



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2011년06월09일
(11) 등록번호 10-1039909
(24) 등록일자 2011년06월01일

(51) Int. Cl.

H04L 9/32 (2006.01)

(21) 출원번호 10-2010-0036118

(22) 출원일자 2010년04월19일

심사청구일자 2010년04월19일

(56) 선행기술조사문헌

KR1020070081048 A

KR1020080011342 A

KR1020040014129 A

KR100812411 B1

(73) 특허권자

인하대학교 산학협력단

인천 남구 용현동 253 인하대학교

(72) 발명자

양대현

인천광역시 남구 용현3동 인하대학교 하이테크센터 317호

자야바타르 다그바치

인천광역시 남구 용현3동 인하대학교 인하대학교 하이테크 307호

(74) 대리인

특허법인무한

전체 청구항 수 : 총 5 항

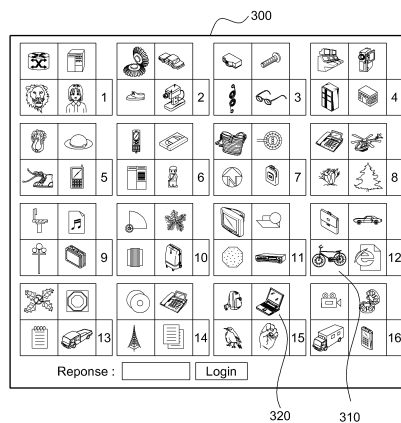
심사관 : 양종필

(54) 해킹에 강한 사용자 인증 시스템 및 방법

(57) 요약

본 발명은 해커가 사용자의 인증 과정에 대한 정보를 수집하는 상황에서도 사용자의 비밀 정보를 노출하지 않고 사용자를 인증할 수 있는 시스템 및 방법이 개시된다. 사용자 인증 시스템은 인증 서비스를 사용하고자 하는 사용자를 등록하고, 상기 사용자가 사용할 이미지 집합과 응답 행렬을 생성하는 등록부; 상기 이미지 집합에 포함된 이미지를 사용하여 질의 행렬을 생성하고, 생성된 질의 행렬을 사용자에게 제공하는 질의 행렬 생성부; 및 사용자로부터 상기 질의 행렬에 포함된 상기 사용자만의 비밀 이미지에 따라 상기 응답 행렬에서 선택된 정보를 입력 받고, 입력된 정보에 따라 상기 사용자를 인증하는 인증부를 포함하고, 상기 이미지 집합은 기 설정된 숫자인 s개의 상기 비밀 이미지를 포함하고, s개의 원소를 가지는 부분 집합들의 합 집합일 수 있다.

대표도 - 도3



특허청구의 범위

청구항 1

인증 서비스를 사용하고자 하는 사용자를 등록하고, 상기 사용자가 사용할 이미지 집합과 응답 행렬을 생성하는 등록부;

상기 이미지 집합에 포함된 이미지를 사용하여 질의 행렬을 생성하고, 생성된 질의 행렬을 사용자에게 제공하는 질의 행렬 생성부; 및

사용자로부터 상기 질의 행렬에 포함된 상기 사용자 만의 비밀 이미지에 따라 상기 응답 행렬에서 선택된 정보를 입력 받고, 입력된 정보에 따라 상기 사용자를 인증하는 인증부

를 포함하고,

상기 이미지 집합은 기 설정된 숫자인 s개의 상기 비밀 이미지를 포함하고, s개의 원소를 가지는 부분 집합들의 합 집합인 것을 특징으로 하는 사용자 인증 시스템.

청구항 2

제1항에 있어서,

상기 질의 행렬 생성부는,

상기 이미지 집합에 포함된 각각의 부분 집합에서 2개의 이미지를 선택하고, 동일한 부분 집합에서 선택된 이미지는 상기 질의 행렬의 서로 다른 원소에 포함되도록 배치하여 상기 질의 행렬을 생성하는 것을 특징으로 하는 사용자 인증 시스템.

청구항 3

제1항에 있어서,

상기 등록부는 하기 수학식 2를 만족하는 상기 이미지 집합을 생성하는 것을 특징으로 하는 사용자 인증 시스템.

[수학식 2]

$$p = (s * k * m * n) / 2$$

(이때, p 는 상기 이미지 집합에 포함된 이미지의 개수이고, s는 사용자가 기억하는 비밀 이미지의 개수며, k는 질의 행렬에서 하나의 원소에 포함되는 이미지의 개수이다. 또한, n과 m은 질의 행렬을 구성하는 행과 열의 개수이다.)

청구항 4

제1항에 있어서,

상기 이미지 집합은,

적어도 하나의 문자로 구성된 문자 집합, 적어도 하나의 기호로 구성된 기호 집합, 적어도 하나의 숫자로 구성된 숫자 집합 중 어느 하나로 대체되는 것을 특징으로 하는 사용자 인증 시스템.

청구항 5

인증 서비스를 사용하고자 하는 사용자를 등록하고, 상기 사용자가 사용할 이미지 집합과 응답 행렬을 생성하는 단계;

상기 이미지 집합에 포함된 이미지를 사용하여 질의 행렬을 생성하고, 생성된 질의 행렬을 사용자에게 제공하는 단계; 및

사용자로부터 상기 질의 행렬에 포함된 상기 사용자 만의 비밀 이미지에 따라 상기 응답 행렬에서 선택된 정보

를 입력 받고, 입력된 정보에 따라 상기 사용자를 인증하는 단계
를 포함하고,

상기 이미지 집합은 기 설정된 숫자인 s 개의 상기 비밀 이미지를 포함하고, s 개의 원소를 가지는 부분 집합들의 합 집합인 것을 특징으로 하는 사용자 인증 방법.

명세서

기술 분야

[0001] 본 발명은 사용자 인증 시스템에 관한 것으로서, 보다 상세하게는 해커가 사용자의 인증 과정에 대한 정보를 수집하는 상황에서도 사용자의 비밀 정보를 노출하지 않고 사용자를 인증하는 사용자 인증 기술에 관한 것이다.

배경 기술

[0002] 네트워크 망의 발전에 따라 네트워크 망을 사용하여 다른 사용자의 정보를 유출하는 해커나 해킹 프로그램이 증가하고 있다.

[0003] 해커나 해킹 프로그램이 사용자가 사용하는 단말기의 화면을 해킹한 상태에서 사용자가 로그인과 같은 인증 절차를 수행하면 사용자가 입력한 비밀 번호가 해커에게 노출이 되어 2차 피해가 발생하고 있는 실정이다.

[0004] 그에 따라 해킹을 방지하기 위한 프로그램이나 기술이 개발되고 있으나, 해킹 관련 기술도 빠르게 발전하고 있으므로 해킹에서 100% 안전하다는 장담을 하기 어려운 실정이다.

[0005] 따라서, 해커나 해킹 프로그램이 사용자가 사용하는 단말기의 화면 또는 입력 정보를 확인하더라도, 사용자가 인증 받기 위한 비밀 번호가 노출되지 않도록 하는 방법이 요구된다.

발명의 내용

해결하려는 과제

[0006] 본 발명의 일실시예는 해커가 사용자의 인증 과정에 대한 정보를 수집하는 상황에서도 사용자의 비밀 정보를 노출하지 않고 사용자를 인증할 수 있는 시스템 및 방법을 제공한다.

과제의 해결 수단

[0007] 본 발명의 일실시예에 따른 사용자 인증 시스템은 인증 서비스를 사용하고자 하는 사용자를 등록하고, 상기 사용자가 사용할 이미지 집합과 응답 행렬을 생성하는 등록부; 상기 이미지 집합에 포함된 이미지를 사용하여 질의 행렬을 생성하고, 생성된 질의 행렬을 사용자에게 제공하는 질의 행렬 생성부; 및 사용자로부터 상기 질의 행렬에 포함된 상기 사용자 만의 비밀 이미지에 따라 상기 응답 행렬에서 선택된 정보를 입력 받고, 입력된 정보에 따라 상기 사용자를 인증하는 인증부를 포함하고, 상기 이미지 집합은 기 설정된 숫자인 s 개의 상기 비밀 이미지를 포함하고, s 개의 원소를 가지는 부분 집합들의 합 집합이다.

[0008] 본 발명의 일실시예에 따른 사용자 인증 방법은 인증 서비스를 사용하고자 하는 사용자를 등록하고, 상기 사용자가 사용할 이미지 집합과 응답 행렬을 생성하는 단계, 상기 이미지 집합에 포함된 이미지를 사용하여 질의 행렬을 생성하고, 생성된 질의 행렬을 사용자에게 제공하는 단계; 및 사용자로부터 상기 질의 행렬에 포함된 상기 사용자 만의 비밀 이미지에 따라 상기 응답 행렬에서 선택된 정보를 입력 받고, 입력된 정보에 따라 상기 사용자를 인증하는 단계를 포함하고, 상기 이미지 집합은 기 설정된 숫자인 s 개의 상기 비밀 이미지를 포함하고, s 개의 원소를 가지는 부분 집합들의 합 집합이다.

발명의 효과

[0009] 본 발명의 일실시예에 따르면, 사용자가 기억하는 비밀 이미지와 다른 이미지를 조합하여 생성한 질의 행렬을 사용자에게 제공하고, 사용자는 기억하는 비밀 이미지의 위치에 따라 응답 행렬에서 선택한 문자를 입력하여 인증함으로써 사용자가 적은 숫자의 비밀 이미지만을 기억해도 다양한 질의 행렬이 제공될 수 있으므로 보안성이 높은 효과가 있다.

[0010] 또한, 본 발명의 일실시예에 따르면, 또한, 인증을 수행하는 서버에 사용자의 비밀 이미지를 저장하지 않으므로

서버가 공격 당해도 사용자의 비밀은 외부에 노출되지 않는 효과도 있다.

도면의 간단한 설명

도 1은 본 발명에 따른 사용자 인증 시스템의 구성을 도시한 도면이다.

도 2는 본 발명에 따른 응답 행렬이 $m=n=4$ 인 경우의 일례이다.

도 3은 본 발명에 따른 질의 행렬의 일례이다.

도 4는 본 발명에 따른 사용자 인증 방법을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

이하, 본 발명의 실시예를 첨부된 도면을 참조하여 상세하게 설명한다.

도 1은 본 발명에 따른 사용자 인증 시스템의 구성을 도시한 도면이다.

도 1을 참고하면, 사용자 인증 시스템은 등록부(110)와 질의 행렬 생성부(120) 및 인증부(130)로 구성될 수 있다.

등록부(110)는 인증 서비스를 사용하고자 하는 사용자를 등록하고, 사용자가 사용할 이미지 집합과 응답 행렬을 생성한다.

이때, 이미지 집합인 P 는 s 개의 비밀 이미지와 $|P|-s$ 개의 일반 이미지로 구성될 수 있다. 이때, s 는 기 설정된 숫자일 수 있다.

또한, 이미지 집합 P 은 수학적 식 1과 같이 원소의 개수가 s 인 t 개의 부분 집합 $S_1, S_2, \dots, S_t$ 의 합집합일 수 있다.

수학적 식 1

$$P = \bigcup_{i=1}^t S_i, |S_i| = s, |P| = ts$$

이때, 이미지 집합 P 의 부분 집합들 $S_1, S_2, \dots, S_t$ 중 하나인 S 는 상기 비밀 이미지들로 구성된 집합이며, 사용자가 비밀로써 기억해야 하는 이미지이다.

그리고, 이미지 집합 P 의 원소들은 사용자마다 다르게 쓸 필요는 없으나, 동일한 원소로 이루어진 부분 집합을 가지지 않도록 한다.

즉, 사용자의 부분 집합 $S_{1,1}, S_{1,2}, \dots, S_{1,t}$ 과 다른 사용자의 부분 집합 $S_{2,1}, S_{2,2}, \dots, S_{2,t}$ 는 모두 서로 다른 집합이다.

또한, 등록부(110)는 사용자들의 비밀 이미지 집합 S 를 비밀 이미지 집합으로 구분하여 저장하지 않을 수 있다.

이때, 등록부(110)는 비밀 이미지 각각은 저장하지 않으나 질의 행렬 생성시 비밀 이미지 집합에서 선택된 이미지가 어떤 원소에 있는지에 대한 정보를 저장하여 인증부에서 사용자가 입력한 문자가 올바른 문자인 지 여부를 확인하기 위하여 사용할 수 있다.

그리고, 등록부(110)가 생성하는 응답 행렬은 사용자가 입력하는 정보와 사용자가 기억하는 비밀 이미지 간의 관계를 감추기 위한 행렬이다.

이때, 응답 행렬은 등록부(110)에 등록한 모든 사용자가 동일한 응답 행렬을 공동으로 사용할 수도 있다.

또한, 응답 행렬은 nm 열과 mn 행을 가지는 대칭 행렬이며, 이하 도 2를 참조하여 응답 행렬의 구조를 상세히 설명한다.

질의 행렬 생성부(120)는 등록부(110)가 생성한 이미지 집합 P 에 포함된 이미지를 사용하여 질의 행렬을 생성한

다.

- [0028] 이때, 질의 행렬에 포함된 각각의 원소는 기 설정된 숫자인 k개의 이미지와 각기 다른 인덱스 번호로 구성될 수 있다.
- [0029] 구체적으로 먼저, 질의 행렬 생성부(120)는, 이미지 집합 P에 포함된 각각의 부분 집합에서 2개의 이미지를 선택할 수 있다.
- [0030] 다음으로 질의 행렬 생성부(120)는 동일한 부분 집합에서 선택된 이미지는 상기 질의 행렬의 서로 다른 원소에 포함되도록 배치하여 질의 행렬을 생성할 수 있다. 이때, 이미지 집합 P에 포함된 각각의 부분 집합 중에는 비밀 이미지 집합 S가 포함되어 있으므로 질의 행렬에는 비밀 이미지 2개가 각기 다른 원소로 포함될 수 있다.
- [0031] 그리고, 질의 행렬 생성부(120)는 생성한 질의 행렬을 사용자에게 제공할 수 있다.
- [0032] 이때, 질의 행렬이 $n \times m$ 행렬인 경우에 이미지 집합 P는 하기된 수학적 2를 만족할 수 있다.

수학적 2

$$p = (s * k * m * n) / 2$$

- [0033]
- [0034] 이때, p 는 이미지 집합 P 에 포함된 이미지의 개수이고, s는 사용자가 기억하는 비밀 이미지의 개수며 k는 질의 행렬에서 하나의 원소에 포함되는 이미지의 개수이다.
- [0035] 질의 행렬 생성부(120)가 생성하는 질의 행렬의 구조는 이하 도 3을 참조하여 상세히 설명한다.
- [0036] 인증부(130)는 사용자로부터 질의 행렬에 포함된 사용자 만의 비밀 이미지에 따라 응답 행렬에서 선택된 정보를 입력 받고, 입력된 정보에 따라 사용자를 인증한다.
- [0037] 이때, 사용자는 제공 받은 질의 행렬 중에서 자신이 기억하고 있는 비밀 이미지가 포함된 원소의 인덱스 번호를 확인할 수 있다. 이때, 질의 행렬에 포함된 2개의 비밀 이미지는 각기 다른 원소에 포함되므로 사용자가 확인한 인덱스 번호는 서로 다른 인덱스 번호일 수 있다.
- [0038] 다음으로 사용자는 등록부(110)로부터 제공받은 응답 행렬에서 확인한 두 개의 인덱스 번호에 해당하는 행과 열 또는, 행과 열에 위치한 문자를 인증부(130)에 입력할 수 있다.
- [0039] 예를 들어, 인증부(130)는 k개의 이미지와 하나의 인덱스 번호로 이루어진 원소를 포함하는 질의 행렬 C를 사용자에게 제공한다. 그러면, 사용자는 서로 다른 인덱스 번호 두 개 c1과 c2를 찾아낼 수 있다. 사용자는 응답 행렬에서 두 인덱스 번호에 해당하는 c1 행과 c2열 (또는 c2 행과 c1 열)에 위치한 문자를 입력할 수 있다.
- [0040] 이때, 인증부(130)는 사용자가 입력한 문자가 올바른 문자인 지 여부를 확인할 수 있다. 이 후, 인증부(130)는 상기 과정을 n번 반복하고, 반복하여 입력한 문자가 모두 올바른 문자인 경우에 사용자를 인증할 수도 있다. 즉, 사용자를 인증하는 것은 비밀 이미지를 알고 있는 허가된 사용자를 의미한다.
- [0041] 도 2는 본 발명에 따른 응답 행렬이 $m=n=4$ 인 경우의 일례이다.
- [0042] 본 발명에 따른 응답 행렬(200)은 도 2에 도시된 바와 같이 각 열과 행이 개의 서로 다른 문자를 가지고 있다.
- [0043] 또한, 응답 행렬(200)에서는 동일한 문자가 각 열과 행에 배치될 수 있다. 따라서, 사용자가 자신의 비밀 이미지를 찾아 응답 행렬을 이용하여 입력 값을 결정하는 것을 공격자가 해킹 프로그램을 사용하여 보더라도 이 값이 응답 행렬의 몇 번째 열과 몇 번째 행을 이용하여 생성하였는지 알 수 없다.
- [0044] 일례로, 사용자가 A라는 문자를 입력한 경우에 A는 1행2열부터 16행 9열까지 16 장소에 배치되어 있으므로 어떤 행과 열을 선택하여 A가 입력된 것인지 판단하기 어렵다.
- [0045] 또한, 응답 행렬(200)은 nm열과 mn행을 가지는 대칭 행렬이므로 1행16열(210)과 16행1열(220)처럼 사용자는 비밀 이미지에 따라 선택한 인덱스 번호 중 어떤 것을 행으로 하고 어떤 것을 열로 하든지 인덱스 번호에 따라 동일한 문제를 확인할 수 있다.

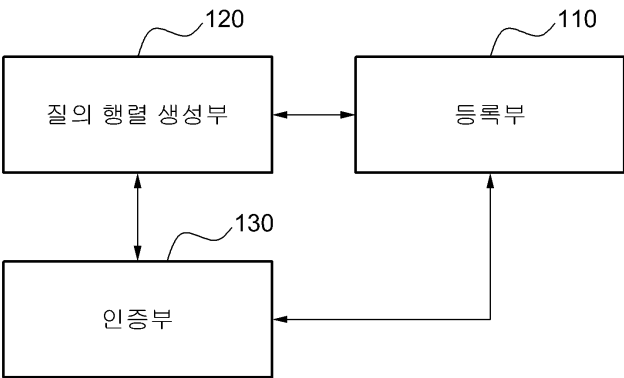
- [0046] 도 3은 본 발명에 따른 질의 행렬의 일례이다.
- [0047] 본 발명에 따른 질의 행렬(300)은 도 3에 도시된 바와 같이 복수의 이미지와 하나의 인덱스를 포함한 원소들의 행렬이다.
- [0048] 이때, 질의 행렬(300)에 포함된 이미지 중 사용자의 비밀 이미지가 자전거(310)과 노트북(320)라고 가정한다. 그러면, 사용자가 선택할 인덱스 번호는 자전거(310)가 포함된 원소의 인덱스 번호 12와 노트북(320)이 포함된 원소의 인덱스 번호 15일 수 있다. 즉, 사용자의 비밀 이미지가 '자전거(310)'와 '노트북(320)'인 경우, 질의 행렬에서 인덱스 번호 c1은 12, 인덱스 번호 c2는 15이다.
- [0049] 이때, 사용자는 도 2의 응답 행렬(200)에 인덱스 번호 12와 15를 사용하여 인증부(130)에 입력할 문자를 확인할 수 있다.
- [0050] 구체적으로 사용자는 응답 행렬(200)의 12번째 열의 15번째 문자인 J를 인증부(130)에 입력할 수 있다. 이때, 응답 행렬(200)의 15번째 열의 12번째 문자도 J이다. 따라서, 2개의 인덱스 번호는 어느 쪽을 행으로 사용하고 어느 쪽을 열로 사용하던 결과는 같다. 사용자가 'J'를 입력한 경우, 사용자의 입력이 옳기 때문에 인증부(130)는 다음 질의 행렬을 생성하여 사용자에게 전송할 수 있다. 도 3의 과정은 n번동안 반복됨으로써, 사용자의 인증 과정이 완료될 수 있다.
- [0051] 도 4는 본 발명에 따른 사용자 인증 방법을 도시한 순서도이다.
- [0052] 단계(S410)에서 등록부(110)는 인증 서비스를 사용하고자 하는 사용자를 등록하고, 상기 사용자가 사용할 이미지 집합과 응답 행렬을 생성한다.
- [0053] 단계(S420)에서 질의 행렬 생성부(120)는 단계(S410)에서 생성된 이미지 집합에 포함된 이미지를 사용하여 질의 행렬을 생성한다.
- [0054] 단계(S430)에서 질의 행렬 생성부(120)는 단계(S410)에서 생성된 질의 행렬을 사용자에게 제공한다.
- [0055] 단계(S440)에서 인증부(130)는 사용자로부터 단계(S430)에서 제공한 질의 행렬에 포함된 사용자 만의 비밀 이미지에 따라 상기 응답 행렬에서 선택된 정보를 입력 받는다.
- [0056] 단계(S450)에서 인증부(130)는 단계(S440)에서 입력 받은 정보가 정답인지 여부를 확인한다.
- [0057] 단계(S460)에서 인증부(130)는 단계(S450)에서 정답으로 확인된 정보를 입력한 사용자를 인증한다.
- [0058] 본 발명에서는 사용자가 사용하는 비밀 정보가 이미지인 경우만을 서술하였으나 사용자가 특정 문자, 숫자들을 비밀 정보로 사용하는 경우에도 등록부(110)가 비밀 숫자가 포함된 숫자 집합, 비밀 문자가 포함된 문자 집합을 생성하여 적용할 수 있다.
- [0059] 본 발명은 사용자가 기억하는 비밀 이미지와 다른 이미지를 조합하여 생성한 질의 행렬을 사용자에게 제공하고, 사용자는 기억하는 비밀 이미지의 위치에 따라 응답 행렬에서 선택한 문자를 입력하여 인증함으로써 사용자가 적은 숫자의 비밀 이미지만을 기억해도 다양한 질의 행렬이 제공될 수 있으므로 보안성이 높은 효과가 있다.
- [0060] 또한, 인증을 수행하는 서버에 사용자의 비밀 이미지를 저장하지 않으므로 서버가 공격 당해도 사용자의 비밀은 외부에 노출되지 않는 효과도 있다.
- [0061] 이상과 같이 본 발명은 비록 한정된 실시예와 도면에 의해 설명되었으나, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상의 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.
- [0062] 그러므로, 본 발명의 범위는 설명된 실시예에 국한되어 정해져서는 아니 되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

- [0063] 110: 등록부
120: 질의 행렬 생성부
130: 인증부

도면

도면1

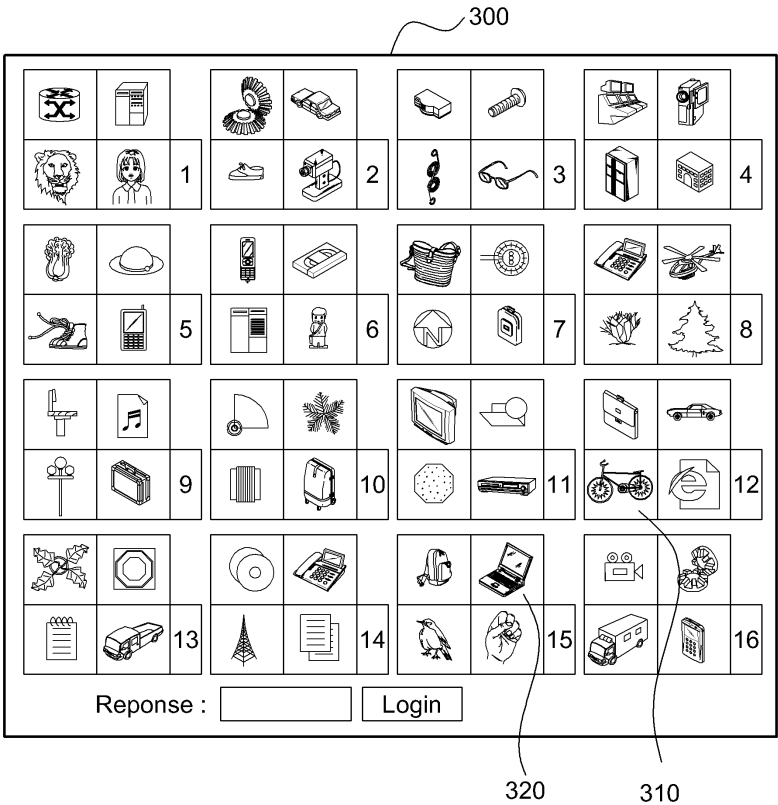


도면2

200

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	220
1	-	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	1
2	A	-	C	D	E	F	G	H	I	J	K	L	M	N	O	B	2
3	B	C	-	E	F	G	H	I	J	K	L	M	N	O	A	D	3
4	C	D	E	-	G	H	I	J	K	L	M	N	O	A	B	F	4
5	D	E	F	G	-	I	J	K	L	M	N	O	A	B	C	H	5
6	E	F	G	H	I	-	K	L	M	N	O	A	B	C	D	J	6
7	F	G	H	I	J	K	-	M	N	O	A	B	C	D	E	L	7
8	G	H	I	J	K	L	M	-	O	A	B	C	D	E	F	N	8
9	H	I	J	K	L	M	N	O	-	B	C	D	E	F	G	A	9
10	I	J	K	L	M	N	O	A	B	-	D	E	F	G	H	C	10
11	J	K	L	M	N	O	A	B	C	D	-	F	G	H	I	E	11
12	K	L	M	N	O	A	B	C	D	E	F	-	H	I	J	G	12
13	L	M	N	O	A	B	C	D	E	F	G	H	-	J	K	I	13
14	M	N	O	A	B	C	D	E	F	G	H	I	J	-	M	K	14
15	N	O	A	B	C	D	E	F	G	H	I	J	K	M	-	M	15
16	O	B	D	F	H	J	L	N	A	C	E	G	I	K	M	-	16
210	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	

도면3



도면4

