(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2022년01월06일
(11) 등록번호 10-2348769
(24) 등록일자 2022년01월04일

(51) 국제특허분류(Int. Cl.)
G06F 21/31 (2013.01) *G06F 21/60* (2013.01)
G06F 3/0488 (2013.01)
(52) CPC특허분류
G06F 21/31 (2013.01)
G06F 21/602 (2013.01)
(21) 출원번호 10-2017-7037744
(22) 출원일자(국제) 2016년04월28일
심사청구일자 2020년06월03일
(85) 번역문제출일자 2017년12월28일
(65) 공개번호 10-2018-0014774
(43) 공개일자 2018년02월09일
(86) 국제출원번호 PCT/CN2016/080440
(87) 국제공개번호 WO 2016/188297
국제공개일자 2016년12월01일
(30) 우선권주장
201510282846.3 2015년05월28일 중국(CN)
(56) 선행기술조사문헌
JP2010079562 A*
(뒷면에 계속)
전체 청구항 수 : 총 7 항

(73) 특허권자
어드밴스드 뉴 테크놀로지스 씨오., 엘티디.
케이만 군도, 그랜드 케이만 케이와이1-9008, 조지 타운, 27 하스피탈 로드, 케이만 코포레이트 센터
(72) 발명자
허 용
중국 항저우 310099 완탕 로드 넘버 18 후앙롱 타임즈 플라자 빌딩 비 17층 앤츠 페이턴트 팀 내
(74) 대리인
김태홍, 김진희

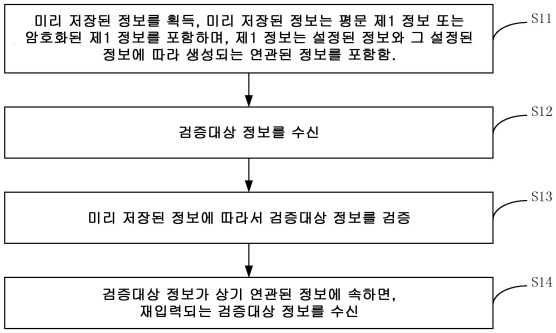
심사관 : 윤혜숙

(54) 발명의 명칭 **정보 입력 방법 및 장치**

(57) 요 약

본 출원은 정보 입력 방법 및 장치를 제공한다. 상기 정보 입력 방법은, 미리 저장된 정보를 획득하는 단계로서, 상기 미리 저장된 정보는 평문 제1 정보 또는 암호화된 제1 정보를 포함하며, 상기 제1 정보는 설정된 정보 및 상기 설정된 정보에 따라서 생성되는 연관된 정보를 포함하는 것인, 상기 미리 저장된 정보를 획득하는 단계; 검증 대상 정보를 수신하는 단계; 상기 미리 저장된 정보에 따라 상기 검증 대상 정보를 검증하는 단계; 및 상기 검증 대상 정보가 상기 연관된 정보에 속하면, 검증을 다시 수행하는 단계를 포함한다. 이 방법은 의도하지 않은 오류를 악의적인 오류로부터 효과적으로 구별할 수 있으므로, 의도하지 않은 입력 오류에 의해 야기된 정보 검증 실패를 감소시킬 수 있다.

대 표 도



(52) CPC특허분류
G06F 3/04886 (2013.01)

(56) 선행기술조사문헌
JP2005149388 A*
KR1020140007470 A*
JP2014137423 A*
KR1020120134484 A
*는 심사관에 의하여 인용된 문헌

명 세 서

청구범위

청구항 1

정보 입력 장치(50)에 의해 수행되는 정보 입력 방법에 있어서,

미리 저장된 정보를 획득하는 단계 - 상기 미리 저장된 정보는 평문(plaintext) 제1 정보 또는 암호화된 제1 정보를 포함하며, 상기 제1 정보는 설정된 정보 및 상기 설정된 정보에 따라서 생성된 연관된 정보를 포함하며(S11), 상기 연관된 정보를 생성하는 것(S10)은,

상기 설정된 정보로부터 정보 항목을 랜덤하게 선택하는 것,

상기 선택된 정보 항목에 대응하는 새로운 정보 항목을 획득하는 것 - 키보드 상의 상기 새로운 정보 항목과 상기 선택된 정보 항목의 위치들 사이의 거리는 미리 설정된 범위 내에 있음 -,

상기 연관된 정보를 획득하기 위하여 상기 설정된 정보 내의 상기 선택된 정보 항목을 상기 새로운 정보 항목으로 대체하는 것을 포함함 -;

검증 대상(to-be-verified) 정보를 수신하는 단계(S12);

상기 미리 저장된 정보에 따라 상기 검증 대상 정보를 검증하는 단계(S13)

를 포함하되,

그 후, 상기 검증 대상 정보가 상기 연관된 정보에 속하면(S14):

재입력되는 검증 대상 정보를 수신하고, 상기 재입력되는 검증 대상 정보를 수신한 후에 재입력되는 검증 대상 정보의 평문 표시 시간을 연장시키고(S141), 연장된 재입력되는 검증 대상 정보의 평문 표시 시간 후 비평문(non-plain text) 정보를 이용하여 상기 재입력되는 검증 대상 정보를 마스킹하는 것;

그 이외에는:

상기 검증 대상 정보가 상기 설정된 정보와 동일하면, 상기 검증이 성공하였다고 결정하는 것(S15); 그 이외에는

상기 검증 대상 정보가 상기 설정된 정보와 상이하고 상기 연관된 정보에 속하지 않으면, 상기 검증이 실패하였다고 결정하는 것(S16)

을 포함하는 정보 입력 방법.

청구항 2

제1항에 있어서, 재입력되는 검증 대상 정보를 검증하는 단계(S142)를 더 포함하는 정보 입력 방법.

청구항 3

제1항에 있어서, 상기 미리 저장된 정보가 상기 암호화된 제1 정보일 때, 상기 미리 저장된 정보에 따라 상기 검증 대상 정보를 검증하는 단계는,

상기 제1 정보의 암호화 알고리즘과 동일한 암호화 알고리즘을 이용하여 상기 검증 대상 정보를 암호화하여 암호화된 검증 대상 정보를 획득하는 단계; 및

상기 암호화된 검증 대상 정보를 상기 미리 저장된 정보와 비교하는 단계를 포함하는 것인 정보 입력 방법.

청구항 4

제3항에 있어서, 상기 암호화 알고리즘은 해시 알고리즘인 것인 정보 입력 방법.

청구항 5

정보 입력 장치(50)에 있어서,

미리 저장된 정보를 획득하도록 구성된 획득 모듈(51) - 상기 미리 저장된 정보는 평문 제1 정보 또는 암호화된 제1 정보를 포함하며, 상기 제1 정보는 설정된 정보 및 상기 설정된 정보에 따라서 생성된 연관된 정보를 포함하고, 상기 연관된 정보를 생성하는 것은,

설정 모듈(55)에 의해, 상기 설정된 정보로부터 정보 항목을 랜덤하게 선택하는 것,

상기 설정 모듈(55)에 의해, 상기 선택된 정보 항목에 대응하는 새로운 정보 항목을 획득하는 것 - 키보드 상의 상기 새로운 정보 항목과 상기 선택된 정보 항목의 위치들 사이의 거리는 미리 설정된 범위 내에 있음 -,

상기 설정 모듈(55)에 의해, 상기 연관된 정보를 획득하기 위하여 상기 설정된 정보 내의 상기 선택된 정보 항목을 상기 새로운 정보 항목으로 대체하는 것을 포함함 -;

검증 대상 정보를 수신하도록 구성된 제1 수신 모듈(52);

상기 미리 저장된 정보에 따라 상기 검증 대상 정보를 검증하도록 구성된 검증 모듈(53);

(i) 상기 검증 대상 정보가 상기 설정된 정보와 동일하면, 상기 검증이 성공하였다고 결정하고, (ii) 상기 검증 대상 정보가 상기 설정된 정보와 상이하고 상기 연관된 정보에 속하지 않으면, 상기 검증이 실패하였다고 결정하도록 구성된 판정 모듈(56); 및

상기 검증 대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증 대상 정보를 수신하고, 재입력되는 검증 대상 정보가 수신된 후에 재입력되는 검증 대상 정보의 평문 표시 시간을 연장시키고, 연장된 재입력되는 검증 대상 정보의 평문 표시 시간 후 비평문 정보를 이용하여 상기 재입력되는 검증 대상 정보를 마스킹하도록 구성된 제2 수신 모듈(54)

을 포함하는 정보 입력 장치.

청구항 6

제5항에 있어서, 상기 제2 수신 모듈(54)은 또한, 재입력되는 검증 대상 정보를 검증하도록 구성되는 것인 정보 입력 장치.

청구항 7

제5항에 있어서, 상기 미리 저장된 정보가 상기 암호화된 제1 정보일 때, 상기 검증 모듈은 구체적으로,

상기 제1 정보의 암호화 알고리즘과 동일한 암호화 알고리즘을 이용하여 상기 검증 대상 정보를 암호화하여 암호화된 검증 대상 정보를 획득하고,

상기 암호화된 검증 대상 정보를 상기 미리 저장된 정보와 비교하도록 구성되는 것인 정보 입력 장치.

청구항 8

삭제

청구항 9

삭제

청구항 10

삭제

청구항 11

삭제

발명의 설명

기 술 분 야

[0001] 본 출원은 데이터 처리 기술 분야에 관한 것으로서, 특히 정보 입력 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 이동 통신 기술의 발달로, 사용자는 종종 모바일 디바이스에 정보를 입력해야 한다. 특히 휴대 전화에 정보가 입력되는 경우, 휴대 전화의 제한된 크기로 인하여 물리적 키보드 또는 가상 키보드의 크기가 상대적으로 작아, 사용자가 정보를 잘못 입력하기 쉽다. 예를 들어, 사용자는 문자 a를 입력하려고 하지만, 실제로는 문자 a에 인접한 문자, 예를 들어 s를 입력하게 된다.

발명의 내용

해결하려는 과제

과제의 해결 수단

[0003] 본 출원은 관련된 기술 분야의 기술적 문제점들 중 하나를 적어도 어느 정도 해결하는 것을 목적으로 한다.

[0004] 따라서, 본 출원의 하나의 목적은 소형 키보드에 의해 야기된 입력 오류를 줄이고 입력 효과를 향상시킬 수 있는 정보 입력 방법을 제안하는 것이다.

[0005] 본 출원의 다른 목적은 정보 입력 장치를 제안하는 것이다.

[0006] 상기 목적을 달성하기 위해, 본 출원의 제1 양태에 따른 실시형태에 의해 제안된 정보 입력 방법은, 미리 저장된 정보를 획득하는 단계 - 상기 미리 저장된 정보는 평문(plaintext) 제1 정보 또는 암호화된 제1 정보를 포함하며, 상기 제1 정보는 설정된 정보 및 상기 설정된 정보에 따라서 생성되는 연관된 정보를 포함함 - ; 검증 대상(to-be-verified) 정보를 수신하는 단계; 상기 미리 저장된 정보에 따라 상기 검증 대상 정보를 검증하는 단계; 및 상기 검증 대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증 대상 정보를 수신하는 단계를 포함한다.

[0007] 본 출원의 제1 양태에 따른 실시형태에 의해 제안되는 정보 입력 방법은, 설정된 정보를 생성할 수 있을 뿐만 아니라, 상기 설정된 정보에 따라 획득되는 연관된 정보를 생성할 수 있고, 검증 대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증 대상 정보를 수신할 수 있다. 따라서, 따라서 소형 키보드 또는 기타 이유에 의해 입력 오류가 야기된 후에 사용자가 검증을 위한 다른 기회를 가질 수 있으므로, 소형 키보드에 의해 야기된 입력 오류를 줄이고 입력 효과를 향상시킬 수 있다.

[0008] 상기 목적을 달성하기 위해, 본 출원의 제2 양태에 따른 실시형태에 의해 제안되는 정보 입력 장치는, 미리 저장된 정보를 획득하도록 구성된 획득 모듈 - 상기 미리 저장된 정보는 평문 제1 정보 또는 암호화된 제1 정보를 포함하며, 상기 제1 정보는 설정된 정보 및 상기 설정된 정보에 따라서 생성된 연관된 정보를 포함함 -; 검증 대상 정보를 수신하도록 구성된 제1 수신 모듈; 상기 미리 저장된 정보에 따라 상기 검증 대상 정보를 검증하도록 구성된 검증 모듈; 및 상기 검증 대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증 대상 정보를 수신하도록 구성된 제2 수신 모듈을 포함한다.

[0009] 본 출원의 제2 양태에 따른 실시형태에 의해 제안된 정보 입력 장치는, 설정된 정보를 생성할 뿐만 아니라, 상기 설정된 정보에 따라 획득되는 연관된 정보를 생성할 수 있고, 검증 대상 정보가 상기 연관된 정보에 속할 때, 재입력되는 검증 대상 정보를 수신할 수 있다. 따라서, 소형 키보드 또는 기타 이유에 의해 입력 오류가 야기된 후에 사용자가 검증을 위한 다른 기회를 가질 수도 있으므로, 소형 키보드에 의해 야기된 입력 오류를 줄이고 입력 효과를 향상시킬 수 있다.

[0010] 본 출원의 부가적인 양태 및 이점은 부분적으로 이하의 설명에 제공되고, 부분적으로 이하의 설명으로부터 명백해 질 것이며, 또는 본 출원의 실시를 통해 공지될 것이다.

도면의 간단한 설명

[0011] 본 출원의 상기 및/또는 부가적인 양태 및 이점은, 첨부된 도면을 참조하여 실시형태들의 설명으로부터 명백하

게 되고 쉽게 이해될 것이다.

도 1은 본 출원의 실시형태에 따른 정보 입력 방법의 개략적인 흐름도이다.

도 2는 본 출원의 다른 실시형태에 따른 정보 입력 방법의 개략적인 흐름도이다.

도 3은 본 출원의 다른 실시형태에 따른 정보 입력 방법의 개략적인 흐름도이다.

도 4는 본 출원의 다른 실시형태에 따른 정보 입력 방법의 개략적인 흐름도이다.

도 5는 본 출원의 다른 실시형태에 따른 정보 입력 장치의 개략적인 구성도이다.

도 6은 본 출원의 다른 실시형태에 따른 정보 입력 장치의 개략 구성도이다.

발명을 실시하기 위한 구체적인 내용

[0012] 본 출원의 실시형태는 이하에서 상세하게 설명될 것이며, 실시형태들의 예는 첨부 도면들에 도시되며, 첨부 도면들에서는 동일 또는 유사한 참조 부호가, 동일 또는 유사한 모듈들 또는 텍스트 전반에 걸쳐 동일 또는 유사한 기능을 가지는 모듈들을 나타낸다. 첨부 도면들을 참조하여 이하에 설명된 실시형태들은 예시적이며 본 출원을 단지 설명하기 위한 것이며, 본 출원을 제한하는 것으로 구성되지는 않는다. 이와 반대로, 본 발명의 실시형태는 첨부된 청구 범위의 사상 및 함축의 범위 내에 포함되는 모든 변경, 수정, 및 등가물을 포함한다.

[0013] 도 1은 본 출원의 실시형태에 따른 정보 입력 방법의 개략적인 흐름도이며, 이 방법은, 이하의 것을 포함한다.

[0014] S11. 미리 저장된 정보가 획득되며, 상기 미리 저장된 정보는 평문 제1 정보 또는 암호화된 제1 정보를 포함하며, 상기 제1 정보는 설정된 정보 및 상기 설정된 정보에 따라서 생성되는 연관된 정보를 포함한다.

[0015] 이 실시형태의 방법은 예를 들어 패스워드 검증(password verification), ID 카드 번호 검증, 은행 카드 번호 검증, 휴대 전화 번호 검증 등에 대한 다양한 시나리오에서 정보 검증을 위해 사용될 수도 있다. 이 실시형태에서, 패스워드 검증이 일례로서 취해진다.

[0016] 패스워드 검증 전에, 사용자가 패스워드를 미리 설정할 수 있다. 예를 들어, 패스워드는 x로 설정된다. 사용자에 의해 설정된 패스워드 x는 하나 이상의 정보 항목을 포함할 수도 있고, 각 정보 항목은 숫자, 문자 등일 수 있음을 이해할 수 있다.

[0017] 또한, 예로서 휴대 전화 단말에 패스워드가 저장되어있는 것을 감안하면, 패스워드는 휴대 전화 단말기에 평문으로 저장될 수도 있고, 예를 들어, x로 직접 저장될 수도 있다. 또는, 보안을 강화하기 위해, 평문 패스워드는 저장되기 전에 암호화되며, 예를 들어, 암호화된 x가 휴대 전화 단말기에 저장된다. 예를 들어, 특히 해시(Hash) 알고리즘인 다양한 암호화 알고리즘이 있다는 것을 이해할 수 있다. 이 실시형태에서, 휴대 전화 단말기에 저장된 해시 암호화된 패스워드가 일례로서 취해진다. 해시 암호화가 수행된 후, x가 H(x)로 표현된다고 가정한다.

[0018] 종래 기술에서, 미리 저장된 정보는 많아야 H(x)이고, 사용자가 입력한 것이 x가 아닌 경우 검증은 실패할 것이다.

[0019] 본 실시형태에서는, H(x)이 기억될 뿐만 아니라, x에 따라서 연관된 정보가 획득될 수 있고, 그 연관된 정보에 대하여 해시 암호화가 수행된 후에 획득된 정보는 휴대 전화 단말기에 추가로 저장된다.

[0020] 구체적으로는, 도 2를 참조하면, 본 실시형태의 방법은, 이하의 내용을 더 포함할 수도 있다.

[0021] S10. 연관된 정보는 설정된 정보에 따라 생성된다.

[0022] 선택적으로, 상기 설정된 정보에 따라 연관된 정보를 생성하는 단계는,

[0023] 상기 설정된 정보로부터 정보 항목을 랜덤하게 선택하고, 그 선택된 정보 항목에 대응하는 새로운 정보 항목을 획득하는 단계 - 키보드 상의 상기 새로운 정보 항목과 상기 선택된 정보 항목의 위치들 사이의 거리는 미리 설정된 범위 내에 있음 -; 및

[0024] 상기 설정된 정보 내의 상기 선택된 정보 항목을 상기 새로운 정보 항목으로 대체하여 상기 연관된 정보를 획득하는 단계를 포함한다.

[0025] 예를 들어, 사용자에 의해 설정된 패스워드 x의 하나의 항목이 a이면, 그 후, 가상 키보드 또는 물리적 키보드에서 a에 대하여 작은 거리에 있는 문자가 a에 대응하는 새로운 문자로서 선택된다. 새로운 문자가 a' 로 표시

된다고 가정하면, a'는 새로운 패스워드 x'을 작성하기 위하여 a를 배치하는데 사용된다. 새로운 패스워드 x'는 x의 연관된 정보이다. 해시 암호화가 수행된 후, 암호화된 연관된 정보는 H(x'), H(x"), ... 로 표현될 수도 있으며, 이 시퀀스는 H'로 기록된다. 구체적으로, 예를 들어, x가 abcd이고, a에 대하여 작은 거리에 있는 문자가 a'를 포함한다고 가정하면, x의 연관된 정보는 a'bcd를 포함한다. 또한, a에 대하여 작은 거리에 있는 문자가 a"를 더 포함한다고 가정하면, x의 연관된 정보는 a"bcd를 더 포함한다. 또한, b에 대하여 작은 거리에 있는 문자가 b'를 포함한다고 가정하면, x의 연관된 정보는 ab'cd를 더 포함하고, 나머지는 동일한 방식으로 수행되어 모든 연관된 정보가 획득될 수 있다.

[0026] 위의 작은 거리의 구체적인 의미는 실제 요구에 따라 설정될 수도 있음을 이해할 수있다. 예를 들어, 인접하는 4개의 키에 대응하는 문자가 작은 거리의 문자로서 결정될 수도 있거나, 2개 이하의 키의 거리에 있는 문자가 모두 작은 거리의 문자로서 결정될 수 있으며 기타의 것들이 존재한다.

[0027] S12. 검증 대상(To-be-verified) 정보가 수신된다.

[0028] 사용자는 키보드를 통해 검증 대상 정보를 입력할 수도 있다.

[0029] 예를 들어, 사용자는 휴대 전화의 가상 키보드를 이용하여 패스워드 등을 입력한다.

[0030] S13. 검증 대상 정보는 미리 저장된 정보에 따라 검증된다.

[0031] 휴대 전화 단말기가 평문 패스워드를 직접 저장할 때, 입력 정보는 미리 저장된 정보와 직접 비교될 수도 있고, 이들이 동일할 때, 검증이 성공하며; 그렇지 않으면, 검증이 실패한다.

[0032] 본 실시형태는 암호화된 제1 정보를 일례로서 저장하는 것을 취한다.

[0033] 상기 미리 저장된 정보가 암호화된 제1 정보일 때, 상기 미리 저장된 정보에 따라 상기 검증 대상 정보를 검증하는 단계는,

[0034] 상기 제1 정보의 암호화 알고리즘과 동일한 암호화 알고리즘을 이용하여 상기 검증 대상 정보를 암호화하여 암호화된 검증 대상 정보를 획득하는 단계와,

[0035] 상기 암호화된 검증 대상 정보를 상기 미리 저장된 정보와 비교하는 단계를 포함한다.

[0036] 사용자에 의해 입력된 검증 대상 정보가 y이고 해시 암호화 알고리즘이 채용된다고 가정하면, 먼저 H(y)이 계산될 수도 있고, 그 후 H(y)는 H(x) 및 H'와 비교된다.

[0037] S14. 상기 검증 대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증 대상 정보가 수신된다.

[0038] 예를 들어, H(y)가 H'에 속하면, 재입력되는 검증 대상 정보가 수신될 수도 있다. 그 후, 검증이 다시 수행될 수도 있다.

[0039] 도 3을 참조하면, 본 실시형태에서, 검증 대상 정보가 상기 연관된 정보에 속할 때, 이하의 단계들이 구체적으로 수행될 수 있다.

[0040] S141. 재입력된 검증 대상 정보가 수신되고, 가이딩(guiding)이 수행되거나 명백한 프롬프트가 제공된다.

[0041] 특히, 가이딩을 수행하거나 확실한 프롬프트를 제공하는 단계는, 이하의 것을 포함할 수도 있다.

[0042] 재입력되는 검증 대상 정보가 수신되기 전에 사용자에게 프롬프트 정보를 표시하는 단계 - 상기 프롬프트 정보는 상기 사용자에게 키보드 키에 주목하도록 촉구하기 위해 사용됨 - ; 또는

[0043] 재입력되는 검증 대상 정보가 수신된 후에, 재입력되는 검증 대상 정보의 평문 표시 시간을 연장시키는 단계; 또는

[0044] 재입력되는 검증 대상 정보가 수신된 후에, 평문으로 재입력되는 검증 대상 정보를 직접 표시하는 단계.

[0045] 예를 들어, 사용자가 연관된 정보에 속하는 y를 입력할 때, 키의 작은 크기로 인하여 사용자의 의도하지 않은 입력 오류가 발생할 가능성이 크다. 이 때, 사용자는 키보드에 주목하여 상기시켜질 수도 있어 키보드의 작은 크기로 인한 입력 오류를 피할 수 있습니다. 또는,

[0046] 기호 *와 같은 비평문 정보는, 일반적으로 패스워드 검증 중에 최종적으로 표시되며, 기호 *가 표시되기 전에 사용자에 의해 입력된 평문 정보가 잠깐 동안 표시될 수도 있다.

[0047] 이 실시형태에서, 평문 표시 시간이 연장될 때, 검증 대상 정보의 각 정보 항목의 평문 표시 시간이 연장될 수

도 있거나, 전회에 잘못 입력된 정보 항목의 평문 표시 시간만이 연장된다. 예를 들면, 검증 대상 정보가 abcd이고, 최초 검출 중에 a에 오류가 발생하면, a의 평문 표시 시간만 연장될 수도 있거나, a, b, c, 및 d의 평문 표시 시간이 모두 연장될 수도 있다. 또한, 평문으로 표시하는 동안, 유사한 실행이 또한 수행될 수 있다. 예를 들어, 전회에 잘못 입력된 정보 항목만이 평문으로 표시되거나, 모든 정보 항목이 평문으로 표시된다.

[0048] 그 후, 이하의 단계들이 더 수행될 수도 있다.

[0049] S142. 검증이 다시 수행된다.

[0050] 예를 들어, 사용자는 프롬프트 정보 또는 평문으로 표시된 정보에 따라 재입력되는 검증 대상 정보를 확인할 수도 있다. 사용자에 의해 재입력된 검증 대상 정보가 휴대 전화 단말기에서 수신된 후에, 그 정보는 미리 저장된 정보와 비교되어, 검증 결과를 획득할 수도 있다.

[0051] 이 실시형태에서, 평문 입력 정보를 표시하는 시간이 연장될 수도 있어, 사용자는 자신이 입력한 정보를 더 잘 볼 수 있어서, 정보가 정확하게 입력되었는지 여부를 검증할 수 있다. 특정 연장 시간이 설정될 수도 있다. 또는, 입력 정보가 평문으로 직접 표시되어, 사용자가 쉽게 확인할 수 있다.

[0052] 다른 양태에서, 도 4를 참조하면, 사용자가 입력된 검증 대상 정보를 검증한 후에, 상기 방법은 이하의 것을 더 포함할 수도 있다.

[0053] S15. 검증 대상 정보가 상기 설정된 정보와 동일하면, 검증이 성공한 것으로 판정된다.

[0054] 예를 들어, 해시 암호화 후에 획득된 값이 저장되고, 사용자에 의해 입력된 검증 대상 정보가 y이면, y는 H(y)를 얻기 위해 해싱되고, H(y)가 H(x)와 동일하면, 검증이 성공한다.

[0055] S16. 검증 대상 정보가 상기 설정된 정보와 상이하고 연관된 정보에 속하지 않으면, 검증이 실패한 것으로 판정된다.

[0056] 예를 들어, H(y)가 H(x)와 다르며, H(y)가 H' 에 속하지 않으면, 검증이 실패한 것으로 판단된다. 이때, 패스워드가 잘못 입력되었음을 나타내는 정보가 사용자에게 표시된다.

[0057] 이 실시형태에서, 설정된 정보뿐만 아니라 설정된 정보에 따라 획득되는 연관된 정보가 생성될 수도 있고, 검증 대상 정보가 상기 연관된 정보에 속할 때, 검증이 다시 수행된다. 사용자의 입력 오류가 소형의 키보드 또는 기타 이유에 의해 야기된 후에 검증을 위한 다른 기회가 제공될 수 있어, 소형의 키보드에 의해 야기된 입력 오류를 줄이고, 입력 효과를 향상시킬 수 있다. 이는 악의적인 입력 오류로 인한 직접 검증 실패와는 달리, 의도하지 않은 오류를 악의적인 오류로부터 효과적으로 구별하고, 의도하지 않은 입력 오류에 의해 야기된 정보 확인 실패를 줄일 수 있다.

[0058] 도 5는 본 출원의 다른 실시형태에 따른 정보 입력 장치의 개략적인 구성도이다. 장치(50)는 획득 모듈(51), 제1 수신 모듈(52), 검증 모듈(53), 및 제2 수신 모듈 (54)을 포함한다.

[0059] 획득 모듈(51)은 미리 저장된 정보를 획득하도록 구성되며, 상기 미리 저장된 정보는 평문 제1 정보 또는 암호화된 제1 정보를 포함하며, 상기 제1 정보는 설정된 정보 및 상기 설정된 정보에 따라 생성되는 연관된 정보를 포함한다.

[0060] 본 실시형태의 방법은 예를 들어 패스워드 검증, ID 카드 번호 검증, 은행 카드 번호 검증, 휴대 전화 번호 검증 등에 대한 다양한 시나리오에서 정보 검증을 위해 사용될 수도 있다. 이 실시형태에서, 패스워드 검증이 예로서 취해진다.

[0061] 패스워드 확인 전에, 사용자는 패스워드를 미리 설정할 수도 있다. 예를 들어, 패스워드는 x로 설정된다. 사용자에 의해 설정된 패스워드 x가 하나 이상의 정보 항목을 포함할 수도 있고, 각 정보 항목은 숫자, 문자 등일 수도 있음을 이해할 수 있다.

[0062] 또한, 예로서 휴대 전화 단말기에 패스워드가 저장되어 있는 것을 감안하면, 패스워드는 휴대 전화 단말기에 평문으로 저장될 수도 있는데, 예를 들어, x로 직접 저장된다. 또는, 보안을 강화하기 위해, 평문 패스워드가 저장되기 전에 암호화되며, 예를 들어 암호화 된 x가 휴대 전화 단말기에 저장된다. 예를 들어, 특히 해시 알고리즘인 다양한 암호화 알고리즘이 있다는 것을 이해할 수 있다. 본 실시형태에서, 휴대 전화 단말기에 저장된 해시 암호화된 패스워드가 일례로서 취해진다. 해시 암호화가 수행된 후에 x가 H(x)로 표현된다고 가정한다.

[0063] 종래 기술에서, 미리 저장된 정보는 많아야 H(x)이고, 사용자가 입력한 것이 x가 아닌 경우에 검증은 실패할 것

이다.

[0064] 본 실시형태에서는, H(x)가 저장될 뿐만 아니라, 연관된 정보가 x에 따라 획득될 수 있고, 해시 암호화가 수행된 후에 상기 연관된 정보에 대하여 획득된 정보가 휴대 전화 단말기에 추가로 저장된다.

[0065] 도 6을 참조하면, 장치(50)는 이하의 것을 더 포함한다.

[0066] 설정 모듈(55)로서, 설정된 정보로부터 정보 항목을 랜덤하게 선택하고, 상기 선택된 정보 항목에 대응하는 새로운 정보 항목을 획득하도록 구성되며, 여기서 키보드 상의 새로운 정보 항목과 선택된 정보 항목의 위치들 사이의 거리는 미리 설정된 범위 내에 있으며, 상기 설정된 정보 내의 상기 선택된 정보 항목을 상기 새로운 정보 항목으로 대체하여 연관된 정보를 획득한다.

[0067] 예를 들어, 사용자에 의해 설정된 패스워드 x의 하나의 항목이 a이고, 가상 키보드 또는 물리적 키보드에서 a에 대하여 작은 거리에 있는 문자가 a에 대응하는 새로운 문자로서 선택된다. 새로운 문자가 a’로 표시된다고 가정하면, a’는 새로운 패스워드 x’을 작성하기 위하여 a를 배치하는데 사용된다. 새로운 패스워드 x’는 x의 연관된 정보이다. 해시 암호화가 수행된 후에, 암호화되는 연관된 정보는 H(x’), H(x”), ...로 표현될 수도 있으며, 이 시퀀스는 H’로 기록된다. 구체적으로, 예를 들어, x가 abcd이고, a에 대하여 작은 거리에 있는 문자가 a’를 포함한다고 가정하면, x의 연관된 정보는 a’bcd를 포함한다. 또한, a에 대하여 작은 거리에 있는 문자가 a”를 더 포함한다고 가정하면, x의 연관된 정보는 a”bcd를 더 포함한다. 또한, b에 대하여 작은 거리에 있는 문자가 b’를 포함한다고 가정하면, x의 연관된 정보는 ab’cd를 더 포함하고, 나머지는 동일한 방식으로 행해져서, 모든 연관된 정보가 획득될 수 있다.

[0068] 위의 작은 거리의 구체적인 의미는 실제 요구에 따라 설정될 수도 있음을 이해할 수 있다. 예를 들어, 인접하는 4개의 키에 대응하는 문자가 작은 거리의 문자로서 결정되거나, 2개의 키 이하의 거리의 문자가 모두 작은 거리의 문자로서 결정될 수 있으며, 기타의 것들이 존재한다.

[0069] 제1 수신 모듈(52)은 검증 대상 정보를 수신하도록 구성되고;

[0070] 여기서 상기 사용자는 키보드를 통해 상기 검증 대상 정보를 입력할 수도 있다.

[0071] 예를 들어, 사용자는 휴대 전화의 가상 키보드를 이용하여 패스워드 등을 입력한다.

[0072] 검증 모듈(53)은 미리 저장된 정보에 따라 검증 대상 정보를 검증하도록 구성되고;

[0073] 휴대 전화 단말기가 평문 패스워드를 직접 저장하는 경우, 입력 정보는 미리 저장된 정보와 직접 비교될 수도 있고, 이들이 동일할 때, 검증이 성공하며; 그렇지 않으면, 검증이 실패한다.

[0074] 이 실시형태는 암호화된 제1 정보를 일례로서 저장하는 것을 취한다.

[0075] 미리 저장된 정보가 암호화된 제1 정보일 때, 검증 모듈(53)은 구체적으로,

[0076] 상기 제1 정보의 암호화 알고리즘과 동일한 암호화 알고리즘을 이용하여 검증 대상 정보를 암호화하여 암호화된 검증 대상 정보를 획득하고,

[0077] 상기 암호화된 검증 대상 정보와 상기 미리 저장된 정보를 비교하도록 구성된다.

[0078] 사용자에 의해 입력된 검증 대상 정보가 y이고, 해시 암호화 알고리즘이 채용된다고 가정하면, 먼저 H(y)이 계산될 수도 있고, 그 후, H(y)는 H(x) 및 H’와 비교된다.

[0079] 제2 수신 모듈(54)은 검증 대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증 대상 정보를 수신하도록 구성된다.

[0080] 예를 들어, H(y)가 H’에 속하면, 재입력되는 검증 대상 정보가 수신될 수도 있다. 그 후, 검증이 다시 수행될 수도 있다.

[0081] 선택적으로, 상기 제2 수신 모듈은 또한,

[0082] 재입력되는 검증 대상 정보가 수신되기 전에, 사용자에게 프롬프트 정보를 표시하고 - 상기 프롬프트 정보는 사용자에게 키보드 키들에 주목하도록 촉구하는데 사용됨 -, 또는

[0083] 재입력되는 검증 대상 정보가 수신된 후에, 재입력되는 검증 대상 정보의 평문 표시 시간을 연장시키고, 또는

[0084] 재입력되는 검증 대상 정보가 수신된 후에, 평문으로 재입력되는 검증 대상 정보를 직접 표시하도록 구성된다.

[0085] 예를 들어, 사용자가 연관된 정보에 속하는 y를 입력할 때, 키의 작은 크기로 인해 사용자의 의도하지 않은 입력 오류가 발생할 가능성이 크다. 이 때, 사용자는 키보드에 주목하여 상기시켜질 수도 있어, 키보드의 작은 크기로 인한 입력 오류를 피할 수 있다. 또는,

[0086] 기호 *와 같은 비평문 정보는, 일반적으로 패스워드 검증 중에 최종적으로 표시되며, 기호 *가 표시되기 전에 사용자가 입력한 평문 정보가 잠깐 동안 표시될 수도 있다.

[0087] 이 실시형태에서, 평문 표시 시간이 연장될 때, 검증 eotkde 정보의 각 정보 항목의 평문 표시 시간이 연장될 수도 있거나, 전회에 잘못 입력된 정보 항목의 평문 표시 시간만이 연장될 수도 있다. 예를 들어, 검증 대상 정보가 abcd이고, 최초 검출 동안에 a에 오류가 발생하면, a의 평문 표시 시간만이 연장되거나, a, b, c 및 d의 평문 표시 시간이 모두 연장될 수도 있다. 또한, 평문으로 표시하는 동안에 유사한 실행이 또한 수행될 수도 있다. 예를 들어, 전회에 잘못 입력된 정보 항목만이 평문으로 표시되거나, 모든 정보 항목이 일평문으로 표시된다.

[0088] 이 실시형태에서, 평문 입력 정보를 디스플레이하기 위한 시간이 연장될 수도 있어, 사용자는 자신이 입력한 정보를 더 잘 보아, 그 입력이 정확한지 여부를 검증할 수도 있다. 특정 연장 시간이 설정될 수도 있다. 또는, 입력 정보가?평문으로 직접 표시되어, 사용자가 용이하게 확인할 수 있다.

[0089] 도 6을 참조하면, 장치(50)는,

[0090] 검증 대상 정보가 설정된 정보와 동일하면, 상기 검증이 성공한 것으로 판정하거나 또는

[0091] 상기 검증 대상 정보가 상기 설정된 정보와 상이하고 상기 연관된 정보에 속하지 않으면, 상기 검증이 실패한 것으로 판정하도록 구성된 판정 모듈(56)을 더 포함한다.

[0092] 예를 들어, 해시 암호화 후에 획득된 값이 저장되고, 사용자에 의해 입력된 검증 대상 정보가 y이면, y는 H(y)를 획득하기 위하여 해싱되고, H(y)가 H(x)와 동일하면, 검증이 성공한다.

[0093] 예를 들어, H(y)가 H(x)와 다르고, H(y)가 H’에 속하지 않으면, 검증이 실패한 것으로 판정된다. 이때, 패스워드가 잘못 입력되었음을 나타내는 정보가, 사용자에게 표시된다.

[0094] 본 실시형태에서, 설정된 정보뿐만 아니라 상기 설정된 정보에 따라 획득되는 연관된 정보가 생성될 수도 있고, 검증 대상 정보가 연관된 정보에 속할 때, 검증이 다시 수행된다.

[0095] 소형 키보드 또는 기타 이유에 의해 사용자의 입력 오류가 야기된 후에 검증을 위한 다른 기회가 제공될 수 있어, 소형 키보드에 의해 야기된 입력 오류를 줄이고 입력 효과를 향상시킬 수 있다. 이는 악의적인 입력 오류로 인한 직접 검증 실패와는 달리, 의도하지 않은 오류를 악의적인 오류로부터 효과적으로 구별하고, 의도하지 않은 입력 오류에 의해 야기된 정보 검증 실패를 줄일 수 있다.

[0096] 본 출원의 설명에서, “제1” 및 “제2”는 단지 설명의 목적을 위해 사용되며, 상대적 중요성을 나타내거나 암시하는 것으로 해석될 수 없다는 점에 주목해야 한다. 또한, 본 출원의 설명에 있어서, “복수”는, 달리 특정되지 않는 한, 2 이상을 의미한다.

[0097] 흐름도에 설명되거나 본 명세서의 임의의 다른 방식으로 기술된 임의의 프로세스 또는 방법은, 특정 논리 기능 또는 프로세스 단계를 실현하는 실행 가능한 명령어 코드를 위한 하나 이상의 모듈, 세그먼트 또는 부분을 포함하는 것으로 이해될 수도 있다. 또한, 본 출원의 바람직한 실시형태는, 관련 기능에 기초한 실질적으로 동시적인 방식 또는 반대의 순서를 포함하여, 도시되거나 논의된 것과 상이한 순서로 기능이 수행될 수도 있는 다른 구현예를 포함한다. 이는 본 출원의 실시형태가 속하는 기술 분야의 당업자에 의해 이해되어야 한다.

[0098] 본 출원의 각 부분은 하드웨어, 소프트웨어, 펌웨어 또는 이들의 조합에 의해 실현될 수도 있음을 이해하여야 한다. 상기 실시형태들에서, 복수의 단계들 또는 방법들은 메모리에 저장된 소프트웨어 또는 펌웨어에 의해 구현될 수도 있고 적절한 명령어 실행 시스템에 의해 실행될 수도 있다. 예를 들어, 하드웨어에 의해 구현되는 경우, 다른 실시형태에서와 마찬가지로, 단계들 또는 방법들은 당해 분야에 공지된 이하의 기술 중 하나 또는 조합에 의해 구현될 수도 있는데, 상기 기술은 데이터 신호의 논리 기능을 실현하기 위한 논리 게이트 회로를 갖는 이산 논리 회로, 적절한 조합 논리 게이트 회로를 갖는 주문형 집적 회로, 프로그램 가능한 게이트 어레이(PGA), 필드 프로그래머블 게이트 어레이(FPGA) 등을 포함한다.

[0099] 당업자는 상기 실시형태 방법의 단계들의 전부 또는 일부가 관련 하드웨어를 프로그램들로 명령함으로써 달성될 수도 있음을 이해할 것이다. 프로그램은 컴퓨터 판독가능한 저장 매체에 저장될 수도 있으며, 실행될 때, 프로

그램은 방법 실시형태에서 단계들 중 하나 또는 그 조합을 포함한다.

[0100] 또한, 본 출원의 실시형태에서의 기능 유닛은 처리 모듈에 통합될 수도 있거나, 상기 유닛은 물리적으로 별개의 방식 제공될 수도 있거나, 2개 이상의 유닛이 하나의 모듈에 통합될 수도 있다. 통합 모듈은 하드웨어의 형태로 또는 소프트웨어 기능 모듈의 형태로 실현 될 수도 있다. 통합 모듈이 소프트웨어 기능 모듈의 형태로 실현되고, 독립형 제품으로서 판매 또는 사용될 때, 통합 모듈은 또한 컴퓨터 판독가능한 저장 매체에 저장될 수도 있다.

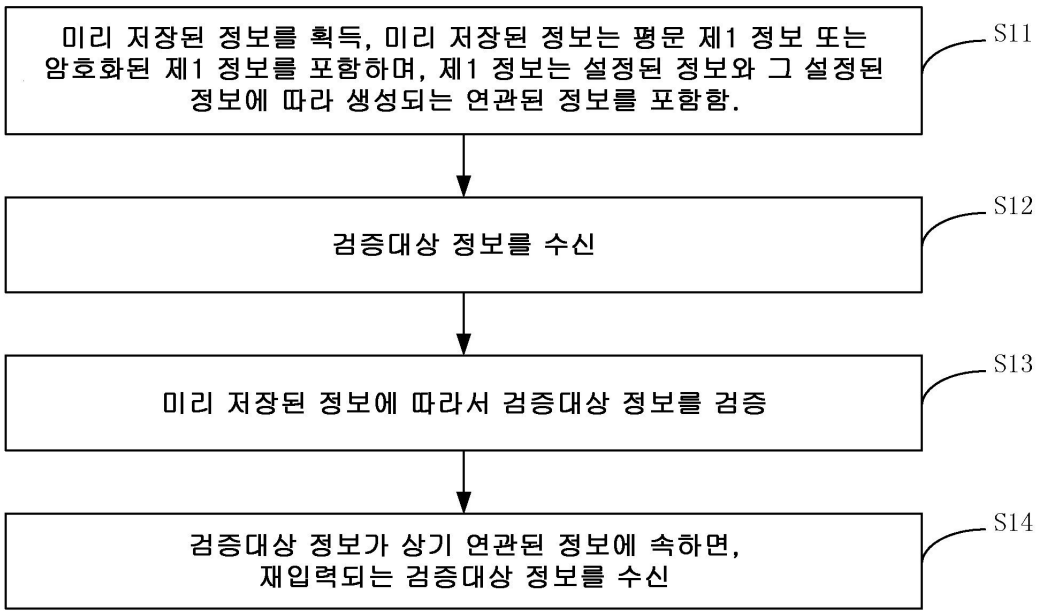
[0101] 상술한 저장 매체는 판독 전용 메모리, 자기 디스크, CD 등일 수도 있다.

[0102] 본 명세서 전반에 걸쳐서 “실시형태”, “일부 실시형태”, “실시예”, “특정 실시예”, 또는 “일부 실시예”에 대한 참조는, 이러한 실시형태 또는 실시예와 관련하여 설명된 특정의 특징, 구조, 재료, 또는 특성이 본 출원의 적어도 하나의 실시형태 또는 실시예에 포함된다는 것을 의미한다. 본 명세서 전반에 걸쳐 이러한 용어의 예시적인 표현은 반드시 동일한 실시형태 또는 실시예를 언급하지는 않는다. 또한, 특정의 특징, 구조, 재료, 또는 특성은 하나 이상의 실시형태 또는 실시예에서 임의의 적합한 방식으로 조합될 수도 있다.

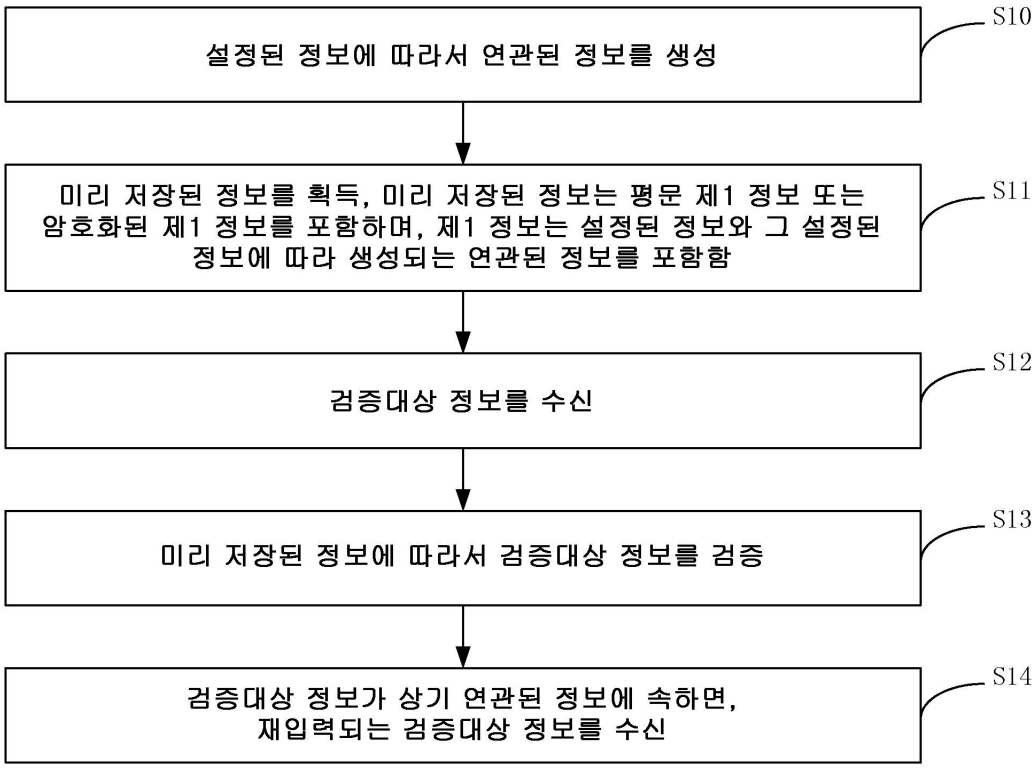
[0103] 본 출원의 실시형태가 위에서 도시되고 설명되었지만, 상기 실시형태는 예시적이고 본 출원을 제한하는 것으로 해석될 수 없고, 당업자는 본 출원의 범위 내에서 실시형태에서 변경, 수정, 대체 및 교체를 행할 수 있음을 인식할 것이다.

도면

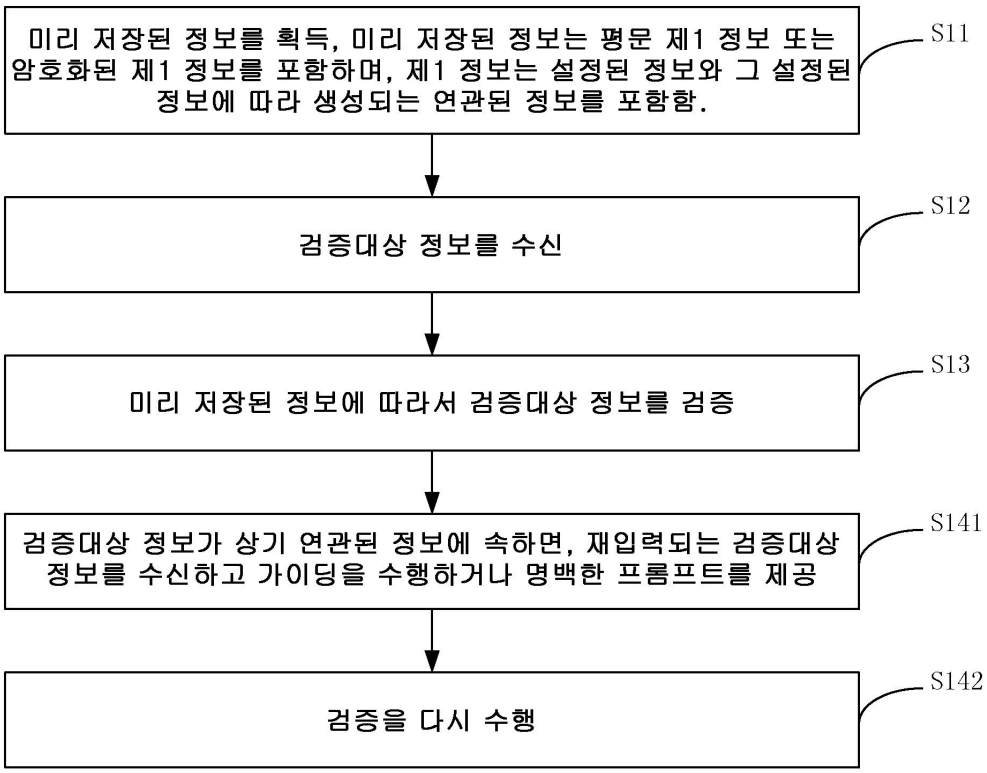
도면1



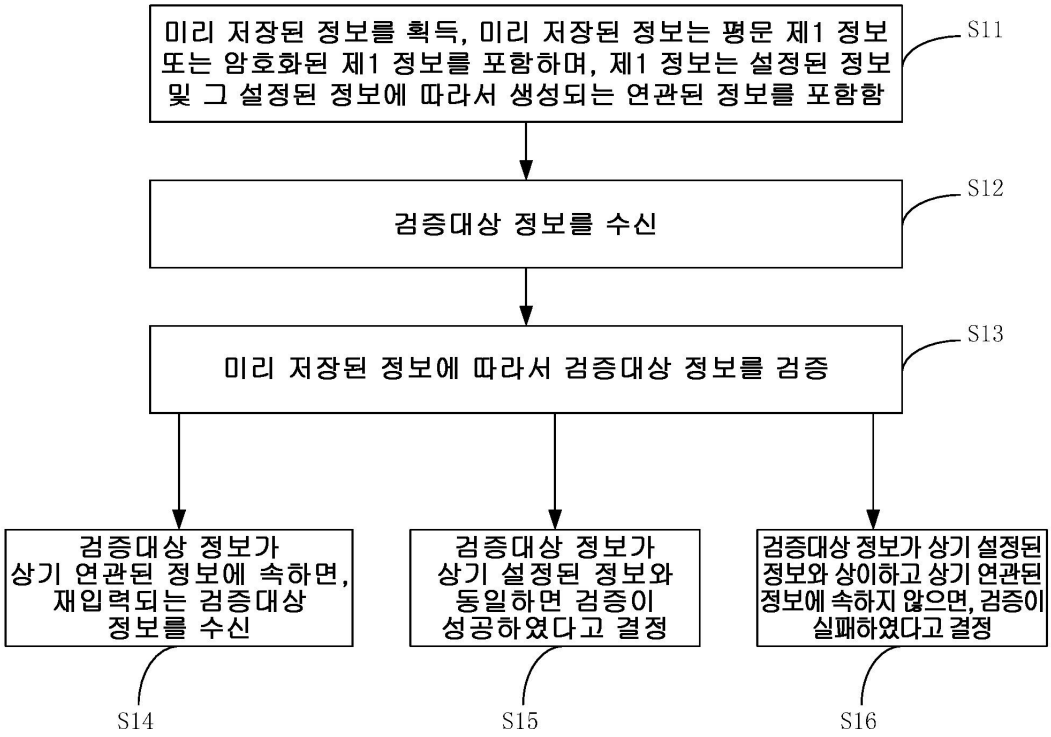
도면2


설정된 정보에 따라서 연관된 정보를 생성
S10
미리 저장된 정보를 획득, 미리 저장된 정보는 평문 제1 정보 또는 암호화된 제1 정보를 포함하며, 제1 정보는 설정된 정보와 그 설정된 정보에 따라 생성되는 연관된 정보를 포함함
S11
검증대상 정보를 수신
S12
미리 저장된 정보에 따라서 검증대상 정보를 검증
S13
검증대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증대상 정보를 수신
S14

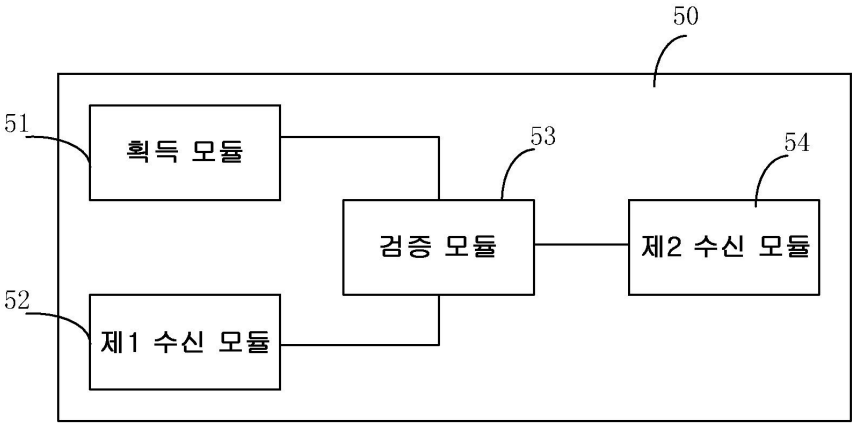
도면3


미리 저장된 정보를 획득, 미리 저장된 정보는 평문 제1 정보 또는 암호화된 제1 정보를 포함하며, 제1 정보는 설정된 정보와 그 설정된 정보에 따라 생성되는 연관된 정보를 포함함.
S11
검증대상 정보를 수신
S12
미리 저장된 정보에 따라서 검증대상 정보를 검증
S13
검증대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증대상 정보를 수신하고 가이딩을 수행하거나 명백한 프롬프트를 제공
S141
검증을 다시 수행
S142

도면4


미리 저장된 정보를 획득, 미리 저장된 정보는 평문 제1 정보 또는 암호화된 제1 정보를 포함하며, 제1 정보는 설정된 정보 및 그 설정된 정보에 따라서 생성되는 연관된 정보를 포함함
S11
검증대상 정보를 수신
S12
미리 저장된 정보에 따라서 검증대상 정보를 검증
S13
검증대상 정보가 상기 연관된 정보에 속하면, 재입력되는 검증대상 정보를 수신
S14
검증대상 정보가 상기 설정된 정보와 동일하면 검증이 성공하였다고 결정
S15
검증대상 정보가 상기 설정된 정보와 상이하고 상기 연관된 정보에 속하지 않으면, 검증이 실패하였다고 결정
S16

도면5


50
51
획득 모듈
53
54
검증 모듈
제2 수신 모듈
52
제1 수신 모듈

도면6

