를 포함하고,

상기 2차원 바코드 또는 워터마크 코드는 상기 인증 서버에서 생성 또는 선택된 적어도 하나의 부호를 포함하고,

상기 화면에 표시된 2차원 바코드 또는 워터마크 코드는 휴대기기의 카메라를 통해 휴대기기로 입력되어 해석되어 상기 휴대기기의 화면에 상기 적어도 하나의 부호가 표시되는, 신원 확인 인증 방법.

청구항 15

사용자 컴퓨터의 화면에 표시된 2차원 바코드 또는 워터마크 코드가 카메라를 통해 이미지 형태로 인식되는 경우, 상기 2차원 바코드 또는 워터마크 코드를 해석 및 복호화하여 적어도 하나의 부호를 추출하는 단계; 및

상기 추출된 적어도 하나의 부호를 화면에 표시하는 단계

를 포함하고,

상기 2차원 바코드 또는 워터마크 코드는 상기 적어도 하나의 부호를 이용하여 인증 서버에서 생성되어 상기 사용자 컴퓨터로 전송되고,

상기 사용자 컴퓨터를 통해 사용자가 입력하는 부호가 상기 인증 서버로 전송되고, 상기 인증 서버에서 상기 입력된 부호와 상기 적어도 하나의 부호를 비교하여 상기 사용자의 신원이 확인되는, 신원 확인 인증 방법.

청구항 16

사용자 컴퓨터로부터의 신원 확인 요청에 따라, 가상 키보드, 상기 가상 키보드의 키캡들에 표시될 적어도 하나의 부호 및 상기 적어도 하나의 부호의 상기 가상 키보드 상에서의 위치 정보를 생성하는 생성부;

상기 적어도 하나의 부호 및 상기 위치 정보를 포함하는 데이터를 암호화하는 암호화부;

상기 암호화된 데이터를 이용하여 2차원 바코드 또는 워터마크 코드를 생성하는 코드 생성부;

상기 2차원 바코드 또는 워터마크 코드를 상기 사용자 컴퓨터로 전송하는 전송부;

상기 사용자 컴퓨터에서 상기 사용자 컴퓨터의 사용자에 의해 상기 가상 키보드를 통해 입력된 정보를 수신하는 수신부; 및

상기 수신된 정보를 이용하여 상기 사용자의 신원을 확인하는 신원 확인부

를 포함하는 인증 서버.

청구항 17

제16항에 있어서,

상기 암호화부는,

상기 사용자와 미리 공유된 비밀키 또는 상기 사용자의 공인 인증서의 공개키를 이용하여 상기 데이터를 암호화하는, 인증 서버.

청구항 18

제16항에 있어서,

상기 2차원 바코드 또는 워터마크 코드는 상기 사용자 컴퓨터의 화면을 통해 표시되고,

상기 2차원 바코드 또는 워터마크 코드를 카메라를 통해 이미지 형태로 입력받은 휴대기기에서 상기 2차원 바코드 또는 워터마크 코드가 해석 및 복호화되어 상기 적어도 하나의 부호가 추출되고,

상기 적어도 하나의 부호는 상기 휴대기기의 화면에 표시되되, 상기 위치 정보에 기초하여 상기 사용자 컴퓨터의 화면에 표시된 가상 키보드의 해당 키캡의 위치에 대응하여 표시되는, 인증 서버.

청구항 19

제18항에 있어서,

상기 복호화는 상기 사용자와 미리 공유된 비밀키 또는 상기 사용자의 공인 인증서의 공개키에 대응하는 비밀키를 이용하여 수행되는, 인증 서버.

청구항 20

제18항에 있어서,

상기 신원 확인부는,

상기 수신된 정보와 상기 사용자의 비밀번호를 서로 비교하여 상기 사용자의 신원을 확인하는, 인증 서버.

청구항 21

제18항에 있어서,

상기 적어도 하나의 부호는 문자, 숫자, 그림, 도형 중 적어도 하나를 포함하는, 인증 서버.

청구항 22

인증 서버로 전송한 신원 확인 요청에 따라 상기 인증 서버로부터 수신된 2차원 바코드 또는 워터마크 코드를 화면에 표시하고, 상기 인증 서버로부터 더 수신된 가상 키보드를 화면에 더 표시하는 표시부; 및

사용자에 의해 상기 가상 키보드를 통해 입력되는 정보를 상기 인증 서버로 전송하는 전송부

를 포함하고,

상기 2차원 바코드 또는 워터마크 코드는 상기 가상 키보드의 키캡들에 표시될 적어도 하나의 부호 및 상기 적어도 하나의 부호의 상기 가상 키보드 상에서의 위치 정보를 포함하고,

상기 2차원 바코드 또는 워터마크 코드를 카메라를 통해 입력받는 휴대기기에서 상기 2차원 바코드 또는 워터마크 코드가 해석되고, 상기 적어도 하나의 부호가 상기 위치 정보에 기초하여 상기 가상 키보드의 해당 키캡에 대응하여 상기 휴대기기의 화면에 표시되는, 사용자 컴퓨터.

청구항 23

제22항에 있어서,

상기 인증 서버로 전송된 정보와 상기 사용자의 비밀번호에 기초하여 상기 인증 서버에서 상기 사용자의 신원이 확인되는, 사용자 컴퓨터.

청구항 24

제22항에 있어서,

상기 적어도 하나의 부호 및 상기 위치 정보는 상기 사용자와 상기 인증 서버간에 미리 공유된 비밀키 또는 상기 사용자의 공인 인증서의 공개키를 이용하여 상기 인증 서버에서 암호화되고, 상기 비밀키 또는 상기 공개키에 대응하는 비밀키를 이용하여 상기 휴대기기에서 복호화되는, 사용자 컴퓨터.

청구항 25

사용자 컴퓨터의 화면에 표시된 2차원 바코드 또는 워터마크 코드가 카메라를 통해 이미지 형태로 인식되는 경우, 상기 2차원 바코드 또는 워터마크 코드를 해석 및 복호화하여 가상 키보드의 키캡들에 표시될 적어도 하나의 부호 및 상기 적어도 하나의 부호의 상기 가상 키보드 상에서의 위치 정보를 추출하는 추출부; 및

상기 추출된 위치 정보에 기초하여 상기 적어도 하나의 부호를 상기 가상 키보드 상의 해당 키캡에 대응하여 표시하는 표시부

를 포함하고,

상기 가상 키보드는 상기 사용자 컴퓨터의 화면에 상기 2차원 바코드 또는 워터마크 코드와 함께 표시되는, 휴대기기.

청구항 26

제25항에 있어서,

상기 2차원 바코드 또는 워터마크 코드는, 상기 가상 키보드와 함께 상기 사용자 컴퓨터와 통신하는 인증 서버에서 생성되어 상기 사용자 컴퓨터로 전송되고,

상기 사용자 컴퓨터의 화면에 표시된 가상 키보드를 통해 입력되는 정보를 통해 상기 인증 서버에서 사용자의 신원이 확인되는, 휴대기기.

청구항 27

제25항에 있어서,

상기 적어도 하나의 부호 및 상기 위치 정보는 상기 사용자 컴퓨터와 통신하는 인증 서버와 사용자 간에 미리 공유된 비밀키 또는 상기 사용자의 공인 인증서의 공개키를 이용하여 상기 인증 서버에서 암호화되고,

상기 추출부는,

상기 비밀키 또는 상기 공개키에 대응하는 비밀키를 이용하여 상기 암호화된 적어도 하나의 부호 및 위치 정보를 복호화하는, 휴대기기.

청구항 28

사용자 컴퓨터로부터의 신원 확인 요청에 따라 생성 또는 선택된 적어도 하나의 부호를 암호화하는 암호화부;

상기 암호화된 부호를 이용하여 2차원 바코드 또는 워터마크 코드를 생성하는 코드 생성부;

상기 2차원 바코드 또는 워터마크 코드를 상기 사용자 컴퓨터로 전송하는 전송부;

상기 사용자 컴퓨터에서 상기 사용자 컴퓨터의 사용자에 의해 입력된 부호를 수신하는 수신부; 및

상기 수신된 부호와 상기 생성 또는 선택된 적어도 하나의 부호를 비교하여 상기 사용자의 신원을 확인하는 신원 확인부

를 포함하는 인증 서버.

청구항 29

인증 서버로부터 수신된 2차원 바코드 또는 워터마크 코드를 화면에 표시하는 표시부;

사용자에 의해 입력되는 부호를 상기 인증 서버로 전송하는 전송부

를 포함하고,

상기 2차원 바코드 또는 워터마크 코드는 상기 인증 서버에서 생성 또는 선택된 적어도 하나의 부호를 포함하고,

상기 화면에 표시된 2차원 바코드 또는 워터마크 코드는 휴대기기의 카메라를 통해 휴대기기로 입력되어 해석되어 상기 휴대기기의 화면에 상기 적어도 하나의 부호가 표시되는, 사용자 컴퓨터.

청구항 30

사용자 컴퓨터의 화면에 표시된 2차원 바코드 또는 워터마크 코드가 카메라를 통해 이미지 형태로 인식되는 경우, 상기 2차원 바코드를 해석 및 복호화하여 적어도 하나의 부호를 추출하는 추출부; 및

상기 추출된 적어도 하나의 부호를 화면에 표시하는 표시부

를 포함하고,

상기 2차원 바코드 또는 워터마크 코드는 상기 적어도 하나의 부호를 이용하여 인증 서버에서 생성되어 상기 사용자 컴퓨터로 전송되고,

상기 사용자 컴퓨터를 통해 사용자가 입력하는 부호가 상기 인증 서버로 전송되고, 상기 인증 서버에서 상기 입력된 부호와 상기 적어도 하나의 부호를 비교하여 상기 사용자의 신원이 확인되는, 휴대기기.

명 세 서

기 술 분 야

[0001] 본 발명은 인증 방법 및 시스템에 관한 것으로, 보다 상세하게는 인증 서버로부터 가상 키보드를 제공받아 사용자에 따른 비공개 암호의 입력을 통해 보다 신뢰성 있는 신원 확인을 제공할 수 있는 신원 확인 인증방법 및 이를 이용한 시스템에 관한 것이다.

배 경 기 술

[0002] 본 발명은 전자상거래 보안분야에 관련된 것으로서, 좀 더 상세히 기술하면 휴대용 플래시메모리를 이용하여 자신의 지문데이터 및 디지털인증키를 항상 저장 및 휴대한 상태에서 네트웍에 접속시 사용자(user)의 신원을 정확히 파악할 수 있도록 하는 신원인증시스템의 운용방법에 관한 것이다.

[0003] 최근 들어 인터넷이 급속히 확산됨에 따라 오프라인보다 온라인에 기반을 둔 전자상거래가 점점 더 활성화되고 있음은 주지할 만한 사실이다.

[0004] 이에 따라 상기 전자상거래의 확산과 더불어 이에 관련한 개인정보의 유출 및 각종 컴퓨터 범죄 또한 만연하고 있는 실정이다.

[0005] 특히, 인터넷 뱅킹 등과 같은 분야에서는 엄청난 사이버 캐쉬가 거래되는 바, 개인정보의 유출 및 급증하는 컴퓨터 범죄에 대한 해결책으로 다양한 형태의 신원인증시스템이 연구 개발되고 있다.

[0006] 일례로 종래에는 이러한 신원인증시스템으로서 통상 사용자가 네트워크에 접속시 신원을 확인하기 위해 미리 설정해둔 ID/PASSWORD를 입력해야만 각 사의 대상 서버에 로그인할 수 있도록 하는 방식이 고작이었다.

[0007] 그러나, 상기와 같이 ID와 PASSWORD를 이용한 신원인증시스템은 자신이 모르는 사이 디스플레이 상에 남겨진 개인정보가 쉽게 누출되는 폐단이 있을 뿐만 아니라, 컴퓨터 해킹 등을 통해서도 쉽게 빼낼 수 있는 것이 사실이므로 이에 대한 대책이 시급한 실정이었다.

[0008] 따라서, 최근 이에 대한 대비책의 하나로 통상 퍼스널 컴퓨터에 디지털인증키(예로서, PKI인증키)를 설치하여 로그인 시 이를 통해 신원인증을 하고 있으나, 상기한 디지털인증키는 인터넷 뱅킹을 비롯한 각종 On-Line 금융거래에 사용되고 있는 통상 한번 인증키를 발급 받아 퍼스널 컴퓨터에 설치한 후, 이를 다른 퍼스널 컴퓨터를 이용해 로그인할 때에는 기존의 인증키를 폐기한 후, 새로 인증키를 설치하거나 아니면 디스켓에 저장하여 가지

고 다녀야 하므로 사용상 불편함이 있었다.

[0009] 또한 이러한 디지털 인증키가 컴퓨터 드라이브에 설치된 경우에는 상기 디지털인증키에 대한 ID/PASSWORD만 파악하면 누구나 얼마든지 서버에 쉽게 접속이 가능하므로 이에 대한 근본적인 대비책이 시급한 실정이다.

발명의 내용

해결하려는 과제

[0010] 본 발명에 해결하고자 하는 과제는 디지털 인증키가 컴퓨터 드라이브에 설치된 경우에는 디지털 인증키에 대한 ID/password만 파악하면 누구나 얼마든지 서버에 쉽게 접속이 가능하므로 이에 문제점을 해결할 수 있는 신원 확인 인증 방법 및 이를 이용한 시스템을 제공하는 것이다.

과제의 해결 수단

[0011] 상기 과제를 해결하기 위한 본 발명의 신원 확인 인증 시스템은 신원 확인 해독 프로그램이 설치된 컴퓨터 및 상기 컴퓨터로부터 신원 확인 요청을 수신한 후, 가상 키보드를 생성한 후, 상기 신원 확인 요청에 상응하는 데이터를 데이터 베이스로부터 추출하여 암호화 된 2차원 바코드를 상기 가상 키보드 상의 QR 키캡에 신원 확인 승인 여부의 2차원 바코드를 발급하는 인증 서버를 포함한다.

[0012] 상기 과제를 해결하기 위한 본 발명의 신원 확인 인증 시스템은 컴퓨터, 상기 컴퓨터로부터 신원 확인 요청을 수신한 후, 상기 컴퓨터의 화면 상에 가상 키보드를 생성하고, 상기 신원 확인 요청에 상응하는 데이터를 데이터 베이스로부터 추출하여 암호화된 데이터를 상기 가상 키보드 상의 키캡들에 워터마크 코드를 발급하는 인증 서버 및 상기 가상 키보드를 영상 이미지로 수신하여 상기 워터마크 코드를 해독하는 신원 확인 해독 프로그램이 프로그래밍된 카메라를 포함하며, 상기 컴퓨터는 암호화된 데이터를 복호화하는 것을 특징으로 한다.

[0013] 상기 과제를 해결하기 위한 본 발명의 신원 확인 인증 시스템은 컴퓨터, 상기 컴퓨터로부터 신원 확인 요청을 수신한 후, 상기 컴퓨터의 화면 상에 가상 키보드를 생성하고, 상기 신원 확인 요청에 상응하는 데이터를 데이터 베이스로부터 추출하여 암호화된 2차원 바코드를 상기 가상 키보드 상의 QR 키캡에 신원 확인 승인 여부의 2차원 바코드를 발급하는 인증 서버 및 상기 가상 키보드를 영상 이미지로 수신하여 상기 2차원 바코드를 해독하는 신원 확인 해독 프로그램이 프로그래밍된 카메라를 포함하며, 상기 컴퓨터는 암호화된 2차원 바코드를 복호화하는 것을 특징으로 한다.

[0014] 상기 2차원 바코드는 상기 컴퓨터 내에 설치된 신원 확인 해독 프로그램을 통해 상기 가상 키보드 상의 키캡들에 나타나는 것을 특징으로 한다.

[0015] 상기 가상 키보드의 키캡들 각각은 아무런 문자, 숫자, 부호가 표시되어 있지 않고, 빈 키캡만을 가지거나 또는 의미 없는 무늬를 갖는 것을 특징으로 한다.

[0016] 상기 컴퓨터는 상기 인증 서버와 유무선 접속이 가능한, 휴대용단말기, 휴대인터넷장치(Mobile Internet Device), MP3, MP4, PMP(Portable Multimedia Player), 노트북 컴퓨터, UMPC(Ultra Mobile PC), 또는 PC(personal computer), 휴대전화(cellular phone), 스마트폰, 또는 PDA(personal digital assistants)을 포함하는 각종 전자장치인 것을 특징으로 한다.

[0017] 상기 워터마크 코드는 디지털 워터마킹 기술을 이용하여 생성되는 그림 또는 문자인 것을 특징으로 한다.

[0018] 상기 과제를 해결하기 위한 본 발명의 신원 확인 인증 방법은 사용자 휴대 단말기(컴퓨터)를 통해 인증 서버로 접속하는 제1 단계, 인증 서버로부터 사용자 신원 확인을 위한 데이터를 수신하는 제2 단계, 수신된 데이터를 복호화 및 암호화하여 가상 키보드로 디스플레이하는 제3 단계, 상기 가상 키보드 상에 사용자에 따라 서로 다르게 전송된 2차원 바코드를 해석하여 신원 확인을 인증하는 제4 단계를 포함한다.

[0019] 상기 제3단계는 상기 사용자의 공인 인증서의 공개키를 이용하여 디스플레이하는 단계인 것을 특징으로 한다.

[0020] 상기 제4단계는 상기 사용자 컴퓨터 내에 설치된 암호 해독 프로그램을 통해 상기 2차원 바코드를 해석하여 신원 확인이 인증되는 단계인 것을 특징으로 한다.

[0021] 상기 과제를 해결하기 위한 본 발명의 신원 확인 인증 방법은 사용자 휴대 단말기(컴퓨터)를 통해 인증 서버로 접속하는 제1 단계, 인증 서버로부터 사용자 신원 확인을 위한 데이터를 수신하는 제2 단계, 수신된 데이터를 복호화 및 암호화하여 가상 키보드로 디스플레이하는 제3 단계 및 휴대 카메라에 저장된 신원 확인 해독 프로그

램을 실행시켜, 상기 가상 키보드 상에 사용자에 따라 서로 다르게 전송된 2차원 바코드를 상기 카메라의 영상 이미지로 해석하여 신원 확인을 인증하는 제4 단계를 포함한다.

[0022] 상기 제4단계는 상기 휴대 카메라 내에 설치된 암호 해독 프로그램을 통해 상기 사용자 컴퓨터의 화면에 디스플레이된 상기 2차원 바코드를 이미지 영상으로 해석하여 신원 확인이 인증되는 단계인 것을 특징으로 한다.

발명의 효과

[0023] 본 발명에 따르면, 인증 서버에 로그인 시 본인의 공인인증서의 공개키 및 인증 서버로부터의 디지털 인증키를 이용함으로써 2중의 신원 확인 과정을 통해 개인 정보의 유출 및 도용에 따른 폐단을 원천적으로 방지할 수 있는 효과가 있다.

[0024] 또한 본 발명에 따르면, 다양한 인증 수단을 이용하더라도 각 인증 수단으로 인한 취약점을 제거함으로써 여전히 강한 안전성을 유지할 수 있다.

[0025] 또한 본 발명에 따르면, 패스워드의 경우는 서버의 데이터 베이스가 해킹(hacking)되는 경우에도 사용자의 패스워드 정보가 노출되지 않는 효과가 있다.

[0026] 또한 본 발명에 따르면, 다양한 인증 수단을 가진 통합 사용자 인증 프로토콜을 제공하여, 홈 네트워크 산업과 같이 노인이나 어린이 등 IT 환경에 익숙하지 않은 사용자가 많은 상황에서도 쉽고 안전한 보안 서비스를 선택적으로 제공할 수 있으므로 산업적 활용도를 크게 높이는 효과가 있다.

도면의 간단한 설명

[0027] 도 1은 본 발명의 실시 예에 따른 신원 확인 인증 시스템의 블록도를 나타낸 예시도이다.

도 2는 도 1에 도시된 가상 키보드의 예를 나타낸 예시도이다.

도 3는 도 1에 도시된 가상 키보드의 다른 예를 나타낸 예시도이다.

도 4는 본 발명의 실시 예에 따른 신원 확인 인증 방법을 나타낸 플로우 챠트이다.

도 5는 본 발명의 실시 예에 따른 신원 확인 인증 시스템을 나타낸 블록도이다.

도 6은 본 발명의 실시 예에 있어서, 가상 키보드의 부호를 휴대기기의 화면에 나타낸 도면이다.

도 7은 본 발명의 실시 예에 따른 신원 확인 인증 방법을 도시한 흐름도이다.

도 8은 본 발명의 실시 예에 있어서, 2차원 바코드를 통해 전송된 그림을 휴대기기 및 사용자 컴퓨터의 화면에 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

[0028] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며, 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0029] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다. 또한, 명세서에 기재된 "~부","~기" 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

[0030] 본 발명과 본 발명의 동작상의 이점 및 본 발명의 실시에 의하여 달성되는 목적을 충분히 이해하기 위해서는 본 발명의 바람직한 실시 예를 예시하는 첨부 도면 및 도면에 기재된 내용을 참조하여야 한다.

[0031] 도 1은 본 발명의 실시 예에 따른 신원 확인 인증 시스템의 블록도를 나타낸 예시도이다.

[0032] 도 1에 도시된 바와 같이, 신원 확인 인증 시스템(200)은 사용자 컴퓨터(50), 인증 서버(100), 데이터 베이스(60) 및 가상 키보드(70)를 포함한다.

[0033] 또한, 다른 실시예로, 상기 신원 확인 인증 시스템(200)은 암호화 데이터를 해독할 수 있는 응용프로그램이 설치된 도 3에 도시된 카메라(85)를 더 포함할 수 있다.

[0034] 상기 사용자 컴퓨터(50)는 상기 인증 서버(100)로부터 암호화 데이터를 해독할 수 있는 응용 프로그램을 다운로드할 수 있고, 다운로드된 응용 프로그램은 프로세서(51)에 의해 상기 사용자 컴퓨터(50)의 하드웨어 내에 저장 및 실행될 수 있다.

[0035] 상기 사용자 컴퓨터(50)는 상기 인증 서버(100)와 유무선 접속이 가능한, 휴대용단말기, 휴대인터넷장치(Mobile Internet Device), MP3, MP4, PMP(Portable Multimedia Player), 노트북 컴퓨터, UMPC(Ultra Mobile PC), 또는 PC(personal computer), 휴대전화(cellular phone), 스마트폰, 또는 PDA(personal digital assistants)와 같은 각종 전자장치가 될 수 있다.

[0036] 또한, 상기 사용자 컴퓨터(50)가 휴대 단말기일 경우, SIM(subscribe identity module)을 내장하는 기존의 CDMA(code division multiple access)용 단말기뿐만 아니라, 상기 SIM을 탑재한 카드를 탈부착할 수 있는 GSM(Global system for mobile communication)용 단말기를 포함할 수 있다.

[0037] 상기 인증 서버(100)는 상기 사용자 컴퓨터(50)로부터 전송된 신원 확인 요청을 수신하여 상기 사용자의 신원 확인 데이터를 상기 인증 서버(100)와 접속된 데이터 베이스(60)로부터 추출하여 암호화 과정을 수행한다.

[0038] 여기서, 신원 확인 요청은 사용자가 상기 사용자 컴퓨터(50)를 이용하여 은행 사이트나 포털 사이트 등과 같이 사용자의 신원 확인이 필요한 사이트나 시스템과 연계된 상기 인증 서버(100)에 접속하여 자신의 로그인 아이디 등의 정보를 입력함으로써, 발생할 수 있다.

[0039] 이때, 상기 인증 서버(100)는 상기 사용자 컴퓨터(50)에 저장된 공인 인증서의 공개키 또는 다른 인증 수단과 상기 데이터 베이스(60)로부터 추출된 사용자 신원 확인 데이터의 매칭 유·무에 따라 상기 사용자 컴퓨터(50)의 화면상에 가상 키보드(70)를 전송한다.

[0040] 참고로, 상기 인증 서버(100)는 구성 모양에 따라 Star형, Tree and Hyper Tree형으로 구분될 수 있는 통신망, 거리에 따라 개인 통신망(Personal Area Network), 근거리 통신망(LAN: Local Area Network), 도시 간 통신망(MAN: Metropolitan Area Network) 또는 국가 간 통신망(WAN: Wide Area Network)으로 구분될 수 있는 통신망 및 부가가치 통신망(VAN: Value Added Network), ISDN(Integrated Service Network)과 같은 통신망 등의 다양한 통신망들 중 적어도 하나를 이용하여 상기 사용자 컴퓨터(50)와 연결될 수 있다.

[0041] 상기 가상 키보드(70)는 상기 데이터 베이스(60)로부터 전송된 암호화된 2차원 바코드가 입력된 키캡을 포함할 수 있다.

[0042] 여기서, 상기 2차원 바코드는 상기 인증 서버(100)와 사용자간에 미리 공유된 비밀키나 상기 사용자의 공인 인증서의 공개키에 의해 암호화된 정보를 포함할 수 있다. 여기서, 상기 정보는 상기 가상 키보드(70)와 관련된 정보로서, 이후 더욱 자세히 설명한다.

[0043] 또한, 다른 실시예로, 상기 2차원 바코드는 상기 인증 서버(100)로부터 생성될 수도 있다. 또한, 상기 2차원 바코드는 상기 가상 키보드(70)의 키캡에 입력될 수도 있으나, 상기 가상 키보드(70)의 특정 공간에 삽입될 수도 있고, 상기 가상 키보드(70)와는 별도로 상기 가상 키보드(70)와 함께 사용자 컴퓨터(50)로 전송될 수도 있다.

[0044] 예를 들어, 상기 2차원 바코드가 입력된 키캡은 상기 가상 키보드(70) 최외각에 위치할 수 있으며, 상기 2차원 바코드가 입력된 키캡을 제외한 다수의 키캡들 각각은 눈으로 식별 가능한 문자, 숫자, 도형과 같은 부호가 아닌 불특정 무늬나 모양 또는 빈 키캡만으로 형성되도록 상기 가상 키보드 상에 배열된다.

[0045] 이때, 사용자가 2차원 바코드가 입력된 키캡을 주변기기(예를 들어, 마우스나 키보드)를 이용하여 선택하거나 또는 사용자 터치(예컨대, 상기 사용자 컴퓨터(50)의 화면이 터치스크린일 경우)를 통해 누르게 되면, 상기 2차원 바코드는 상기 사용자 컴퓨터(50)에 저장된 신원 확인 해독 프로그램을 통해 해독되어, 상기 가상 키보드 상에 2차원 바코드가 도형 또는 식별 문자, 부호 등으로 배열될 수 있다.

[0046] 예를 들어, 상술한 바와 같이, 상기 2차원 바코드는 암호화된 정보를 포함하고, 상기 정보는 상기 가상 키보드(70)의 키캡들을 통해 배열될 문자, 숫자, 도형과 같은 적어도 하나의 부호를 포함할 수 있다. 또한, 상기 정보는 상기 부호에 대응되는 키캡에 대한 정보(즉, 상기 부호가 표시될 위치 정보)를 더 포함할 수 있다.

[0047] 즉, 사용자 컴퓨터(50)에 상기 가상 키보드(70)가 표시되면, 사용자 컴퓨터(50)는 상기 인증 서버(100)에서 전송되는 상기 가상 키보드(70)에 포함된 상기 2차원 바코드 또는 상기 인증 서버(100)에서 상기 가상 키보드(7

0)와 함께 전송되는 상기 2차원 바코드를 신원 확인 해독 프로그램을 통해 해독하여 상기 2차원 바코드에 포함된 암호화된 정보를 얻을 수 있고, 상술한 비밀키나 공인 인증서의 공개키를 이용하여 상기 정보를 복호화할 있다. 따라서, 사용자 컴퓨터(50)는 상기 적어도 하나의 부호와 상기 부호의 위치 정보를 얻을 수 있고, 상기 적어도 하나의 부호를 상기 위치 정보에 따라 상기 가상 키보드(70)에 배열할 수 있다. 이 경우, 사용자는 사용자 컴퓨터(50)가 포함하는 주변기기나 터치스크린 등의 사용자 입력 인터페이스를 이용하여 상기 가상 키보드(70)에 비밀번호와 같은 신원 확인 정보를 입력할 수 있다. 상기 가상 키보드(70)를 통해 입력된 신원 확인 정보는 상기 인증 서버(100)로 전송될 수 있고, 상기 인증 서버(100)는 최초 전달된 로그인 아이디와 상기 신원 확인 정보를 통해 사용자의 신원을 확인할 수 있게 된다.

[0048] 또한, 상기 2차원 바코드로는 Quic Response 코드(이하, QR 코드), Aztec 코드, Data Matrix 코드, Cuecat 코드, Sema 코드, shot 코드들 중 적어도 하나가 이용될 수 있다.

[0049] 이 경우, 상기 카메라(85)는 상기 가상 키보드(70) 상에 배치된 2차원 바코드를 이미지 영상으로 수신하여 상기 카메라(85)에 설치된 신원 확인 해독 프로그램을 구동시킴으로써 상기 2차원 바코드가 해석된 상기 적어도 하나의 부호를 사용자에게 눈으로 확인시켜줄 수 있다.

[0050] 이미 설명한 바와 같이, 상기 2차원 바코드는 상기 가상 키보드(70)의 키캡 중 하나를 통해 표시될 수도 있으나, 상기 가상 키보드(70)의 다른 특정 영역을 통해 표시될 수도 있고, 상기 가상 키보드(70) 내부가 아니라 별도로 상기 가상 키보드(70)와 함께 사용자 컴퓨터(50)로 전송되어, 상기 가상 키보드(70)와는 별도로 사용자 컴퓨터(50)의 화면을 통해 표시될 수도 있다.

[0051] 상기 카메라(85)는 상기 사용자 컴퓨터(50)의 화면을 통해 표시되는 상기 2차원 바코드를 이미지 영상으로 입력받고, 이미지 영상에서 상기 2차원 바코드를 추출하여 상기 신원 확인 해독 프로그램을 통해 상기 추출된 2차원 바코드를 해석하여 암호화된 정보를 얻을 수 있다. 상기 암호화된 정보는 상술한 비밀키나 공인 인증서의 공개키를 통해 복호화할 수 있고, 상기 정보가 포함하는 부호들이 상기 가상 키보드(70)의 해당 키캡과 대응하여 표시될 수 있다. 이때, 사용자는 비밀번호와 같은 신원 확인 정보를 상기 가상 키보드(70)를 통해 입력할 수 있고, 입력된 신원 확인 정보는 상기 인증 서버(100)로 전송되어 상기 사용자를 인증하는데 이용될 수 있다.

[0052] 도 2는 도 1에 도시된 가상 키보드의 예를 나타낸 예시도이며, 도 3는 도 1에 도시된 가상 키보드의 다른 예를 나타낸 예시도이다.

[0053] 도 1 및 도 2를 참조하면, 상기 가상 키보드(70)는 도 1에 도시된, 상기 인증 서버(100)로부터 생성되어 상기 사용자 컴퓨터(50)의 디스플레이에 나타난다.

[0054] 상기 가상 키보드(70) 내에 배치된 다수의 키캡들 각각은 눈으로 식별 가능한 문자, 숫자, 도형 등의 부호가 아닌 불특정 무늬, 모양 또는 빈 키캡 일 수 있다.

[0055] 또한, 상기 2차원 바코드가 입력된 키캡은 상기 가상 키보드 최외각에 위치하며, 이때, 사용자가 2차원 바코드가 입력된 키캡을 주변기기 또는 사용자 터치(예컨대, 상기 사용자 컴퓨터(50)의 화면이 터치스크린일 경우)를 통해 누르게 되면, 상기 복조 및 암호화된 2차원 바코드는 상기 사용자 컴퓨터(50)에 저장된 신원 확인 해독 프로그램을 통해 해독되어, 상기 가상 키보드(70) 상에 2차원 바코드가 도형 또는 식별 문자, 부호 등으로 배열될 수 있다.

[0056] 도 1 및 도 3을 참조하면, 상기 사용자 컴퓨터(50)가 휴대 단말기일 경우, 상기 가상 키보드(71)는 상기 인증 서버(100)로부터 생성되어 사용자의 휴대 단말기(50-1)의 디스플레이에 나타난다.

[0057] 상기 가상 키보드(70)는 도 1에 도시된, 상기 인증 서버(100)로부터 생성되어 상기 사용자 컴퓨터(50)의 디스플레이에 나타난다.

[0058] 상기 가상 키보드(71) 내에 배치된 다수의 키캡들 각각은 눈으로 식별 가능한 문자, 기호, 부호가 아닌 불특정 모양 또는 빈 키캡 일 수 있다.

[0059] 또한, 상기 가상 키보드(71) 내에 배치된 다수의 키캡들 각각은 암호화된 2차원 바코드가 나타나도록 배열될 수 있다.

[0060] 상기 암호화된 2차원 바코드에는 인증 서버(100)가 무작위로 고른 단어, 문장, 또는 그림 등이 암호화되어 있다.

[0061] 또한, 상기 가상 키보드(71) 내에 배치된 다수의 키캡들 각각은 2차원 바코드 대신 디지털 워터마크(예컨대, 그

림, 도형 등)로 대체하여 배치될 수 있다.

[0062] 예를 들어, 상기 인증 서버에서 암호화한 정보를 워터마킹 기술을 이용하여 어떤 그림에 상기 암호화한 정보를 삽입하고, 이를 사용자에게 보여준다.

[0063] 참고로, 상기 워터마킹 기술은 텍스트, 이미지, 비디오, 오디오 등의 원본 데이터에 본래 소유주만이 아는 마크(Mark)를 사람의 육안이나 귀로는 구별할 수 없게 삽입하는 기술을 말한다.

[0064] 만약 일반 사용자들이 디지털 정보를 불법 복제해 정당한 대가나 허락 없이 상업용 혹은 기타 용도로 사용했을 때 원 소유자는 자신의 워터마크를 추출함으로써 자신의 소유임을 밝힐 수 있다. 이는 재산권 행사의 결정적인 증거가 된다. 워터마크를 할 경우 흐린 바탕무늬나 로고와 같은 마크가 디지털 이미지 원본에 삽입된다. 사용자가 이미지를 보거나 소프트웨어를 사용하는데 전혀 지장을 주지 않으면서도 복제를 방지할 수 있다.

[0065] 이는 또 원본의 출처를 밝히거나 누구에게 전달된 정보인지를 추적할 때도 사용되기 때문에 원천적인 복제 방지뿐 아니라 복제 경로를 추적하는 데도 자주 이용된다. 기존의 예술품에 화가의 도장이나 서명을 넣어두던 낙관이 디지털 시대에 그 형태가 바뀐 것으로 '디지털 낙관'이라고 할 수 있다.

[0066] 특히 전자 상거래 시대에는 전자책, 인터넷 신문과 잡지, 비디오, 음악 등이 네트워크 상에서 거래되기 때문에 워터마크 기술의 중요성은 더욱 높아지고 있다.

[0067] 그리고 나서, 사용자는 신원 확인 해독 프로그램이 프로그래밍된 카메라를 이용하여 상기 가상 키보드(71)의 이미지 영상을 해독한 2차원 바코드 또는 워터마크를 카메라 영상으로 통해 확인할 수 있다.

[0068] 상기 카메라(85)는 2차원 바코드 또는 워터마크를 식별하기 위해 설치된 신원 확인 프로그램을 구동시켜 암호화된 2차원 바코드 또는 워터마크를 복호화하여 상기 인증 서버(100)가 전송한 문자, 기호, 도형을 판별할 수 있다.

[0069] 따라서, 본 발명의 2차원 바코드는 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다.

[0070] 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

[0071] 도 4는 본 발명의 실시 예에 따른 신원 확인 인증 방법을 나타낸 플로우 챠트이다.

[0072] 도 4에 도시된 바와 같이, 본 발명의 실시 예에 따른 신원 확인 인증 방법은 사용자 휴대 단말기를 통해 인증 서버로 접속하는 단계(S10), 인증 서버로부터 사용자 신원 확인을 위한 암호화된 데이터를 수신하는 단계(S20), 수신된 데이터를 가상 키보드로 디스플레이하는 단계(S30) 및 상기 가상 키보드 상에 사용자에 따라 서로 다른 2차원 바코드를 해석하여 신원 확인을 인증하는 단계(S40)를 포함할 수 있다.

[0073] 보다 구체적으로, 상기 S10은 사용자의 휴대 단말기(컴퓨터)를 통해 인증 서버로 접속하는 단계일 수 있다.

[0074] 상기 S20은 상기 인증 서버와 연결된 데이터 베이스로부터 사용자 신원 확인 요청에 상응하는 데이터를 추출하고, 상기 사용자 컴퓨터(사용자 휴대 단말기)는 상기 인증 서버로부터 생성된 가상 키보드 데이터를 수신하는 단계일 수 있다.

[0075] 상기 S30은 상기 데이터 베이스로부터 추출된 데이터를 복호화 및 암호화하여 상기 가상 키보드 내에 위치하는 2차원 바코드(예컨대, QR 코드) 키캡에 저장시키는 단계와 상기 사용자 컴퓨터(사용자 휴대 단말기)는 프로세서를 통해 상기 가상 키보드를 디스플레이시키는 단계를 포함할 수 있다.

[0076] 상기 S40은 상기 사용자 컴퓨터(사용자 휴대 단말기) 내에 저장된 응용 프로그램(예컨대, 신원 확인 해독 프로그램)을 실행시켜 2차원 바코드(예컨대, QR 코드) 키캡에 저장된 2차원 바코드를 해석하여 상기 가상 키보드 상에 배열된 키캡들을 지정하는 단계일 수 있다.

[0077] 또한, 상기 S40은 상기 가상 키보드 상에 배열된 빈 키캡들 표면에 그림 및 문자로 상기 2차원 바코드(예컨대, QR 코드)를 나타내는 단계일 수 있다.

[0078] 다른 실시 예로, 본 발명의 신원 확인 인증 방법은 사용자 컴퓨터를 통해 인증 서버로 접속하는 제1 단계, 인증

서버로부터 사용자 신원 확인을 위한 데이터를 수신하는 제2 단계, 수신된 데이터를 복호화 및 암호화하여 가상 키보드로 디스플레이하는 제3 단계 및 휴대 카메라에 저장된 신원 확인 해독 프로그램을 실행시켜, 상기 가상 키보드 상에 사용자에 따라 서로 다르게 전송된 2차원 바코드를 상기 카메라의 영상 이미지로 해석하여 신원 확인을 인증하는 제4 단계를 포함한다.

[0079] 상기 제1 단계 내지 제3 단계는 앞에서 서술한 내용과 동일함으로 추가 설명을 생략하도록 한다.

[0080] 상기 제4단계는 상기 휴대 카메라 내에 설치된 암호 해독 프로그램을 통해 상기 사용자 컴퓨터의 화면에 디스플레이된 상기 2차원 바코드를 이미지 영상으로 해석하여 신원 확인이 인증되는 단계일 수 있다.

[0081] 이후에는 본 발명의 다른 실시예에 따른 신원 확인 인증 시스템 및 신원 확인 인증 방법을 설명한다.

[0082] 도 5는 본 발명의 실시 예에 따른, 신원 확인 인증 시스템을 나타낸 블록도이다. 본 실시예에 따른 신원 확인 인증 시스템(500)은 도 5에 도시된 바와 같이, 사용자(510), 사용자 컴퓨터(520), 인증 서버(530) 및 휴대기기(540)를 나타내고 있다. 여기서, 상기 사용자 컴퓨터(520)는 PC나 노트북과 같이 상기 사용자(110)가 상기 인증 서버(530)에 유무선 네트워크를 통해 접근하는데 이용되는 단말기를 의미할 수 있고, 상기 인증 서버(530)는 상기 사용자(510)가 접근하고자 하는 사이트와 연계하여 사용자(510)의 신원을 확인하는 시스템을 의미할 수 있다. 또한, 휴대기기(540)는 카메라를 포함하는 휴대용 장치를 의미할 수 있다.

[0083] 상기 사용자(510)는 상기 사용자 컴퓨터(520)를 이용하여 상기 인증 서버(530)에 접근할 수 있고, 로그인 아이디와 같은 상기 사용자(510)의 식별자를 사용자 컴퓨터(520)에 입력할 수 있다. 사용자 컴퓨터(520)는 식별자를 상기 인증 서버(530)로 전송하고, 상기 인증 서버(530)는 접근을 요청하는 상기 사용자(510)의 상기 사용자 컴퓨터(520)로 2차원 바코드를 생성하여 전송할 수 있다. 이때, 상기 2차원 바코드는 상기 인증 서버(530)가 무작위로 선택한 단어, 문장, 숫자, 그림, 도형 등의 다양한 부호 중 적어도 하나의 부호를 암호화하여 포함할 수 있다. 이때, 암호화는 상기 사용자(510)와 상기 인증 서버(530)간에 미리 공유된 비밀키나 상기 사용자(510)의 공인 인증서의 공개키를 이용하여 상기 인증 서버(530)에서 수행될 수 있다.

[0084] 상기 인증 서버(530)는 생성한 상기 2차원 바코드를 상기 사용자 컴퓨터(520)로 전송하고, 상기 사용자 컴퓨터(520)는 화면에 전송된 상기 2차원 바코드를 표시할 수 있다. 이때, 상기 사용자(510)는 상기 휴대기기(540)의 카메라를 통해 상기 2차원 바코드가 표시된 화면을 촬영할 수 있다. 이 경우, 휴대기기(540)는 카메라를 통해 입력되는 이미지 영상에서 상기 2차원 바코드를 추출하고, 상기 2차원 바코드를 해석하여 상기 암호화된 적어도 하나의 부호를 추출할 수 있다. 여기서, 상술한 바와 같이, 상기 암호화는 상기 비밀키나 공개키를 통해 수행되었기 때문에, 휴대기기(540)는 역으로, 상기 비밀키나 상기 공개키에 대응하는 비밀키를 이용하여 상기 암호화된 부호를 복호화할 수 있다.

[0085] 이때, 상기 사용자(510)는 상기 복호화된 부호를 상기 사용자 컴퓨터(520)를 통해 입력할 수 있다. 예를 들어, 상기 부호가 단어 '해리포터'인 경우, 상기 사용자(510)는 상기 사용자 컴퓨터(520)의 입력 인터페이스(일례로, 키보드)를 이용하여 '해리포터'를 입력할 수 있고, 상기 사용자 컴퓨터(520)는 상기 부호 '해리포터'를 상기 인증 서버(530)로 전송할 수 있다. 이때, 상기 인증 서버(530)는 상기 부호를 상기 2차원 바코드를 통해 전송한 부호와 비교하여, 서로 동일한 부호인 경우, 상기 사용자(510)의 신원을 확인할 수 있다. 만약 두 부호가 서로 다르다면, 상기 사용자(510)를 적법하지 않은 사용자로 판단할 수 있다.

[0086] 이때, 다른 실시예로, 도 1 내지 도 4를 통해 설명한 가상 키보드가 더 이용될 수도 있다. 이를 위해, 상기 인증 서버(530)는 상기 2차원 바코드에 상기 적어도 하나의 부호가 상기 가상 키보드의 어느 키캡에 해당하는가에 대한 정보를 더 포함시켜 상기 2차원 바코드를 생성할 수 있고, 상기 가상 키보드를 더 생성하여 상기 사용자 컴퓨터(520)로 전송할 수 있다. 이 경우, 휴대기기(540)는 상기 2차원 바코드를 통해 획득한 부호와 함께, 상기 부호가 상기 사용자 컴퓨터(520)의 화면에 표시된 상기 가상 키보드의 키캡들 중 어느 키캡에 해당하는 가에 대한 정보를 상기 사용자(510)에게 더 제공할 수 있고, 사용자(510)는 상기 사용자 컴퓨터(520)의 입력 인터페이스를 이용하여 가상 키보드의 해당 키캡을 선택(예를 들어, 마우스 클릭)함으로써, 상기 부호가 상기 사용자 컴퓨터(520)를 통해 상기 인증 서버(530)로 전송되도록 할 수 있다. 예를 들어, 상기 부호가 별모양의 도형인 경우, 휴대기기(540)의 카메라를 통해 입력되는 상기 가상 키보드의 이미지에는 적어도 하나의 키캡에 상기 별모양의 도형이 표시될 수 있고, 상기 사용자(510)는 상기 사용자 컴퓨터(520)의 입력 인터페이스(일례로, 마우스)를 이용하여 해당 키캡을 선택할 수 있다. 이 경우, 상기 사용자 컴퓨터(520)는 상기 인증 서버(530)로 상기 별 모양의 도형에 대한 정보를 전송할 수 있다.

[0087] 또 다른 실시예로, 상기 2차원 바코드와 함께, 복수의 부호들에 대한 정보가 더 이용될 수도 있다. 즉, 상기 2

차원 바코드와 함께, 복수의 부호들에 대한 정보는 상기 인증 서버(530)에서 생성되어 상기 사용자 컴퓨터(520)의 화면을 통해 표시될 수 있다. 이때, 상기 복수의 부호들은 상기 2차원 바코드에 포함된 부호를 적어도 포함할 수 있다. 상기 2차원 바코드는 상술한 바와 같이, 휴대기기(540)의 카메라를 통해 입력될 수 있고, 휴대기기(540)는 2차원 바코드에 포함된 적어도 하나의 부호를 얻을 수 있다. 이 경우, 상기 사용자(510)는 휴대기기(540)에서 얻어진 부호와 동일한 부호를 상기 사용자 컴퓨터(520)의 화면에 표시된 복수의 부호들 중에서 선택(일례로, 마우스를 이용한 선택)함으로써, 사용자 컴퓨터(520)가 선택된 부호에 대한 정보를 상기 인증 서버(530)로 전송하도록 할 수 있다. 이미 설명한 바와 같이, 상기 인증 서버(530)는 상기 사용자 컴퓨터(520)로부터 수신된 부호와 상기 2차원 바코드에 포함시킨 부호를 비교하여 상기 사용자(510)의 신원을 확인할 수 있다.

[0088] 즉, 본 발명의 실시예들에서는 상기 사용자(510)와 상기 인증 서버(530)간에 미리 공유된 비밀키나 공인 인증서의 공개키를 기반으로 문자, 숫자, 도형, 그림과 같은 부호를 암호화하고, 이러한 부호를 2차원 바코드를 통해 상기 사용자(510)에게 전달하고, 상기 사용자(510)의 휴대기기(540)를 통해 인식된 부호를 다시 전달받음으로써, 상기 사용자(510)의 신원을 확인할 수 있다. 이때, 가상 키보드나 복수의 부호들과 같이 상기 부호를 다시 전달받기 위한 인터페이스를 상기 사용자(510)에게 제공함으로써, 상기 사용자(510)가 보다 편리하게 상기 부호를 재입력하도록 할 수 있다.

[0089] 또한, 이미 설명한 바와 같이, 각각의 실시예들에서 이용되는 상기 2차원 바코드는 상기 디지털 워터마크로 대체하여 이용할 수도 있다.

[0090] 뿐만 아니라, 가상 키보드를 사용하는 실시예들에서는 상기 휴대기기(540)에도 가상 키보드가 표시될 수 있다. 이 경우, 상기 휴대기기(540)가 획득한 부호는 상기 휴대기기(540)의 가상 키보드 중 대응하는 키캡에 표시되어 상기 가상 키보드와 함께 표시될 수 있다. 또한, 상기 사용자(510)의 편의를 위해, 사용자 컴퓨터(520)의 화면에 표시되는 가상 키보드와 상기 휴대기기(540)의 화면에 표시되는 가상 키보드는 각각 서로 동일한 키캡이 서로 동일한 무늬나 색깔을 나타내도록 표시할 수도 있다.

[0091] 도 6은 본 발명의 실시 예에 있어서, 가상 키보드의 부호를 휴대기기의 화면에 나타낸 도면이다. 즉, 도 6은 도 5에서 사용자 컴퓨터(520)의 화면에는 빈 키캡만이 나타나지만, 2차원 바코드(610)를 스캔하여 부호에 대한 정보와 위치 정보를 획득한 휴대기기(540)에서는 각 키캡에 대응하는 부호가 화면에 표시되는 모습을 나타내고 있다.

[0092] 즉, 점선박스(610)는 상기 사용자 컴퓨터(520)의 화면에 표시되는 가상 키보드를 나타낸다. 이때, 2차원 바코드(610)를 스캔하여 부호에 대한 정보와 위치 정보를 획득한 휴대기기(540)의 화면(630)에는 가상 키보드의 키캡들에 각각 해당하는 부호들이 표시됨을 나타내고 있다. 이 경우, 사용자는 휴대기기(540)의 화면(630)을 이용하여 사용자 컴퓨터(520)의 화면에 표시된 가상 키보드를 통해 원하는 부호를 선택할 수 있게 된다. 이 경우 이미 설명한 바와 같이, 사용자 컴퓨터(520)에 표시되는 가상 키보드의 키캡들과 휴대기기(540)의 화면(630)에 표시되는 가상 키보드의 키캡들은 서로 대응되는 키캡들간에 서로 동일한 무늬나 색깔을 갖도록 함으로써, 사용자가 쉽게 서로 대응되는 키캡들을 선택할 수 있도록 할 수 있다.

[0093] 또한, 도 1 내지 도 4를 통해 설명한 실시예에서는 사용자가 도 6과 같이 휴대기기(540)의 화면(630)에 나타난 가상 키보드의 부호들을 이용하여 사용자의 비밀번호를 입력할 수도 있다.

[0094] 도 7은 본 발명의 실시 예에 따른 신원 확인 인증 방법을 도시한 흐름도이다. 본 실시예에 따른 신원 확인 인증 방법은 도 5를 통해 설명한 신원 확인 인증 시스템의 사용자 컴퓨터(520), 인증 서버(530) 및 휴대기기(540)에 의해 수행될 수 있다.

[0095] 사용자 컴퓨터(520)는 사용자로부터 신원 확인 정보를 수신(701)하고, 수신된 신원 확인 정보를 인증 서버(530)로 전송(702)한다. 여기서 신원 확인 정보는 사용자의 로그인 아이디와 같이 인증 서버(530)와 사용자간에 공유된 상기 사용자의 식별자를 의미할 수 있다.

[0096] 인증 서버(530)는 문자, 숫자, 그림, 도형과 같은 적어도 하나의 부호를 사용자와 미리 공유된 비밀키 또는 상기 사용자의 공인 인증서의 공개키로 암호화(703)하고, 암호화된 부호를 포함하는 2차원 바코드를 생성(704)하여 사용자 컴퓨터(520)로 전송(705)한다.

[0097] 사용자 컴퓨터(520)는 2차원 바코드를 화면에 표시(706)한다. 여기서, 점선 화살표(707)는 화면에 표시된 2차원 바코드가 휴대기기(540)의 카메라를 통해 휴대기기(540)로 입력될 수 있음을 나타낸다.

[0098] 휴대기기(540)는 2차원 바코드를 해석하여 암호화된 부호를 추출(708)할 수 있고, 암호화된 부호를 인증 서버

(530)와 미리 공유된 비밀키 또는 공인 인증서의 공개키에 대응하는 비밀키로 복호화(709)할 수 있다. 따라서, 휴대기기(540)는 사용자의 신원 확인을 위해 인증 서버(530)에서 생성 또는 선택된 부호를 얻을 수 있고, 상술한 다양한 실시예들을 이용하여 부호를 다시 인증 서버(530)로 전송함으로써, 인증 서버(530)가 사용자의 신원을 확인하도록 할 수 있다. 부호를 다시 인증 서버(530)로 전송하는 방법들에 대해서는 이미 자세히 설명하였기에 반복적인 설명은 생략한다.

[0099] 도 8은 본 발명의 실시 예에 있어서, 2차원 바코드를 통해 전송된 그림을 휴대기기 및 사용자 컴퓨터의 화면에 나타낸 도면이다. 도 8은 사용자 컴퓨터의 화면(810)과 휴대기기의 화면(820)을 나타내고 있다. 여기서, 사용자 컴퓨터와 휴대기기는 각각 도 5를 통해 설명한 사용자 컴퓨터(520) 및 휴대기기(540)에 대응할 수 있다.

[0100] 우선, 사용자 컴퓨터의 화면(810)에는 인증서버에서 전송한 2차원 바코드(811)와 복수개의 그림들(812)이 나타나 있다. 여기서, 인증서버는 도 5를 통해 설명한 인증 서버(530)에 대응할 수 있다. 이때, 휴대기기의 카메라를 통해 2차원 바코드(811)가 촬영되어 휴대기기로 입력되면, 휴대기기는 2차원 바코드(811)를 해석하고, 해석된 정보를 복호화하여 휴대기기의 화면(820)에서와 같이, 복호화된 정보를 표시할 수 있다.

[0101] 사용자는 마우스와 같은 사용자 컴퓨터의 입력 인터페이스를 이용하여, 휴대기기의 화면(820)에 표시된 그림과 동일한 그림을 복수개의 그림들(812) 중에서 선택할 수 있다. 이 경우, 사용자 컴퓨터는 사용자에 의해 선택된 그림과 관련된 정보를 인증 서버로 전송할 수 있고, 인증 서버는 전송된 그림과 2차원 바코드(811)의 생성에 이용한 그림이 동일한지 여부를 판단함으로써, 사용자의 신원을 확인할 수 있다.

[0102] 이 경우에도, 그림에 대한 정보의 암호화/복호화는 사용자와 인증서버간에 미리 공유된 비밀키를 이용하거나, 사용자의 공인 인증서의 공개키/비밀키를 통해 수행될 수 있다.

[0103] 또한, 도 8에서는 하나의 그림에 대한 정보만이 2차원 바코드(811)에 포함되어 있으나, 둘 이상의 그림에 대한 정보를 2차원 바코드(811)에 포함시켜, 사용자가 사용자 컴퓨터를 통해 둘 이상의 그림을 선택하도록 할 수도 있다. 또한, 이 경우 둘 이상의 그림에 대한 순서정보를 더 포함하도록 2차원 바코드(811)를 생성하여, 사용자가 해당 순서에 맞게 그림을 선택하도록 할 수도 있다.

[0104] 도 5 내지 도 8을 통해 설명한 2차원 바코드는 상술한 워터마크 코드로 대체하여 사용될 수 있다.

[0105] 본 발명에 따르면, 인증 서버에 로그인 시 본인의 공인인증서의 공개키 및 인증 서버로부터의 전송된 디지털 인증키(예컨대, 2차원 바코드)를 이용함으로써 2 중의 신원 확인 과정을 통해 개인 정보의 유출 및 도용에 따른 폐단을 원천적으로 방지할 수 있는 효과가 있다.

[0106] 또한, 본 발명에 따르면, 다양한 인증 수단을 이용하더라도 각 인증 수단으로 인한 취약점을 제거함으로써 여전히 강한 안전성을 유지할 수 있다.

[0107] 또한, 본 발명에 따르면, 패스워드의 경우는 서버의 데이터 베이스가 해킹(hacking)되는 경우에도 사용자의 패스워드 정보가 노출되지 않는 효과가 있다.

[0108] 또한, 본 발명에 따르면, 다양한 인증 수단을 가진 통합 사용자 인증 프로토콜을 제공하여, 홈 네트워크 산업과 같이 노인이나 어린이 등 IT 환경에 익숙하지 않은 사용자가 많은 상황에서도 쉽고 안전한 보안 서비스를 선택적으로 제공할 수 있으므로 산업적 활용도를 크게 높이는 효과가 있다.

[0109] 본 발명은 상술한 특정의 바람직한 실시 예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형의 실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 범위 내에 있게 된다.

부호의 설명

[0110] 50: 사용자 컴퓨터 51: 프로세서

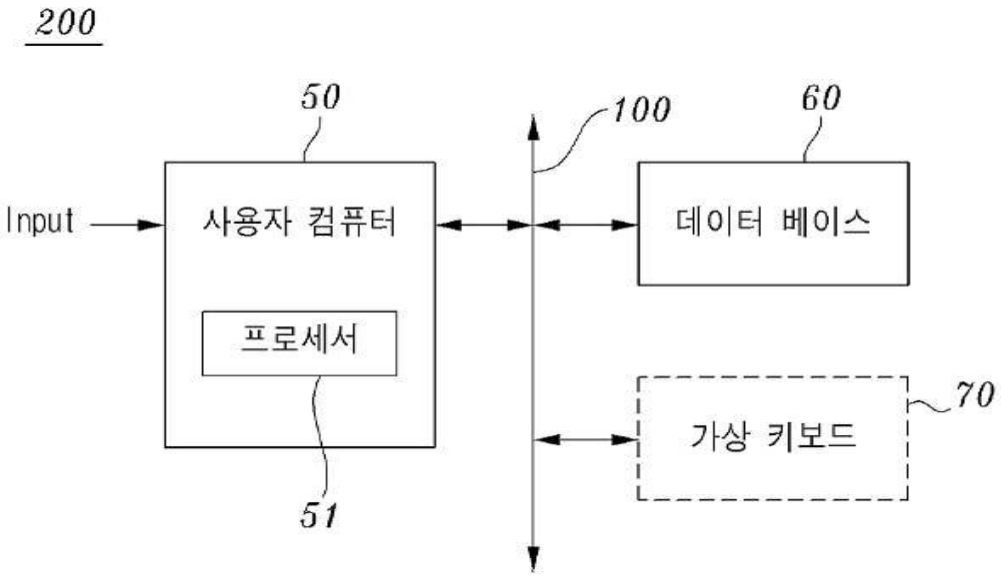
60: 데이터 베이스 70: 가상 키보드

85: 카메라 100: 인증 서버

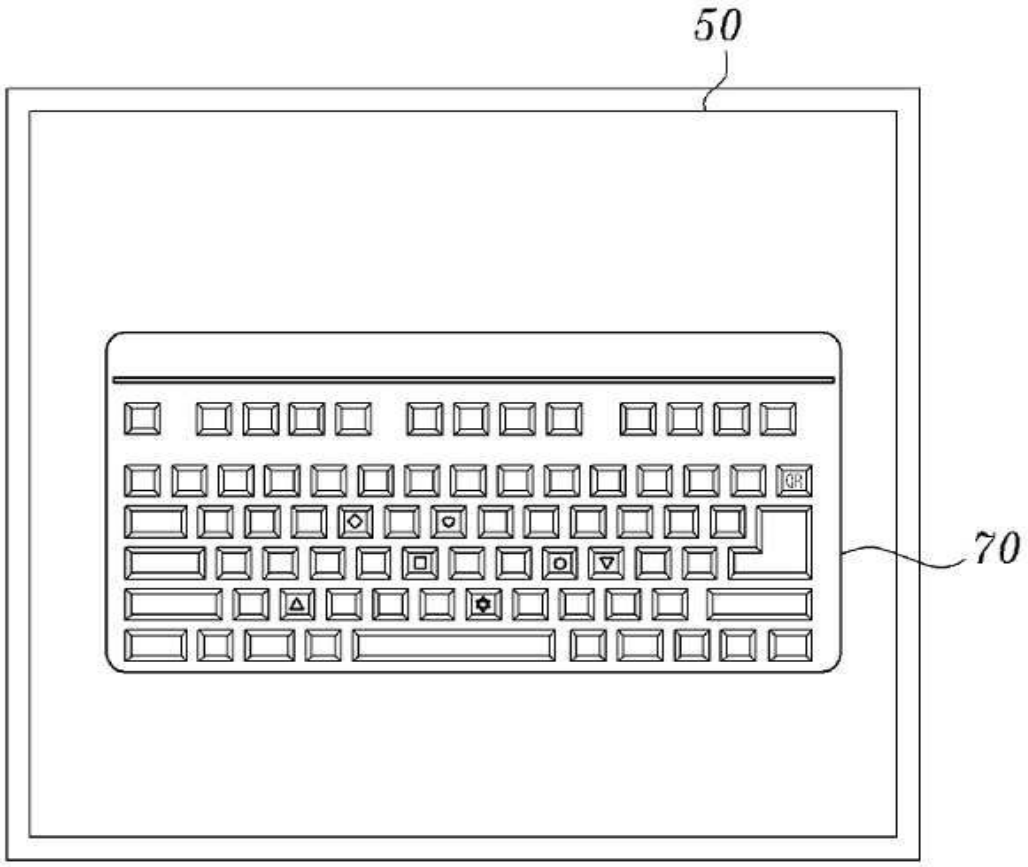
200: 신원 확인 인증 시스템

도면

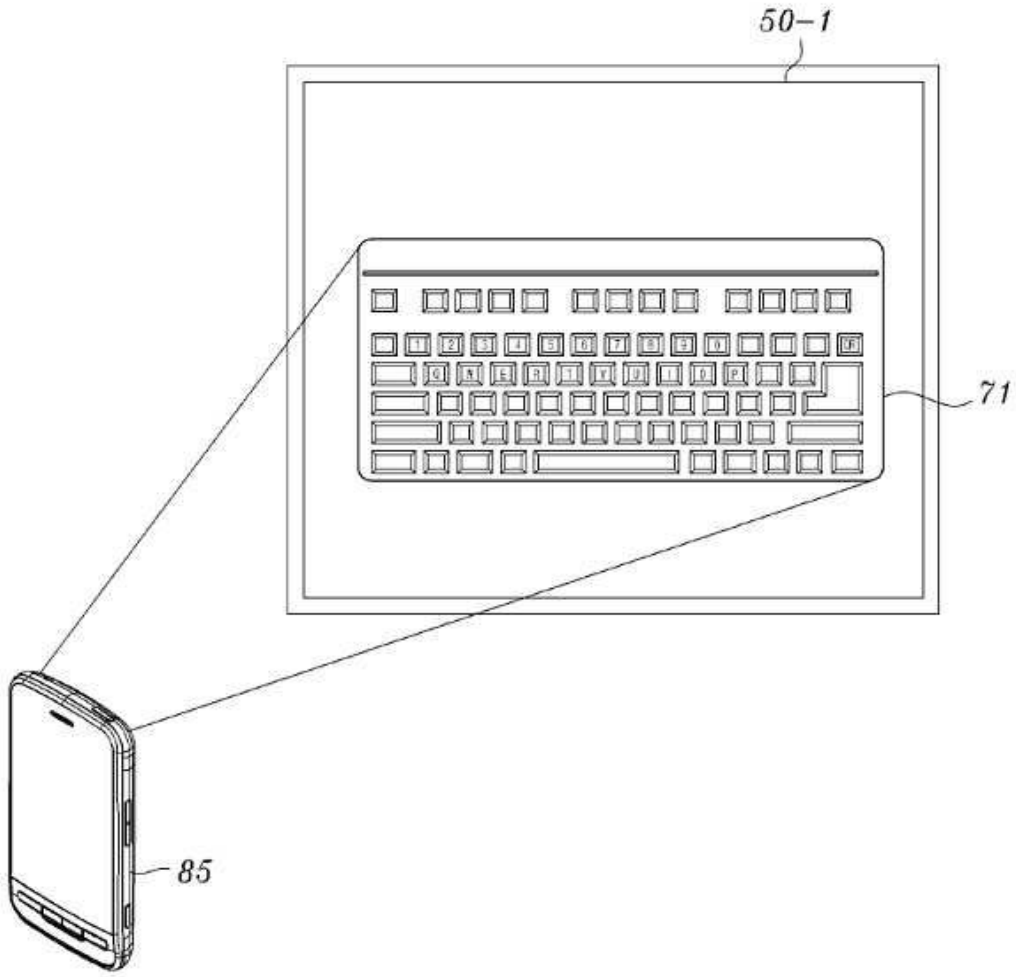
도면1



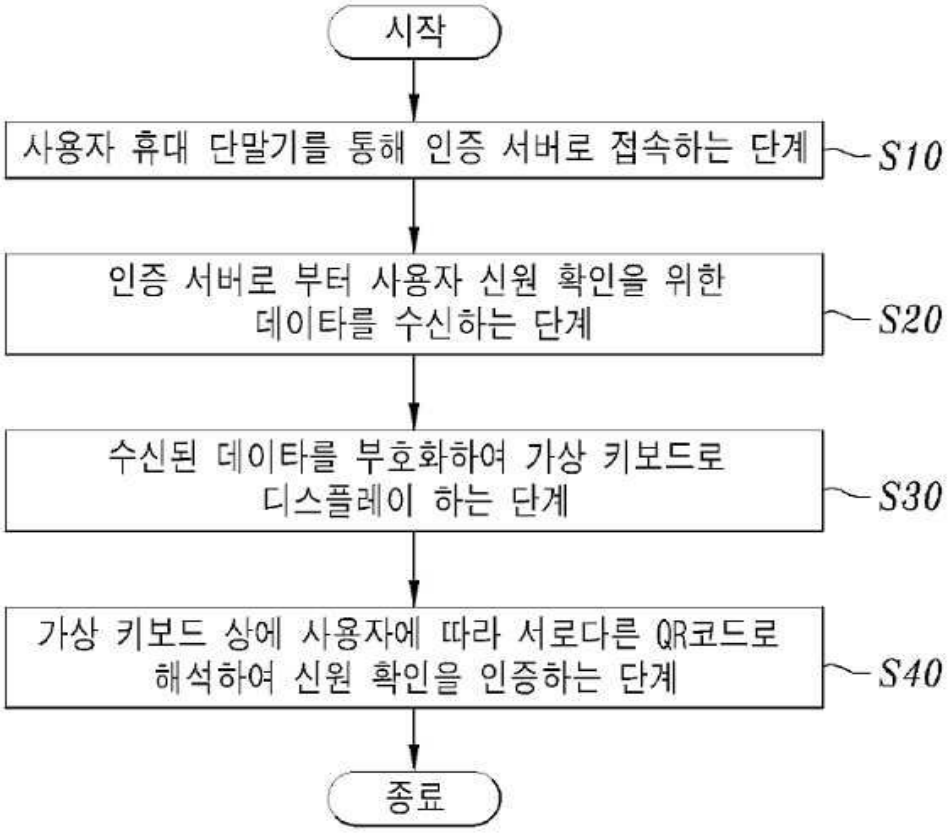
도면2



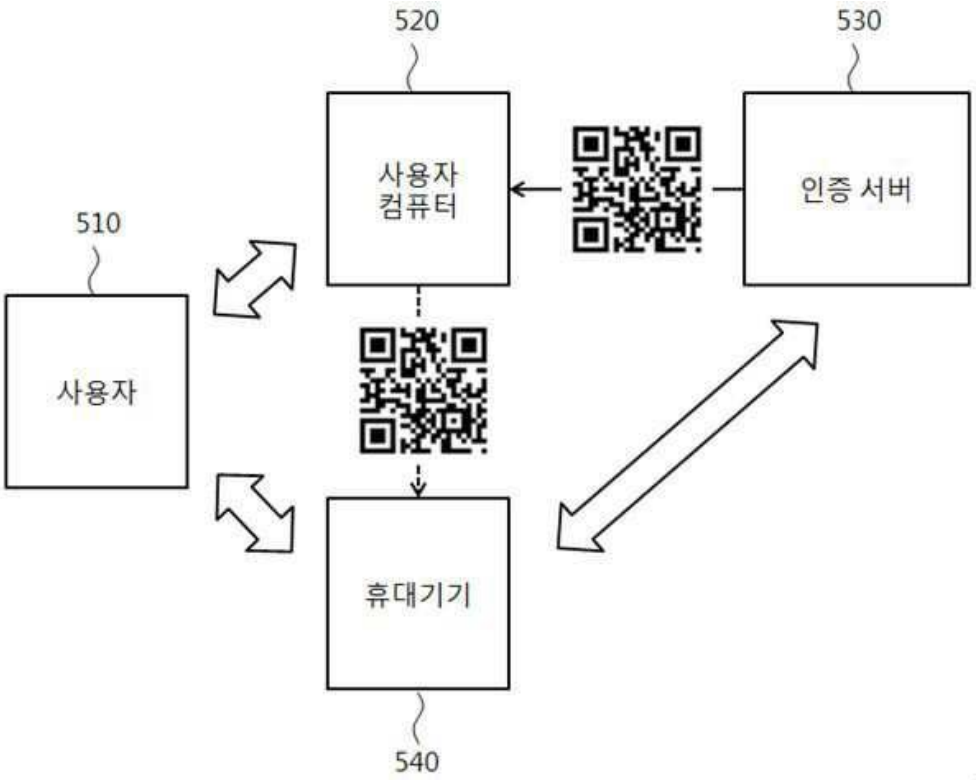
도면3



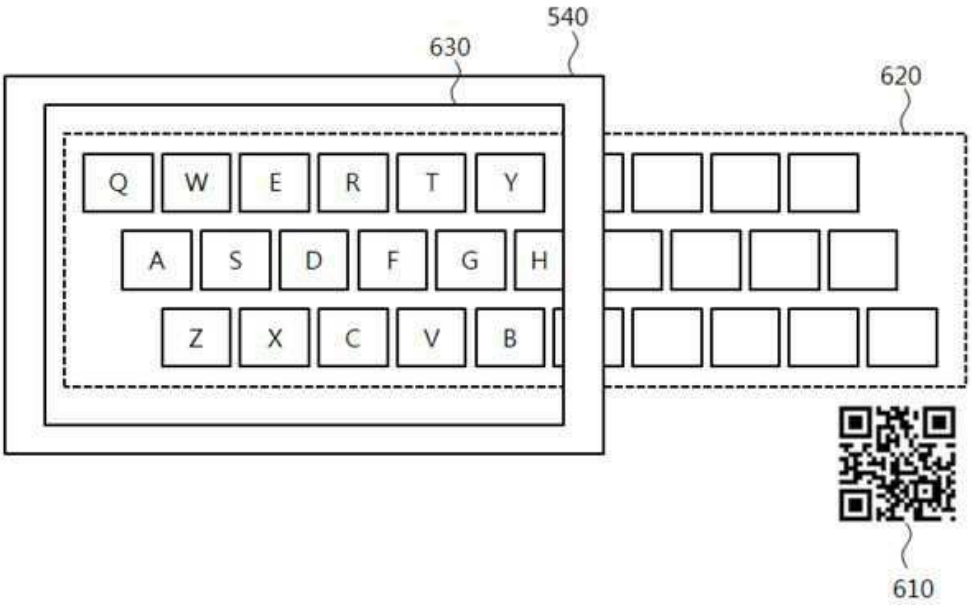
도면4


시작
사용자 휴대 단말기를 통해 인증 서버로 접속하는 단계
S10
인증 서버로 부터 사용자 신원 확인을 위한 데이타를 수신하는 단계
S20
수신된 데이타를 부호화하여 가상 키보드로 디스플레이 하는 단계
S30
가상 키보드 상에 사용자에 따라 서로다른 QR코드로 해석하여 신원 확인을 인증하는 단계
S40
종료

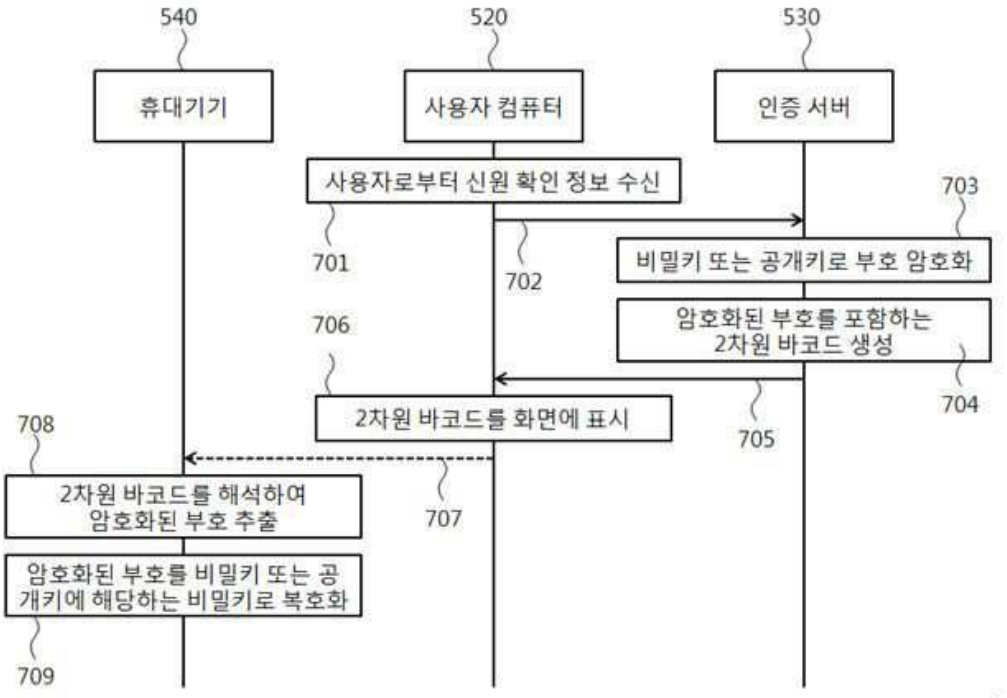
도면5


520
530
사용자 컴퓨터
인증 서버
510
사용자
휴대기기
540

도면6


540
630
620
Q
W
E
R
T
Y
A
S
D
F
G
H
Z
X
C
V
B
610

도면7


540
520
530
휴대기기
사용자 컴퓨터
인증 서버
사용자로부터 신원 확인 정보 수신
701
702
703
비밀키 또는 공개키로 부호 암호화
706
암호화된 부호를 포함하는
2차원 바코드 생성
704
2차원 바코드를 화면에 표시
705
708
707
2차원 바코드를 해석하여
암호화된 부호 추출
암호화된 부호를 비밀키 또는 공
개키에 해당하는 비밀키로 복호화
709

도면8