(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2011-0040267
(43) 공개일자 2011년04월20일

(51) Int. Cl.
H04L 9/32 (2006.01)
(21) 출원번호 10-2009-0097467
(22) 출원일자 2009년10월13일
심사청구일자 2009년10월13일

(71) 출원인
인하대학교 산학협력단
인천 남구 용현동 253 인하대학교
(72) 발명자
이문규
경기도 부천시 원미구 상동 진달래마을 효성아파트 2226동 501호
송정은
서울특별시 강서구 화곡4동 464-3 대흥 102호
김창순
광주광역시 북구 용봉동 현대 아이파크 104동 1601호
(74) 대리인
김건우

전체 청구항 수 : 총 5 항

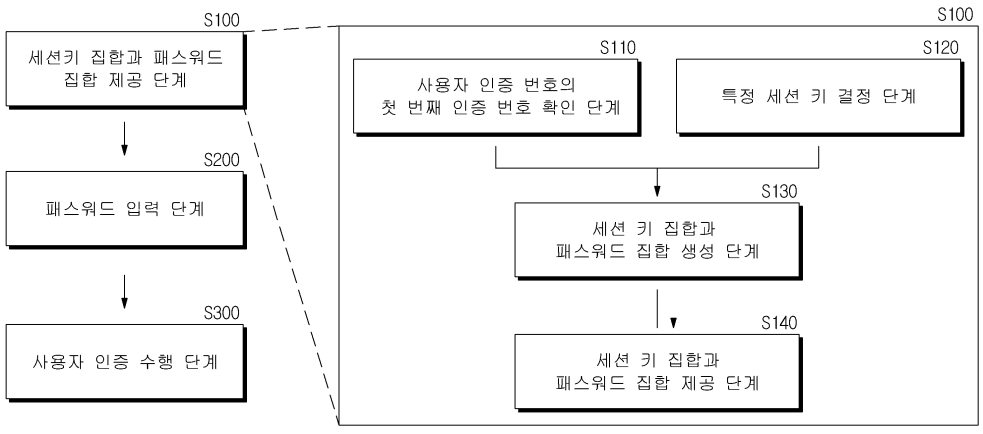
(54) 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법

(57) 요 약

본 발명은 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법에 관한 것으로서, 보다 구체적으로는 (1) 일회성 세션 키 집합과, 상기 세션 키 집합과 대응하는 패스워드 문자들을 임의로 배열하여 사용자에게 세션 키를 간접적으로 전달하는 단계; (2) 사용자 인증 패스워드를 간접적으로 입력하는데 사용될 기호 집합과, 상기 기호 집합과 대응하는 패스워드 문자들을 임의로 배열하여 사용자에게 제공하는 단계; (3) 상기 패스워드 문자들로부터 특정 문자를 상기 세션 키 집합 중의 특정 세션 키와 매칭시키도록 함으로써, 상기 특정 문자를 사용자로부터 입력받는 단계; 및 (4) 입력받은 상기 특정 문자가 상기 사용자의 사용자 인증 패스워드와 일치하는지 여부를 확인함으로써, 사용자 인증을 수행하는 단계를 포함하되, 상기 단계 (1)에서, 상기 특정 세션 키를 미리 결정하고, 상기 결정된 특정 세션 키를 상기 사용자의 사용자 인증 패스워드 중 첫 번째 인증 문자와 매칭시켜 사용자에게 제공하는 것을 특징으로 하는, 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법이다.

본 발명의 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법에 따르면, 사용자 인증 시스템이 세션 키를 임의로 결정하여 사용자에게 제공함으로써, 사용자의 선호도나 습관에 의하여 세션 키가 외부로 노출되는 것을 효과적으로 방지할 수 있다. 뿐만 아니라, 사용자 인증 시스템이 세션 키를 임의로 결정하여 사용자에게 제공하는 구성을, 사용자가 패스워드 문자들 대신에 패스워드 문자를 포함하는 패스워드 부분 집합들을 입력하게 하는 구성과 결합시킴으로써, 녹화가 가능한 장치를 이용한 엿보기 공격과 같은 공격에 훨씬 효과적으로 대응할 수 있다.

대 표 도 - 도1



이 발명을 지원한 국가연구개발사업
과제고유번호 2008-F-045-01
부처명 산업자원부
연구관리전문기관
연구사업명 IT핵심기술개발사업
연구과제명 장애인 및 고령자를 위한 Digital Guardian 기술개발
기여율
주관기관 한국과학기술연구원
연구기간 2009.03~2010.02

특허청구의 범위

청구항 1

2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용하여 사용자를 인증하기 위한 사용자 인증 방법으로서,

(1) 일회성 세션 키 집합과, 상기 세션 키 집합과 대응하는 패스워드 문자들을 임의로 배열하여 사용자에게 세션 키를 간접적으로 전달하는 단계;

(2) 사용자 인증 패스워드를 간접적으로 입력하는데 사용될 기호 집합과, 상기 기호 집합과 대응하는 패스워드 문자들을 임의로 배열하여 사용자에게 제공하는 단계;

(3) 상기 패스워드 문자들로부터 특정 문자를 상기 세션 키 집합 중의 특정 세션 키와 매칭시키도록 함으로써, 상기 특정 문자를 사용자로부터 입력받는 단계; 및

(4) 입력받은 상기 특정 문자가 상기 사용자의 사용자 인증 패스워드와 일치하는지 여부를 확인함으로써, 사용자 인증을 수행하는 단계를 포함하되,

상기 단계 (1)에서, 상기 특정 세션 키를 미리 결정하고, 상기 결정된 특정 세션 키를 상기 사용자의 사용자 인증 패스워드 중 첫 번째 인증 문자와 매칭시켜 사용자에게 제공하는 것을 특징으로 하는, 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법.

청구항 2

제1항에 있어서,

상기 단계 (1)에서, 상기 세션 키 집합 원소들과 상기 패스워드 문자들이 1:N의 비율로 대응하도록 임의로 생성하고,

상기 단계 (2)에서, 상기 기호집합과 대응하는 패스워드 문자들을 1:N 대응이 되도록 임의로 배열 하여 사용자에게 제공하며,

상기 단계 (3)에서, 상기 패스워드 문자열 집합으로부터 크기 N인 패스워드 문자 집합을 상기 세션 키 집합 중의 특정 세션 키와 매칭시키도록 함으로써, 상기 크기 N인 패스워드 문자 집합을 사용자로부터 입력받고,

상기 단계 (4)에서, 입력받은 상기 크기 N인 패스워드 문자 집합 중에 상기 사용자의 사용자 인증 문자가 포함되어 있는지 여부를 확인함으로써, 사용자 인증을 수행하는 것을 특징으로 하는, 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법.

청구항 3

제2항에 있어서,

상기 단계 (1)에서, 상기 세션 키 집합 1행에 대하여 상기 패스워드 문자 배열 N행을 매칭시켜 생성하고, 상기 생성된 N+1행의 세션 키 집합 및 패스워드 문자 배열을 사용자에게 제공하며,

상기 단계 (2)에서, 상기 세션 키 집합 1행은 고정시킨 채, 상기 패스워드 문자 배열 N행을 사용자가 이동시키거나 상기 패스워드 문자 배열 N행을 고정시킨 채, 상기 세션 키 집합 1행을 사용자가 이동시킬 수 있도록 함으로써, 상기 크기 N인 패스워드 문자 집합을 상기 특정 세션 키와 매칭시키도록 하는 것을 특징으로 하는, 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법.

청구항 4

제3항에 있어서,

상기 단계 (1)에서, 상기 세션 키 집합 1행에 대하여 상기 패스워드 문자 배열 N행을 매칭시켜 생성하되, 상기 N행의 패스워드 문자 배열을 구성하는 각각의 행에 대응하도록 상기 세션 키 집합 1행을 반복하여 표시하는 것을 특징으로 하는, 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법.

청구항 5

제1항에 있어서,

사용자 인증 패스워드가 L(L>1)개의 문자로 구성될 경우, 상기 첫 번째 인증 문자를 제외한 상기 사용자 인증 패스워드를 구성하는 L-1개의 문자 각각에 대하여 순서대로 상기 단계 (2) 내지 단계 (4)를 반복하여 수행하는 것을 특징으로 하는, 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법.

명 세 서

발명의 상세한 설명

기 술 분 야

[0001] 본 발명은 사용자 인증 방법에 관한 것으로서, 보다 구체적으로는 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법에 관한 것이다.

배 경 기 술

[0002] 정보통신 기술이 발달한 현대 사회에서 개인 정보를 보호하면서 컴퓨터나 KIOSK 단말기, 은행 단말기(ATM), 모바일 단말기 등의 장치에 대한 접근 관리를 위해 개인 식별 번호(Personal Identification Number: PIN)와 패스워드에 의한 사용자 인증 방법을 많이 사용하고 있다. 이 방법은, 컴퓨터 등 장치에 저장되어 있는 패스워드나 개인 식별 번호(사용자 인증번호)를 사용자에 의해 입력된 값을 비교하여 일치 여부를 판단한 후 접근에 대한 허용 여부를 결정하는 방법이다.

[0003] 개인 식별 번호(사용자 인증 번호)는 일반적으로 4자리 숫자로 이루어져 있다. 0000부터 9999까지의 범위 내의 숫자를 이용할 수 있어 10000가지 경우의 수를 갖는다. 장치에 따라 1111과 같은 연속된 숫자나 개인 정보와 연관된 숫자는 개인 식별 번호(사용자 인증 번호)로 사용할 때 제한받을 수 있어 경우의 수가 10000가지 미만일 수 있다. 이러한 개인 식별 번호(사용자 인증 번호)를 이용한 사용자 인증 방법은 개인 식별 번호(사용자 인증 번호)를 알고 있는 경우 장치에 대한 접근 권한을 얻을 수 있고, 그렇지 않을 경우 접근 권한을 얻을 수 없기 때문에 개인 식별에 대한 애매모호함이 없다. 또한 추가적인 장치의 필요 없이 사용자의 기억력에 의존하여 단말기를 통해 인증을 시도하기 때문에 별도의 비용이 요구되지 않으므로 추가적인 관리나 유지보수 비용을 고려할 필요가 없다.

[0004] 그러나 이러한 방법은 사용자가 개인 식별 번호(사용자 인증 번호)를 입력하는 순간 공격자가 어깨너머로 슬쩍 엿보는 것만으로 개인 식별 번호를 손쉽게 알아낼 수 있기 때문에 그 안전성에 문제가 있다. 이를 해결하기 위하여, 개인 식별 번호(사용자 인증 번호)를 직접 입력하지 않고 사용자만이 알고 있는 기호 또는 숫자(이하 '세션 키'라고 함)와의 매칭을 통해 개인 식별 번호(사용자 인증 번호)를 간접적으로 입력하는 방법이 제안되었다. 그러나 세션 키를 이용하는 기존 사용자 인증 시스템의 경우, 세션 키를 사용자가 직접 결정하도록 함으로써, 사용자의 선호도나 습관에 의하여 세션 키가 고정되어 공격자에게 쉽게 노출될 수 있다는 문제점이 있다. 특히, 공격자가 소형 캠코더 등으로 녹화할 경우, 더욱이 같은 사용자에 대하여 여러 번 녹화하였을 경우 세션 키 노출에 의한 사용자 인증 번호의 노출은 더욱 큰 문제가 된다.

발명의 내용

해결 하고자하는 과제

[0005] 본 발명은 기존 방법들의 상기와 같은 문제점을 해결하기 위해 제안된 방법으로서, 사용자 인증 시스템이 세션 키를 임의로 결정하여 사용자에게 제공함으로써, 사용자의 선호도나 습관에 의하여 세션 키가 외부로 노출되는 것을 효과적으로 방지할 수 있는 사용자 인증 방법을 제공하는 것을 그 목적으로 한다.

[0006] 또한, 사용자 인증 시스템이 세션 키를 임의로 결정하여 사용자에게 제공하는 구성을, 사용자가 패스워드 문자를 직접 입력하는 대신에 패스워드 문자를 포함하는 패스워드 부분 집합들을 입력하게 하는 구성과 결합시킴으로써, 녹화가 가능한 장치를 이용한 엿보기 공격과 같은 공격에 훨씬 효과적으로 대응할 수 있는 사용자 인증 방법을 제공하는 것을 또 다른 목적으로 한다.

과제 해결수단

[0007] 상기한 목적을 달성하기 위한 본 발명의 특징에 따른, 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법은,

[0008] (1) 일회성 세션 키 집합과, 상기 세션 키 집합과 대응하는 패스워드 문자들을 임의로 배열하여 사용자에게 세션 키를 간접적으로 전달하는 단계;

[0009] (2) 사용자 인증 패스워드를 간접적으로 입력하는데 사용될 기호 집합과, 상기 기호집합과 대응하는 패스워드 문자들을 임의로 배열하여 사용자에게 제공하는 단계;

[0010] (3) 상기 패스워드 문자들로부터 특정 문자를 상기 세션 키 집합 중의 특정 세션 키와 매칭시키도록 함으로써, 상기 특정 문자를 사용자로부터 입력받는 단계;

[0011] (4) 입력받은 상기 특정 문자가 상기 사용자의 사용자 인증 패스워드와 일치하는지 여부를 확인함으로써, 사용자 인증을 수행하는 단계를 포함하되,

[0012] 상기 단계 (1)에서, 상기 특정 세션 키를 미리 결정하고, 상기 결정된 특정 세션 키를 상기 사용자의 사용자 인증 패스워드 중 첫 번째 인증 문자와 매칭시켜 사용자에게 제공하는 것을 그 구성상의 특징으로 한다.

[0013] 바람직하게는,

[0014] 상기 단계 (1)에서, 상기 세션 키 집합의 원소와 상기 패스워드 문자들이 1:N (N > 1)의 비율로 대응하도록 임의로 생성하고,

[0015] 상기 단계 (2)에서, 상기 기호집합과 대응하는 패스워드 문자들을 1:N 대응이 되도록 임의로 배열하여 사용자에게 제공하며,

[0016] 상기 단계 (3)에서, 상기 패스워드 문자열 집합으로부터 크기 N인 패스워드 문자 집합을 상기 세션 키 집합 중의 특정 세션 키와 매칭시키도록 함으로써, 상기 크기 N인 패스워드 문자 집합을 사용자로부터 입력받아서,

[0017] 상기 단계 (4)에서, 입력받은 상기 크기 N인 패스워드 문자 집합 중에 상기 사용자의 사용자 인증 문자가 포함되어 있는지 여부를 확인함으로써, 사용자 인증을 수행할 수 있다.

[0018] 더욱 바람직하게는,

[0019] 상기 단계 (1)에서, 상기 세션 키 집합 1행에 대하여 상기 패스워드 문자 배열 N행을 매칭시켜 생성하고, 상기 생성된 N+1행의 세션 키 집합 및 패스워드 문자 배열을 사용자에게 제공하며,

[0020] 상기 단계 (2)에서, 상기 세션 키 집합 1행은 고정시킨 채, 상기 패스워드 문자 배열 N행을 사용자가 이동시키거나 상기 패스워드 문자 배열 N행을 고정시킨 채, 상기 세션 키 집합 1행을 사용자가 이동시킬 수 있도록 함으로써, 상기 크기 N인 패스워드 문자 집합을 상기 특정 세션 키와 매칭시키도록 할 수 있다.

[0021] 더더욱 바람직하게는, 상기 단계 (1)에서, 상기 세션 키 집합 1행에 대하여 상기 패스워드 문자 배열 N행을 매

칭시켜 생성하되, 상기 N행의 패스워드 문자 배열을 구성하는 각각의 행에 대응하도록 상기 세션 키 집합 1행을 반복하여 표시할 수 있다.

[0022] 바람직하게는, 사용자 인증 패스워드가 L(L>1)개의 문자로 구성될 경우, 상기 첫 번째 인증 문자를 제외한 상기 사용자 인증 패스워드를 구성하는 L-1개의 문자 각각에 대하여 순서대로 상기 단계 (2) 내지 단계 (4)를 반복하여 수행할 수 있다.

효 과

[0023] 본 발명의 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법에 따르면, 사용자 인증 시스템이 세션 키를 임의로 결정하여 사용자에게 제공함으로써, 사용자의 선호도나 습관에 의하여 세션 키가 외부로 노출되는 것을 효과적으로 방지할 수 있다.

[0024] 뿐만 아니라, 사용자 인증 시스템이 세션 키를 임의로 결정하여 사용자에게 제공하는 구성을, 사용자가 패스워드 문자들을 대신에 패스워드 문자를 포함하는 패스워드 부분 집합들을 입력하게 하는 구성과 결합시킴으로써, 녹화가 가능한 장치를 이용한 엿보기 공격과 같은 공격에 훨씬 효과적으로 대응할 수 있다.

발명의 실시를 위한 구체적인 내용

[0025] 이하에서는 첨부된 도면들을 참조하여, 본 발명에 따른 실시예에 대하여 상세하게 설명하기로 한다.

[0026] 도 1은 본 발명의 일실시예에 따른 사용자 인증 방법의 구성을 나타내는 도면이다. 도 1에 도시된 바와 같이, 본 발명의 일실시예에 따른 사용자 인증 방법은, 세션 키 결정 단계(S000), 세션 키 집합과 패스워드 문자열 집합 제공 단계(S100), 패스워드 입력 단계(S200), 사용자 인증 수행 단계(S300)를 포함하며, 특히 단계 S000은, 사용자 인증 패스워드의 첫 번째 인증 문자를 확인하는 단계(S010), 특정 세션 키를 결정하는 단계(S020), 결정된 특정 세션 키가 사용자 인증 패스워드의 첫 번째 인증 문자와 매칭되도록 세션 키 집합과 패스워드 문자열 집합을 생성하는 단계(S030)를 포함한다.

[0027] 단계 S000에서는, 사용자 인증 문자를 간접적으로 입력하는데 사용될 일회성 세션 키 집합과, 상기 세션 키 집합과 대응하는 패스워드 문자열 집합을 임의로 생성한다. 여기서 "사용자 인증 문자를 간접적으로 입력"한다는 의미는, 기존 사용자 입력 방식과 같이, 사용자 인증 문자를 '1234'와 같이 직접 입력하는 대신에, 사용자만이 알고 있는 특정 세션 키에 '1234'를 차례로 매칭시키는 것과 같은 방식으로 간접적으로 입력하는 것을 의미한다. 또한, '일회성' 세션 키 집합이라고 한 것은, 세션 키 집합과 패스워드 문자열 집합이 생성될 때마다 세션 키 집합이 랜덤하게 바뀌어 임의로 생성된다는 것을 의미한다. 단계 S000은, 단계 S010 내지 단계 S030을 포함할 수 있다.

[0028] 단계 S010에서는, 사용자 인증 절차를 진행하고자 하는 사용자의 사용자 인증 문자 중 첫 번째 인증 문자를 확인한다. 예를 들어, 본 단계는, 사용자 인증 절차를 진행하고자 하는 사용자 인증 패스워드가 '1234'일 경우, 첫 번째 인증 문자인 '1'을 확인하는 단계이다.

[0029] 단계 S020에서는, 금번 사용자 인증 절차에 사용될 특정 세션 키를 결정한다. 물론, 단계 S010과 단계 S020은 서로 순서가 바뀌어도 무관하다.

[0030] 단계 S030에서는, 단계 S020에서 결정된 특정 세션 키가, 단계 S010에서 확인된 사용자 인증 문자의 첫 번째 인증 문자와 매칭되도록 세션 키 집합과 패스워드 문자열 집합을 생성한다. 패스워드 문자열 집합의 형태는 사용자 인증 시스템에 따라 고정되는 경우가 대부분이므로, 세션 키 집합을 임의로 생성하게 된다. 즉, 본 단계에

서는 패스워드 문자열 집합 중 사용자 인증 패스워드의 첫 번째 인증 문자에 해당하는 패스워드에 단계 S020에서 결정된 특정 세션 키가 매칭되도록 세션 키 집합을 생성하게 된다.

[0031] 단계 S100에서는 단계 S000에서 생성된 세션 키 집합의 원소들을 재배열하고 패스워드 문자열 집합과 함께 사용자에게 제공한다.

[0032] 단계 S200에서는, 단계 S100에서 제공된 패스워드 문자열 집합으로부터 특정 패스워드 문자를 세션 키 집합 중의 특정 세션 키와 매칭시키도록 함으로써, 특정 패스워드를 사용자로부터 입력받는다. 특정 패스워드를 특정 세션 키와 매칭시킨다는 의미는, 예를 들어 특정 패스워드가 '1'이고 특정 세션 키가 '♥'일 경우, '1'과 '♥'가 동일 열에 위치시키는 것을 의미한다. 이와 같이, 특정 패스워드를 직접 입력하도록 하는 대신에 특정 패스워드와 특정 세션 키를 매칭시키는 방식으로 특정 패스워드를 입력하도록 함으로써, 엿보기 공격에 효과적으로 대응할 수 있게 된다.

[0033] 단계 S300에서는, 단계 S200에서 입력받은 특정 패스워드가 사용자의 사용자 인증 패스워드와 일치하는지 여부를 확인함으로써, 사용자 인증을 수행한다. 예를 들어, 단계 S200을 통해 사용자로부터 입력받은 특정 패스워드가 '1'일 경우, 이 값이 사용자의 사용자 인증 패스워드 중 이번 순서에서 인증되어야 하는 순서의 인증 문자와 일치하는지 여부를 확인함으로써, 정당한 사용자인지 여부를 인증하게 된다.

[0034] 실시예에 따라서는, 단계 S100에서 세션 키 집합과 패스워드 문자열 집합이 1:N의 비율로 대응하도록 임의로 생성하여 사용자에게 제공할 수 있다. 이 경우, 단계 S200에서는, 패스워드 문자열 집합으로부터 N개의 패스워드 부분 집합을 세션 키 집합 중의 특정 세션 키와 매칭시키도록 함으로써, N개의 패스워드 부분 집합을 사용자로부터 입력받을 수 있다. 또한, 단계 S300에서는, 입력받은 N개의 패스워드 부분 집합 중에 사용자의 사용자 인증 패스워드가 포함되어 있는지 여부를 확인함으로써, 사용자 인증을 수행하게 된다. 여기서, 세션 키 집합과 패스워드 문자열 집합이 1:N의 비율이라고 한 것은, 만약 세션 키 집합이 10개의 원소로 구성될 경우, 패스워드 문자열 집합은 10xN개의 원소로 구성된다는 것을 의미한다. 예를 들어, N이 3일 경우, 10개의 원소로 구성된 세션 키 집합에 대하여, 패스워드 문자열 집합의 원소의 수는 30개가 된다. N은 1보다 크므로, 세션 키 집합의 총 원소 수보다 패스워드 문자열 집합의 총 원소 수가 더 많게 된다. 본 실시예의 단계 S200에서는, 앞서 설명한 바와 같이, 특정 패스워드 문자를 특정 세션 키와 매칭시키도록 하는 대신에, 특정 패스워드 문자를 포함하는 패스워드 부분 집합을 특정 세션 키와 매칭시키도록 한다. 즉, 세션 키 집합의 특정 세션 키에 대하여 패스워드 문자, 예컨대 '1'을 매칭시키는 것이 아니라, '1'을 포함하는 패스워드 부분 집합 {1, a, k}를 매칭시키게 된다. 물론, 특정 세션 키와 매칭시켜져야 할 패스워드 부분 집합의 원소의 개수가 N개로 제한되는 것은 아니나, 대칭 구조를 이용하여 발명의 구현을 용이하게 하기 위하여 바람직한 실시예에서는 N개로 한다. 또한, 본 실시예의 단계 S300에서는, 특정 패스워드 문자를 입력받는 것이 아니라, 특정 패스워드 문자를 포함하는 패스워드 부분 집합을 입력받기 때문에, 사용자로부터 입력받은 패스워드 문자가 사용자 인증 패스워드와 일치하는지 여부를 확인하는 대신에, 사용자로부터 입력받은 패스워드 부분 집합 중에 사용자 인증 패스워드가 포함되어 있는지 여부를 확인함으로써, 사용자 인증 절차를 수행한다.

[0035] 또 다른 실시예에서는, 단계 S100에서, 세션 키 집합 1행에 대하여 패스워드 문자열 집합 N행을 매칭시켜 생성하고, 생성된 N+1행의 세션 키 집합 및 패스워드 문자열 집합을 사용자에게 제공할 수도 있다. 이 경우, 단계 S200에서는, 세션 키 집합 1행은 고정시킨 채, 패스워드 문자열 집합 N행을 사용자가 이동시킬 수 있도록 함으로써, N개의 패스워드 부분 집합을 특정 세션 키와 매칭시키도록 구성할 수 있다. 또는 패스워드 문자열 집합 N행을 고정시킨 채 세션 키 집합을 이동시킬 수 있도록 구성하는 것도 가능하다. 물론, 세션 키 집합 1행에 대하여 패스워드 문자열 집합 N행을 매칭시켜 생성하되, N행의 패스워드 문자열 집합을 구성하는 각각의 행에 대응하도록 세션 키 집합 1행을 반복하여 복수 회 표시할 수도 있다. 이것은 사용자가 세션 키 집합의 원소와 패스워드 문자열 집합의 원소의 매칭을 손쉽게 확인할 수 있도록 하기 위함이다.

[0036] 사용자 인증 패스워드는 대부분 2개 이상의 문자로 구성되는데, 이 경우 단계 S100 내지 단계 S300이 사용자 인증 패스워드를 구성하는 문자의 개수만큼 반복 수행되어야 한다. 물론, 본 발명에 따르면, 사용자 인증 패스워드의 첫 번째 인증 문자는 특정 세션 키와 매칭시켜 제공되는 과정(단계 S000)에서 자동으로 인증 절차를 완료하기 때문에, 사용자 인증 패스워드의 두 번째 이후 인증 문자에 대해서만 단계 S100 내지 단계 S300이 수행되면 된다. 이를 일반화하여 표현하면, 사용자 인증 패스워드가 L개의 문자로 구성될 경우, L-1개의 문자 각각에 대하여 순서대로 단계 S100 내지 단계 S300을 반복하여 수행하게 된다.

[0037] 도 2는 본 발명의 일실시예에 따른 사용자 인증 방법을 구현하기 위한 사용자 인증 장치의 구성을 나타낸 도면이다. 도 2에 도시된 바와 같이, 본 발명의 일실시예에 따른 사용자 인증 장치는, 입력 모듈(210), 저장 모듈(220), 연산 모듈(230), 디스플레이 모듈(240)을 포함하여 구성될 수 있다.

[0038] 입력 모듈(210)은, 키보드, 마우스, 터치스크린, 키패드, RFID, 스마트카드, 바이오 인식(지문, 홍채, 음성, 안면) 및 기타 방법을 통해 사용자로부터 정보를 입력받기 위한 모듈이다. 사용자는 입력 모듈(210)을 통해 자신의 고유 ID를 입력하고, 입력 모듈(210)은 입력받은 ID를 연산 모듈(230)로 전송하여, 입력받은 사용자의 ID가 유효할 경우 접근 권한에 따라 사용자 인증 방법을 통해 패스워드(개인 식별 번호(Personal Identification Number: PIN), 비밀번호, 사용자 인증 번호 등을 모두 포함)를 입력받아 사용자의 접근을 수용하게 된다. 도 3은 본 발명의 일실시예에 따른 사용자 인증 장치의 입력 모듈의 구성을 나타내는 도면이다. 도 3에 도시된 바와 같이, 본 발명의 일실시예에 따른 사용자 인증 장치의 입력 모듈은, 터치스크린 방식을 이용한 입력 모듈(도 3a), 버튼을 이용한 입력 모듈(도 3b)로 구현될 수 있으며, 그 밖에 도면으로 도시하지는 않았지만 스마트폰의 경우 핑거마우스, 노트북의 경우 터치패드, 또한 G-센서를 이용해 기울기나 동작을 통한 입력 방법 등 시스템 환경에 따라서 다양한 입력 방식을 채택할 수 있다.

[0039] 저장 모듈(220)에서는 사용자의 ID와 이에 대응하는 사용자 인증 패스워드를 저장하고 있다. 연산 모듈(230)에서는 입력 모듈(210)로부터 전송받은 ID를 저장 모듈(220)에 있는 ID 목록에서 검색하여 유효한 사용자 ID 인지 판단하고, 유효한 ID일 경우 이에 대응하는 사용자 인증 패스워드를 가져오고, 입력 모듈(210)을 통해 입력된 개인 식별 패스워드와 저장 모듈(220)에 저장되어 있는 패스워드를 비교하여 일치할 경우 접근을 수용한다. 유효하지 않은 ID일 경우 디스플레이 모듈(240)에 유효하지 않은 ID임을 표시한다. 또한, 입력 모듈(210)로부터 입력받은 값에 따라 기호를 배열하여 디스플레이 모듈(240)로 전송한다. 디스플레이 모듈(240)은, 예컨대 패스워드 입력에 필요한 문자 배열과 세션 키로 사용될 기호들을 2차원 형태의 배열로 화면에 표시하고 사용자에게 사용법이나 오류 메시지 등의 안내 메시지를 제공할 수 있다. 입력 모듈(210)과 디스플레이 모듈(240)은 통합된 하나의 장치로 구현될 수도 있다.

[0040] 도 4는 본 발명의 일실시예에 따른 사용자 인증 방법에 있어서, 디스플레이 모듈에서 표시될 수 있는 사용자 인증 패스워드 입력 화면의 일례를 도시한 도면이다. 도 4에 도시된 바와 같이, 사용자 인증 패스워드 입력 화면은, 1행의 세션 키 집합과 이와 대응하는 N행의 패스워드 문자열 집합으로 구성될 수 있다. 1행의 세션 키 집합은, 예컨대 M개의 기호로 이루어질 수 있으며, 각각의 기호는 사용자 인증 패스워드를 간접적으로 입력하는데 사용될 일회성 세션 키를 나타낸다. 여기서 세션 키로 사용될 수 있는 기호는, 도형 이미지뿐만 아니라 다양한 이미지나 기호 및 색깔 등 사용자가 구분하기 쉬운 모든 수단이 사용 가능하다. 제2행부터 시작하는 N행의 패스워드 문자열 집합은, 사용자 인증 패스워드에 사용될 수 있는 기호들로 숫자 또는 문자 등 표현 가능한 모든 문자열이 사용될 수 있다. 사용자가 입력 가능한, 즉 패스워드를 구성할 수 있는 문자들의 수는 N×M개이고, N과 M은 시스템 환경에 따라 변경이 가능하다. 만약 N을 2 이상의 수로 선택할 경우, 사용자가 패스워드 문자들 대신 패스워드 문자를 포함하는 패스워드 부분 집합들을 차례로 입력하게 함으로써, 여러 차례의 숄더 서핑 공격(엿보기 또는 녹화)에 대해서도 기존의 인증 방법보다 강한 안전성을 제공할 수 있다. 사용자들이 패스워드를 입력하는데 있어서 각 행들의 구분을 쉽게 할 수 있도록 행 별로 색이나 무늬 등의 추가적인 정보를 제공할 수 있다. 또한, 세션 키 집합의 위치는 도 4에 도시된 바와 같이 제1 행으로 제한되는 것이 아니라, 매트릭스의 중간이나 마지막 행에 위치할 수도 있으며, 사용자의 편의를 위해 같은 기호를 여러 행 반복해서 표시할 수도 있다(도면 6 참조). 도 4에 도시된 사용자 인증 패스워드 입력 화면에서, (N+1)×M 행렬에 대한 1회 조작으로

사용자 인증 패스워드 중 한 자리를 입력할 수 있으며, 이를 L-1회 반복하면 두 번째 자리부터 L번째까지 L-1자리 사용자 인증 패스워드를 입력할 수 있게 된다. 단, 패스워드의 첫 번째 자리는 인증용이 아닌 세션 키 제공용으로 사용되며, 이에 대한 사용자 입력은 받지 않는다.

[0041] 이하 도 5 및 도 6을 참조하여, 본 발명에서 제안하고 있는 사용자 인증 방법에서의 자세한 조작 과정을 살펴보기로 한다.

[0042] 도 5는 본 발명에서 제안하고 있는 사용자 인증 방법에 따라, 네 자리 사용자 인증 패스워드(즉 L=4인 경우)를 입력하는 과정을 나타내는 도면이다. 도 5에 도시된 실시예에서는 터치 입력 방법으로 설명하고 있으나, 이것으로 제한되는 것은 아니며 다른 입력 방법에 대해서도 동일하게 동작될 수 있다. 도 5에 도시된 실시예는, 숫자로 이루어진 네 자리 패스워드 '1317'을, 패스워드 문자열 집합의 행수(N)가 2이고, 한 행의 세션 키 집합 또는 한 행의 패스워드 문자열 집합의 원소의 수(M)가 5인 경우에 대하여 인증받는 과정이다.

[0043] 먼저, 사용자 인증 시스템이, 5개의 원소로 구성된 세션 키 집합(제 1행)과, 세션 키 집합과 1:2의 비율로 대응하는 패스워드 문자열 집합을 임의로 생성하여 사용자에게 제공한다(도 5a). 이를 위해, 사용자 인증 시스템은, 먼저 사용자 인증 패스워드('1317')의 첫 번째 인증 숫자('1')를 파악한 후, 금번 사용자 인증 과정에서 사용할 세션 키(도 5의 실시예에서는 '♥')를 결정한다. 도 5a로부터, 사용자 인증 패스워드('1317')의 첫 번째 인증 문자('1')가 사용될 세션 키('♥')와 동일한 열에 위치하는 방식으로 매칭되어 제공된 것을 확인할 수 있다.

[0044] 다음으로, 사용자는 제공된 세션 키 집합과 패스워드 문자열 집합의 조합으로부터 세션 키를 파악한다(도 5b). 즉, 사용자는 자신의 사용자 인증 패스워드의 첫 번째 문자(=1)에 대응하는 세션 키(♥)를 찾음으로써 인증 절차에 사용할 세션 키를 파악하게 된다. 이와 같이 사용될 세션 키를 파악한 사용자는, 다음 단계에서 인증 시스템이 세션 키 집합과 패스워드 문자열 집합을 임의로 재배열하여 다시 제시하면 사용자 인증 패스워드의 두 번째 문자(=3)가 세션 키(♥)와 같은 열에 위치하도록 패스워드 문자열 집합을 좌우로 이동시킨다(도 5c). 도 5c에 도시된 과정을 거쳐 사용자 인증 패스워드의 두 번째 문자(=3)가 세션 키(♥)와 같은 열에 위치하게 되면, 입력 버튼을 이용하여 사용자 인증 패스워드의 두 번째 문자가 입력됨을 사용자 인증 시스템에 알린다(도 5d). 도 5c 내지 도 5d와 마찬가지 과정으로, 사용자 인증 패스워드의 세 번째 문자(=1)와 네 번째 문자(=7)도 사용자 인증 시스템에 입력한다(도 5e, 도 5f). 사용자 인증 패스워드의 입력이 모두 완료되면, 사용자 인증이 완료된다(도 5g).

[0045] 도 6은 본 발명에서 제안하고 있는 사용자 인증 방법을 적용하기 위한 사용자 인증 패스워드 입력 화면으로서, 사용자 인증 패스워드가 문자 및 숫자의 조합으로 된 경우를 위한 입력 화면이다. 도 6에 도시된 바와 같이, 사용자 인증 패스워드가 숫자뿐만 아니라 문자도 포함하고 있으므로, 패스워드 문자열 집합은 원소로서 숫자뿐만 아니라 문자도 함께 포함하게 된다(a~z, 0~9). 또한, 동일한 세션 키 집합자뿐만 아니라 문자도 함께 포함하여 사이마다 위치시킴으로써, 사용자가 세션 키 집합과 패스워드 문자열 집합 사이의 대응관계를 더욱 쉽게 확인할 수 있도록 하고 있다. 하부의 입력 버튼을 살펴보면, 좌측 이동 버튼(left), 우측 이동 버튼(right), 및 시작 버튼(start)으로 구성되는데, 시작 버튼의 경우 사용자 인증 과정이 시작되면 입력 버튼(enter)으로 변경되어 표시될 수 있다.

[0046] 이상 살펴본 바와 같이, 본 발명에서 제안하고 있는, 2개 이상의 문자로 구성되는 사용자 인증 패스워드를 이용한 사용자 인증 방법에 따르면, 사용자 인증 시스템이 세션 키를 임의로 결정하여 사용자에게 제공함으로써, 사용자의 선호도나 습관에 의하여 세션 키가 외부로 노출되는 것을 효과적으로 방지할 수 있다. 뿐만 아니라, 사용자 인증 시스템이 세션 키를 임의로 결정하여 사용자에게 제공하는 구성을, 사용자가 패스워드 문자들 대신에 패스워드 문자를 포함하는 패스워드 부분 집합들을 입력하게 하는 구성과 결합시킴으로써, 녹화가 가능한 장치

를 이용한 엿보기 공격과 같은 공격에 훨씬 효과적으로 대응할 수 있다.

[0047] 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

[0048] 도 1은 본 발명의 일실시예에 따른 사용자 인증 방법의 구성을 나타내는 도면.

[0049] 도 2는 본 발명의 일실시예에 따른 사용자 인증 방법을 구현하기 위한 사용자 인증 장치의 구성을 나타낸 도면.

[0050] 도 3은 본 발명의 일실시예에 따른 사용자 인증 장치의 입력 모듈의 구성을 나타내는 도면.

[0051] 도 4는 본 발명의 일실시예에 따른 사용자 인증 방법에 있어서, 디스플레이 모듈에서 표시될 수 있는 사용자 인증 패스워드 입력 화면의 일례를 도시한 도면.

[0052] 도 5는 본 발명에서 제안하고 있는 사용자 인증 방법에 따라, 네 자리 개인 식별 번호를 입력하는 과정을 나타내는 도면.

[0053] 도 6은 본 발명에서 제안하고 있는 사용자 인증 방법을 적용하기 위한 사용자 인증 패스워드 입력 화면으로서, 사용자 인증 패스워드가 문자 및 숫자의 조합으로 된 경우를 위한 입력 화면.

[0054] <도면의 주요 부분에 대한 부호의 설명>

[0055] S000: 세션 키 결정 단계

[0056] S100: 세션 키 집합과 패스워드 문자열 집합 제공 단계

[0057] S200: 패스워드 부분 집합 입력 단계

[0058] S300: 사용자 인증 수행 단계

[0059] 210: 입력 모듈

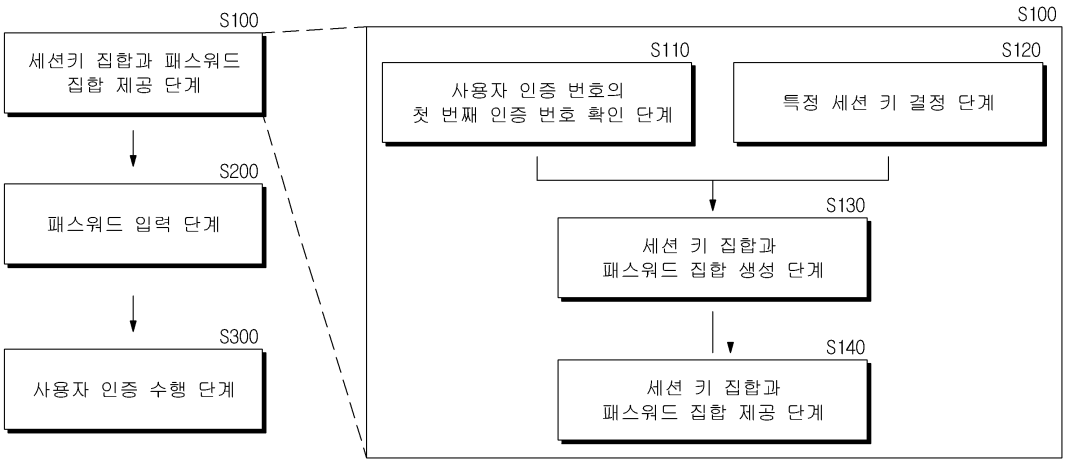
[0060] 220: 저장 모듈

[0061] 230: 연산 모듈

[0062] 240: 디스플레이 모듈

도면

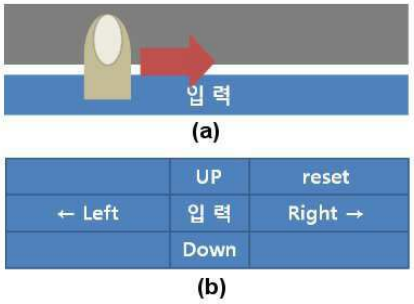
도면1



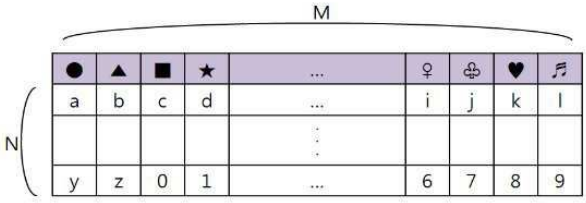
도면2

210
입력 모듈
240
디스플레이 모듈
220
저장 모듈
230
연산 모듈

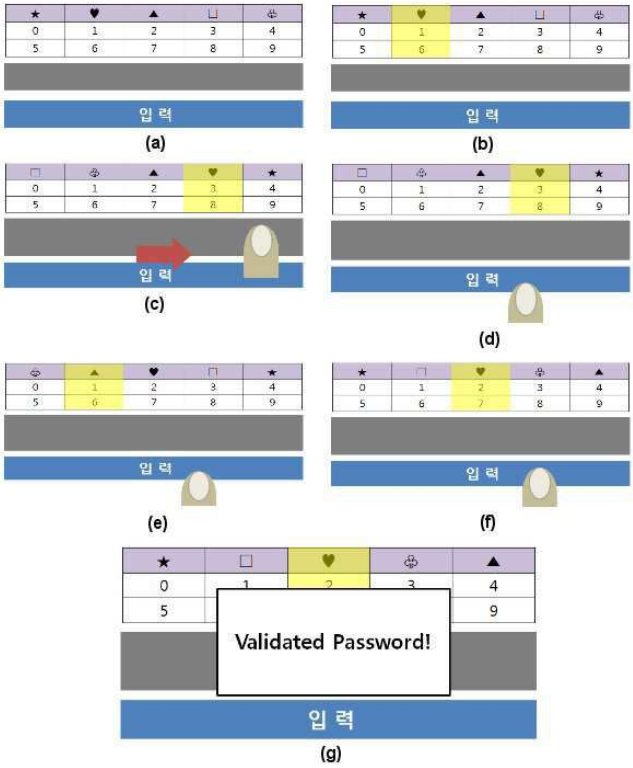
도면3


입 력
(a)
UP
reset
← Left
입 력
Right →
Down
(b)

도면4


M
N
● ▲ ■ ★ ... ♀ ♣ ♥ ♬
a b c d ... i j k l
y z 0 1 ... 6 7 8 9

도면5


입 력
(a)
입 력
(b)
입 력
(c)
입 력
(d)
입 력
(e)
입 력
(f)
Validated Password!
입 력
(g)

도면6

GST_NONCO 5:24 ok
a b c d e f g h i
j k l m n o p q r
s t u v w x y z 0
1 2 3 4 5 6 7 8 9
left
start
right
Orientation