



(19) 대한민국특허청(KR)  
(12) 등록특허공보(B1)

(45) 공고일자 2008년03월31일  
(11) 등록번호 10-0817767  
(24) 등록일자 2008년03월24일

(51) Int. Cl.  
G06F 17/00 (2006.01) G06F 15/00 (2006.01)  
(21) 출원번호 10-2008-0003986  
(22) 출원일자 2008년01월14일  
심사청구일자 2008년01월14일  
(65) 공개번호 10-2008-0011342  
(43) 공개일자 2008년02월01일  
(56) 선행기술조사문헌  
KR1020060118965A  
KR1020000024587A

(73) 특허권자  
알서포트 주식회사  
서울특별시 송파구 방이동 149-11 나노빌딩 2층  
(72) 발명자  
서형수  
경기도 안양시 동안구 비산동 1102-4 관악아파트  
209동 1104호  
(74) 대리인  
강현석

전체 청구항 수 : 총 3 항

심사관 : 신준호

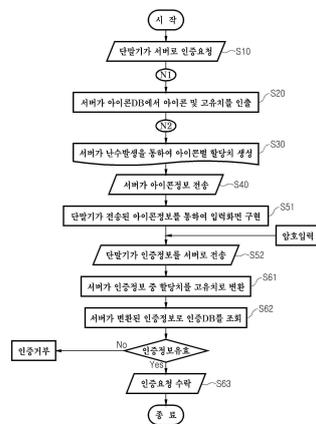
(54) 아이콘 암호를 이용한 인증방법

(57) 요약

본 발명은 통신망을 통하여 연결된 서버 및 단말기를 운용함에 있어서 단말기의 사용자 인증방법에 관한 것으로, 인증시 필요한 암호를 숫자 또는 문자가 아닌 아이콘으로 입력하도록 함으로써 암호의 유출 및 도용을 방지한 것이다.

본 발명을 통하여 정보처리기기 및 통신망에서의 암호처리과정상 보안성을 제고함은 물론, 사용자의 입력과정에서 암호가 노출되는 것을 근본적으로 방지함으로써 인증과정 전반의 신뢰성을 확보하는 효과를 얻을 수 있다.

대표도 - 도5



## 특허청구의 범위

### 청구항 1

서버(10)와 통신망을 통하여 연결된 단말기(20)의 사용자 인증방법에 있어서,  
 서버(10)에는 아이콘데이터베이스(11) 및 인증데이터베이스(12)가 연결되며, 아이콘데이터베이스(11)에는 고유치가 부여된 다수의 아이콘이 수록되고, 인증데이터베이스(12)에는 사용자별 암호가 포함된 인증정보가 수록되어;  
 단말기(20)가 통신망을 통하여 서버(10)로 인증을 요청하는 인증요청단계(S10)와;  
 서버(10)가 아이콘데이터베이스(11)에서 고유치 및 이에 각각 대응되는 아이콘을 인출하는 아이콘인출단계(S20)와;  
 서버(10)가 비중복난수발생(非重複亂數發生)을 통하여 상기 인출된 고유치와 동수(同數)의 아이콘별 할당치를 생성하는 할당치생성단계(S30)와;  
 서버(10)가 통신망을 통하여 할당치를 포함하는 아이콘정보를 단말기(20)로 전송하는 아이콘전송단계(S40)와;  
 단말기(20)가 전송된 아이콘정보를 통하여 암호입력화면을 구현하는 입력대기단계(S51)와;  
 단말기(20)가 선택된 할당치를 포함하는 인증정보를 통신망을 통하여 서버(10)로 전송하는 입력단계(S52)와;  
 서버(10)가 전송된 인증정보 중 할당치를 대응되는 고유치로 변환하는 변환단계(S61)와;  
 서버(10)가 할당치가 변환된 인증정보로 인증데이터베이스(12)를 조회하는 조회단계(S62)와;  
 인증정보가 유효할 경우 서버(10)가 인증요청을 수락하는 인증단계(S63)로 이루어짐을 특징으로 하는 아이콘 암호를 이용한 인증방법.

### 청구항 2

제1항에 있어서, 아이콘데이터베이스(11)에는 동일한 고유치가 부여된 다수의 아이콘이 수록되고;  
 아이콘인출단계(S20)는 서버(10)가 아이콘데이터베이스(11)에서 고유치 및 고유치별 다수의 아이콘 중 하나의 아이콘을 무작위로 추출함을 특징으로 하는 아이콘 암호를 이용한 인증방법.

### 청구항 3

제1항에 있어서, 아이콘데이터베이스(11)에는 특성치가 부여된 다수의 아이콘이 수록되고, 인증데이터베이스(12)에는 사용자별 암호 및 특성치목록이 포함된 인증정보가 수록되며;  
 아이콘인출단계(S20)에는  
 서버(10)가 인증데이터베이스(12)에서 특성치목록을 인출하는 목록조회단계(S21)와;  
 서버(10)가 아이콘데이터베이스(11)에서 고유치를 특성치로하는 아이콘을 무작위로 추출하는 아이콘추출단계(S22)와;  
 추출된 아이콘이 복수의 특성치를 가지는 다중아이콘이고 추출된 아이콘의 특성치중 특성치목록에 포함되는 중복치가 복수일 경우 또는 추출된 아이콘이 다중아이콘이고 중복치가 단수이며 중복치가 고유치와 일치하지 않을 경우 아이콘추출단계(S22)를 재 실행하는 아이콘취사(取捨)단계(S23)가 포함되며;  
 이들 아이콘추출단계(S22) 및 아이콘취사단계(S23)를 각 고유치별로 반복함을 특징으로 하는 아이콘 암호를 이용한 인증방법.

## 명세서

### 발명의 상세한 설명

#### 기술분야

<1> 본 발명은 통신망을 통하여 연결된 서버 및 단말기를 운용함에 있어서 단말기의 사용자 인증방법에 관한 것으로, 인증시 필요한 암호를 숫자 또는 문자가 아닌 아이콘으로 입력하도록 함으로써 암호의 유출 및 도용을 방지한 것이다.

**배경 기술**

<2> 인터넷 및 이동통신 등 전자통신망의 발달로 상거래, 금융, 행정 및 통신 등 광범위한 분야에 있어서 전자거래가 이루어지고 있으며, 그에 따라 거래의 안전을 위한 다양한 인증기법이 개발되어 사용되고 있다.

<3> 전자통신망을 통한 전자거래 상 인증기법에 있어서 암호는 가장 보편적인 요소임과 동시에 핵심적인 요소라 할 수 있으며, 인증주체와 인증객체간의 직접 대면이 배제된 전자거래에 있어서 사실상 유일한 인증수단이라 할 수 있다.

<4> 통상의 전자거래용 암호는 숫자열, 문자열 또는 이들이 혼합되어 구성되며, 사용자가 컴퓨터, 이동통신기기 또는 ATM(Automated Teller Machine;자동입출금기)등 단말기의 키보드 또는 키패드를 조작하여 입력하게 된다.

**발명의 내용**

**해결 하고자하는 과제**

<5> 키보드 또는 키패드 조작에 의한 암호의 입력 및 전송과정에서 키보드해킹(keyboard hacking)이나 도청을 통하여 암호가 유출될 가능성이 있으며, 이에 단말기의 표시장치(display)에 키보드 또는 키패드 형태의 입력화면을 구현하고 마우스 또는 터치스크린을 이용하여 암호를 입력하도록 한 방식이 개발된 바 있다.

<6> 그러나 전술한 인증방식은 공히 숫자 또는 문자를 기반으로 한 암호가 사용되는 방식으로서, 암호의 입력과정의 주변의 타인에게 노출될 수 있을 뿐 아니라 해킹프로그램에 의하여 화면이 전송되는 경우 암호가 유출될 수 밖에 없는 문제점이 있었다.

**과제 해결수단**

<7> 본 발명은 전술한 문제점을 감안하여 창안한 것으로, 서버(10)와 통신망을 통하여 연결된 단말기(20)의 사용자 인증방법에 있어서, 서버(10)에는 아이콘데이터베이스(11) 및 인증데이터베이스(12)가 연결되며, 아이콘데이터베이스(11)에는 고유치가 부여된 다수의 아이콘이 수록되고, 인증데이터베이스(12)에는 사용자별 암호가 포함된 인증정보가 수록되어, 단말기(20)가 통신망을 통하여 서버(10)로 인증을 요청하는 인증요청단계(S10)와, 서버(10)가 아이콘데이터베이스(11)에서 고유치 및 이에 각각 대응되는 아이콘을 인출하는 아이콘인출단계(S20)와, 서버(10)가 비중복난수발생(非重複亂數發生)을 통하여 상기 인출된 고유치와 동수(同數)의 아이콘별 할당치를 생성하는 할당치생성단계(S30)와, 서버(10)가 통신망을 통하여 할당치를 포함하는 아이콘정보를 단말기(20)로 전송하는 아이콘전송단계(S40)와, 단말기(20)가 전송된 아이콘정보를 통하여 암호입력화면을 구현하는 입력대기단계(S51)와, 단말기(20)가 선택된 할당치를 포함하는 인증정보를 통신망을 통하여 서버(10)로 전송하는 입력단계(S52)와, 서버(10)가 전송된 인증정보 중 할당치를 대응되는 고유치로 변환하는 변환단계(S61)와, 서버(10)가 할당치가 변환된 인증정보로 인증데이터베이스(12)를 조회하는 조회단계(S62)와, 인증정보가 유효할 경우 서버(10)가 인증요청을 수락하는 인증단계(S63)로 이루어짐을 특징으로 하는 아이콘 암호를 이용한 인증방법이다.

<8> 또한 상기 아이콘데이터베이스(11)에는 동일한 고유치가 부여된 다수의 아이콘이 수록되고, 아이콘인출단계(S20)는 서버(10)가 아이콘데이터베이스(11)에서 고유치 및 고유치별 다수의 아이콘 중 하나의 아이콘을 무작위로 추출함을 특징으로 하는 아이콘 암호를 이용한 인증방법이며, 상기 아이콘데이터베이스(11)에는 특성치가 부여된 다수의 아이콘이 수록되고, 인증데이터베이스(12)에는 사용자별 암호 및 특성치목록이 포함된 인증정보가 수록되며, 아이콘인출단계(S20)에는 서버(10)가 인증데이터베이스(12)에서 특성치목록을 인출하는 목록조회단계(S21)와, 서버(10)가 아이콘데이터베이스(11)에서 고유치를 특성치로하는 아이콘을 무작위로 추출하는 아이콘추출단계(S22)와, 추출된 아이콘이 복수의 특성치를 가지는 다중아이콘이고 추출된 아이콘의 특성치중 특성치목록에 포함되는 중복치가 복수일 경우 또는 추출된 아이콘이 다중아이콘이고 중복치가 단수이며 중복치가 고유치와 일치하지 않을 경우 아이콘추출단계(S22)를 제 실행하는 아이콘취사(取捨)단계(S23)가 포함되며, 이들 아이콘추출단계(S22) 및 아이콘취사단계(S23)를 각 고유치별로 반복함을 특징으로 하는 아이콘 암호를 이용한 인증방법이다.

**효과**

<9> 본 발명을 통하여 정보처리기기 및 통신망에서의 암호처리과정상 보안성을 제고함은 물론, 사용자의 입력과정에서 암호가 노출되는 것을 근본적으로 방지함으로써 인증과정 전반의 신뢰성을 확보하는 효과를 얻을 수 있다.

**발명의 실시를 위한 구체적인 내용**

- <10> 본 발명의 상세한 구성을 첨부된 도면을 통하여 설명하면 다음과 같다.
- <11> 우선 도 1은 본 발명의 수행을 위한 구성요소를 도시한 것으로 전자통신망을 기반으로 연결된 서버(server)(10) 및 단말기(20)와 서버(10)에 연결된 아이콘데이터베이스(11) 및 인증데이터베이스(12)로 구성된다.
- <12> 여기서 전자통신망은 도 1에 도시된 바와 같이, PSTN(Public Switched Telephone Network;공중전화교환망), PSDN(Public Switched Data Network;공중교환데이터망), VAN(Value Added Network;부가가치통신망), LAN(Local Area Network;근거리정보통신망), WAN(Wide Area Network;원거리통신망), 인터넷 및 이동통신망 등을 들 수 있는데, 상기에 나열된 전자통신망들은 물리적으로 명확히 구분되는 개별적인 개념이라 할 수 없으며, 본 발명은 전자통신망 자체의 구성 또는 정보의 유통기법 자체에 관한 것이 아니라 사용자의 인증기법에 관한 것이므로 전자통신망 자체에 대한 청구범위의 구체적인 한정은 하지 않는다.
- <13> 본 발명에서 단말기(20)로는 컴퓨터, 이동통신기기 또는 ATM(Automated Teller Machine) 등 입출력수단이 구성된 다양한 전자기기가 적용될 수 있으며, 구체적인 예로서 도 1에 도시된 바와 같이 모뎀(Modem) 및 PSTN을 통하여 또는 유, 무선 LAN을 통하여 인터넷에 접속되는 컴퓨터와, 이동국(移動局)으로서 이동통신망에 접속되는 휴대전화와, VAN에 접속되는 사설ATM 및 금융광역통신망에 접속되는 ATM 등을 들 수 있다.
- <14> 한편, 전송한 전자통신망을 통하여 단말기(20)가 접속되는 서버(10)에는 본 발명의 수행을 위한 아이콘(Icon)관련 정보가 저장되는 아이콘데이터베이스(11)와 사용자별 암호를 비롯한 인증정보가 저장되는 인증데이터베이스(12)가 연결되는데, 이들 각각의 데이터베이스(Database)는 반드시 물리적으로 서버(10)와 분리될 필요는 없으며 서버(10)내 기억장치에 구축될 수도 있다.
- <15> 즉, 본 발명에서의 데이터베이스는 서버(10)내 자체 기억장치에 구축되거나 원격지의 별도 서버(10) 또는 스토리지(storage)에 구축되는 등 다양한 형태를 취할 수 있는 것으로, 도 1에 표현된 서버(10) 및 데이터베이스의 연결상태는 물리적인 연결상태를 한정하는 것이 아니며, 인증을 수행하는 서버프로그램과 데이터베이스간의 논리적 연결을 의미하는 것이다.
- <16> 또한 이들 데이터베이스에 수록되는 정보는 서버(10) 또는 데이터베이스에 대한 해킹이나 운영자에 의한 절취를 방지하기 위하여 암호화될 수도 있는데 이는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 선택실시할 수 있는 사항이므로 이에 대한 청구범위의 구체적인 한정은 하지 않는다.
- <17> 본 발명은 기본적으로 종래의 숫자 또는 문자 기반의 암호체계를 탈피한 것으로, 암호가 숫자열 또는 문자열로써 구성되는 것이 아니라 식별성을 구비한 아이콘(Icon)의 순열 또는 조합으로 구성되며, 도 2에서와 같이 단말기(20)의 화면에 구성된 아이콘을 선택하는 방식으로 암호의 입력이 진행된다.
- <18> 즉, 사용자는 암호를 "1, 2, 3, 4"와 같은 수열로 기억하는 것이 아니라 "자동차, 꽃, 비행기, 책"과 같은 아이콘의 순열로 기억하게 된다.
- <19> 한편 각각의 아이콘에는 도 3에서와 같이 전산처리를 위한 고유치가 부여되는데, 도 3에 도시된 실시예에서는 총12개의 아이콘에 전화기의 키패드와 동일한 정수 및 부호가 부여되었으나, 고유치에는 이러한 정수외에도 문자 또는 문자와 숫자의 조합 등 다양한 데이터가 부여될 수 있다.
- <20> 여기서 고유치는 전산처리과정에서의 아이콘 식별을 위하여 아이콘별로 부여된 데이터로서, 사용자는 오로지 암호를 구성하는 아이콘만 인식할 뿐 아이콘에 부여된 고유치는 인식하지 못하므로, 고유치와 동수(同數)의 할당치를 생성하고 단말기(20)로의 아이콘정보 전송시 고유치를 할당치로 대체하여 전송함으로써 고유치의 유출을 근본적으로 방지할 수 있다.
- <21> 즉, 도 4에 도시된 바와 같이 고유치와 동수의 비중복난수(非重複亂數)를 생성하여 이를 각 아이콘에 할당하고 이들 할당치와 아이콘으로 구성된 아이콘정보를 단말기(20)에 전송함으로써 아이콘데이터베이스(11)에 저장된 고유치가 외부로 유출되는 것을 방지하는 것으로, 설사 전자통신망의 도청을 통하여 송신정보를 절취하거나 단말기(20)내 해킹프로그램을 통하여 입출력 정보를 절취한다 하여도 원래의 아이콘별 고유치를 확인할 수 없으므로 보안성을 확보할 수 있다.

- <22> 도 4에 도시된 실시예에서는 고유치로서 0이상 9이하의 정수가 설정되고 각 고유치는 해당 아이콘의 입력화면상 위치를 지정하며, 할당치 역시 고유치와 동수(同數)의 0이상 9이하의 정수로 구성되며 그 순서가 변경된 형태로써 고유치와 동일한 범위의 정수에 대한 비중복난수발생(非重複亂數發生)을 통하여 생성된다.
- <23> 이렇듯 생성된 할당치와 아이콘으로 구성된 아이콘정보는 서버(10)에서 단말기(20)로 전송되는데, 아이콘정보를 수신한 단말기(20)는 입력화면을 구현하게 되며, 도 4에 도시된 실시예에서는 할당치가 아이콘의 입력화면상 표시위치를 지정하게 되어 결과적으로 사용자는 매번 무작위로 변경된 형태의 입력화면을 통하여 암호를 입력하게 된다.
- <24> 각 아이콘별로 할당된 할당치는 전술한 바와 같이, 고유치와 동수의 비중복난수이므로, 고유치와 일대일 대응관계를 가지게 되고, 따라서 사용자가 아이콘을 선택하는 방식으로 암호를 입력하여 아이콘별로 할당된 할당치를 포함하는 인증정보가 서버(10)로 전송되면 서버(10)는 인증정보 중 할당치를 기 설정된 대응관계에 의하여 고유치로 변환할 수 있으며 이들 고유치의 유효성을 판단하여 인증을 수락 또는 거부하게 된다.
- <25> 도 5는 아이콘, 고유치 및 할당치가 적용되어 수행되는 본 발명의 흐름도로서 이를 상세히 설명하면 다음과 같다.
- <26> 우선 단말기(20)가 통신망을 통하여 서버(10)로 인증을 요청하는 인증요청단계(S10)를 통하여 본 발명의 인증과정이 개시되며, 인증요청이 접수됨에 따라 서버(10)가 아이콘데이터베이스(11)에서 고유치 및 이에 각각 대응되는 아이콘을 인출하는 아이콘인출단계(S20)가 수행된다.
- <27> 아이콘데이터베이스(11)에는 고유치 및 이에 각각 대응되는 아이콘이 수록되는데, 도 3에서와 같이 하나의 고유치에 하나의 아이콘이 대응되는 단순한 방식 뿐 아니라, 도 7에서와 같이 하나의 고유치에 다수의 아이콘이 대응되는 방식도 가능하며, 이 경우 동일한 고유치가 부여되는 아이콘들은 도 7에 도시된 바와 같이 사용자에게 동일성을 가진 아이콘으로 인식됨과 동시에 타 아이콘과의 식별력을 구비할 수 있도록 구성된다.
- <28> 이렇듯 아이콘데이터베이스(11)에 동일한 고유치가 부여된 다수의 아이콘이 수록되는 경우, 아이콘인출단계(S20)는 서버(10)가 아이콘데이터베이스(11)에서 고유치 및 고유치별 다수의 아이콘 중 하나의 아이콘을 무작위로 추출함으로써 수행되며, 그에 따라 다양한 조합의 아이콘으로 구성된 입력화면을 구현할 수 있어 보안성을 확보할 수 있다.
- <29> 아이콘인출단계(S20)가 완료되면 서버(10)가 비중복난수발생(非重複亂數發生)을 통하여 상기 인출된 고유치와 동수(同數)의 아이콘별 할당치를 생성하는 할당치생성단계(S30)와 통신망을 통하여 할당치를 포함하는 아이콘정보를 단말기(20)로 전송하는 아이콘전송단계(S40)가 수행된다.
- <30> 아이콘정보에는 기본요소인 할당치외에도 아이콘의 이미지데이터 등 아이콘과 관련된 정보가 포함될 수 있는데, 이러한 아이콘정보의 구성은 통신부하나 전자통신망의 특성에 따라 변경될 수 있으며, 이 아이콘정보에 아이콘의 이미지데이터가 포함되지 않는 경우 단말기(20)의 기억장치에 아이콘의 이미지데이터를 저장하고 아이콘정보에 아이콘의 이미지를 식별할 수 있는 정보를 포함하여 전송하는 방식으로 입력화면을 구현할 수도 있다.
- <31> 아이콘정보를 수신한 단말기(20)는 전송된 아이콘정보를 통하여 암호입력화면을 구현하는 입력대기단계(S51)를 수행하며, 이후 사용자가 암호에 해당되는 아이콘을 선택하면 단말기(20)가 선택된 아이콘의 할당치를 포함하는 인증정보를 통신망을 통하여 서버(10)로 전송하는 입력단계(S52)가 수행되는데, 사용자의 암호 입력은 마우스나 터치스크린 등을 통하여 아이콘을 선택함으로써 이루어진다.
- <32> 사용자의 식별정보(identification)와 아이콘 암호, 즉 할당치 등을 포함한 인증정보가 서버(10)에 수신되면, 서버(10)가 인증정보 중 할당치를 대응되는 고유치로 변환하는 변환단계(S61)를 수행한 후, 할당치가 변환된 인증정보로 인증데이터베이스(12)를 조회하는 조회단계(S62) 및 인증정보가 유효할 경우 인증요청을 수락하는 인증단계(S63)를 통하여 사용자를 인증하게 된다.
- <33> 도 6은 본 발명의 수행을 위한 컴퓨터프로그램의 처리과정을 예시한 흐름도로서, 동 도면의 실시예에서는 n개의 요소를 가지는 배열변수 "ICON", "ORIG" 및 "DIST"가 선언되고, 각각 아이콘, 고유치 및 할당치로 사용되는데, 본 실시예에서 이들 아이콘, 고유치 및 할당치는 배열변수로서 표현되나 이는 전산처리상 소정의 기억용량을 할당한다는 의미로서 수학적 의미의 변수에 국한되는 의미는 아니며, 이미지데이터, 숫자 또는 문자 등의 상이한 성상을 가질 수 있다.
- <34> 도 6에 도시된 흐름도는 전자통신망을 통한 송수신과정을 기준으로 좌측, 중간 및 우측의 3개 부분으로 구성되는데 각각 서버(10), 단말기(20) 및 서버(10)에 의하여 순차적으로 수행되는 과정을 나타내는 것으로, 중간부의

단말기(20)에 의한 처리과정 및 우측의 서버(10)에 의한 처리과정에서도 m개의 요소를 가지는 배열변수로서 "EVENT" 및 "PW"가 선언되며 이들은 각각 사용자가 선택한 아이콘 및 인증데이터베이스(12)에 수록된 당해 사용자의 암호에 해당된다.

- <35> 한편, 본 발명에서 암호를 구성하는 아이콘은 숫자 또는 문자와 달리 하나의 아이콘이 다수의 의미로 인식될 수 있는 특성이 있는 바, 이러한 다중아이콘을 통하여 인증과정에서의 보안성을 제고할 수 있다.
- <36> 도 8에서와 같이, 아이콘이 내포한 의미에 따라 특성치를 부여하면, 도 9에서와 같이 복수의 특성치를 가지는 다중아이콘이 도출될 수 있으며, 이러한 특성치를 아이콘과 함께 아이콘데이터베이스(11)에 수록하고 암호입력 화면의 구현시 활용함으로써, 설사 암호의 입력과정에서 선택된 아이콘이 모두 노출된다 할지라도 사용자의 입력의도를 파악할 수 없도록 할 수 있다.
- <37> 즉, 아이콘 자체를 암호로써 사용하는 것이 아니라 특성치가 부여되는 아이콘의 의미를 암호로써 사용하는 것으로, 도 8의 아이콘이 적용되는 실시예의 경우 사용자는 아이콘의 순열로 암호를 기억하는 것이 아니라 "동물, 식물, 사람, 음식"과 같이 특성의 순열로 암호를 기억하게 되는 것이다.
- <38> 다만, 사용자가 아이콘을 선택하는 과정에서 다중아이콘으로 인한 혼동이 발생할 수 있으므로, 도 10 및 도 11에서와 같은 과정을 통하여 소요 아이콘을 인출하고 입력화면을 구현함으로써 사용자의 정확한 입력이 가능하도록 한다.
- <39> 이렇듯 다중아이콘이 적용되는 경우 사용자의 암호에 따라, 암호입력화면을 구성할 아이콘이 취사(取捨)되어야 하므로 아이콘데이터베이스(11)에서 소요 아이콘을 추출하기에 앞서 암호를 구성하는 특성치목록을 조회하는 과정이 선행되어야 하는데, 여기서 특성치목록이란 암호를 구성하는 특성치의 조합을 의미하는 것으로, 암호를 특성치의 순열(順列)이라 할때 특성치목록은 해당 특성치의 조합(組合)이 되며, 하나의 특성치목록에 해당되는 특성치의 순열은 다수의 경우의 수를 가지므로, 초기단계인 아이콘인출단계(S20)에서 암호를 직접 인출하지 않고 특성치목록만을 인출하는 것이 보안상 유리하다.
- <40> 도 11은 도 8과 같은 형태의 아이콘데이터베이스(11)가 적용된 실시예에서 사용자가 "날씨, 동물, 바다, 하늘"로 암호를 기억하는 경우, 즉 특성치로 표시된 암호가 "4, 0, 7, 6"일 경우의 암호입력화면에 사용될 아이콘을 취사하는 과정을 예시한 것으로, 도 10의 흐름도에 표시된 절차에 입각하여 설명하면 다음과 같다.
- <41> 우선 서버(10)가 인증데이터베이스(12)에서 해당 사용자의 특성치목록을 인출하는 목록조회단계(S21), 서버(10)가 아이콘데이터베이스(11)에서 소정의 고유치를 특성치로하는 아이콘을 무작위로 추출하는 아이콘추출단계(S22)가 수행된다.
- <42> 이때 아이콘추출단계(S22)에서 추출된 아이콘이 복수의 특성치를 가지는 다중아이콘이고 추출된 아이콘의 특성치중 특성치목록에 포함되는 중복치가 복수일 경우, 또는 추출된 아이콘이 다중아이콘이고 중복치가 단수이며 중복치가 고유치와 일치하지 않을 경우 상기 아이콘추출단계(S22)를 재 실행하는 아이콘취사(取捨)단계(S23)가 실행된다.
- <43> 여기서 상기 아이콘추출단계(S22) 및 아이콘취사단계(S23)는 각 고유치별로 반복되어 수행되어 결국 고유치와 동수(同數)의 아이콘이 설정된다.
- <44> 도 12는 도 11의 실시예에 의하여 구현된 입력화면을 예시한 것으로, 사용자가 자신의 암호인 "날씨, 동물, 바다, 하늘"의 의미를 가진 아이콘을 선택하면, 해당 아이콘의 고유치인 "4, 0, 7, 6"이 암호로서 전송되며, 이 경우 선택된 아이콘 중 2개의 다중아이콘으로 인하여 암호의 경우의 수는 도시된 바와 같이 3이 된다.
- <45> 이렇듯 숫자 및 문자가 배제된 본 발명의 아이콘 암호체계를 통하여 종래의 숫자 및 문자 기반 암호에 비하여 월등한 보안성을 달성할 수 있으며, 진술한 할당치 및 다중아이콘을 혼용할 경우 더욱 향상된 보안효과를 얻을 수 있다.

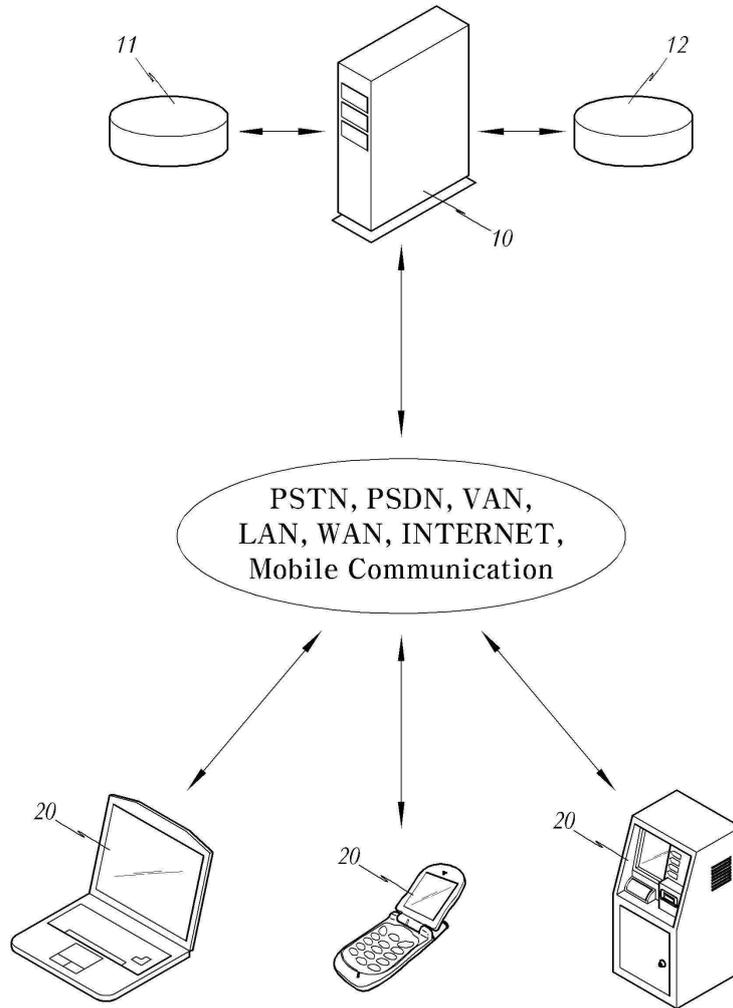
**도면의 간단한 설명**

- <46> 도 1은 본 발명의 수행을 위한 시스템 구성도
- <47> 도 2는 본 발명의 입력화면 예시도
- <48> 도 3은 본 발명의 아이콘데이터베이스 수록정보 예시도

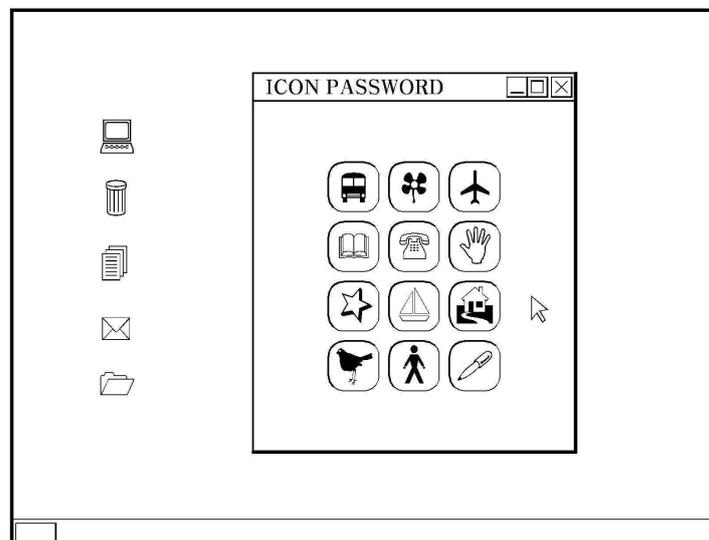
- <49> 도 4는 본 발명의 할당치 적용을 통한 입력화면 구현 설명도
- <50> 도 5는 본 발명의 흐름도
- <51> 도 6은 본 발명의 컴퓨터프로그램 처리과정을 예시한 흐름도
- <52> 도 7은 본 발명의 변형된 실시예의 아이콘데이터베이스 수록정보 예시도
- <53> 도 8은 특성치가 부여된 본 발명의 아이콘데이터베이스 수록정보 예시도
- <54> 도 9는 도 8 실시예의 다중아이콘 설명도
- <55> 도 10은 다중아이콘이 적용된 본 발명 실시예의 아이콘인출단계 흐름도
- <56> 도 11은 본 발명의 아이콘취사과정 설명도
- <57> 도 12는 본 발명의 다중아이콘을 통한 입력화면 예시도
- <58> <도면의 주요부분에 대한 부호설명>
- <59> 10 : 서버
- <60> 11 : 아이콘데이터베이스
- <61> 12 : 인증데이터베이스
- <62> 20 : 단말기
- <63> S10 : 인증요청단계
- <64> S20 : 아이콘인출단계
- <65> S21 : 목록조회단계
- <66> S22 : 아이콘추출단계
- <67> S23 : 아이콘취사단계
- <68> S30 : 할당치생성단계
- <69> S40 : 아이콘전송단계
- <70> S51 : 입력대기단계
- <71> S52 : 입력단계
- <72> S61 : 변환단계
- <73> S62 : 조회단계
- <74> S63 : 인증단계

도면

도면1



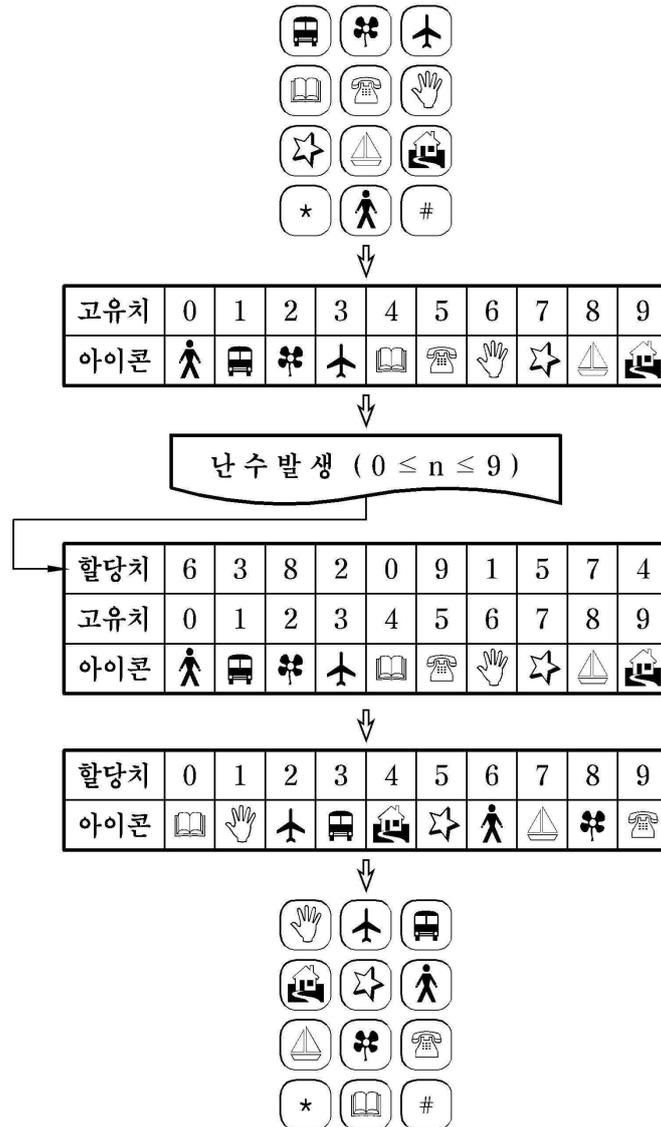
도면2



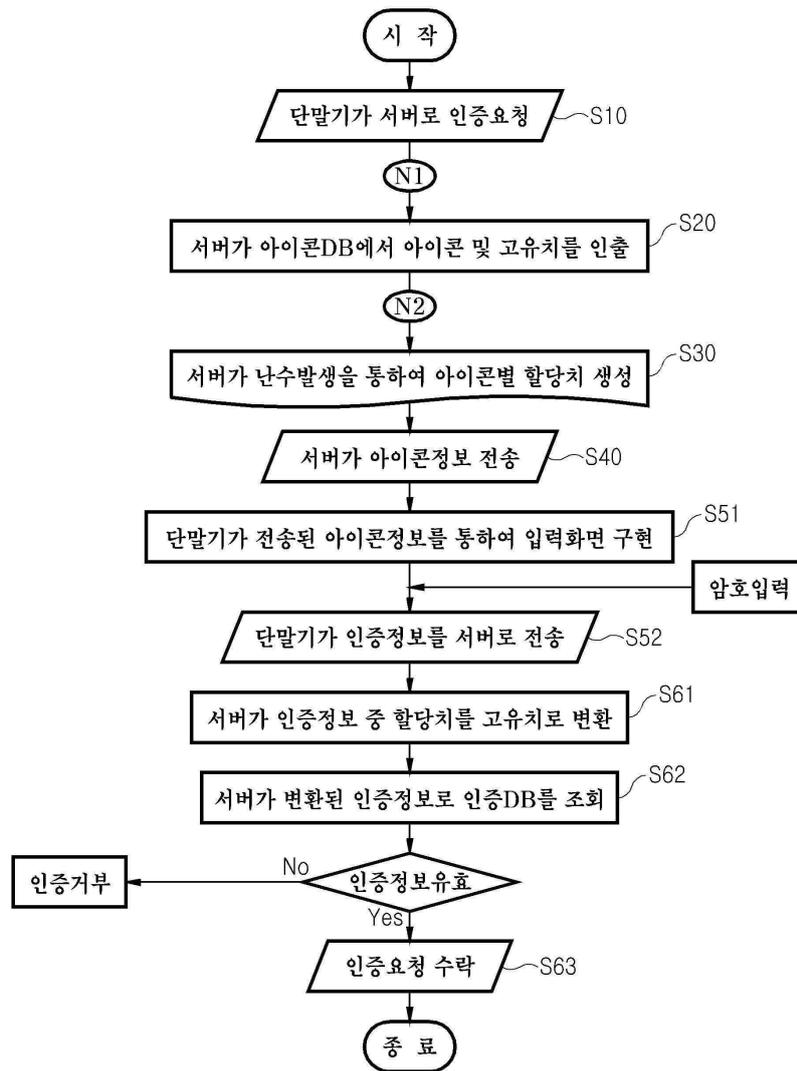
도면3

아이콘												
고유치	1	2	3	4	5	6	7	8	9	*	0	#

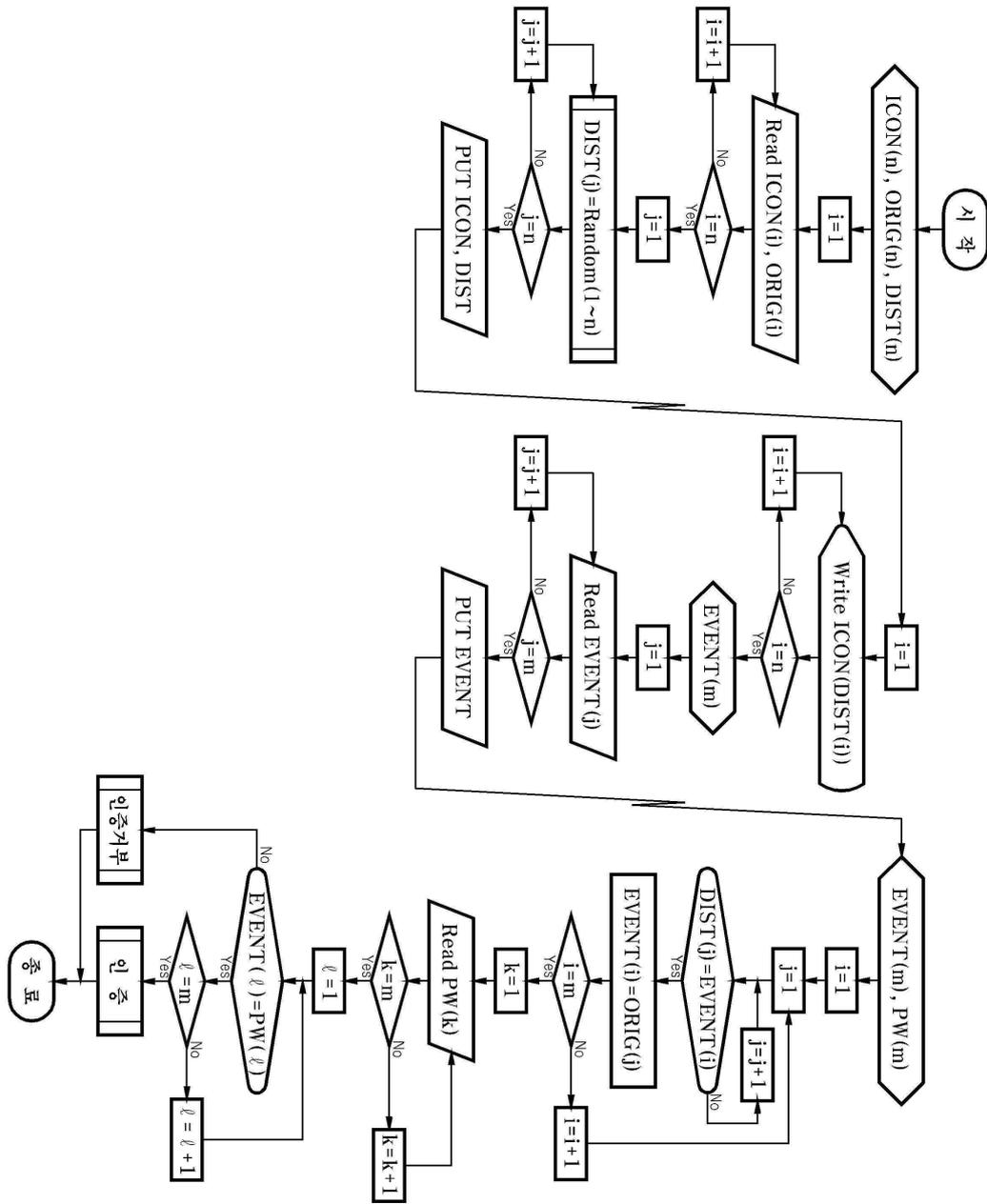
도면4



도면5



도면6



도면7

고유치	1	2	3	4	5	6	7	8	9	*	0	#
아이콘												

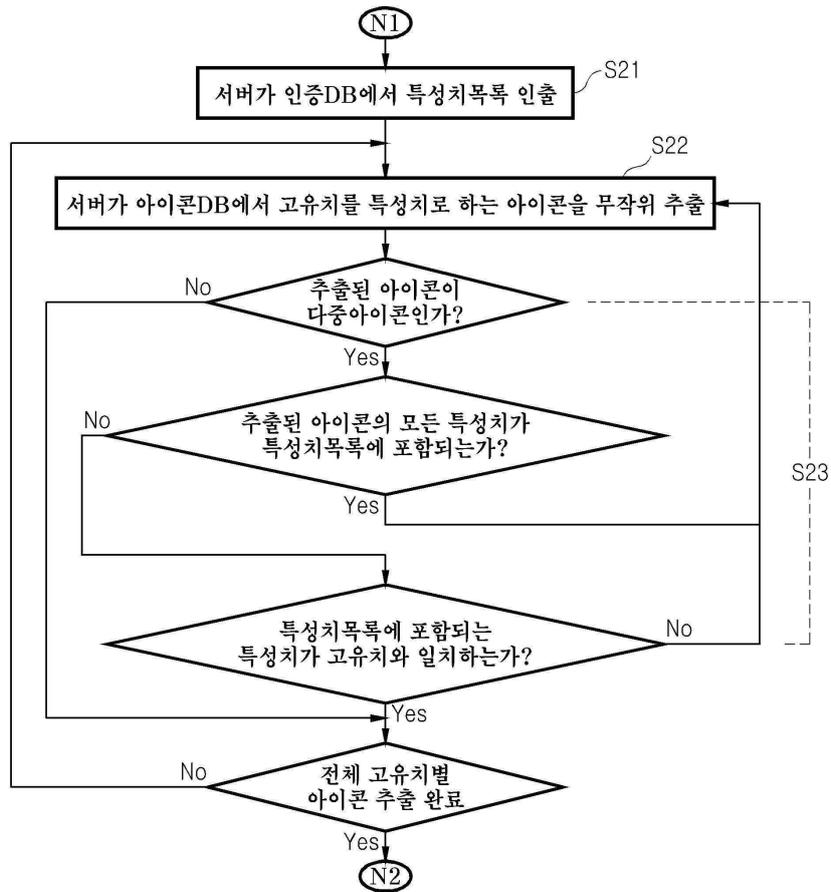
도면8

특 성	특성치	아 이 콘				
동 물	0					
식 물	1					
사 람	2					
음 식	3					
날 씨	4					
교통수단	5					
하 늘	6					
바 다	7					
건 물	8					
표지판	9					

도면9

아이콘	특 성		특성치	
	동 물	하 늘	0	6
	동 물	바 다	0	7
	동 물	표지판	0	9
	식 물	바 다	1	7
	사 람	표지판	2	9
	음 식	표지판	3	9
	날 씨	하 늘	4	6
	날 씨	하 늘	4	6
	교통수단	바 다	5	7
	교통수단	바 다	5	7
	교통수단	하 늘	5	6

도면10



도면11

특 성	날씨	동물	바다	하늘
암호(특성치)	4	0	7	6
특성치목록	0, 4, 6, 7			



고유치		0	1	2	3	4	5	6	7	8	9	구분
단일아이콘												사용 가능
중복없음												
다 중 아 이 콘	중복치 = 고유치											
	중복치 ≠ 고유치											
전체중복												

도면12

