(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2014-0011010
(43) 공개일자 2014년01월28일

(51) 국제특허분류(Int. Cl.)
G06F 21/30 (2013.01) *H04L 9/32* (2006.01)
(21) 출원번호 10-2012-0056748
(22) 출원일자 2012년05월29일
심사청구일자 2012년05월29일

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145 (안암동5가, 고려대학교안암캠퍼스)
(72) 발명자
차성덕
서울특별시 성북구 종암로23길 35 (종암동, 래미안세레니티) 210-1401
김영갑
경기도 과천시 별양로 110 주공아파트 614-303 (별양동, 주공아파트)
권신일
서울특별시 동대문구 무학로45길 37, 309호 (용두동)
(74) 대리인
최관락, 송인호, 민영준

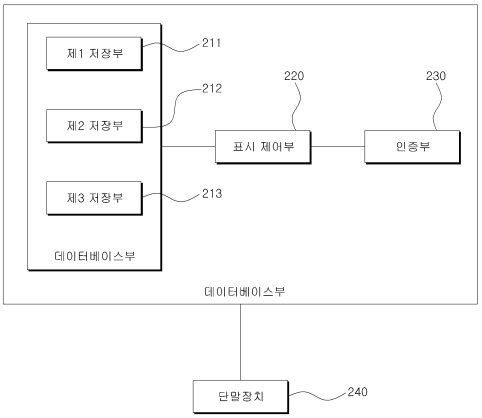
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **캡차를 이용한 사용자 인증 장치 및 방법**

(57) 요 약

캡차를 이용한 사용자 인증 장치 및 방법이 개시된다. 개시된 사용자 인증 장치는 캡차를 위한 텍스트(text) 및 다수의 이미지가 단말장치에 표시되도록 제어하는 표시 제어부; 및 상기 다수의 이미지 중 상기 단말장치를 통해 상기 텍스트에 대한 정답으로서 선택된 적어도 하나의 이미지를 이용하여 상기 단말장치의 사용자가 정상 사용자인지를 인증하는 인증부를 포함하되, 상기 다수의 이미지는 하나 이상의 정답 이미지, 하나 이상의 오답 이미지 및 하나 이상의 더미(dummy) 이미지를 포함하고, 상기 인증부는 상기 선택된 적어도 하나의 이미지에 상기 정답 이미지 및 상기 오답 이미지가 포함되는지 여부를 이용하여 상기 사용자를 인증하고, 상기 선택된 적어도 하나의 이미지에 상기 더미 이미지가 포함되는지 여부는 상기 사용자의 인증에 이용하지 않는다.

대 표 도 - 도2



특허청구의 범위

청구항 1

캡차(CAPTCHA)를 위한 텍스트(text) 및 다수의 이미지가 단말장치에 표시되도록 제어하는 표시 제어부; 및

상기 다수의 이미지 중 상기 단말장치를 통해 상기 텍스트에 대한 정답으로서 선택된 적어도 하나의 이미지를 이용하여 상기 단말장치의 사용자가 정상 사용자인지를 인증하는 인증부를 포함하되,

상기 다수의 이미지는 하나 이상의 정답 이미지, 하나 이상의 오답 이미지 및 하나 이상의 더미(dummy) 이미지를 포함하고,

상기 인증부는 상기 선택된 적어도 하나의 이미지에 상기 정답 이미지 및 상기 오답 이미지가 포함되는지 여부를 이용하여 상기 사용자를 인증하고, 상기 선택된 적어도 하나의 이미지에 상기 더미 이미지가 포함되는지 여부는 상기 사용자의 인증에 이용하지 않는 것을 특징으로 하는 캡차를 이용한 사용자 인증 장치.

청구항 2

제1항에 있어서,

상기 인증부는 상기 하나 이상의 정답 이미지의 일부 또는 모두가 상기 선택된 적어도 하나의 이미지에 포함되고, 상기 하나 이상의 오답 이미지 모두가 상기 선택된 적어도 하나의 이미지에 포함되지 않는 경우 상기 사용자를 정상 사용자로 인증하는 것을 특징으로 하는 캡차를 이용한 사용자 인증 장치.

청구항 3

제1항에 있어서,

다수의 정답 이미지를 저장하는 제1 저장부, 다수의 오답 이미지를 저장하는 제2 저장부 및 다수의 더미 이미지를 저장하는 제3 저장부를 포함하는 데이터베이스부를 더 포함하되,

상기 표시 제어부는 상기 다수의 정답 이미지 중에서 상기 하나 이상의 정답 이미지를 상기 제1 저장부에서 추출하고, 상기 다수의 오답 이미지 중에서 상기 하나 이상의 오답 이미지를 상기 제2 저장부에서 추출하고, 상기 다수의 더미 이미지 중에서 상기 하나 이상의 더미 이미지를 상기 제3 저장부에서 추출하며, 상기 추출된 하나 이상의 정답 이미지, 상기 추출된 하나 이상의 오답 이미지 및 상기 추출된 하나 이상의 더미 이미지를 조합하여 상기 단말장치에 표시하는 것을 특징으로 하는 캡차를 이용한 사용자 인증 장치.

청구항 4

제3항에 있어서,

상기 다수의 정답 이미지는 다수의 후보 이미지 중 상기 사용자 인증 장치의 관리자에 의해 상기 텍스트의 정답으로 분류되어 상기 제1 저장부에 저장된 이미지이고, 상기 다수의 오답 이미지는 상기 다수의 후보 이미지 중 상기 관리자에 의해 상기 텍스트와 무관한 오답으로 분류되어 상기 제2 저장부에 저장된 이미지이며, 상기 다수의 더미 이미지는 상기 다수의 후보 이미지 중 상기 관리자에 의해 상기 텍스트에 대한 정답 또는 오답으로 분류되지 않고 상기 제3 저장부에 저장된 이미지인 것을 특징으로 하는 캡차를 이용한 사용자 인증 장치.

청구항 5

제4항에 있어서,

상기 다수의 더미 이미지 중에서 상기 텍스트에 대한 정답으로 선택된 횟수가 많은 상위 n(1 이상 100 이하의 정수임)% 개의 더미 이미지 각각은 상기 관리자에 의해 상기 텍스트에 대한 정답으로 분류되어 상기 정답 이미지로서 상기 제1 저장부로 이동되어 저장되거나 상기 텍스트와 무관한 오답으로 분류되어 상기 오답 이미지로서 상기 제2 저장부로 이동되어 저장되는 것을 특징으로 하는 캡차를 이용한 사용자 인증 장치.

청구항 6

제3항에 있어서,

상기 표시 제어부는 상기 다수의 정답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제1 기준 확률보다 높은 정답 이미지를 제외시키고 상기 하나 이상의 정답 이미지를 상기 제1 저장부에서 추출하고, 상기 다수의 오답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제2 기준 확률보다 낮은 오답 이미지를 제외시키고 상기 하나 이상의 오답 이미지를 제2 저장부에서 추출하는 것을 특징으로 하는 캡차를 이용한 사용자 인증 장치.

청구항 7

제3항에 있어서,

상기 표시 제어부는 상기 다수의 정답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제3 기준 확률보다 낮은 정답 이미지를 필수적으로 포함시켜 상기 하나 이상의 정답 이미지를 상기 제1 저장부에서 추출하고, 상기 다수의 오답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제4 기준 확률보다 높은 오답 이미지를 필수적으로 포함시켜 상기 하나 이상의 오답 이미지를 제2 저장부에서 추출하는 것을 특징으로 하는 캡차를 이용한 사용자 인증 장치.

청구항 8

캡차를 위한 텍스트 및 다수의 이미지가 단말장치에 표시되도록 제어하는 단계; 및

상기 다수의 이미지 중 상기 단말장치를 통해 상기 텍스트에 대한 정답으로서 선택된 적어도 하나의 이미지를 이용하여 상기 단말장치의 사용자가 정상 사용자인지를 인증하는 단계를 포함하되,

상기 다수의 이미지는 하나 이상의 정답 이미지, 하나 이상의 오답 이미지 및 하나 이상의 더미 이미지를 포함하고,

상기 인증하는 단계는 상기 선택된 적어도 하나의 이미지에 상기 정답 이미지 및 상기 오답 이미지가 포함되는지 여부를 이용하여 상기 사용자를 인증하고, 상기 선택된 적어도 하나의 이미지에 상기 더미 이미지가 포함되는지 여부는 상기 사용자의 인증에 이용하지 않는 것을 특징으로 하는 캡차를 이용한 사용자 인증 방법.

청구항 9

제8항에 있어서,

상기 인증하는 단계는 상기 하나 이상의 정답 이미지의 일부 또는 모두가 상기 선택된 적어도 하나의 이미지에 포함되고, 상기 하나 이상의 오답 이미지 모두가 상기 선택된 적어도 하나의 이미지에 포함되지 않는 경우 상기 사용자를 정상 사용자로 인증하는 것을 특징으로 하는 캡차를 이용한 사용자 인증 방법.

청구항 10

제8항에 있어서,

상기 제어하는 단계는 상기 다수의 정답 이미지 중에서 상기 하나 이상의 정답 이미지를 상기 제1 저장부에서 추출하고, 상기 다수의 오답 이미지 중에서 상기 하나 이상의 오답 이미지를 상기 제2 저장부에서 추출하고, 상기 다수의 더미 이미지 중에서 상기 하나 이상의 더미 이미지를 상기 제3 저장부에서 추출하며, 상기 추출된 하나 이상의 정답 이미지, 상기 추출된 하나 이상의 오답 이미지 및 상기 추출된 하나 이상의 더미 이미지를 조합하여 상기 단말장치에 표시하는 것을 특징으로 하는 캡차를 이용한 사용자 인증 방법.

명 세 서

기 술 분 야

[0001] 본 발명의 실시예들은 캡차(CAPTCHA)를 이용한 사용자 인증 장치 및 방법에 관한 것으로서, 더욱 상세하게는 악의적 사용자 내지 악의적 사용자 측에 의해 구동되는 악의적 프로그램으로부터의 자동화된 공격으로부터 보다 방어성을 높일 수 있는 사용자 인증 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 최근 인터넷 상에서는 사용자가 인간인지, 아니면 컴퓨터(또는 프로그램)인지를 판별하기 위한 다양한 인증 방법(사용자 인증 방법)이 사용되고 있다. 이는 스팸 메일 등의 생성을 위하여 컴퓨터를 이용하여 가짜 계정을 만드는 등의 악의적인 사용자를 구별하기 위함이다.

[0003] CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart)는 인터넷 상에서 프로그램, 특히 봇넷(Bot-net)을 이용하여 자동으로 회원가입을 시도하는 것을 방지하기 위하여 시행되는 튜링 테스트(Turing test, 프로그램은 풀기 힘들고 인간은 풀기 쉬운 문제를 제시하여 그 결과를 보고 인간 혹은 프로그램을 판별)의 일종이다.

[0004] 도 1에서는 현재 사용되고 있는 여러 종류의 사용자 인증 방법을 도시하고 있다.

[0005] 먼저, 도 1의 (a)에서는 특정 문자를 인간만이 알아볼 수 있도록 왜곡이나 변형을 한 후, 해당 문자를 입력하도록 하여 사용자를 인증하는데 이용되는 이미지의 일례를 도시하고 있다.

[0006] 다음으로, 도 1의 (b)에서는 맨 아래에 위치하는 도형(오각형)과 유사한 도형이 왼쪽(육각형)과 오른쪽(오각형) 중 어떤 것인지를 선택하도록 하여 사용자를 인증하는데 이용되는 이미지의 일례(bongo)를 도시하고 있다. 방법 찾는 방법이다.

[0007] 계속하여, 도 1의 (c)에서는 위쪽의 큰 이미지(고양이)와 동일한 종류의 이미지를 아래 작은 이미지들 중에서 선택하도록 하여 사용자를 인증하는데 이용되는 이미지의 일례(Asirra)를 도시하고 있다.

[0008] 마지막으로, 도 1의 (d)에서는 유사한 패턴을 갖는 이미지로부터 인간의 얼굴 형상(굵은 사각형)을 찾도록 하여 사용자를 인증하는데 이용되는 이미지의 일례(ARTiFACIAL)를 도시하고 있다.

[0009] 한편, CAPTCHA 기술과 관련하여, 한국특허공개공보 2011-0030045에는 인증 정보를 저장하고, 인증 보안을 위한 인증 정보 변경 조건을 생성하여 제공하며, 저장된 인증 정보를 생성된 인증 정보 변경 조건에 따라 변환하여 변환된 정보와 인증 정보 변경 조건에 따라 사용자가 입력한 정보를 비교하여 사용자 인증을 수행하는 인증 보안 시스템에 관한 내용이 개시되어 있다.

[0010] 또한 일본특허공개공보 2009-175988에는 컴퓨터 처리에 의하여 일정한 시인성을 유지하면서, 정량적으로 공격 내성을 올리는 것이 가능한 CAPTCHA를 이용한 인증방법, 인증 프로그램 및 인증 서버 장치에 관한 내용이 개시되어 있다.

[0011] 그런데 기존의 CAPTCHA를 이용한 사용자 인증은 실제 사용에 있어 여러 가지 문제점을 갖는다.

[0012] 즉, 악의적 프로그램으로부터의 공격을 효율적으로 차단하기 위해 사용자 인증 질의의 난이도는 점점 높아지게 되는데, 이로 인해 인간조차도 해결하기 어려운 문제가 인증용 질의로 제시되는 경우가 발생하게 되었다. 따라서, 따라서 질의의 난이도를 높이는 것은 더 이상 효율적인 사용자 인증 방법이 되지 못한다.

[0013] 또한 새로운 인증 방법과 새로운 인증용 질의가 개발되더라도, 악의적인 사용자들은 다수의 컴퓨터 및 끊임없는 시도를 통해 해당 방법과 질의를 통과하는 알고리즘을 개발하고 있다. 이러한 알고리즘이 개발되면, 해당 인증용 질의는 그 본래의 목적을 상실하게 되며, 또다시 새로운 인증용 질의가 개발되기 전까지 악의의 사용자의 공격에 무방비로 노출된다는 문제도 있다.

발명의 내용

해결하려는 과제

[0014] 상기한 바와 같은 종래기술의 문제점을 해결하기 위해, 본 발명에서는 악의적 사용자 내지 악의적 사용자 측에 의해 구동되는 악의적 프로그램으로부터의 자동화된 공격으로부터 보다 방어성을 높일 수 있는 사용자 인증 장치 및 방법을 제안하고자 한다.

[0015] 본 발명의 다른 목적들은 하기의 실시예를 통해 당업자에 의해 도출될 수 있을 것이다.

과제의 해결 수단

[0016] 상기한 목적을 달성하기 위해 본 발명의 바람직한 일 실시예에 따르면, 캡차(CAPTCHA)를 위한 텍스트(text) 및 다수의 이미지가 단말장치에 표시되도록 제어하는 표시 제어부; 및 상기 다수의 이미지 중 상기 단말장치를 통해 상기 텍스트에 대한 정답으로서 선택된 적어도 하나의 이미지를 이용하여 상기 단말장치의 사용자가 정상 사

용자인지를 인증하는 인증부를 포함하되, 상기 다수의 이미지는 하나 이상의 정답 이미지, 하나 이상의 오답 이미지 및 하나 이상의 더미(dummy) 이미지를 포함하고, 상기 인증부는 상기 선택된 적어도 하나의 이미지에 상기 정답 이미지 및 상기 오답 이미지가 포함되는지 여부를 이용하여 상기 사용자를 인증하고, 상기 선택된 적어도 하나의 이미지에 상기 더미 이미지가 포함되는지 여부는 상기 사용자의 인증에 이용하지 않는 것을 특징으로 하는 캡차를 이용한 사용자 인증 장치가 제공된다.

[0017] 상기 인증부는 상기 하나 이상의 정답 이미지의 일부 또는 모두가 상기 선택된 적어도 하나의 이미지에 포함되고, 상기 하나 이상의 오답 이미지 모두가 상기 선택된 적어도 하나의 이미지에 포함되지 않는 경우 상기 사용자를 정상 사용자로 인증할 수 있다.

[0018] 다수의 정답 이미지를 저장하는 제1 저장부, 다수의 오답 이미지를 저장하는 제2 저장부 및 다수의 더미 이미지를 저장하는 제3 저장부를 포함하는 데이터베이스부를 더 포함하되, 상기 표시 제어부는 상기 다수의 정답 이미지 중에서 상기 하나 이상의 정답 이미지를 상기 제1 저장부에서 추출하고, 상기 다수의 오답 이미지 중에서 상기 하나 이상의 오답 이미지를 상기 제2 저장부에서 추출하고, 상기 다수의 더미 이미지 중에서 상기 하나 이상의 더미 이미지를 상기 제3 저장부에서 추출하며, 상기 추출된 하나 이상의 정답 이미지, 상기 추출된 하나 이상의 오답 이미지 및 상기 추출된 하나 이상의 더미 이미지를 조합하여 상기 단말장치에 표시할 수 있다.

[0019] 상기 다수의 정답 이미지는 다수의 후보 이미지 중 상기 사용자 인증 장치의 관리자에 의해 상기 텍스트의 정답으로 분류되어 상기 제1 저장부에 저장된 이미지이고, 상기 다수의 오답 이미지는 상기 다수의 후보 이미지 중 상기 관리자에 의해 상기 텍스트와 무관한 오답으로 분류되어 상기 제2 저장부에 저장된 이미지이며, 상기 다수의 더미 이미지는 상기 다수의 후보 이미지 중 상기 관리자에 의해 상기 텍스트에 대한 정답 또는 오답으로 분류되지 않고 상기 제3 저장부에 저장된 이미지일 수 있다.

[0020] 상기 다수의 더미 이미지 중에서 상기 텍스트에 대한 정답으로 선택된 횟수가 많은 상위 n(1 이상 100 이하의 정수임)% 개의 더미 이미지 각각은 상기 관리자에 의해 상기 텍스트에 대한 정답으로 분류되어 상기 정답 이미지로서 상기 제1 저장부로 이동되어 저장되거나 상기 텍스트와 무관한 오답으로 분류되어 상기 오답 이미지로서 상기 제2 저장부로 이동되어 저장될 수 있다.

[0021] 상기 표시 제어부는 상기 다수의 정답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제1 기준 확률보다 높은 정답 이미지를 제외시키고 상기 하나 이상의 정답 이미지를 상기 제1 저장부에서 추출하고, 상기 다수의 오답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제2 기준 확률보다 낮은 오답 이미지를 제외시키고 상기 하나 이상의 오답 이미지를 제2 저장부에서 추출할 수 있다.

[0022] 상기 표시 제어부는 상기 다수의 정답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제3 기준 확률보다 낮은 정답 이미지를 필수적으로 포함시켜 상기 하나 이상의 정답 이미지를 상기 제1 저장부에서 추출하고, 상기 다수의 오답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제4 기준 확률보다 높은 오답 이미지를 필수적으로 포함시켜 상기 하나 이상의 오답 이미지를 제2 저장부에서 추출할 수 있다.

[0023] 또한, 본 발명의 다른 실시예에 따르면, 캡차를 위한 텍스트 및 다수의 이미지가 단말장치에 표시되도록 제어하는 단계; 및 상기 다수의 이미지 중 상기 단말장치를 통해 상기 텍스트에 대한 정답으로서 선택된 적어도 하나의 이미지를 이용하여 상기 단말장치의 사용자가 정상 사용자인지를 인증하는 단계를 포함하되, 상기 다수의 이미지는 하나 이상의 정답 이미지, 하나 이상의 오답 이미지 및 하나 이상의 더미 이미지를 포함하고, 상기 인증하는 단계는 상기 선택된 적어도 하나의 이미지에 상기 정답 이미지 및 상기 오답 이미지가 포함되는지 여부를 이용하여 상기 사용자를 인증하고, 상기 선택된 적어도 하나의 이미지에 상기 더미 이미지가 포함되는지 여부는 상기 사용자의 인증에 이용하지 않는 것을 특징으로 하는 캡차를 이용한 사용자 인증 방법이 제공된다.

발명의 효과

[0024] 본 발명에 따르면, 사용자 인증의 성공을 위한 악의적 프로그램이 공격을 복잡하게 되고, 공격 시도 횟수가 증가하므로, 공격에 대한 방어성이 높아지게 된다.

[0025] 또한, 본 발명에 따르면, 선택 횟수가 높으면서 정답과 관련된 더미 이미지를 이용하여 정답 이미지를 추가적으로 생성할 수 있으므로, 무작위로 수집된 후보 이미지들에서 정답 이미지를 선정하는 것보다 쉽게 정답 이미지를 선정할 수 있게 되어 관리자의 수고가 경감되는 장점이 있다.

[0026] 또한, 본 발명에 따르면, 선택 횟수가 높으면서 정답과 무관한 더미 이미지는 악의적 프로그램이 정답으로 오인할 가능성이 높은 이미지이므로, 이를 오답 이미지로 활용하여 악의적 프로그램으로부터의 공격에 대한 방어성

을 높일 수 있는 장점이 있다.

도면의 간단한 설명

[0027] 도 1에서는 현재 사용되고 있는 여러 종류의 사용자 인증 방법을 도시한 도면이다.

도 2는 본 발명의 일 실시예에 따른 캡차(CAPTCHA)를 이용한 사용자 인증 장치의 개략적인 구성을 도시한 블록도이다.

도 3 내지 도 6은 본 발명의 일 실시예에 따른 사용자 인증 장치의 동작을 설명하기 위한 도면이다.

도 7은 본 발명의 일 실시예에에 따른 사용자 인증 장치의 시뮬레이션 결과를 도시한 도면이다.

도 8은 본 발명의 일 실시예에 따른 캡차를 이용한 사용자 인증 방법의 전체적인 흐름을 도시한 순서도이다.

발명을 실시하기 위한 구체적인 내용

[0028] 본 발명은 다양한 변경을 가할 수 있고 여러 가지 실시예를 가질 수 있는 바, 특정 실시예들을 도면에 예시하고 상세한 설명에 상세하게 설명하고자 한다. 그러나, 이는 본 발명을 특정한 실시 형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 각 도면을 설명하면서 유사한 참조부호를 유사한 구성요소에 대해 사용하였다.

[0029] 이하에서, 본 발명에 따른 실시예들을 첨부된 도면을 참조하여 상세하게 설명한다.

[0030] 도 2는 본 발명의 일 실시예에 따른 캡차(CAPTCHA)를 이용한 사용자 인증 장치(이하, "사용자 인증 장치"라고 함)의 개략적인 구성을 도시한 블록도이다.

[0031] 본 발명의 일 실시예에 따른 사용자 인증 장치는 소정의 텍스트(text, 지문)에 대한 정답과 관련된 이미지의 선택을 통해 캡차를 수행하여 사용자를 인증하는 장치로서, 도 2를 참조하면 사용자 인증 장치(200)는 데이터베이스부(210), 표시 제어부(220) 및 인증부(230)를 포함한다. 이하, 각 구성 요소 별로 그 기능을 상세하게 설명하기로 한다.

[0032] 먼저, 데이터베이스부(210)는 캡차를 위한 이미지들을 저장하며, 제1 저장부(211), 제2 저장부(212) 및 제3 저장부(213)로 구성될 수 있다. 여기서, 제1 저장부(211), 제2 저장부(212) 및 제3 저장부(213)는 물리적으로 분리된 저장소일 수도 있고 논리적으로 분리된 저장소일 수도 있다.

[0033] 보다 상세하게, 제1 저장부(211)에는 텍스트에 대한 다수의 정답 이미지가 저장되고, 제2 저장부(212)에는 텍스트에 대한 다수의 오답 이미지가 저장되며, 제3 저장부(213)에는 더미(dummy) 이미지가 저장될 수 있다.

[0034] 여기서, 정답 이미지는 사용자 인증 장치(200)의 관리자에 의해 텍스트에 대한 정답으로 분류된 이미지를 의미하고, 오답 이미지는 관리자에 의해 텍스트와 무관한 오답으로 분류된 이미지를 의미한다. 그리고, 더미 이미지는 관리자에 의해 텍스트에 대한 정답 또는 오답으로 분류되지 않은 의미없는 이미지를 의미한다.

[0035] 즉, 정답 이미지 및 오답 이미지는 인터넷 등을 통해 수집된 다수의 후보 이미지 중 관리자에 의해 식별/분류되어 제1 저장부(211) 및 제2 저장부(212)에 저장된 이미지로서, 아래에서 상세하게 설명하는 바와 같이 정상 사용자 여부의 판단에 활용되는 이미지이다. 그리고, 더미 이미지는 다수의 후보 이미지 중 관리자에 의해 식별/분류되지 않고 즉시 제3 저장부(213)에 저장된 이미지로서, 아래에서 상세하게 설명하는 바와 같이 정상 사용자 여부의 판단에 활용되지 않는 이미지이다.

[0036] 따라서, 더미 이미지는 해당 텍스트에 대한 정답으로 인식될 수 있는 이미지일 수도 있고, 해당 텍스트와 무관한 오답으로 인식될 수 있는 이미지일 수도 있다.

[0037] 다음으로, 표시 제어부(220)는 캡차를 위한 텍스트(지문) 및 다수의 이미지가 사용자 측에 구비된 단말장치(240)에 표시되도록 제어한다.

[0038] 여기서, 단말장치(240)에 표시되는 다수의 이미지는 하나 이상의 정답 이미지, 하나 이상의 오답 이미지 및 하나 이상의 더미 이미지를 포함할 수 있다. 즉, 표시 제어부(220)는 제1 저장부(211)에서 하나 이상의 정답 이미지를 추출하고, 제2 저장부(212)에서 하나 이상의 오답 이미지를 추출하고, 제3 저장부(213)에서 하나 이상의 더미 이미지를 추출한 후, 이를 조합하여 단말장치(240)에 표시할 수 있다.

[0039] 본 발명의 일 실시예에 따르면, 표시 제어부(220)는 다수의 정답 이미지 중에서 정답 이미지로써 선택되었던 확

률(해당 이미지의 정답 선택 횟수/캡차 수행 횟수)이 소정의 제1 기준 확률(일례로, 80%)보다 높은 정답 이미지를 제외시키고 하나 이상의 정답 이미지를 제1 저장부(211)에서 추출할 수 있다. 이는 선택 확률이 높은 정답 이미지는 변별력이 떨어지기 때문이다.

[0040] 이와 유사하게, 본 발명의 일 실시예에 따르면, 표시 제어부(220)는 다수의 오답 이미지 중에서 정답 이미지로써 선택되었던 확률(해당 이미지의 정답 선택 횟수/캡차 수행 횟수)이 소정의 제2 기준 확률(일례로, 20%)보다 낮은 오답 이미지를 제외시키고 하나 이상의 오답 이미지를 제2 저장부(212)에서 추출할 수 있다. 이는 선택 확률이 낮은 오답 이미지는 변별력이 떨어지기 때문이다.

[0041] 또한, 본 발명의 일 실시예에 따르면, 표시 제어부(220)는 다수의 정답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제3 기준 확률보다 낮은 정답 이미지를 필수적으로 제1 저장부(211)에서 추출할 수 있다. 이는 선택 확률이 낮은 정답 이미지는 변별력이 높기 때문이다.

[0042] 이와 유사하게, 본 발명의 일 실시예에 따르면, 표시 제어부(220)는 다수의 오답 이미지 중에서 정답 이미지로써 선택되었던 확률이 소정의 제4 기준 확률보다 높은 오답 이미지를 제외시키고 하나 이상의 오답 이미지를 제2 저장부(212)에서 추출할 수 있다. 이는 선택 확률이 높은 정답 이미지는 변별력이 높기 때문이다.

[0043] 이 때, 사용자 인증을 위하여, 단말장치(240)의 사용자 내지 단말장치(240)에 설치된 프로그램은 표시된 다수의 이미지 중에서 텍스트에 대한 정답인 것으로 판단되는 적어도 하나의 이미지를 선택하며, 선택 정보는 사용자 인증 장치(200)로 전송된다.

[0044] 인증부(230)는 단말장치(240)를 통해 텍스트에 대한 정답으로서 선택된 적어도 하나의 이미지를 이용하여 이미지 선택을 수행한 단말장치(240)의 사용자가 정상 사용자인지 악의적 사용자(프로그램)인지를 판단(인증)한다.

[0045] 보다 상세하게, 인증부(230)는 선택된 적어도 하나의 이미지에 정답 이미지 및 오답 이미지가 포함되는지 여부를 이용하여 사용자를 인증하며, 선택된 적어도 하나의 이미지에 더미 이미지가 포함되는지 여부는 사용자의 인증에 이용하지 않는다.

[0046] 본 발명의 일 실시예에 따르면, 인증부(230)는 단말장치(240)에 표시된 하나 이상의 정답 이미지 중 적어도 일부(바람직하게는 하나 이상의 정답 이미지 모두)가 선택되고, 표시된 하나 이상의 오답 이미지가 모두 선택되지 않은 경우 사용자를 정상 사용자로 인증한다. 다시 말해, 인증부(230)는 하나 이상의 정답 이미지의 일부 또는 모두가 상기 선택된 적어도 하나의 이미지에 포함되고, 하나 이상의 오답 이미지 모두가 상기 선택된 적어도 하나의 이미지에 포함되지 않는 경우 사용자를 정상 사용자로 인증한다. 이 때, 인증부(230)는 더미 이미지가 선택되었는지 여부는 사용자의 인증에 이용되지 않는다.

[0047] 한편, 인증부(230)는 정답 이미지, 오답 이미지 및 더미 이미지가 선택된 횟수를 카운팅한다. 여기서, 선택된 횟수는 인터넷 사이트 등에 접속하여 해당 캡차를 수행하는 모든 단말장치에서 수행된 선택의 횟수이다.

[0048] 이하, 도 3 내지 도 6을 참조하여 본 발명의 일 실시예에 따른 사용자 인증 장치(200)의 인증 동작의 일례를 보다 상세하게 설명하기로 한다.

[0049] 먼저, 도 3에서는 단말장치(240)에 표시되는 텍스트(지문) 및 이에 대한 보기인 다수의 이미지를 도시하고 있다.

[0050] 여기서, 도 3의 상단 2열에 표시되는 이미지들은 정답 이미지 또는 오답 이미지이고, 하단 2열에 표시되는 이미지들은 더미 이미지이다. 도 4에서는 정답 이미지, 오답 이미지 및 더미 이미지의 위치를 각각 표시하고 있다(정답 이미지는 그대로 표시, 오답 이미지는 검은색으로 표시, 더미 이미지는 회색으로 표시). 물론, 이미지의 배열 형태는 이에 한정되지 않으며, 정답 이미지, 오답 이미지 및 더미 이미지는 랜덤하게 섞여서 표시될 수도 있다.

[0051] 단말장치(240)의 사용자 또는 단말장치(240)에 설치된 프로그램은 텍스트에 대한 정답으로써 빌 게이츠에 대한 이미지를 적어도 하나를 선택함으로써 사용자 인증을 수행한다.

[0052] 이 경우, 상단 2열에 표시되는 이미지들은 정답 이미지 또는 오답 이미지이므로 상단 2열에 표시되는 이미지들 중에서 선택되는 이미지는 사용자 인증에 활용된다. 그러나, 하단 2열에 표시되는 이미지들은 더미 이미지이므로, 하단 2열에 표시되는 이미지들 중에서 선택되는 이미지는 사용자 인증에 활용되지 않는다.

[0053] 따라서, 더미 이미지들 중 어떠한 이미지가 선택되었는지와 무관하게 상단 2열에 표시된 이미지들 중 정답 이미

지의 적어도 일부(바람직하게는 모두)가 선택되고, 오답 이미지가 모두 선택되지 않는 경우, 해당 사용자는 정상 사용자로 인증된다.

[0054] 일례로, 사용자에 의해 도 5와 같은 선택이 수행된 경우(그대로 표시된 이미지가 선택된 이미지이고, 검은색으로 표시된 이미지가 선택되지 않은 이미지임), 상단 2열에 존재하는 정답 이미지가 모두 선택되었으므로, 비록 하단 2열에 존재하는 이미지 중 빌 게이츠가 아닌 이미지(510, 520)가 선택되었다 하더라도, 해당 사용자는 정상 사용자로 인증된다.

[0055] 한편, 더미 이미지는 관리자에 의해 식별/분류되지 않고 제3 저장부(213)에 저장된 이미지이므로, 관리자는 해당 더미 이미지가 텍스트에 대한 정답에 대한 이미지(즉, 빌 게이츠 이미지)인지 정답과 무관한 이미지인지를 알지 못한다.

[0056] 그런데, 더미 이미지들 중에서 사용자 내지 프로그램에 의한 선택 횟수가 높은 이미지는 정답에 대한 이미지이거나, 정답은 아니지만 이와 유사한 이미지일 확률이 높으며, 이러한 이미지들은 정답 이미지 또는 오답 이미지로 활용될 수 있다.

[0057] 따라서, 관리자는 제3 저장부(213)에 저장된 더미 이미지들 중에서 선택 횟수가 높은 더미 이미지를 확인하여 해당 더미 이미지를 정답 이미지 또는 오답 이미지로 분류한다. 분류된 정답 이미지는 제1 저장부(211)로 이동되어 저장되고, 분류된 오답 이미지는 제2 저장부(212)로 이동되어 저장된다.

[0058] 다시 말해, 본 발명의 일 실시예에 따르면, 제3 저장부(213)에 저장된 다수의 더미 이미지 중 텍스트에 대한 정답으로 선택된 횟수가 많은 상위 n(1 이상 100 이하의 정수임)% 개의 더미 이미지 각각은 관리자에 의해 텍스트에 대한 정답으로 분류되어 정답 이미지로서 제1 저장부(211)로 이동되어 저장되거나 텍스트와 무관한 오답으로 분류되어 오답 이미지로서 제2 저장부(212)로 이동되어 저장될 수 있다. 여기서 n의 값은 해당 사이트에서 캡차가 수행되는 일별/월별 횟수 등에 비례하도록 관리자에 의해 설정될 수 있다.

[0059] 이하, 본 발명에 따른 사용자 인증 장치(200)와 종래의 사용자 인증 장치를 비교하여 설명한다.

[0060] 먼저, 종래의 사용자 인증 장치는 정답 이미지와 오답 이미지만을 이용하여 사용자의 인증을 수행하였다. 그런데, 이와 같이 단순히 정답 이미지와 오답 이미지만을 이용하는 경우, 악의적 프로그램은 반복적인 정답의 선택을 통해 정답 이미지에 대한 데이터베이스를 상대적으로 쉽게 구출할 수 있게 된다. 따라서, 종래의 사용자 인증 장치는 악의적 프로그램으로부터의 공격을 효과적으로 방어하지 못하였다.

[0061] 그러나, 본 발명에 따른 사용자 인증 장치(200)는 정답 이미지/오답 이미지뿐만 아니라 악의적 프로그램의 공격에 혼선을 주기 위한 더미 이미지를 더 활용하여 사용자 인증을 수행하므로, 악의적 프로그램으로부터의 공격에 대한 방어의 정도가 더욱 뛰어난 장점이 있다. 즉, 혼선을 주기 위한 더미 이미지가 더 포함되는 경우, 악의적 프로그램이 공격에 성공하기 위해서는 종래의 경우보다 훨씬 복잡하고 많은 공격을 시도하여야 하므로, 공격에 대한 방어성이 높아지게 된다.

[0062] 일례로서, 정답 이미지와 오답 이미지만을 표시하는 종래의 사용자 인증 장치를 무력화시키기 위한 공격을 시도하는 경우, 공격이 성공하기 위한 필요 공격 횟수는 아래의 수학식 1과 같이 표현될 수 있다.

수학식 1

[0063]
$$N = \frac{T}{n^2} \times 2^n + \frac{T}{n(n-1)} \times 2^{(n-1)} + \ldots + \frac{T}{n(2)} \times 2^{(2)} + \frac{T}{n(1)} \times 2^{(1)}$$

[0064] 여기서, N은 필요 공격 횟수, n은 한번의 캡차 수행 시 표시되는 정답 이미지 및 오답 이미지의 개수, T는 하나의 단말장치(240)의 사용자 내지 프로그램에 의해 검증된 정답과 오답의 개수를 각각 의미한다.

[0065] 이에 비해, 정답 이미지/오답 이미지뿐만 아니라 더미 이미지를 더 표시하는 본 발명에 따른 사용자 인증 장치

(200)를 무력화시키기 위한 공격을 시도하는 경우, 공격이 성공하기 위한 필요 공격 횟수는 아래의 수학식 2와 같이 표현될 수 있다.

수학식 2

[0066]
$$N = \alpha \times \frac{T_u \times \log_2 T_u}{N_u} \times 2^n$$

[0067] 여기서, N은 필요 공격 횟수, α는 소정의 상수(2.4~2.6), T_u는 더미 이미지의 총 개수, N_u는 한번의 캡차 수행 시 표시되는 더미 이미지의 개수, n은 한번의 캡차 수행 시 표시되는 정답 이미지 및 오답 이미지의 개수를 각각 의미한다.

[0068] 두 수학식을 참조하면, 종래의 방식의 경우, T(즉, 관리자에 의해 검증이 완료된 이미지의 개수)가 중요한 파라미터로 작용하지만, 본 발명에 따르면, T_u(즉, 더미 이미지의 총 개수)가 중요한 파라미터로 작용함을 확인할 수 있다. 더미 이미지는 관리자가 검증하지 않은 이미지이므로, 쉽게 총 개수를 증가시킬 수 있다. 따라서, 본 발명에 따른 사용자 인증 장치(200)는 관리자의 시간/노력의 소모를 최소화하면서 외부 공격에 대한 방어성을 높일 수 있는 장점이 있다.

[0069] 이와 함께, 본 발명에 따른 사용자 인증 장치(200)는 과거에는 더미 이미지로 사용되었던 이미지를 추후 정답 또는 오답 이미지로 활용할 수 있으므로, 공격에 대한 방어성을 더욱 높일 수 있게 된다.

[0070] 예를 들어, 악의적 프로그램이 과거에 도 5에 도시된 바와 같이 이미지를 선택하여 사용자 인증을 받은 경우, 악의적 프로그램은 도 6에 도시된 바와 같이 정답에 대한 데이터베이스를 구축한다. 그런데, 더미 이미지였던 이미지(520)가 관리자의 식별에 의해 오답 이미지로 분류되어 제2 저장부(212)로 이동되고, 이후 악의적 프로그램이 다시 캡차를 수행하는 경우에 있어 이미지(520)가 오답 이미지로서 단말장치(240)에 표시된다면 악의적 프로그램은 이미지(520)를 정답 이미지로서 선택하게 되고, 이에 따라 악의적 프로그램에 의한 공격이 무산되게 된다.

[0071] 이와 더불어, 본 발명에 따르면, 선택 횟수가 높은 더미 이미지는 정답과 관련된 이미지일 확률이 높으므로, 관리자는 무작위로 수집된 후보 이미지들에서 정답 이미지를 선정하는 것보다 쉽게 정답 이미지를 선정할 수 있게 되어 관리자의 수고가 경감되는 장점이 있다.

[0072] 한편, 도 3 내지 도 6에서는 정답 이미지, 오답 이미지 및 더미 이미지로 인물 이미지가 이용되는 것으로 설명하였으나, 본 발명은 이에 한정되지 않으며 자연 이미지, 인공물 이미지, 소정의 텍스트를 포함하는 이미지, 도 1의 (b)에 도시된 바와 같은 도형을 포함하는 이미지, 도 1의(d)에 도시된 바와 같은 특정 이미지의 변형된 이미지 등 모든 종류의 이미지가 캡차에 이용될 수 있다.

[0073] 이하, 도 7을 참조하여, 본 발명에 따른 사용자 인증 장치(200)의 시뮬레이션 결과를 설명한다.

[0074] 도 7에서는 3가지 알고리즘을 이용하여 정답 이미지(즉, 빌 게이츠 이미지)를 자동으로 찾아내는 악의적 프로그램을 제작하고, 이를 이용하여 시뮬레이션을 수행한 결과를 도시하고 있다.

[0075] 보다 상세하게, A1은 서치 엔진(구글 이미지 서치)를 이용하여 사진을 식별하여 정답 이미지를 선택하는 알고리즘이고, A2는 이미지를 랜덤하게 선택하여 결과를 학습하고 이를 이용하여 정답 이미지를 선택하는 알고리즘이며, A3은 아무 이미지를 무작위로 선택하여 정답 이미지를 선택하는 알고리즘이다. 그리고, "Before"는 선택 확률이 낮은 정답 이미지와 선택 확률이 높은 오답 이미지를 포함시키기 전의 캡차 수행의 경우이고, "After" 상기 이미지들을 포함시킨 캡차 수행의 경우이다. 그리고 "(A1, A2, A3, 사람)"에서 각 파라미터의 값들은 100번의 캡차(문제풀이) 수행 시 공격 시도의 비율을 의미한다. 또한, 도 7에서는 더미 이미지의 존재를 모르는 상태에서 3가지 알고리즘을 이용하여 공격을 수행하였다.

[0076] 도 7을 참조하면, 정답에 관한 이미지가 아님에도 정답으로써 선택된 더미 이미지가 오답 이미지로 포함되면서, 악의적 프로그램의 공격 성공률이 급격하게 낮아지는 것을 확인할 수 있다.

[0077] 도 8은 본 발명의 일 실시예에 따른 캡차를 이용한 사용자 인증 방법의 전체적인 흐름을 도시한 순서도이다. 이하, 각 단계별로 수행되는 과정을 설명한다.

[0078] 먼저, 단계(S810)에서는 캡차를 위한 텍스트 및 다수의 이미지가 사용자 측에 구비된 단말장치에 표시되도록 제어한다.

[0079] 본 발명의 일 실시예에 따르면, 단계(S810)에서는 다수의 정답 이미지 중에서 하나 이상의 정답 이미지를 제1 저장부에서 추출하고, 다수의 오답 이미지 중에서 하나 이상의 오답 이미지를 제2 저장부에서 추출하고, 다수의 더미 이미지 중에서 하나 이상의 더미 이미지를 제3 저장부에서 추출하며, 추출된 하나 이상의 정답 이미지, 추출된 하나 이상의 오답 이미지 및 추출된 하나 이상의 더미 이미지를 조합하여 단말장치에 표시할 수 있다.

[0080] 그리고, 단계(S820)에서는 다수의 이미지 중 단말장치를 통해 텍스트에 대한 정답으로서 선택된 적어도 하나의 이미지를 이용하여 단말장치의 사용자가 정상 사용자인지를 인증한다.

[0081] 이 때, 표시되는 다수의 이미지는 하나 이상의 정답 이미지, 하나 이상의 오답 이미지 및 하나 이상의 더미 이미지를 포함하고, 단계(S820)에서는 선택된 적어도 하나의 이미지에 정답 이미지 및 오답 이미지가 포함되는지 여부를 이용하여 사용자를 인증하고, 선택된 적어도 하나의 이미지에 더미 이미지가 포함되는지 여부는 사용자의 인증에 이용하지 않는 것을 특징으로 하는 캡차를 이용한 사용자 인증 방법.

[0082] 보다 상세하게, 본 발명의 일 실시예에 따르면, 단계(S820)에서는 하나 이상의 정답 이미지의 일부 또는 모두가 선택된 적어도 하나의 이미지에 포함되고, 하나 이상의 오답 이미지 모두가 선택된 적어도 하나의 이미지에 포함되지 않는 경우 사용자를 정상 사용자로 인증할 수 있다.

[0083] 지금까지 본 발명에 따른 사용자 인증 방법의 실시예들에 대하여 설명하였으며, 이에는 앞서 도 2에서 설명한 사용자 인증 장치(200) 에 관한 구성이 그대로 적용될 수 있다. 따라서, 사용자 인증 방법에 대한 보다 상세한 설명은 생략하기로 한다.

[0084] 또한, 본 발명의 실시예들은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 일 실시예들의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[0085] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

부호의 설명

[0086] 200: 사용자 인증 장치 210: 데이터베이스부

211: 제1 저장부 212: 제2 저장부

213: 제3 저장부 220: 표시 제어부

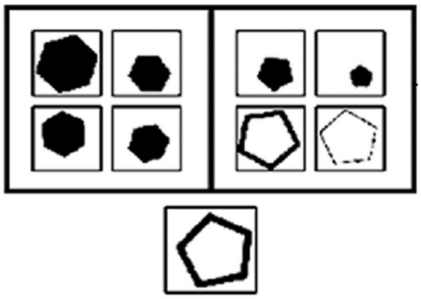
230: 인증부 240: 단말장치

도면

도면1



(a)



(b)

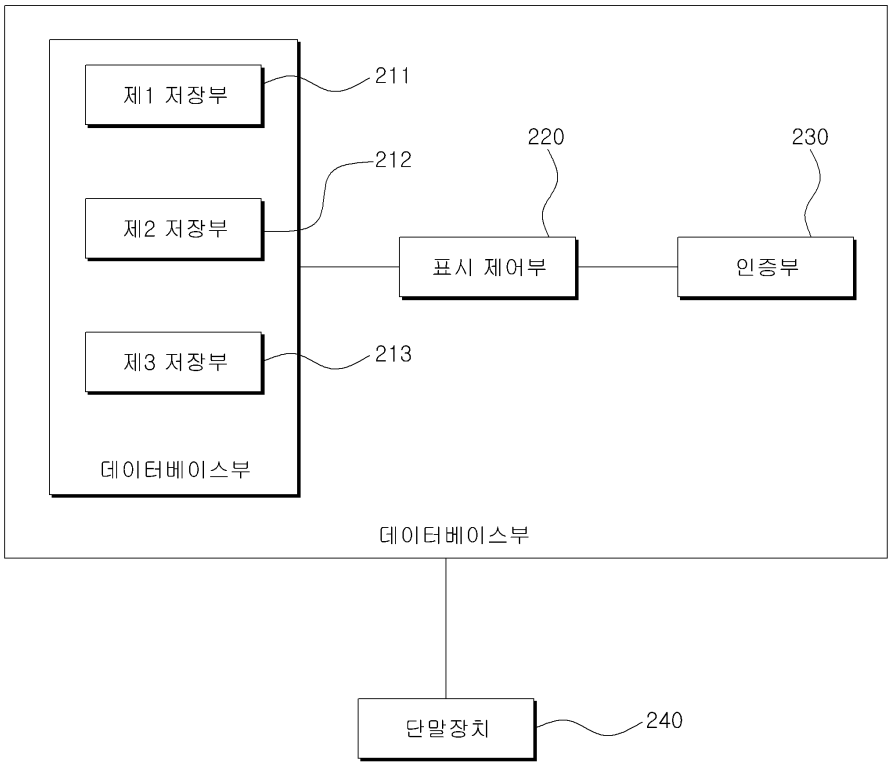

Image from Petfinder.com
Please select all the cat photos:
Adopt me

(c)



(d)

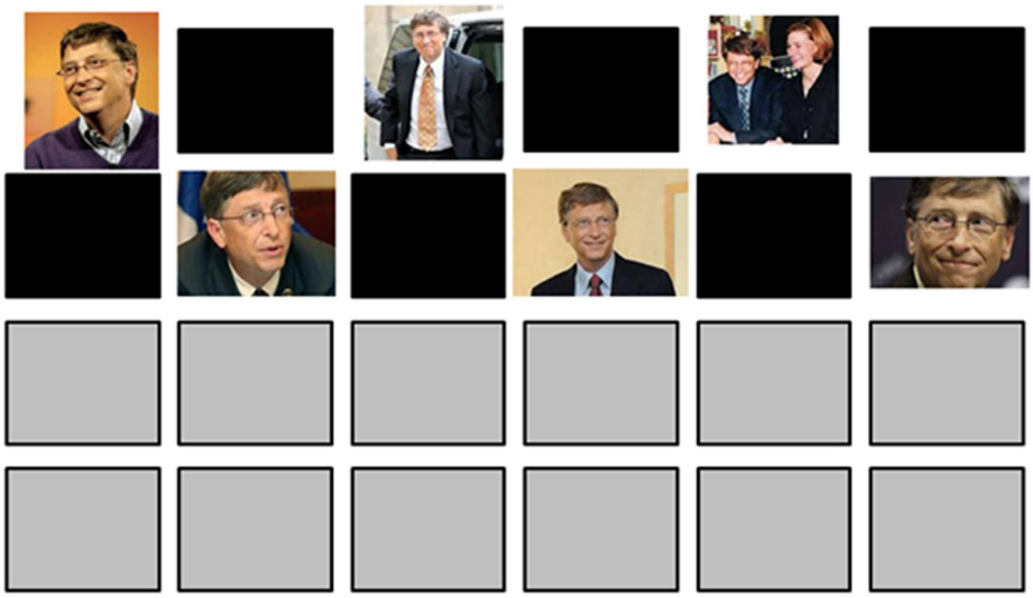
도면2


제1 저장부
211
제2 저장부
212
제3 저장부
213
데이터베이스부
220
표시 제어부
230
인증부
데이터베이스부
단말장치
240

도면3


빌 게이츠를 선택하세요.

도면4



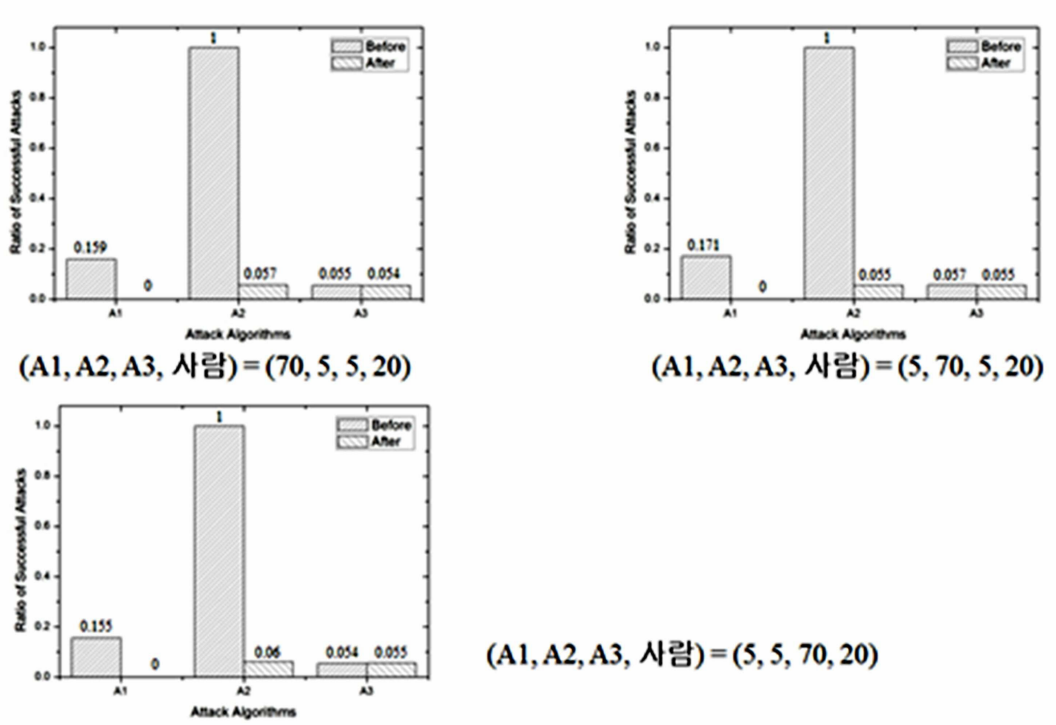
도면5



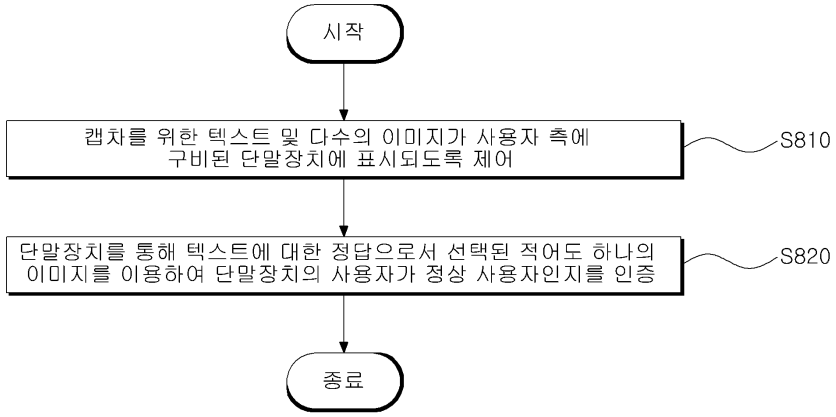
도면6


510
빌게이츠 사진 DB
520

도면7


Ratio of Successful Attacks
Attack Algorithms
Before
After
A1
A2
A3
0.159
0
1
0.057
0.055
0.054
(A1, A2, A3, 사람) = (70, 5, 5, 20)
0.171
0.055
0.057
0.055
(A1, A2, A3, 사람) = (5, 70, 5, 20)
0.155
0.06
(A1, A2, A3, 사람) = (5, 5, 70, 20)

도면8


시작
캡차를 위한 텍스트 및 다수의 이미지가 사용자 측에 구비된 단말장치에 표시되도록 제어
S810
단말장치를 통해 텍스트에 대한 정답으로서 선택된 적어도 하나의 이미지를 이용하여 단말장치의 사용자가 정상 사용자인지를 인증
S820
종료