(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2010년12월14일
(11) 등록번호 10-1000575
(24) 등록일자 2010년12월06일

(51) Int. Cl.
H04L 29/06 (2006.01) *H04W 12/06* (2009.01)
H04L 9/32 (2006.01)
(21) 출원번호 10-2009-0026715
(22) 출원일자 2009년03월29일
심사청구일자 2009년03월29일
(65) 공개번호 10-2010-0108490
(43) 공개일자 2010년10월07일
(56) 선행기술조사문헌
논문:한국정보과학회*
US7127112 B2
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
양대헌
서울 서초구 서초동 삼풍 ATP 3동 405호
자야바타르
인천 남구 용현4동 48-49 광원B주택 B02
(74) 대리인
김건우

전체 청구항 수 : 총 3 항 심사관 : 이성영

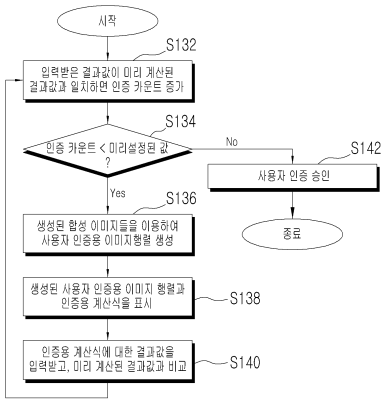
(54) 합성 이미지 기반 인증 프로토콜

(57) 요 약

본 발명은 합성 이미지 기반 인증 프로토콜에 관한 것으로서, 보다 구체적으로는 (1) 사용자 인증을 위한 좌표 추출을 위해 사용되는 적어도 하나 이상의 비밀 이미지를 포함하는 복수의 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하는 단계, (2) 사용자 인증을 위하여 상기 생성된 사용자 인증용 이미지 행렬과, 상기 이미지 행렬로부터 파악되는 비밀 이미지의 좌표값을 적용하기 위한 인증용 계산식을 화면에 표시하는 단계, 및 (3) 사용자로부터 상기 인증용 계산식에 대한 결과 값을 입력받고, 상기 입력받은 결과 값과 미리 계산된 결과 값을 비교하여 상기 사용자를 인증하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

본 발명의 합성 이미지 기반 인증 프로토콜에 따르면, 이미지를 이용하여 사용자 인증을 수행함으로써 아이디나 패스워드를 잊어버린 경우에도 인증이 가능하고, 이미지 행렬을 통해 파악되는 좌표값을 이용함으로써 쉽게 추측될 수 없는 값이 인증에 이용되므로 악성 프로그램의 키보드 해킹을 통한 아이디와 패스워드의 노출 확률이 거의 없으며, 각종 피싱 사이트에도 대비할 수 있는 안전하고 신뢰성 있는 사용자 인증의 수행이 가능하다.

대 표 도 - 도3



특허청구의 범위

청구항 1

합성 이미지 기반 인증 프로토콜에 있어서,

(1) 사용자 인증을 위한 좌표 추출을 위해 사용되는 적어도 하나 이상의 비밀 이미지를 포함하는 복수의 이미지들을 이용하여 생성한 합성 이미지의 벡터로 구성되는 사용자 인증용 이미지 행렬을 생성하는 단계;

(2) 사용자 인증을 위하여 상기 생성된 사용자 인증용 이미지 행렬과, 상기 이미지 행렬로부터 파악되는 비밀 이미지의 좌표 값을 적용하기 위한 인증용 계산식을 화면에 표시하는 단계; 및

(3) 사용자로부터 상기 인증용 계산식에 대한 결과 값을 입력받고, 상기 입력받은 결과 값과 미리 계산된 결과 값을 비교하여 상기 사용자를 인증하는 단계를 포함하되,

상기 단계 (1)은,

(1-1) 사용자 인증을 위한 좌표 추출을 위해 사용되는 적어도 하나 이상의 비밀 이미지를 포함하는 복수의 이미지들을 이용하여 합성 이미지를 생성하는 단계; 및

(1-2) 상기 생성된 합성 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하는 단계를 포함하며,

상기 단계 (1-1)에서는,

적어도 하나 이상의 비밀 이미지와 복수 개의 일반 이미지들로 이루어진 미리 입력된 이미지들 중 중복되지 않은 임의의 이미지들을 추출하고, 상기 추출된 이미 지들을 미리 설정된 개수씩 이미지들의 투명도를 조절하여 오버레이 형식으로 합성 이미지를 생성하는 것을 특징으로 하는 합성 이미지 기반 인증 프로토콜.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 단계 (2)에서 인증용 계산식은 아래의 수학식이고,

상기 단계 (3)에서 미리 계산된 결과 값은 아래의 수학식을 만족하는 R값인 것을 특징으로 하는 합성 이미지 기반 인증 프로토콜.

<수학식>

$R = x_l^{(o,p)} + y_k^{(o,p)}$ 또는 $R = x_p^{(k,l)} + y_o^{(k,l)}$

여기서, 좌표 (o,p)와 (k,l)은 질의 행렬에서 사용자의 비밀 이미지를 포함하는 원소의 위치를 나타낸다.

청구항 4

삭제

청구항 5

제1항에 있어서, 상기 단계 (1-2)는,

상기 생성된 합성 이미지, 상기 합성 이미지의 상 또는 하행에 위치한 벡터 x와 상기 합성 이미지의 좌 또는 우열에 위치한 벡터 y로 이루어진 원소들로 구성된 사용자 인증용 이미지 행렬을 생성하고,

상기 사용자 인증용 이미지 행렬의 각 원소들은 임의의 벡터 x와 y로 표현되며,

상기 이미지 행렬의 i번째 행과 j번째 열에 있는 임의 벡터 x와 y는 아래의 수학식을 만족하며,

<수학식>

모든 $1 \leq i \leq n$, $1 \leq j \leq m$에 대해서,

$$X^{(i,j)}=[x_1^{(i,j)},x_2^{(i,j)},,x_n^{(i,j)}],\ Y^{(i,j)} = [y_1^{(i,j)},y_2^{(i,j)},,y_m^{(i,j)}]^T$$

여기서, $X^{(i,j)}$는 행 벡터(n x 1)이고, $Y^{(i,j)}$는 열 벡터(1 x m)이다.

모든 $1 \leq k \leq n$, $1 \leq l \leq m$에 대해서,

$$x_k^{(i,j)},\ y_l^{(i,j)} \in_R \{t \mid -q \leq t \leq q\}$$

여기서, q는 m x n인 양의 정수이다.

상기 단계 (3)은,

상기 입력받은 결과 값이 미리 계산된 결과 값과 일치하면 인증 카운트를 증가시키고, 다음 질의를 생성하는 단계; 및

상기 인증 카운트가 미리 설정된 값 미만이면 다시 상기 단계 (1-2) 내지 단계 (4)의 과정을 수행하고, 상기 인증 카운트가 미리 설정된 값과 일치하면 사용자 인증을 승인하는 단계로 구성되는 것을 특징으로 하는 합성 이미지 기반 인증 프로토콜.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 인증 프로토콜에 관한 것으로서, 보다 구체적으로는 합성 이미지 기반 인증 프로토콜에 관한 것이다.

배 경 기 술

[0002] 스파이웨어와 같은 악성 프로그램에 의한 피해 사례 및 금융기관을 사칭한 피싱 사이트, 게임 아이템 및 이벤트 당첨을 미끼로 정보를 요구하는 피싱 사이트 등 무수히 많은 피싱 사례가 쏟아지고 있는 것이 현실인 요즘, 컴퓨터 사용을 위한 사용자 인증 방법으로 대부분 텍스트 기반의 아이디/패스워드를 사용하고 있는데, 이 방법은 다음과 같은 몇 가지 약점을 가지고 있다.

[0003] 첫째는, 사용자가 아이디(ID), 패스워드(Password)를 잊어버리는 경우가 많고, 둘째는, 쉽게 추측될 수 있는 값, 예를 들면 주민등록번호나 이름의 약자, 전화 번호, 생년월일 등에 해당하는 단어 등을 패스워드로 사용하는 경우가 많아 사전단어 공격(dictionary attack)이 가능하다. 통계적으로 30초 이내에 80% 이상의 암호가 공격되는 것으로 알려져 있다.

[0004] 셋째, 스파이웨어와 같은 악성 프로그램에 취약하다는 것인데, '키보드 해킹' 으로 알려져 있는 키 로깅(key logging)에 의해 사용자의 아이디와 패스워드가 쉽게 노출될 수 있다는 점이다. 특히 세 번째 문제점은 악성 프로그램뿐만 아니라 각종의 피싱 사이트 등에서도 동일하게 문제가 되며, 생활 속에서 인터넷을 이용한 사무 또는 작업들이 늘어나는 만큼 이러한 사전단어공격(dictionary attack)이나 스파이웨어 및 각종 피싱 사이트 등에 대비한 보다 안전하고 신뢰성 있는 개인 인증 방법이 필요하다는 문제점이 대두되고 있다.

발명의 내용

해결 하고자하는 과제

[0005] 본 발명은 기존에 제안된 방법들의 상기와 같은 문제점들을 해결하기 위해 제안된 것으로서, 이미지를 이용하여 사용자 인증을 수행함으로써 아이디나 패스워드를 잊어버린 경우에도 인증이 가능한 합성 이미지 기반 인증 프로토콜을 제공하는 것을 그 목적으로 한다. 또한, 이미지 행렬을 통해 파악되는 좌표 값을 이용함으로써 쉽게

추측될 수 없는 값이 인증에 이용되므로 악성 프로그램의 키보드 해킹을 통한 아이디와 패스워드의 노출 확률이 거의 없으며, 각종 피싱 사이트에도 대비 가능한 안전하고 신뢰성 있는 합성 이미지 기반 인증 프로토콜을 제공하는 것을 그 목적으로 한다.

과제 해결수단

[0006] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른 합성 이미지 기반 인증 프로토콜은,

[0007] (1) 사용자 인증을 위한 좌표 추출을 위해 사용되는 적어도 하나 이상의 비밀 이미지를 포함하는 복수의 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하는 단계;

[0008] (2) 사용자 인증을 위하여 상기 생성된 사용자 인증용 이미지 행렬과, 상기 이미지 행렬로부터 파악되는 비밀 이미지의 좌표값을 적용하기 위한 인증용 계산식을 화면에 표시하는 단계; 및

[0009] (3) 사용자로부터 상기 인증용 계산식에 대한 결과 값을 입력받고, 상기 입력받은 결과 값과 미리 계산된 결과 값을 비교하여 상기 사용자를 인증하는 단계를 포함하는 것을 그 구성상의 특징으로 한다.

[0010] 바람직하게는, 상기 단계 (1)은,

[0011] (1-1) 사용자 인증을 위한 좌표 추출을 위해 사용되는 적어도 하나 이상의 비밀 이미지를 포함하는 복수의 이미지들을 이용하여 합성 이미지를 생성하는 단계; 및

[0012] (1-2) 상기 생성된 합성 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하는 단계로 구성될 수 있다.

[0013] 바람직하게는,

[0014] 상기 단계 (2)에서 인증용 계산식은 아래의 수학식이고,

[0015] 상기 단계 (3)에서 미리 계산된 결과 값은 아래의 수학식을 만족하는 R값으로 구성될 수 있다.

[0016] <수학식>

[0017] $R = x_l^{(o,p)} + y_k^{(o,p)}$ 또는 $R = x_p^{(k,l)} + y_o^{(k,l)}$

[0018] 여기서, 좌표 (o,p)와 (k,l)은 질의 행렬에서 사용자의 비밀 이미지를 포함하는 원소의 위치를 나타낸다.

[0019] 더욱 바람직하게는, 상기 단계 (1-1)은, 적어도 하나 이상의 비밀 이미지와 복수개의 일반 이미지들로 이루어진 미리 입력된 이미지들 중 중복되지 않은 임의의 이미지들을 추출하고, 상기 추출된 이미지들을 미리 설정된 개수씩 이미지들의 투명도를 조절하여 오버레이 형식으로 합성 이미지를 생성할 수 있다.

[0020] 더욱 바람직하게는, 상기 단계 (1-2)는,

[0021] 상기 생성된 합성 이미지, 상기 합성 이미지의 상 또는 하행에 위치한 벡터 x와 상기 합성 이미지의 좌 또는 우열에 위치한 벡터 y로 이루어진 원소들로 구성된 사용자 인증용 이미지 행렬을 생성하고,

[0022] 상기 사용자 인증용 이미지 행렬의 각 원소들은 임의의 벡터 x와 y로 표현되며,

[0023] 상기 이미지 행렬의 i번째 행과 j번째 열에 있는 임의 벡터 x와 y는 아래의 수학식을 만족할 수 있다.

[0024] <수학식>

[0025] 모든 $1 \le i \le n$, $1 \le j \le m$에 대해서,

[0026] $X^{(i,j)}=[x_1^{(i,j)}, x_2^{(i,j)}, , x_n^{(i,j)}]$, $Y^{(i,j)} = [y_1^{(i,j)}, y_2^{(i,j)}, , y_m^{(i,j)}]^T$

[0027] 여기서, $X^{(i,j)}$는 행 벡터(n x 1)이고, $Y^{(i,j)}$는 열 벡터(1 x m)이다.

[0028] 모든 $1 \le k \le n$, $1 \le l \le m$에 대해서,

[0029] $x_k^{(i,j)}$, $y_l^{(i,j)} \in_R \{t \mid -q \le t \le q\}$

[0030] 여기서 q는 m x n 인 양의 정수이다.

[0031] 더욱 바람직하게는, 사용자를 인증하는 상기 단계 (3)는,

[0032] 상기 입력받은 결과 값이 미리 계산된 결과 값과 일치하면 인증 카운트를 증가시키고, 다음 질의를 생성하는 단계; 및

[0033] 상기 인증 카운트가 미리 설정된 값 미만이면 다시 상기 단계 (1-2) 내지 단계 (4)의 과정을 수행하고, 상기 인증 카운트가 미리 설정된 값과 일치하면 사용자 인증을 승인하는 단계로 구성될 수 있다.

효 과

[0034] 본 발명의 합성 이미지 기반 인증 프로토콜 방법에 따르면, 이미지를 이용하여 사용자 인증을 수행함으로써 아이디나 패스워드를 잊어버린 경우에도 인증이 가능하고, 이미지 행렬을 통해 파악되는 좌표 값을 이용함으로써 쉽게 추측될 수 없는 값이 인증에 이용되므로 악성 프로그램의 키보드 해킹을 통한 아이디와 패스워드의 노출 확률이 거의 없으며, 각종 피싱 사이트에도 대비할 수 있는 안전하고 신뢰성 있는 사용자 인증의 수행이 가능하다.

발명의 실시를 위한 구체적인 내용

[0035] 이하에서는 첨부된 도면들을 참조하여, 본 발명에 따른 실시예에 대하여 상세하게 설명하기로 한다.

[0036] 도 1은 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 흐름도이다. 도 1에 도시된 바와 같이, 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜은, 복수의 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하는 단계(S110), 생성된 사용자 인증용 이미지 행렬과 인증용 계산식을 표시하는 단계(S120), 및 인증용 계산식에 대한 결과 값을 입력받고, 미리 계산된 결과 값과 비교하여 사용자를 인증하는 단계(S130)를 포함한다.

[0037] 단계 S110은, 복수의 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하는 과정으로서, 키보드 피싱 또는 각종 피싱 사이트에서의 각종 인증에 사용되는 아이디 또는 패스워드의 노출을 막기 위하여 사용자의 비밀 이미지를 이용해 사용자 인증용 이미지 행렬을 생성한다. 여기서, 사용자의 비밀 이미지는 사용자 인증을 위한 좌표 추출을 위해 사용되며, 적어도 하나 이상의 비밀 이미지를 포함하는 복수의 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하게 된다. 이러한 사용자 인증용 이미지 행렬을 생성하는 방법은 도 2를 통해 보다 상세히 설명한다.

[0038]

[0039] 도 2는 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜에서 사용자 인증용 이미지 행렬을 생성하는 방법의 흐름도이다. 도 2에 도시된 바와 같이, 본 발명의 일실시예에 따른 사용자 인증용 이미지 행렬을 생성하는 방법은, 복수의 이미지들을 이용하여 합성 이미지를 생성하는 단계(S112), 및 생성된 합성 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하는 단계(S114)를 포함한다.

[0040] 단계 S112는, 사용자 인증을 위한 좌표 추출을 위해 사용되는 적어도 하나 이상의 비밀 이미지를 포함하는 복수의 이미지들을 이용하여 합성 이미지를 생성한다. 즉, 적어도 하나 이상의 비밀 이미지와 복수 개의 일반 이미지들로 이루어진 미리 입력된 이미지들 중 중복되지 않은 임의의 이미지들을 추출하고, 추출된 이미지들을 미리 설정된 개수씩 이미지들의 투명도를 조절하여 오버레이 형식으로 합성 이미지를 생성하게 된다. 본 발명에서 합성 이미지에 기초한 인증 프로토콜은 크게 세 단계에 의해 수행되는데, 그 첫 번째는 이미지를 합성하는 단계이고, 둘째는 이미지 행렬에 의해 질의를 생성하는 단계이며, 마지막은 생성된 질의에 의해 사용자를 인증 단

계이다. 우선 이미지를 합성하는 단계는, 단계 S112를 통해 이미지의 투명도를 조절하여 오버레이하는 과정으로서, S를 사용자 비밀 이미지의 집합, P를 사용자에 대한 전체 이미지의 집합이라고 하면, 사용자 가입 시 서버는 사용자에게 이미지 집합 P를 만들어 준다. 이때 P는 s개의 비밀 이미지와 p-s개의 일반 이미지로 이루어진다. 서버는 집합 P에서 일정 개수의 이미지들을 3개씩 합성하여 사용자에게 보내는데 그 중 정확히 2개는 사용자 비밀 이미지이며, 모든 이미지들은 중복하여 추출되지 않는다. 이러한 이미지 합성을 통해 생성된 합성 이미지는 도 4에 도시되어 있다.

[0041] 도 4는 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 이미지 합성을 나타낸 도면이다. 도 4에 도시된 바와 같이, 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 이미지 합성은, 사용자 인증을 위한 좌표 추출에 이용되는 사용자 비밀 이미지를 포함하는 전체 이미지들 중 3개의 이미지를 추출하여 이루어진다. 도 4에서는 슈퍼마리오의 이미지, 수박의 이미지, 타이어의 이미지의 3개의 이미지를 합성하는데, 우선 수박의 이미지와 슈퍼마리오의 이미지의 투명도를 조절하여 오버레이한 후에 다시 세 번째 이미지인 타이어 이미지의 투명도를 조절하여 오버레이 함으로써 합성 이미지를 생성하게 된다. 이렇게 생성된 합성 이미지는 이후 인증을 위해 사용자가 3가지 이미지가 오버레이된 합성 이미지 중 자신의 비밀 이미지가 포함된 합성 이미지를 선택하여 좌표를 얻는데 사용된다.

[0042] 단계 S114는, 그 다음 단계인 질의 생성 단계에 대한 것으로서, 단계 S112에서 생성된 합성 이미지들을 이용하여 사용자 인증을 위한 질의를 위해 사용자 인증용 이미지 행렬을 생성한다. 즉, 여기에서 질의 생성이란 인증 시 서버가 사용자에게 제공하는 m x n 행렬인 질의를 생성하는 단계로서, 생성된 합성 이미지, 합성 이미지의 상 또는 하행에 위치한 벡터 x와 합성 이미지의 좌 또는 우열에 위치한 벡터 y로 이루어진 원소들로 구성된 사용자 인증용 이미지 행렬을 생성한다. 이때 사용자 인증용 이미지 행렬의 각 원소들은 임의의 벡터 x와 y로 표현되며, 이 행렬을 질의 행렬이라고 하면 질의 행렬의 각 원소들은 하나의 합성 이미지 및 두 개의 임의 벡터 x와 y로 이루어진다. 질의 행렬의 i번째 행, j번째 열에 있는 임의 벡터 x와 y는 각각 다음과 같은 수학식 1 및 수학식 2를 만족하는 값에 해당한다.

수학식 1

[0043] 모든 $1 \le i \le n$, $1 \le j \le m$에 대해서,

[0044] $X^{(i,j)}=[x_1^{(i,j)}, x_2^{(i,j)}, , x_n^{(i,j)}]$, $Y^{(i,j)} = [y_1^{(i,j)}, y_2^{(i,j)}, , y_m^{(i,j)}]^T$

[0045] 여기서, $X^{(i,j)}$는 행 벡터(n x 1)이고, $Y^{(i,j)}$는 열 벡터(1 x m)이다.

수학식 2

[0046] 모든 $1 \le k \le n$, $1 \le l \le m$에 대해서,

[0047] $x_k^{(i,j)}$, $y_l^{(i,j)} \in_R \{t \mid -q \le t \le q\}$

[0048] 여기서, q는 m x n인 양의 정수이다.

[0049] 이렇게 생성된 이미지 행렬은 이후에 설명하는 도 5를 통해 확인할 수 있다.

[0050] 단계 S120은, 사용자 인증용 이미지 행렬과 인증용 계산식을 사용자의 화면에 표시하는 과정으로서, 사용자 인증을 위하여 단계 S110에서 생성된 사용자 인증용 이미지 행렬과, 이미지 행렬로부터 파악되는 비밀 이미지의 좌표값을 적용하기 위한 인증용 계산식을 화면에 표시한다. 여기서 사용자가 아이디나 패스워드를 입력하는 대신에 사용하는 이미지, 즉, 자신의 비밀 이미지를 포함한 원소들의 위치를 좌표 (k,l)과 (o,p)라고 가정할 때, 인증용 계산식은 $R = x_l^{(o,p)} + y_k^{(o,p)}$ 또는 $R = x_p^{(k,l)} + y_o^{(k,l)}$과 같이 나타낼 수 있다. 따라서 사용자는 화면에 표시된 인증용 이미지 행렬을 보고, 인증용 계산식에 대한 결과 값을 입력하게 된다.

[0051] 단계 S130은, 마지막인 사용자 인증 단계에 대한 것으로서, 인증용 계산식에 대한 결과 값을 입력받고, 미리 계산된 결과 값과 비교하여 사용자를 인증한다. 본 발명에 따른 합성 이미지 기반 인증 프로토콜은 사용자로부터 인증용 계산식에 대한 결과 값을 입력받고, 그 값의 옳고 그름에 따라 사용자 인증을 수행하게 되므로 우선, 사용자로부터 인증용 계산식에 대한 결과 값을 입력받고, 이렇게 입력받은 결과 값과 미리 계산된 결과 값을 비교하여 사용자를 인증하게 된다. 보다 상세히 설명하면, 사용자 인증 단계에서 사용자는 화면을 통해 서버로부터 임의로 합성된 이미지를 포함하는 질의 행렬을 제공받고, 합성된 이미지들 속에서 자기 비밀 이미지가 들어간 합성 이미지 두 개를 인식한다. 이때 두 개의 비밀 이미지는 같은 원소에 속하지 않으며, 전체적인 사용자 인증 과정은 다음과 같이 나타낼 수 있다.

[0052] 1. 서버는 임의로 합성된 이미지를 포함하는 m x n 크기의 질의 행렬을 보낸다.

[0053] 2. 사용자는 자신의 비밀 이미지를 포함한 원소들을 찾는다. 여기서, 그 원소들의 위치를 좌표 (k,l)과 (o,p)라고 가정한다.

[0054] 3. 사용자는 다음 수학식 3 중 하나를 임의로 골라 답 R을 계산한다.

수학식 3

[0055] $R = x_l^{(o,p)} + y_k^{(o,p)}$ 또는 $R = x_p^{(k,l)} + y_o^{(k,l)}$

[0056] 4. 사용자는 R을 입력한다.

[0057] 5. 서버는 R을 확인하고 맞으면 다음 질의를 보낸다.

[0058] 6. 사용자는 A번의 질의를 맞추면 인증된다.

[0059] 사용자가 화면에 표시된 합성 이미지 행렬 즉, 사용자 인증용 이미지 행렬을 이용하여 결과 값을 계산 또는 서버가 미리 결과 값을 계산하는 과정을 도 5에 나타난 합성 이미지 행렬에 적용하면 다음과 같다.

[0060] 도 5는 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 화면을 나타낸 도면이다. 도 5에 도시된 바와 같이, 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 화면은 m = n = 4이고 q = 16인 질의 행렬을 나타낸다. 도 5에서 사용자 인증을 위한 사용자의 비밀 이미지가 슈퍼마리오와 미키마우스라고 가정하면 각각의 원소들의 위치는 (k,l) = (1,3)과 (o,p) = (4,2)가 된다. 이 각각의 값을 식에 대입하여 R 값을 구하면 $R= x_l^{(o,p)} + y_k^{(o,p)} = x_3^{(4,2)} + y_1^{(4,2)}$이 되는데, 여기서 $x_3^{(4,2)} + y_1^{(4,2)}$는 이미지 행렬의 4행, 2열에 있는 원소의 x축 3번째 숫자와 y축 1번째 숫자를 더하는 것을 의미하므로 합성 이미지 행렬에서 4행, 2열의 x축 3번째 숫자인 -5 와 y축 1번째 숫자인 14를 더하면 9가 되고, 여기서 구해진 결과 값인 9가 인증을 위한 숫자가 된다. 이때 x축은 왼쪽에서부터 오른쪽으로 순서가 증가하고, y축은 위에서 아래로 순서가 증가한다. 또한, $R = x_p^{(k,l)} + y_o^{(k,l)} = x_2^{(1,3)} + y_4^{(1,3)}$의 경우, 1행, 3열의 x축에서 2번째 숫자와 y축에서 4번째 숫자를 더한 값이므로 -3과 -15에 의해 -18이 R 값이 된다. 이렇게 구해진 R 값인 9 또는 -18이 사용자 인증을 위한 결과 값이 되고, 사용자가 R의 결과 값으로 9 또는 -18을 입력하면 사용자 인증이 이루어지게 된다. 물론, 사용자 인증을 위하여 여러 번의 질의를 거치고자 할 경우에는 처음 사용자가 입력한 R 값이 맞으면, 다음 질의를 제공해 미리 정해진 질의를 모든 거친 후에 사용자 인증을 완료하도록 할 수 있으며, 그러한 경우, 도 3과 같은 방법에 의해 사용자 인증을 수행할 수 있다.

[0061] 도 3은 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 사용자 인증을 수행하는 방법의 흐름도이다. 도 3에 도시된 바와 같이, 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 사용자 인증 수행 방법은, 사용자로부터 입력받은 결과 값이 미리 계산된 결과 값과 일치하면 인증카운트를 증가시키고(S132), 인증 카운트의 값이 미리 설정된 값에 해당하는지 비교한다(S134). 만약 인증 카운트가 미리 설정된 값(예를

들어, 사용자 인증을 위하여 A번의 인증을 거치도록 한 경우라면, 미리 설정된 값은 A가 된다.) 미만이면 다시 단계 S114에서와 같이 생성된 합성 이미지들을 이용하여 사용자 인증용 이미지 행렬을 생성하고(S136), 단계 S136에서 생성된 사용자 인증용 이미지 행렬과 인증용 계산식을 사용자의 화면에 표시한 뒤(S138), 사용자로부터 인증용 계산식에 대한 결과 값을 입력받고, 미리 계산된 결과 값과 비교한다(S140). 만약, 단계 S134에서 인증 카운트가 인증 카운트가 미리 설정된 값(여기서는 A)과 일치하면 사용자 인증을 승인하게 된다(S142).

[0062] 이상 설명한 본 발명은 본 발명이 속한 기술분야에서 통상의 지식을 가진 자에 의하여 다양한 변형이나 응용이 가능하며, 본 발명에 따른 기술적 사상의 범위는 아래의 특허청구범위에 의하여 정해져야 할 것이다.

도면의 간단한 설명

[0063] 도 1은 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 흐름도.

[0064] 도 2는 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜에서 사용자 인증용 이미지 행렬을 생성하는 방법의 흐름도.

[0065] 도 3은 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 사용자 인증을 수행하는 방법의 흐름도.

[0066] 도 4는 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 이미지 합성을 나타낸 도면.

[0067] 도 5는 본 발명의 일실시예에 따른 합성 이미지 기반 인증 프로토콜의 화면을 나타낸 도면.

[0068] <도면 중 주요 부분에 대한 부호의 설명>

[0069] S110: 사용자 인증용 이미지 행렬 생성 단계

[0070] S112: 합성 이미지를 생성하는 단계

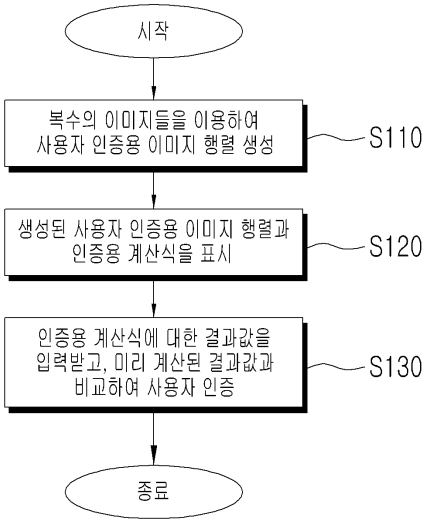
[0071] S114: 사용자 인증용 이미지 행렬을 생성하는 단계

[0072] S120: 생성된 사용자 인증용 이미지 행렬과 인증용 계산식을 표시하는 단계

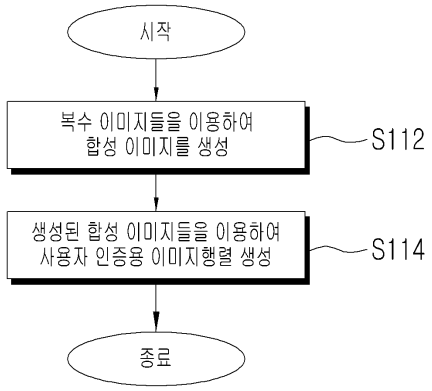
[0073] S130: 사용자 인증을 수행하는 단계

도면

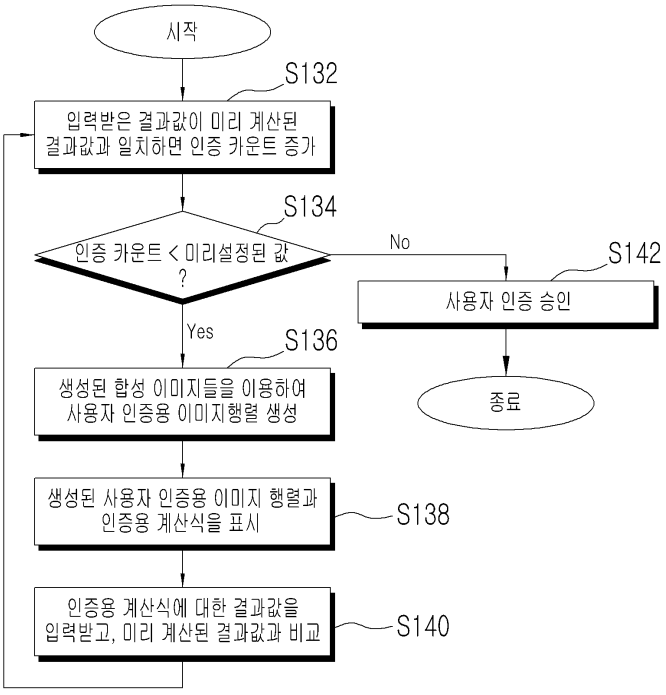
도면1



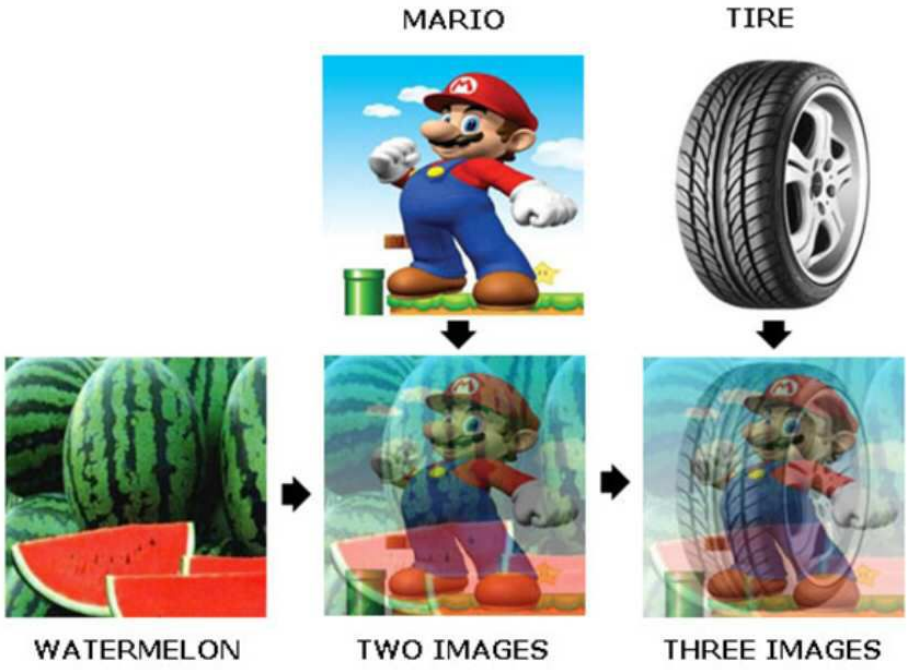
도면2


시작
복수 이미지들을 이용하여
합성 이미지를 생성
S112
생성된 합성 이미지들을 이용하여
사용자 인증용 이미지행렬 생성
S114
종료

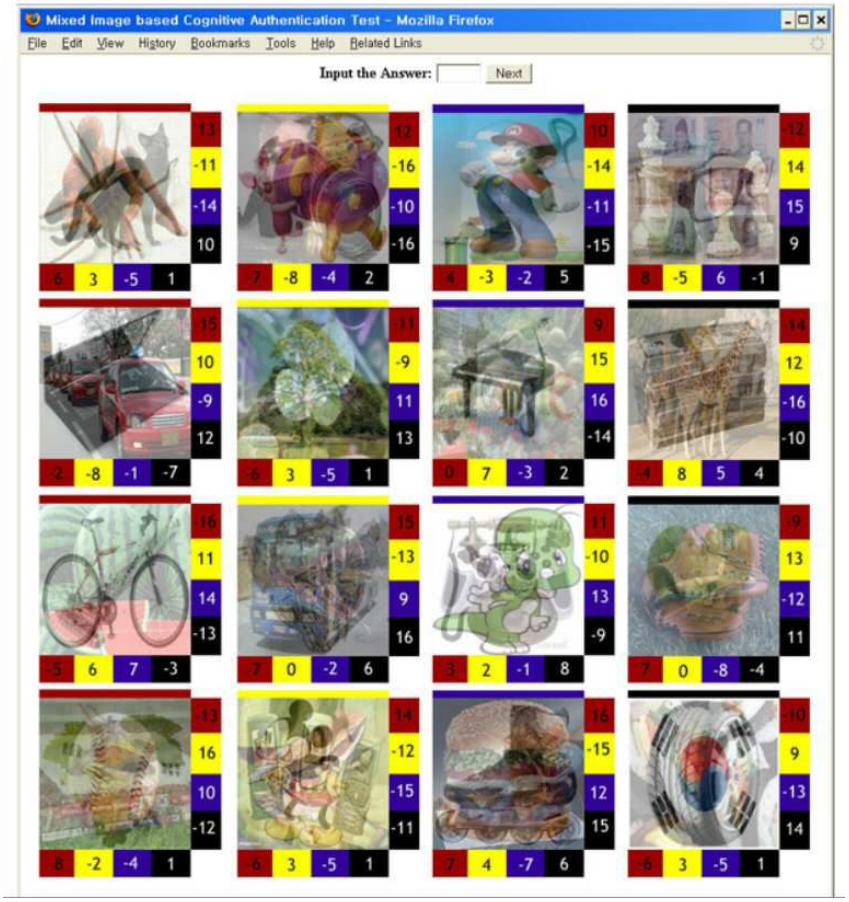
도면3


시작
S132
입력받은 결과값이 미리 계산된
결과값과 일치하면 인증 카운트 증가
S134
인증 카운트 < 미리설정된 값
?
No
S142
사용자 인증 승인
종료
Yes
S136
생성된 합성 이미지들을 이용하여
사용자 인증용 이미지행렬 생성
생성된 사용자 인증용 이미지 행렬과
인증용 계산식을 표시
S138
인증용 계산식에 대한 결과값을
입력받고, 미리 계산된 결과값과 비교
S140

도면4


MARIO
TIRE
WATERMELON
TWO IMAGES
THREE IMAGES

도면5


Mixed Image based Cognitive Authentication Test - Mozilla Firefox
File Edit View History Bookmarks Tools Help Related Links
Input the Answer:
Next