(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2013-0026171
(43) 공개일자 2013년03월13일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *E05B 49/00* (2006.01)
(21) 출원번호 10-2011-0089629
(22) 출원일자 2011년09월05일
심사청구일자 2011년09월05일

(71) 출원인
한국기술교육대학교 산학협력단
충청남도 천안시 동남구 병천면 충절로 1600 (한국기술교육대학교)
(72) 발명자
주승환
충청남도 천안시 동남구 병천면 충절로 1638, 105동 408호 (신한아파트)
서희석
경기도 의왕시 내손중앙로 46-13, B동 202호 (내손동)
(74) 대리인
특허법인태백

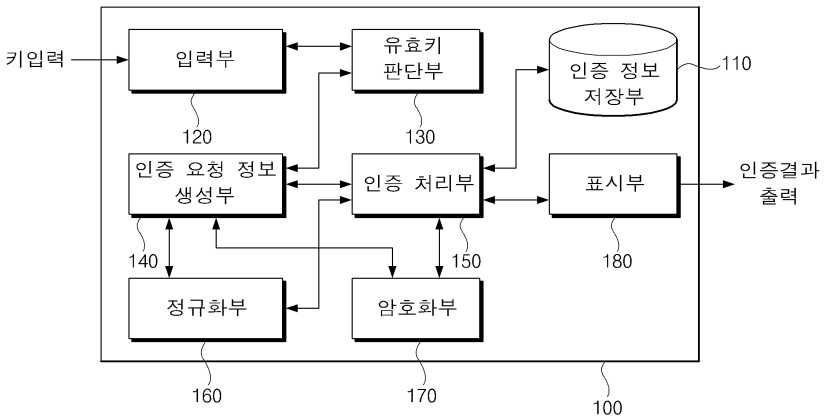
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **인증 처리 장치 및 그 방법**

(57) 요 약

본 발명은 사용자 인증 처리 기술에 관한 것으로, 본 발명의 일 실시예에 따른 인증 처리 장치는, 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 키의 조합에 대한 인증 정보가 저장되는 인증 정보 저장부와, 사용자에 의해 순차적으로 선택된 적어도 하나의 키로부터 인증 요청을 입력받는 입력부와, 상기 선택된 적어도 하나의 키의 입력 시간을 감지하여, 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 유효키를 판단하는 유효키 판단부와, 상기 유효키의 조합을 이용하여 인증 요청 정보를 생성하는 인증 요청 정보 생성부와, 상기 인증 요청 정보와 상기 인증 정보를 비교하여 상기 사용자에 대한 인증을 처리하는 인증 처리부를 포함한다. 이에 따라, 비밀번호를 해킹하기 위해 시도되는 경우의 수를 증가시켜 비밀번호 해킹으로 인한 피해를 줄일 수 있다.

대 표 도 - 도1



특허청구의 범위

청구항 1

복수의 키를 통해 인증을 요청하는 사용자에 대한 인증을 처리하는 장치에 있어서,

키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 키의 조합에 대한 인증 정보가 저장되는 인증 정보 저장부;

사용자에 의해 순차적으로 선택된 적어도 하나의 키로부터 인증 요청을 입력받는 입력부;

상기 선택된 적어도 하나의 키의 입력 시간을 감지하여, 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 유효키를 판단하는 유효키 판단부;

상기 유효키의 조합을 이용하여 인증 요청 정보를 생성하는 인증 요청 정보 생성부; 및

상기 인증 요청 정보와 상기 인증 정보를 비교하여 상기 사용자에 대한 인증을 처리하는 인증 처리부를 포함하는 인증 처리 장치.

청구항 2

제1항에 있어서, 상기 유효키 판단부는,

복수의 키가 동시에 선택된 경우, 상기 복수의 키 중 가장 늦게 선택된 키와 상기 복수의 키 중 가장 먼저 선택 해제된 키 사이의 시간을 미리 설정된 유효 시간과 비교하여, 상기 유효 시간 동안 키 선택이 유지되는 키를 유효키로 판단하는 인증 처리 장치.

청구항 3

제1항에 있어서,

상기 생성된 인증 요청 정보를 오름차순 또는 내림차순으로 정규화하는 정규화부를 더 포함하는 인증 처리 장치.

청구항 4

제1항에 있어서,

상기 생성된 인증 요청 정보를 일방향함수로 암호화하여 상기 인증 처리부로 전송하는 암호화부를 더 포함하고,

상기 인증 처리부는 상기 암호화된 인증 요청 정보를 복호화하는 인증 처리 장치.

청구항 5

제1항에 있어서,

상기 인증 처리부의 인증 처리 결과를 음성 또는 영상으로 표시하는 표시부를 더 포함하는 인증 처리 장치.

청구항 6

복수의 키를 통해 인증을 요청하는 사용자에 대한 인증을 처리하는 방법에 있어서,

사용자에 의해 순차적으로 선택된 적어도 하나의 키로부터 인증 요청을 입력받는 단계;

상기 선택된 적어도 하나의 키의 입력 시간을 감지하여, 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 유효키를 판단하는 단계;

상기 유효키의 조합을 이용하여 인증 요청 정보를 생성하는 단계; 및

상기 인증 요청 정보를 기 설정된 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 키의 조합에 대한 인증 정보와 비교하여 상기 사용자에 대한 인증을 처리하는 단계를 포함하는 인증 처리 방법.

청구항 7

제6항에 있어서, 상기 유효키를 판단하는 단계는,

복수의 키가 동시에 선택된 경우, 상기 복수의 키 중 가장 늦게 선택된 키와 상기 복수의 키 중 가장 먼저 선택 해제된 키 사이의 시간을 미리 설정된 유효 시간과 비교하여, 상기 유효 시간 동안 키 선택이 유지되는 키를 유효키로 판단하는 인증 처리 방법.

청구항 8

제6항에 있어서,

상기 생성된 인증 요청 정보를 오름차순 또는 내림차순으로 정규화하는 단계를 더 포함하는 인증 처리 방법.

청구항 9

제6항에 있어서,

상기 생성된 인증 요청 정보를 일방향함수로 암호화하는 단계를 더 포함하고,

상기 인증을 처리하는 단계는 상기 암호화된 인증 요청 정보를 복호화하는 인증 처리 방법.

청구항 10

제6항에 있어서,

상기 인증 처리 결과를 음성 또는 영상으로 표시하는 단계를 더 포함하는 인증 처리 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 사용자 인증 처리 기술에 관한 것으로, 더욱 상세하게는 동시에 복수의 키가 입력되는 인증요청정보를 처리하는 기술에 관한 것이다.

배 경 기 술

[0002] 사용자 인증 처리 기술 중 패스워드(혹은 비밀번호) 기술은 클라이언트-서버 모델에서 일반적으로 가장 많이 사용하고 있는 방식으로 접근 통제를 위해 사용자 자신의 ID에 대해 패스워드를 입력함으로써 인증을 받게 된다. 그러나 이 방식은 패스워드 전송 노출, 패스워드 재전송, 서버 인증 정보 공격에 취약점을 갖는다. 그리고 만약 사용자와 비밀 통신을 수행하려 할 경우 별도의 키를 생성해야 하는 번거로움 발생하는 등의 문제점이 있다.

[0003] 패스워드는 그 자체로도 보안적인 문제가 있기 때문에 패스워드 크래킹은 패스워드와 관련된 문제의 일부분에 지나지 않는다. 오늘날 대부분의 사용자에게 여러 개의 패스워드가 필요하지만 이 패스워드를 모두 기억할 수 없다. 따라서 하나의 패스워드가 여러 곳에서 재사용되므로 모든 패스워드는 그것이 사용되는 곳 중 가장 취약한 곳에 대한 보안성만을 가지게 된다. 만약 제3자가 어떤 사용자의 패스워드 중 하나를 알게 된다면, 그 사용자가 패스워드를 사용하고 있는 다른 곳에서 해당 패스워드의 사용을 시도할 가능성이 높다.

[0004] 또한, 도어락, 금고 등 일상 생활에서도 사용자 인증을 위해서 패스워드 기술이 사용되고 있다. 사용자는 자신만이 알고 있는 패스워드를 설정하여 이용하게 된다. 그러나, 사용자가 설정할 수 있는 패스워드의 숫자는 제한적이며, 키 버튼을 물리적으로 누르면서 발생하는 키 버튼 음이나, 패스워드에 포함되는 키 버튼의 상대적 마모된 상태 등을 이용하면 제3자가 쉽게 패스워드를 알아낼 수 있는 문제점이 있다. 이에 대해, 종래에는 키 버튼 음을 한 가지로 설정하는 기술, 키 버튼을 터치패드로 구현하는 기술 등이 소개되었으나, 패스워드 조합의 단순성으로 인해 여전히 보안이 취약한 상태이다.

발명의 내용

해결하려는 과제

[0005] 본 발명이 이루고자 하는 기술적인 과제는 동시에 입력되는 복수의 키 입력을 이용한 비밀번호에 대하여 인증을 처리하는 인증 처리 장치, 인증 처리 방법 및 인증 처리 시스템을 제공하기 위한 것이다.

과제의 해결 수단

[0006] 본 발명의 일 실시예에 따른 인증 처리 장치는, 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 키의 조합에 대한 인증 정보가 저장되는 인증 정보 저장부와, 사용자에 의해 순차적으로 선택된 적어도 하나의 키로부터 인증 요청을 입력받는 입력부와, 상기 선택된 적어도 하나의 키의 입력 시간을 감지하여, 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 유효키를 판단하는 유효키 판단부와, 상기 유효키의 조합을 이용하여 인증 요청 정보를 생성하는 인증 요청 정보 생성부와, 상기 인증 요청 정보와 상기 인증 정보를 비교하여 상기 사용자에 대한 인증을 처리하는 인증 처리부를 포함한다.

[0007] 또한, 상기 유효키 판단부는, 복수의 키가 동시에 선택된 경우, 상기 복수의 키 중 가장 늦게 선택된 키와 상기 복수의 키 중 가장 먼저 선택 해제된 키 사이의 시간을 미리 설정된 유효 시간과 비교하여, 상기 유효 시간 동안 키 선택이 유지되는 키를 유효키로 판단할 수 있다.

[0008] 또한, 상기 생성된 인증 요청 정보를 오름차순 또는 내림차순으로 정규화하는 정규화부를 더 포함할 수 있다.

[0009] 또한, 상기 생성된 인증 요청 정보를 일방향함수로 암호화하여 상기 인증 처리부로 전송하는 암호화부를 더 포함하고, 상기 인증 처리부는 상기 암호화된 인증 요청 정보를 복호화할 수 있다.

[0010] 또한, 상기 인증 처리부의 인증 처리 결과를 음성 또는 영상으로 표시하는 표시부를 더 포함할 수 있다.

[0011] 본 발명의 일 실시예에 따른 인증 처리 방법은, 사용자에 의해 순차적으로 선택된 적어도 하나의 키로부터 인증 요청을 입력받는 단계와, 상기 선택된 적어도 하나의 키의 입력 시간을 감지하여, 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 유효키를 판단하는 단계와, 상기 유효키의 조합을 이용하여 인증 요청 정보를 생성하는 단계와, 상기 인증 요청 정보를 기 설정된 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 키의 조합에 대한 인증 정보와 비교하여 상기 사용자에 대한 인증을 처리하는 단계를 포함한다.

발명의 효과

[0012] 이와 같은 본 발명에 따른 인증 처리 장치, 인증 처리 방법은 동시에 입력되는 복수의 키 입력을 이용한 비밀번호에 대하여 인증을 처리함으로써, 비밀번호를 해킹하기 위해 시도되는 경우의 수를 증가시켜 비밀번호 해킹으로 인한 피해를 줄일 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명의 일 실시예에 따른 인증 처리 장치의 구성도,

도 2는 본 발명의 또 다른 실시예에 따른 인증 처리 방법의 순서도,

도 3은 도 1에 따른 입력부에서 동시에 복수의 키를 입력하는 것을 설명하기 위한 예시도이다.

발명을 실시하기 위한 구체적인 내용

[0014] 이하, 첨부된 도면들을 참조하여 본 발명의 실시예를 상세하게 설명한다. 사용되는 용어들은 실시예에서의 기능을 고려하여 선택된 용어들로서, 그 용어의 의미는 사용자, 운용자의 의도 또는 판례 등에 따라 달라질 수 있다. 그러므로 후술하는 실시예들에서 사용된 용어의 의미는, 본 명세서에서 구체적으로 정의된 경우에는 그 정의에 따르며, 구체적인 정의가 없는 경우에는 당업자들이 일반적으로 인식하는 의미로 해석되어야 할 것이다.

[0015] 도 1은 본 발명의 일 실시예에 따른 인증 처리 장치의 구성도이고, 도 2는 도 1에 따른 인증 처리 방법의 순서도이다.

[0016] 도 1과 도 2를 참조하면, 인증 처리 장치(100)는 인증 정보 저장부(110), 입력부(120), 유효키 판단부(130), 인증 요청 정보 생성부(140), 인증 처리부(150), 정규화부(160), 암호화부(170), 표시부(180)를 포함한다. 인증 정보 저장부(110)는 인증 처리 장치(100)에 미리 설정되는 인증 정보가 저장되는 저장소이다. 인증 정보는 키 입력 횟수, 횟수별 키 입력 개수에 대응하는 키의 조합 정보를 포함한다. 인증 정보는 기호, 문자, 숫자 중 적어도 하나를 포함하여 조합되는 비밀번호, 암호, 패스워드, 식별코드를 총칭하는 의미이다.

[0017] 여기서, 키 입력 횟수란 미리 설정된 시간 간격으로 입력되는 키 입력의 횟수를 말한다. 예를 들어, 인증 정보가 ([1],[2],[3],[4])인 경우에는 총 4회의 키 입력이 필요하다. 횟수별 키 입력 개수란 각 횟수에 입력될 수

있는 키 입력의 개수를 의미한다. 예를 들어, 인증 정보가 ([1], [2, 3, 4], [5, 9], [4])인 경우, 키 입력 횟수는 4회이고, 첫 번째 횟수에서는 1개의 키 입력이, 두 번째 횟수에서는 3개의 키 입력이, 세 번째 횟수에서는 2개의 키 입력이, 네 번째 횟수에서는 1개의 키 입력이 설정된 것임을 알 수 있다. 인증 정보는 이와 같이 키 입력 횟수와 횟수별 키 입력 개수에 대응하는 키들의 조합을 의미한다.

[0018] 입력부(120)는 터치패드, 키보드와 같은 입력장치를 포함하며, 사용자에 의해 순차적으로 선택된 적어도 하나의 키로부터 인증 요청을 입력받는다(S200). 이 경우, 입력부(120)가 터치 패드인 경우 감압식, 정전식 터치 패드 모두 사용이 가능하다. 입력부(120)는 기호, 문자, 숫자 중 적어도 하나를 입력받을 수 있으며, 이 경우 복수의 키 입력을 받을 수 있다. 즉, 한 번의 입력 횟수에 복수의 키가 선택되어 입력될 수 있다는 의미이다. 또한, 입력부(120)는 피아노 건반 형태로 구성될 수 있다. 이 경우, 피아노 건반은 각 건반에 대응하는 고유의 키 정보가 설정되거나, 고유의 소리 정보가 설정될 수 있다. 예를 들어, 사용자가 복수의 건반을 동시에 선택하면, 각 건반에 따른 고유의 음이 생성되고, 각 음이 합쳐져서 새로운 소리 정보가 생성된다. 인증 처리 장치(100)는 입력부(120)에서 생성된 소리 정보의 주파수를 분석하여 인증 요청 정보를 파악할 수 있다. 이하, 사용자가 동시에 복수의 키를 입력하는 것과 관련해서 도 3을 참조하여 후술하도록 한다.

[0019] 도 3은 도 1에 따른 입력부에서 동시에 복수의 키를 입력하는 것을 설명하기 위한 예시도이다.

[0020] 도 3을 참조하면, 예를 들어 '0' 부터 '9'까지의 10개의 숫자와 '*', '#'로 구성된 12개의 키 패드로 입력부(120)를 구성한 경우, 인증 정보가 ([1], [0, 5, 6], [3, 4], [8])인 경우에는 두 번째 횟수의 키 입력은 숫자 '0', '5', '6'을 동시에 입력하여야 한다. 입력부(120)는 동시에 복수의 키 입력 인식이 가능하며, 이 경우 두 번째 횟수에 입력되는 3개의 키 입력을 [0, 5, 6]으로 인식하게 된다. 사용자는 한 손 또는 양 손을 모두 사용하여 동시에 다수의 키를 선택할 수 있다. 예를 들어, 키보드와 같이 자판이 긴 경우에는 양 손을 모두 사용하여 동시에 다수의 키를 선택할 수 있으며, 핸드폰과 같이 비교적 크기가 작은 휴대용 단말기의 경우에는 한 손으로 동시에 다수의 키를 선택하는 것이 가능하다.

[0021] 다시 도 1과 도 2를 참조하면, 다음으로 유효키 판단부(130)는 입력부(120)로부터 선택된 적어도 하나의 키의 입력 시간을 감지하여, 키 입력 횟수 및 횟수별 키 입력 개수에 대응하는 유효키를 판단한다(S210). 이 경우, 키 입력 시간은 키 입력 횟수와 횟수별 키 입력 개수를 판단하기 위한 기준 시간을 의미하고, 유효키는 확정된 키 입력을 의미한다. 입력부(120)에서는 동시에 복수의 키 입력을 인식할 수 있기 때문에 사용자가 선택한 키 입력이 다른 횟수의 입력인지, 동일 횟수 내의 복수의 키 입력인지를 구분하는 것이 필요하다. 예를 들어, 입력부(120)에서 입력받은 키 입력이 (5, 3, 2, 1, 9, 8, 4)이고, 인증 정보 저장부(110)에 저장된 인증 정보가 ([5], [3, 2, 1], [9], [8, 4])인 경우에, 사용자는 인증 정보에 포함되는 모두 키 정보를 입력하였으나, 키를 선택하는 시간 차이에 따라 키 입력이 ([5, 3], [2, 1, 9], [8], [4])와 같이 인식되므로 인증에 실패하게 된다.

[0022] 구체적으로, 유효키 판단부(130)는 다음과 같은 방식으로 유효키를 판단할 수 있다. 유효키 판단부(130)는 복수의 키가 동시에 선택된 경우, 복수의 키 중 가장 늦게 선택된 키와 복수의 키 중 가장 먼저 선택 해제된 키 사이의 시간을 미리 설정된 유효 시간과 비교하고, 유효 시간 동안 키 선택이 유지되는 키를 유효키로 판단한다. 예를 들어, 도 3에서 선택된 키의 키 입력시간에 따른 유효키를 다음의 표 1을 통해 설명하도록 한다.

표 1

[0023]

	t1	t2	t3	t4	t5	t6	t7	t8
0	—	—	—	—	—			
5		—	—	—	—	—		
6			—	—	—	—	—	—

[0024] 표 1에서, 세로축(0, 5, 6)은 키를 의미하고, 가로축(t1~t8)은 구간별 시간을 의미하며, '—'은 해당 구간에 해당 키가 선택되고 있음을 의미한다. 이 경우, 키 입력 [0]은 t1~t5 동안 선택되었고, 키 입력 [5]는 t2~t6 동안 선택되었으며, 키 입력 [6]은 t3~t8 동안 선택되었다. 유효키 판단부(130)는 가장 늦게 선택된 키 입력인

[6]부터 가장 먼저 선택이 해제된 키 입력인 [0] 사이의 시간인 't3~t5' 시간을 미리 설정된 유효 시간과 비교한다. 유효 시간이 't3~t5' 시간 보다 같거나 작으면 동 횟수에 입력된 키 입력은 ([0, 5, 6])으로 인정되며, 유효 시간이 't3~t5' 시간 보다 크고, 't2~t5'와 같다면 동 횟수에 입력된 키 입력은 ([0, 5])로 인정된다. 유효키 판단부(130)는 판단된 유효키를 인증 요청 정보 생성부(140)로 출력한다.

[0025] 다음으로, 인증 요청 정보 생성부(140)는 유효키 판단부(130)에서 판단된 유효키의 조합을 이용하여 인증 요청 정보를 생성한다(S220). 인증 요청 정보란 사용자의 키 입력에 따라 인식된 최종 키 입력 정보로, 인증 정보 저장부(110)에 저장된 인증 정보와 비교되는 정보를 말한다. 예를 들어, 유효키 판단부(130)에서 첫 번째 횟수에서는 키 입력 [5], 두 번째 횟수에서는 키 입력 [3, 2, 1], 세 번째 횟수에서는 키 입력 [9], 네 번째 횟수에서는 키 입력 [8, 4]이 유효키로 판단된 경우, 인증 요청 정보 생성부(140)는 ([5], [3, 2, 1], [9], [8, 4])를 하나의 리스트로 조합하여 인증 요청 정보를 생성하게 된다. 인증 요청 정보 생성부(140)는 생성된 인증 요청 정보를 인증 처리부(150)로 출력한다.

[0026] 다음으로, 인증 처리부(150)는 인증 요청 정보 생성부(140)로부터 입력된 인증 요청 정보를 인증 정보 저장부(110)에 저장된 인증 정보와 비교하여 키 입력 사용자에 대한 인증을 처리한다(S230). 인증 처리부(150)는 인증 요청 정보의 키 입력 횟수 및 횟수별 키 입력 개수를 분석하고, 그에 대응하는 키의 조합 데이터를 분석하여 인증 정보와 일치하는지를 판단한다. 예를 들어, 인증 정보는 4회의 키 입력 횟수와, 1회에는 1개의 입력, 2회에는 3개의 입력, 3회에는 2개의 입력, 4회에는 1개의 키 입력 개수가 설정되고, 각 횟수별 키 데이터가 1회에는 [1], 2회에는 [5, 6, 9], 3회에는 [4, 6], 4회에는 [3]으로 설정될 수 있다. 이 경우, 인증 요청 정보가 ([1], [5, 6], [9, 4, 6, 3])과 같이 키 입력 횟수가 일치하지 않거나, ([1], [5, 6], [9, 4, 6], [3])과 같이 횟수별 키 입력 개수가 맞지 않는 경우에는 키 데이터를 비교하지 않고도 인증을 허용하지 않을 수 있다.

[0027] 한편, 본 발명의 인증 처리 장치(100)는 정규화부(160)를 더 포함할 수 있다. 정규화부(160)는 인증 요청 정보 생성부(140), 인증 처리부(150)와 연결되어, 인증 요청 정보 생성부(140)로부터 생성된 인증 요청 정보를 오름차순 또는 내림차순으로 정규화하여 인증 처리부(150)로 출력한다. 입력부(120)에 입력되는 키 입력이 동시에 선택되는 복수의 키 입력인 경우, 동일 횟수에 입력되는 키 데이터의 순서가 경우에 따라 달라질 수 있다. 예를 들어, 인증 정보 중 [5, 7, 8]이 동시에 선택되도록 설정되는 경우, 사용자의 키 선택이 [5, 8, 7] 또는 [8, 7, 5]와 같은 순서로 입력될 수 있다. 비록 사용자가 동시에 누른다고 해도 여러 키를 동시에 누르다 보면 각 키 간에는 선택되는데 시간차가 발생하기 때문이다. 따라서, 정규화부(160)는 해당 횟수에 입력되는 키 입력 데이터를 오름차순 혹은 내림차순으로 정렬하게 된다. 위의 예에서, 사용자가 비록 [8, 7, 5] 순서로 입력을 해도 오름차순으로 정규화를 하면, [5, 7, 8]의 데이터가 입력된 것으로 인식이 된다.

[0028] 한편, 본 발명의 인증 처리 장치(100)는 암호화부(170)를 더 포함할 수 있다. 암호화부(170)는 인증 요청 정보 생성부(140)와 인증 처리부(150)와 연결되며, 인증 요청 정보 생성부(140)에서 생성된 인증 요청 정보를 일방향 함수로 암호화하여 인증 처리부(150)로 전송하게 된다. 이 경우, 인증 처리부(150)는 암호화된 인증 요청 정보를 복호화할 수 있다. 일방향함수(one-way function)는 계산하기는 쉽지만 그 역을 구하는 것이 어려운 함수를 말한다. 다시 말해, 결과값이 주어졌을 때 입력값을 구하는 것이 어려운 함수이다. 공개 키 암호 방식은 극히 일부의 예외를 제외하면 모두 일방향함수가 존재한다.

[0029] 일방함수로는 보통 DES(Data Encryption Standard) 알고리즘을 이용한다. DES는 8바이트의 데이터와 8바이트의 키(key)를 입력하면 8바이트의 암호문을 출력하는 함수로 생각할 수 있다. 일반적으로 암호 알고리즘은 일방함수로도 사용이 가능하며 DES를 일방함수로 사용할 때에는 패스워드를 키로 사용하여 어떤 정해진 상수를 암호화하여 그 결과를 패스워드 파일에 저장한다. 예를 들면 UNIX 시스템에는 패스워드를 비롯하여 시스템이 각 사용자에 대하여 필요한 모든 정보를 포함하고 있는 /etc/passwd 라는 파일이 있다. /etc/passwd 파일에 접근이 가능하지만 파일 내용 중 패스워드에 해당하는 부분은 일방함수인 crypt로 처리되어 있어 읽어도 해독하기가 거의 불가능하다.

[0030] 또한, 암호부는 본 발명의 인증 처리 장치(100)가 네트워크로 연결된 외부의 서버에서 인증 정보를 저장하고, 인증 처리를 하는 경우에는 네트워크로 인증 요청 정보를 전송하는 과정 중 발생할 수 있는 해킹에 대비하기 위한 암호화를 할 수 있다.

[0031] 한편, 본 발명의 인증 처리 장치(100)는 표시부(180)를 더 포함할 수 있다. 표시부(180)는 인증 처리부(150)와 연결되어 인증 처리 결과를 음성 또는 영상으로 표시한다. 예를 들어, 사용자가 입력한 키 입력에 따른 인증 요청 정보가 인증 정보와 일치하지 않는 경우에는 경고음을 발생시키거나, 재입력 안내 음성 멘트를 발생시키거나, 재입력 문자 메시지를 발생시킬 수 있다. 또한, 경고음, 음성 멘트, 문자 메시지를 통합적으로 제공하는 것도 가능하다. 따라서, 사용자는 자신의 키 입력이 성공했는지 여부를 쉽게 판단할 수 있다.

[0032] 한편, 본 발명의 인증 처리 장치(100)는 지문 인식 장치, 홍채 인식 장치, 음성 인식 장치, RF 태그 인식 장치 등과 결합될 수 있다. 예를 들어, 보다 강화된 보안이 요구되는 곳에서는 지문 인식 장치, 홍채 인식 장치, 음성 인식 장치, RF 태그 인식 장치 외에도 추가적으로 본 발명의 인증 처리 장치(100)를 구비함으로써 다중 보안 시스템을 구축할 수 있다.

[0033] 한편, 본 발명의 실시예들은 컴퓨터로 읽을 수 있는 기록 매체에 컴퓨터가 읽을 수 있는 코드로 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록 매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다.

[0034] 컴퓨터가 읽을 수 있는 기록 매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현하는 것을 포함한다. 또한, 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산 방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술 분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

[0035] 이와 같은 본 발명에 따른 인증 처리 장치(100), 인증 처리 방법은 동시에 입력되는 복수의 키 입력을 이용한 비밀번호에 대하여 인증을 처리함으로써, 비밀번호를 해킹하기 위해 시도되는 경우의 수를 증가시켜 비밀번호 해킹으로 인한 피해를 줄일 수 있다.

[0036] 이상에서 본 발명은 도면을 참조하면서 기술되는 바람직한 실시예를 중심으로 설명되었지만 이에 한정되는 것은 아니다. 따라서 본 발명은 기재된 실시예로부터 도출 가능한 자명한 변형예를 포괄하도록 의도된 특허청구범위의 기재에 의해 해석되어져야 한다.

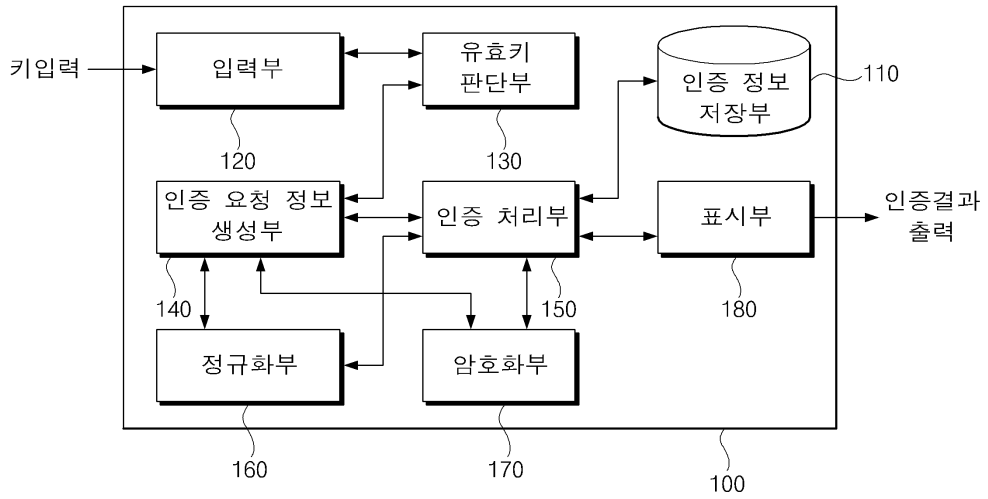
부호의 설명

[0037]

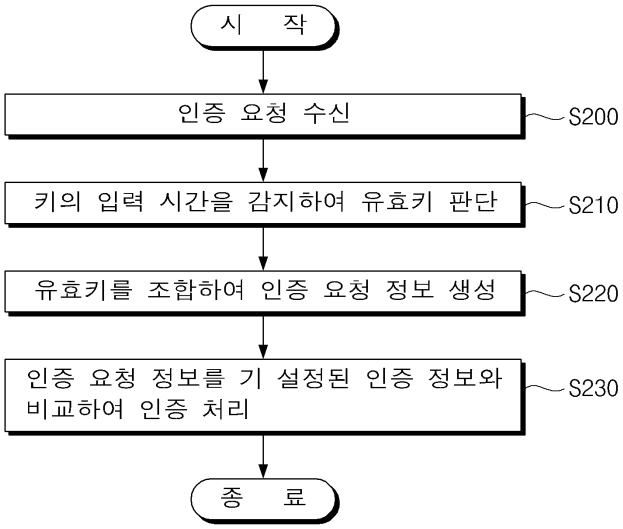
100 : 인증 처리 장치	110 : 인증 정보 저장부
120 : 입력부	130 : 유효키 판단부
140 : 인증 요청 정보 생성부	150 : 인증 처리부
160 : 정규화부	170 : 암호화부
180 : 표시부	

도면

도면1


키입력
입력부
유효키
판단부
인증 정보
저장부
110
120
130
인증 요청 정보
생성부
인증 처리부
표시부
인증결과
출력
140
150
180
정규화부
암호화부
160
170
100

도면2


시 작
인증 요청 수신
S200
키의 입력 시간을 감지하여 유효키 판단
S210
유효키를 조합하여 인증 요청 정보 생성
S220
인증 요청 정보를 기 설정된 인증 정보와
비교하여 인증 처리
S230
종 료

도면3

