



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년09월20일
(11) 등록번호 10-1655439
(24) 등록일자 2016년09월01일

(51) 국제특허분류(Int. Cl.)
G06F 21/35 (2013.01) G06F 21/30 (2013.01)
G06F 21/32 (2013.01)
(52) CPC특허분류
G06F 21/35 (2013.01)
G06F 21/30 (2013.01)
(21) 출원번호 10-2015-0042096
(22) 출원일자 2015년03월26일
심사청구일자 2015년03월26일
(56) 선행기술조사문헌
JP2011504261 A*
KR1020140093556 A*
KR1020140085952 A
KR1020130040454 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
세종대학교산학협력단
서울특별시 광진구 능동로 209 (군자동, 세종대학교)
(72) 발명자
신지선
서울특별시 송파구 올림픽로 435, 311동 2001호
(신천동, 파크리오)
(74) 대리인
두호특허법인

전체 청구항 수 : 총 13 항

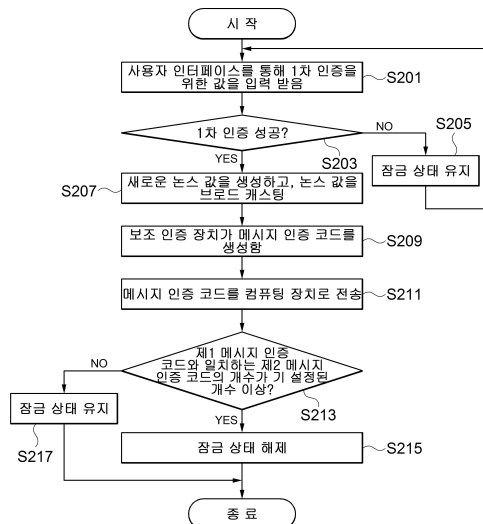
심사관 : 문남두

(54) 발명의 명칭 컴퓨팅 장치의 인증 방법 및 이를 수행하기 위한 장치

(57) 요약

컴퓨팅 장치의 인증 방법 및 이를 수행하기 위한 장치가 개시된다. 본 발명의 일 실시예에 따른 컴퓨팅 장치의 인증 방법은, 컴퓨팅 장치의 인증 방법으로서, 컴퓨팅 장치에서, 사용자의 직접 입력에 의한 인증을 통해 1차 인증을 수행하는 단계 및 1차 인증이 성공되는 경우, 컴퓨팅 장치에서 복수 개의 보조 인증 장치와 무선 통신을 수행하여 2차 인증을 수행하는 단계를 포함한다.

대표도 - 도2



(52) CPC특허분류

G06F 21/32 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 1711012958

부처명 미래부

연구관리전문기관 한국연구재단

연구사업명 신진연구자지원사업

연구과제명 스마트폰의 개인 정보보호와 프라이버시 강화

기 여 율 1/1

주관기관 세종대학교 산학협력단

연구기간 2013.06.01 ~ 2016.05.31

명세서

청구범위

청구항 1

컴퓨팅 장치의 인증 방법으로서,

상기 컴퓨팅 장치에서, 사용자의 직접 입력에 의한 인증을 통해 1차 인증을 수행하는 단계; 및

상기 1차 인증이 성공되는 경우, 상기 컴퓨팅 장치에서 복수 개의 보조 인증 장치와 각각 무선 통신을 수행하여 2차 인증을 수행하는 단계를 포함하고,

상기 2차 인증을 수행하는 단계는,

상기 컴퓨팅 장치에서, 2차 인증된 보조 인증 장치의 개수가 기 설정된 개수 이상인지 여부를 확인하는 단계; 및

2차 인증된 보조 인증 장치의 개수가 상기 기 설정된 개수 이상인 경우, 상기 컴퓨팅 장치에서 상기 컴퓨팅 장치의 잠금 상태를 해제하는 단계를 포함하는, 컴퓨팅 장치의 인증 방법.

청구항 2

청구항 1에 있어서,

상기 복수 개의 보조 인증 장치는,

상기 컴퓨팅 장치의 사용자의 신체 및 사물 중 적어도 하나에 장착되는, 컴퓨팅 장치의 인증 방법.

청구항 3

삭제

청구항 4

청구항 1에 있어서,

상기 2차 인증을 수행하는 단계는,

상기 컴퓨팅 장치에서, 논스 값을 브로드캐스팅하는 단계;

상기 컴퓨팅 장치에서, 상기 논스 값을 이용하여 제1 메시지 인증 코드를 생성하는 단계;

상기 컴퓨팅 장치에서, 상기 논스 값을 수신한 보조 인증 장치들로부터 제2 메시지 인증 코드를 수신하는 단계;

상기 컴퓨팅 장치에서, 상기 제1 메시지 인증 코드와 일치하는 상기 제2 메시지 인증 코드의 개수가 기 설정된 개수 이상인지 여부를 확인하는 단계; 및

상기 제1 메시지 인증 코드와 일치하는 상기 제2 메시지 인증 코드의 개수가 기 설정된 개수 이상인 경우, 상기 컴퓨팅 장치에서 상기 컴퓨팅 장치의 잠금 상태를 해제하는 단계를 포함하는, 컴퓨팅 장치의 인증 방법.

청구항 5

청구항 4에 있어서,

상기 컴퓨팅 장치 및 상기 복수 개의 보조 인증 장치는, 각각 동일한 알고리즘 및 동일한 키(Key) 값을 가지며,

상기 제1 메시지 인증 코드 및 상기 제2 메시지 인증 코드는, 상기 키 값 및 상기 논스 값을 상기 알고리즘에

입력하여 생성되는 것인, 컴퓨팅 장치의 인증 방법.

청구항 6

청구항 4에 있어서,

상기 논스 값을 브로드캐스팅하는 단계는,

상기 컴퓨팅 장치에서, 새로운 논스 값을 생성하는 단계; 및

상기 컴퓨팅 장치에서, 상기 새로운 논스 값을 브로드캐스팅하는 단계를 포함하는, 컴퓨팅 장치의 인증 방법.

청구항 7

컴퓨팅 장치의 인증 방법으로서,

상기 컴퓨팅 장치에서, 복수 개의 보조 인증 장치와 각각 무선 통신을 통해 인증을 수행하는 단계;

상기 컴퓨팅 장치에서, 인증된 상기 보조 인증 장치의 개수를 확인하는 단계; 및

상기 컴퓨팅 장치에서, 인증된 상기 보조 인증 장치의 개수에 따라 상기 컴퓨팅 장치의 인증 방식을 설정하는 단계를 포함하고,

상기 컴퓨팅 장치의 인증 방식을 설정하는 단계는, 상기 컴퓨팅 장치에서, 인증된 상기 보조 인증 장치의 개수에 따라 인증 절차의 개수 및 인증 수단 중 적어도 하나를 다르게 설정하는, 컴퓨팅 장치의 인증 방법.

청구항 8

청구항 7에 있어서,

상기 복수 개의 보조 인증 장치는,

상기 컴퓨팅 장치의 사용자의 신체 및 사물 중 적어도 하나에 장착되는, 컴퓨팅 장치의 인증 방법.

청구항 9

청구항 7에 있어서,

상기 컴퓨팅 장치의 인증 방식을 설정하는 단계는,

인증된 상기 보조 인증 장치의 개수가 적을수록 상기 인증 절차의 개수가 많아지도록 설정하는, 컴퓨팅 장치의 인증 방법.

청구항 10

컴퓨팅 장치의 인증 방법으로서,

상기 컴퓨팅 장치에서, 복수 개의 보조 인증 장치와 각각 무선 통신을 통해 주기적으로 인증을 수행하는 단계;

상기 컴퓨팅 장치에서, 인증된 상기 보조 인증 장치의 개수에 따라 해당 주기의 1차 인증 성공 여부를 판단하는 단계; 및

상기 컴퓨팅 장치에서, 상기 1차 인증이 성공한 경우 2차 인증을 허용하는 단계를 포함하고,

상기 1차 인증의 성공 여부를 판단하는 단계는,

상기 컴퓨팅 장치에서, 인증된 상기 보조 인증 장치의 개수가 기 설정된 개수 이상이 되는지 여부를 확인하는

단계; 및

인증된 상기 보조 인증 장치의 개수가 기 설정된 개수 이상이 되는 경우, 상기 컴퓨팅 장치에서 해당 주기의 1차 인증이 성공된 것으로 판단하는 단계를 포함하는, 컴퓨팅 장치의 인증 방법.

청구항 11

청구항 10에 있어서,

상기 복수 개의 보조 인증 장치는,

상기 컴퓨팅 장치의 사용자의 신체 및 사물 중 적어도 하나에 장착되는, 컴퓨팅 장치의 인증 방법.

청구항 12

삭제

청구항 13

청구항 10에 있어서,

상기 1차 인증이 성공된 것으로 판단하는 단계 이후에,

상기 컴퓨팅 장치에서, 상기 1차 인증 된 상태를 기 설정된 시간 동안 유지하는 단계를 더 포함하는, 컴퓨팅 장치의 인증 방법.

청구항 14

청구항 13에 있어서,

상기 1차 인증이 성공된 것으로 판단하는 단계 이후에,

상기 컴퓨팅 장치에서, 상기 1차 인증 된 상태를 유지하는 동안 2차 인증이 성공되는지 여부를 확인하는 단계; 및

상기 2차 인증이 성공되는 경우, 상기 컴퓨팅 장치에서 상기 컴퓨팅 장치의 잠금 상태를 해제하는 단계를 더 포함하는, 컴퓨팅 장치의 인증 방법.

청구항 15

청구항 10에 있어서,

상기 1차 인증 성공 여부를 판단하는 단계 이후에,

상기 1차 인증이 실패한 경우, 상기 컴퓨팅 장치에서 2차 인증이 시도되는지 여부를 확인하는 단계; 및

상기 2차 인증이 시도되는 경우, 상기 컴퓨팅 장치에서 상기 2차 인증을 차단하는 단계를 더 포함하는, 컴퓨팅 장치의 인증 방법.

청구항 16

청구항 16은(는) 설정등록료 납부시 포기되었습니다.

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,
상기 프로그램은,

사용자의 직접 입력에 의한 인증을 통해 1차 인증을 수행하는 단계; 및

상기 1차 인증이 성공되는 경우, 복수 개의 보조 인증 장치와 각각 무선 통신을 수행하여 2차 인증을 수행하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 프로그램은, 상기 2차 인증을 수행하는 단계에서,

상기 2차 인증된 보조 인증 장치의 개수가 기 설정된 개수 이상인지 여부를 확인하는 단계; 및

상기 2차 인증된 보조 인증 장치의 개수가 기 설정된 개수 이상인 경우, 상기 장치의 잠금 상태를 해제하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 17

삭제

청구항 18

청구항 18은(는) 설정등록료 납부시 포기되었습니다.

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,
상기 프로그램은,

복수 개의 보조 인증 장치와 각각 무선 통신을 통해 인증을 수행하는 단계;

인증된 상기 보조 인증 장치의 개수를 확인하는 단계; 및

인증된 상기 보조 인증 장치의 개수에 따라 컴퓨팅 장치의 인증 방식을 설정하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 프로그램은, 상기 컴퓨팅 장치의 인증 방식을 설정하는 단계에서,

인증된 상기 보조 인증 장치의 개수에 따라 인증 절차의 개수 및 인증 수단 중 적어도 하나를 다르게 설정하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 19

청구항 19은(는) 설정등록료 납부시 포기되었습니다.

청구항 18에 있어서,

상기 프로그램은,

인증된 상기 보조 인증 장치의 개수가 적을수록 상기 인증 절차의 개수가 많아지도록 설정하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 20

청구항 20은(는) 설정등록료 납부시 포기되었습니다.

하나 이상의 프로세서;

메모리; 및

하나 이상의 프로그램을 포함하는 장치로서,

상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며,

상기 프로그램은,

복수 개의 보조 인증 장치와 무선 통신을 통해 주기적으로 인증을 수행하는 단계;

인증된 상기 보조 인증 장치의 개수에 따라 해당 주기의 1차 인증 성공 여부를 판단하는 단계; 및

상기 1차 인증이 성공한 경우 2차 인증을 허용하는 단계를 실행하기 위한 명령어들을 포함하고,

상기 프로그램은, 상기 1차 인증 성공 여부를 판단하는 단계에서,

인증된 상기 보조 인증 장치의 개수가 기 설정된 개수 이상이 되는지 여부를 확인하는 단계; 및

인증된 상기 보조 인증 장치의 개수가 기 설정된 개수 이상이 되는 경우, 해당 주기의 1차 인증이 성공된 것으로 판단하는 단계를 실행하기 위한 명령어들을 포함하는 장치.

청구항 21

청구항 21은(는) 설정등록료 납부시 포기되었습니다.

청구항 20에 있어서,

상기 프로그램은,

상기 1차 인증이 성공된 경우, 상기 1차 인증 된 상태를 기 설정된 시간 동안 유지하는 단계; 및

상기 1차 인증 된 상태를 유지하는 동안 2차 인증의 성공 여부에 따라 상기 장치의 잠금 상태를 해제하는 단계를 더 실행하기 위한 명령어들을 포함하는 장치.

청구항 22

청구항 22은(는) 설정등록료 납부시 포기되었습니다.

청구항 20에 있어서,

상기 프로그램은,

상기 1차 인증이 실패한 경우, 2차 인증이 시도되는지 여부를 확인하는 단계; 및

상기 2차 인증이 시도되는 경우, 상기 2차 인증을 차단하는 단계를 더 실행하기 위한 명령어들을 포함하는 장치.

청구항 23

삭제

청구항 24

삭제

청구항 25

삭제

청구항 26

삭제

발명의 설명

기술 분야

[0001] 본 발명의 실시예는 인증 기술에 관한 것으로서, 보다 상세하게는 컴퓨팅 장치의 인증 방법 및 이를 수행하기 위한 장치에 관한 것이다.

배경 기술

[0002] 스마트 폰은 휴대 전화, 인터넷 통신, 근거리 통신, 정보 검색, 카메라, 게임, 음악 감상, 영화 감상, 스케줄 관리 등 다양한 컴퓨팅 환경을 지원하는 지능형 단말기로서 활용도가 높아 그 수요가 증가하고 있는 추세이다. 스마트 폰은 내부에 저장되어 있는 정보를 타인으로부터 보호하기 위해 사용자 인증을 통해 잠금 상태를 해제하도록 하고 있다. 일반적으로, 스마트 폰의 사용자 인증은 기 설정된 비밀번호를 입력하거나 스마트 폰의 화면에 기 설정된 패턴을 입력하는 것으로 수행된다. 그러나, 이러한 방식의 사용자 인증은 스마트 폰을 분실하거나 사용자의 부재 시 보안성이 취약하다는 문제점이 있다.

선행기술문헌

[0003] 한국등록특허공보 제10-1087695호(2011.11.30)

발명의 내용

해결하려는 과제

[0004] 예시적인 실시예에 따르면 보안성이 강화된 컴퓨팅 장치의 인증 방법 및 이를 수행하기 위한 장치가 제공된다.

과제의 해결 수단

[0005] 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법은, 상기 컴퓨팅 장치에서, 사용자의 직접 입력에 의한 인증을 통해 1차 인증을 수행하는 단계; 및 상기 1차 인증이 성공되는 경우, 상기 컴퓨팅 장치에서 복수 개의 보조 인증 장치와 무선 통신을 수행하여 2차 인증을 수행하는 단계를 포함한다.

[0006] 상기 복수 개의 보조 인증 장치는, 상기 컴퓨팅 장치의 사용자의 신체 및 사물 중 적어도 하나에 장착될 수 있다.

[0007] 상기 2차 인증을 수행하는 단계는, 상기 컴퓨팅 장치에서, 2차 인증된 보조 인증 장치의 개수가 기 설정된 개수 이상인지 여부를 확인하는 단계; 및 2차 인증된 보조 인증 장치의 개수가 상기 기 설정된 개수 이상인 경우, 상기 컴퓨팅 장치에서 상기 컴퓨팅 장치의 잠금 상태를 해제하는 단계를 포함할 수 있다.

[0008] 상기 2차 인증을 수행하는 단계는, 상기 컴퓨팅 장치에서, 논스 값을 브로드캐스팅하는 단계; 상기 컴퓨팅 장치에서, 상기 논스 값을 이용하여 제1 메시지 인증 코드를 생성하는 단계; 상기 컴퓨팅 장치에서, 상기 논스 값을 수신한 보조 인증 장치들로부터 제2 메시지 인증 코드를 수신하는 단계; 상기 컴퓨팅 장치에서, 상기 제1 메시지 인증 코드와 일치하는 상기 제2 메시지 인증 코드의 개수가 기 설정된 개수 이상인지 여부를 확인하는 단계; 및 상기 제1 메시지 인증 코드와 일치하는 상기 제2 메시지 인증 코드의 개수가 기 설정된 개수 이상인 경우, 상기 컴퓨팅 장치에서 상기 컴퓨팅 장치의 잠금 상태를 해제하는 단계를 포함할 수 있다.

[0009] 상기 컴퓨팅 장치 및 상기 복수 개의 보조 인증 장치는, 각각 동일한 암호화 알고리즘 및 동일한 키(Key) 값을 가지며, 상기 제1 메시지 인증 코드 및 상기 제2 메시지 인증 코드는, 상기 키 값 및 상기 논스 값을 상기 알고

리즘에 입력하여 생성되는 것일 수 있다.

- [0010] 상기 논스 값을 브로드캐스팅하는 단계는, 상기 컴퓨팅 장치에서, 새로운 논스 값을 생성하는 단계; 및 상기 컴퓨팅 장치에서, 상기 새로운 논스 값을 브로드캐스팅하는 단계를 포함할 수 있다.
- [0011] 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법은, 상기 컴퓨팅 장치에서, 복수 개의 보조 인증 장치와 무선 통신을 통해 인증을 수행하는 단계; 및 상기 컴퓨팅 장치에서, 인증된 상기 보조 인증 장치의 개수에 따라 상기 컴퓨팅 장치의 인증 방식을 설정하되, 인증된 상기 보조 인증 장치의 개수에 따라 인증 절차의 개수 및 인증 수단 중 적어도 하나를 다르게 설정하는 단계를 포함한다.
- [0012] 상기 복수 개의 보조 인증 장치는, 상기 컴퓨팅 장치의 사용자의 신체 및 사물 중 적어도 하나에 장착될 수 있다.
- [0013] 상기 컴퓨팅 장치의 인증 방식을 설정하는 단계는, 인증된 상기 보조 인증 장치의 개수가 적을수록 상기 인증 절차의 개수가 많아지도록 설정할 수 있다.
- [0014] 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법은, 상기 컴퓨팅 장치에서, 복수 개의 보조 인증 장치와 무선 통신을 통해 주기적으로 인증을 수행하는 단계; 상기 컴퓨팅 장치에서, 인증된 상기 보조 인증 장치의 개수에 따라 해당 주기의 1차 인증 성공 여부를 판단하는 단계; 및 상기 컴퓨팅 장치에서, 상기 1차 인증이 성공한 경우 2차 인증을 허용하는 단계를 포함한다.
- [0015] 상기 복수 개의 보조 인증 장치는, 상기 컴퓨팅 장치의 사용자의 신체 및 사물 중 적어도 하나에 장착될 수 있다.
- [0016] 상기 1차 인증의 성공 여부를 판단하는 단계는, 상기 컴퓨팅 장치에서, 인증된 상기 보조 인증 장치의 개수가 기 설정된 개수 이상이 되는지 여부를 확인하는 단계; 및 인증된 상기 보조 인증 장치의 개수가 기 설정된 개수 이상이 되는 경우, 상기 컴퓨팅 장치에서 해당 주기의 1차 인증이 성공된 것으로 판단하는 단계를 포함할 수 있다.
- [0017] 상기 1차 인증이 성공된 것으로 판단하는 단계 이후에, 상기 컴퓨팅 장치에서, 상기 1차 인증 된 상태를 기 설정된 시간 동안 유지하는 단계를 더 포함할 수 있다.
- [0018] 상기 1차 인증이 성공된 것으로 판단하는 단계 이후에, 상기 컴퓨팅 장치에서, 상기 1차 인증 된 상태를 유지하는 동안 2차 인증이 성공되는지 여부를 확인하는 단계; 및 상기 2차 인증이 성공되는 경우, 상기 컴퓨팅 장치에서 상기 컴퓨팅 장치의 잠금 상태를 해제하는 단계를 더 포함할 수 있다.
- [0019] 상기 1차 인증 성공 여부를 판단하는 단계 이후에, 상기 1차 인증이 실패한 경우, 상기 컴퓨팅 장치에서 2차 인증이 시도되는지 여부를 확인하는 단계; 및 상기 2차 인증이 시도되는 경우, 상기 컴퓨팅 장치에서 상기 2차 인증을 차단할 수 있다.
- [0020] 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법을 수행하기 위한 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 사용자의 직접 입력에 의한 인증을 통해 1차 인증을 수행하는 단계; 및 상기 1차 인증이 성공되는 경우, 복수 개의 보조 인증 장치와 무선 통신을 수행하여 2차 인증을 수행하는 단계를 실행하기 위한 명령어들을 포함한다.
- [0021] 상기 프로그램은, 상기 2차 인증을 수행하는 단계에서, 상기 2차 인증된 보조 인증 장치의 개수가 기 설정된 개수 이상인지 여부를 확인하는 단계; 및 상기 2차 인증된 보조 인증 장치의 개수가 기 설정된 개수 이상인 경우, 상기 장치의 잠금 상태를 해제하는 단계를 실행하기 위한 명령어들을 포함할 수 있다.
- [0022] 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법을 수행하기 위한 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 복수 개의 보조 인증 장치와 무선 통신을 통해 인증을 수행하는 단계; 및 인증된 상기 보조 인증 장치의 개수에 따라 상기 컴퓨팅 장치의 인증 방식을 설정하되, 인증된 상기 보조 인증 장치의 개수에 따라 인증 절차의 개수 및 인증 수단 중 적어도 하나를 다르게 설정하는 단계를 실행하기 위한 명령어들을 포함한다.
- [0023] 상기 프로그램은, 인증된 상기 보조 인증 장치의 개수가 적을수록 상기 인증 절차의 개수가 많아지도록 설정하는 단계를 실행하기 위한 명령어들을 포함할 수 있다.

- [0024] 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법을 수행하기 위한 장치는, 하나 이상의 프로세서; 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 복수 개의 보조 인증 장치와 무선 통신을 통해 주기적으로 인증을 수행하는 단계; 인증된 상기 보조 인증 장치의 개수에 따라 해당 주기의 1차 인증 성공 여부를 판단하는 단계; 및 상기 1차 인증이 성공한 경우 2차 인증을 허용하는 단계를 실행하기 위한 명령어들을 포함한다.
- [0025] 상기 프로그램은, 상기 1차 인증이 성공된 경우, 상기 1차 인증 된 상태를 기 설정된 시간 동안 유지하는 단계; 및 상기 1차 인증 된 상태를 유지하는 동안 2차 인증의 성공 여부에 따라 상기 장치의 잠금 상태를 해제하는 단계를 더 실행하기 위한 명령어들을 포함할 수 있다.
- [0026] 상기 프로그램은, 상기 1차 인증이 실패한 경우, 2차 인증이 시도되는지 여부를 확인하는 단계; 및 상기 2차 인증이 시도되는 경우, 상기 2차 인증을 차단하는 단계를 더 실행하기 위한 명령어들을 포함할 수 있다.
- [0027] 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법을 수행하기 위한 장치는, 하나 이상의 프로세서; 알고리즘, 키 값, 및 자신의 고유 아이디를 저장하는 메모리; 및 하나 이상의 프로그램을 포함하는 장치로서, 상기 하나 이상의 프로그램은 상기 메모리에 저장되고 상기 하나 이상의 프로세서에 의해 실행되도록 구성되며, 상기 프로그램은, 무선 통신을 통해 논스 값을 수신하는 단계; 상기 키 값, 상기 논스 값, 및 상기 고유 아이디를 상기 알고리즘에 입력하여 메시지 인증 코드를 생성하는 단계; 및 상기 메시지 인증 코드를 무선 통신을 통해 전송하는 단계를 실행하기 위한 명령어들을 포함한다.
- [0028] 상기 프로그램은, 상기 메시지 인증 코드를 생성하는 단계에서, 상기 논스 값에 상기 고유 아이디를 패딩(Padding)하여 메시지 인증 코드를 생성하는 단계를 실행하기 위한 명령어들을 포함할 수 있다.
- [0029] 상기 장치는, 컴퓨팅 장치로부터 상기 논스 값을 수신하고, 상기 컴퓨팅 장치의 잠금 상태 해제를 위한 인증에 사용될 수 있다.
- [0030] 상기 장치는, 복수 개가 하나의 세트로 마련되고, 상기 하나의 세트에 마련되는 복수 개의 장치가 각각 상기 컴퓨팅 장치의 사용자의 신체 및 사물 중 적어도 하나에 장착될 수 있다.

발명의 효과

- [0031] 본 발명의 실시예에 의하면, 컴퓨팅 장치와 복수 개의 보조 인증 장치 간에 무선 통신을 통해 인증을 수행함으로써, 컴퓨팅 장치의 보안성을 강화할 수 있으며, 그로 인해 컴퓨팅 장치를 분실하거나 사용자가 컴퓨팅 장치에서 벗어나 있는 경우에도 컴퓨팅 장치가 악의적으로 사용되는 것을 방지할 수 있게 된다.
- [0032] 또한, 무선 통신에 의한 인증을 통해 컴퓨팅 장치에 다양한 인증 방식을 도입할 수 있게 된다.

도면의 간단한 설명

- [0033] 도 1은 예시적인 실시예에 따른 컴퓨팅 장치의 인증 시스템을 나타낸 블록도
 도 2는 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법을 나타낸 흐름도
 도 3은 예시적인 다른 실시예에 따른 컴퓨팅 장치의 인증 방법을 나타낸 흐름도
 도 4는 예시적인 또 다른 실시예에 따른 컴퓨팅 장치의 인증 방법을 나타낸 흐름도
 도 5는 예시적인 실시예들에서 사용되기에 적합한 예시적인 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 나타낸 예시도

발명을 실시하기 위한 구체적인 내용

- [0034] 이하, 도면을 참조하여 본 발명의 구체적인 실시형태를 설명하기로 한다. 이하의 상세한 설명은 본 명세서에서 기술된 방법, 장치 및/또는 시스템에 대한 포괄적인 이해를 돕기 위해 제공된다. 그러나 이는 예시에 불과하며 본 발명은 이에 제한되지 않는다.

- [0035] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.
- [0036] 이하의 설명에 있어서, 신호 또는 정보의 "전송", "통신", "송신", "수신" 기타 이와 유사한 의미의 용어는 일 구성요소에서 다른 구성요소로 신호 또는 정보가 직접 전달되는 것뿐만이 아니라 다른 구성요소를 거쳐 전달되는 것도 포함한다. 특히 신호 또는 정보를 일 구성요소로 "전송" 또는 "송신"한다는 것은 그 신호 또는 정보의 최종 목적지를 지시하는 것이고 직접적인 목적지를 의미하는 것이 아니다. 이는 신호 또는 정보의 "수신"에 있어서도 동일하다. 또한 본 명세서에 있어서, 2 이상의 데이터 또는 정보가 "관련"된다는 것은 하나의 데이터(또는 정보)를 획득하면, 그에 기초하여 다른 데이터(또는 정보)의 적어도 일부를 획득할 수 있음을 의미한다.
- [0037] 또한, 본 명세서에서 기재한 "제1", "제2" 등은 서로 다른 구성 요소임을 구분하기 위해서 지칭하는 것일 뿐, 그 순서에 구애받지 않으며 발명의 상세한 설명과 청구범위에서 그 명칭이 일치하지 않을 수 있다.
- [0038] 도 1은 예시적인 실시예에 따른 컴퓨팅 장치의 인증 시스템을 나타낸 블록도이다. 도 1을 참조하면, 인증 시스템(100)은 컴퓨팅 장치(102) 및 복수 개의 보조 인증 장치(104)를 포함한다. 컴퓨팅 장치(102)와 복수 개의 보조 인증 장치(104)는 무선 네트워크(150)를 통해 통신 가능하게 연결된다. 무선 네트워크(150)는 예를 들어, BCC(Body Coupled Communication), NFC(Near Field Communication), 블루투스(Bluetooth), 와이파이(WiFi), 지그비(Zigbee), WLAN(Wireless Local Area Network), UWB(Ultra Wide Band) 등 비교적 가까운 거리에서 디바이스간의 통신을 가능하도록 하는 무선 네트워크일 수 있다.
- [0039] 컴퓨팅 장치(102)의 예들은 스마트 폰, 휴대폰, 태블릿, PDA(Personal Digital Assistant), 노트북, 스마트 워치와 같은 웨어러블 기기, PC(Personal Computer), 출입 관리 장치, 보안 장치, 서버 등의 통신 장치일 수 있다. 예시적인 실시예에 따른 인증 시스템(100)은 스마트 폰, 휴대폰, 태블릿, PDA(Personal Digital Assistant), 노트북, 스마트 워치와 같은 웨어러블 기기, PC(Personal Computer) 등과 같은 컴퓨팅 장치의 잠금 상태를 해제하기 위한 것일 수 있다. 그러나, 본 발명의 실시예들은 이에 한정되는 것은 아니며, 인증 시스템(100)은 출입 인증 또는 서버 접속 인증 등 뿐만 아니라 그 이외의 다양한 인증 분야에 적용될 수 있음은 물론이다.
- [0040] 컴퓨팅 장치(102)는 이른바 멀티 인증을 통해 잠금 상태를 해제할 수 있다. 본 발명의 실시예에서 멀티 인증이란 복수 개의 서로 다른 인증 수단을 이용하여 잠금 상태를 해제하는 인증 방식을 의미한다. 일 실시예에서, 컴퓨팅 장치(102)는 예를 들어, 터치 스크린 또는 버튼 또는 키 패드 등의 사용자 인터페이스를 통해 사용자로부터 입력되는 값(예를 들어, 비밀번호 또는 소정의 패턴 등)으로부터 1차 인증을 수행할 수 있다. 이하에서, 컴퓨팅 장치(102)의 사용자 인터페이스로부터 입력되는 값을 통해 인증을 수행하는 방식은 "사용자의 직접 입력에 의한 인증"이라 지칭될 수 있다. 또한, 컴퓨팅 장치(102)는 사용자의 직접 입력에 의한 1차 인증이 성공한 경우, 복수 개의 보조 인증 장치(104)와 무선 통신에 의한 2차 인증을 수행할 수 있다. 이하에서, 복수 개의 보조 인증 장치(104)와 무선 통신에 의해 인증을 수행하는 방식은 "무선 통신에 의한 인증"이라 지칭될 수 있다. 컴퓨팅 장치(102)는 1차 인증 및 2차 인증이 모두 성공한 경우, 컴퓨팅 장치(102)의 잠금 상태를 해제할 수 있다.
- [0041] 여기서는, 1차 인증이 "사용자의 직접 입력에 의한 인증"이고 2차 인증이 "무선 통신에 의한 인증"인 것으로 설명하였으나, 이에 한정되는 것은 아니며 1차 인증이 "무선 통신에 의한 인증"이고 2차 인증이 "사용자의 직접 입력에 의한 인증"이 될 수도 있다. 즉, 사용자의 직접 입력에 의한 인증 및 무선 통신에 의한 인증은 순서에 무관하게 사용될 수 있다. 또한, 여기서는, 컴퓨팅 장치(102)가 멀티 인증을 통해 잠금 상태를 해제하는 것으로 설명하였으나, 이에 한정되는 것은 아니며, 실시예에 따라 컴퓨팅 장치(102)는 복수 개의 인증 방식 중 일부를 이용하여 잠금 상태를 해제할 수도 있다.

- [0042] 보조 인증 장치(104)는 컴퓨팅 장치(102)의 잠금 상태를 해제하기 위한 사용자 인증에 사용될 수 있다. 보조 인증 장치(104)는 컴퓨팅 장치(102)를 이용하는 사용자의 신체 또는 사용자가 몸에 지니는 각종 사물 등에 장착될 수 있다. 예를 들어, 보조 인증 장치(104)는 컴퓨팅 장치(102)의 사용자의 신체 중 목, 손목, 발목 등에 착용 가능하게 마련될 수 있다. 또한, 보조 인증 장치(104)는 컴퓨팅 장치(102)의 사용자의 의복, 양말, 장갑 등에 장착(부착) 가능하게 마련될 수 있다. 또한, 보조 인증 장치(104)는 컴퓨팅 장치(102)의 사용자가 소지하는 물건(예를 들어, 지갑, 가방, 노트북, 책 등)에 장착 가능하게 마련될 수 있다.
- [0043] 일 실시예에서, 보조 인증 장치(104)는 복수 개가 하나의 세트로 마련될 수 있다. 하나의 세트로 마련되는 복수 개의 보조 인증 장치(104)는 각각 메시지 인증 코드(Message Authentication Code) 생성을 위한 동일한 키(Key) 값 및 알고리즘을 가지게 된다. 하나의 세트로 마련되는 복수 개의 보조 인증 장치(104)는 각각 고유 아이디가 부여된다. 하나의 세트로 마련되는 복수 개의 보조 인증 장치(104)들은 각각 사용자의 신체 또는 사용자의 사물에 장착될 수 있다. 예를 들어, 4개의 보조 인증 장치(104)가 하나의 세트인 경우, 하나는 사용자의 손목에 장착되고, 다른 하나는 사용자의 의복에 부착되며, 또 다른 하나는 사용자의 지갑에 부착되고, 나머지 하나는 사용자의 양말에 부착되는 등으로 사용자의 신체 또는 주변 사물에 다양하게 장착될 수 있다.
- [0044] 한편, 컴퓨팅 장치(102)는 메시지 인증 코드 생성을 위해 하나의 세트로 마련되는 복수 개의 보조 인증 장치(104)와 동일한 키 값 및 알고리즘을 저장할 수 있다. 컴퓨팅 장치(102)는 외부 장치로부터 복수 개의 보조 인증 장치(104)와 동일한 키 값 및 알고리즘을 수신하여 저장할 수 있다. 예를 들어, 컴퓨팅 장치(102)는 복수 개의 보조 인증 장치(104)의 판매자 장치 또는 판매자 서버 등으로부터 복수 개의 보조 인증 장치(104)와 동일한 키 값 및 알고리즘을 문자 또는 이메일 등으로 수신할 수 있다. 그러나, 이에 한정되는 것은 아니며 컴퓨팅 장치(102)가 별도의 서버 컴퓨팅 장치에 접속하여 키 값 및 알고리즘을 수신할 수도 있다.
- [0045] 본 발명의 실시예에 의하면, 사용자의 신체 또는 사물 등에 장착되는 복수 개의 보조 인증 장치를 사용하여 컴퓨팅 장치의 잠금 상태를 해제함으로써, 컴퓨팅 장치의 보안성을 강화할 수 있으며, 그로 인해 컴퓨팅 장치를 분실하거나 사용자가 컴퓨팅 장치에서 벗어나 있는 경우에도 컴퓨팅 장치가 악의적으로 사용되는 것을 방지할 수 있게 된다.
- [0046] 이하에서는, 컴퓨팅 장치의 인증 방법에 대한 예시적인 실시예들을 구체적으로 설명하기로 한다.
- [0047] 도 2는 예시적인 실시예에 따른 컴퓨팅 장치의 인증 방법을 나타낸 흐름도이다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 추가되어 수행될 수 있다. 또한 실시예에 따라 상기 방법에 도시되지 않은 하나 이상의 단계들이 상기 방법과 함께 수행될 수도 있다.
- [0048] 도 2를 참조하면, 컴퓨팅 장치(102)는 사용자 인터페이스를 통해 1차 인증을 위한 값을 입력받는다(S 201). 컴퓨팅 장치(102)는 상기 1차 인증을 위한 값을 입력받기 위해 잠금 상태에서 소정의 화면을 제공할 수 있다.
- [0049] 다음으로, 컴퓨팅 장치(102)는 1차 인증이 성공하는지 여부를 확인한다(S 203). 즉, 컴퓨팅 장치(102)는 직접 입력에 의한 인증을 통해 1차 인증을 수행할 수 있다. 컴퓨팅 장치(102)는 사용자 인터페이스를 통해 입력받은 값과 기 설정된 인증값을 비교하여 1차 인증을 수행할 수 있다. 컴퓨팅 장치(102)는 사용자 인터페이스를 통해 입력받은 값과 기 설정된 인증값이 일치하는지 여부에 따라 1차 인증의 성공 또는 실패 여부를 판단할 수 있다.
- [0050] 단계 S 203의 확인 결과, 1차 인증이 실패한 경우, 컴퓨팅 장치(102)는 컴퓨팅 장치(102)의 상태를 잠금 상태로 유지한다(S 205).
- [0051] 단계 S 203의 확인 결과, 1차 인증이 성공한 경우, 컴퓨팅 장치(102)는 무선 통신을 통해 새로운 논스(Nonce) 값을 생성하고, 생성한 논스 값을 브로드캐스팅(Broadcasting) 한다(S 207). 논스 값은 2차 인증을 위해 생성되는 임의의 값 또는 문자열을 의미한다. 구체적으로, 1차 인증이 성공한 경우, 컴퓨팅 장치(102)는 새로운 논스 값을 생성할 수 있다. 이때, 논스 값은 랜덤하게 생성될 수 있다. 본 발명의 실시예들에서, 리플레이 어택(Replay Attack)을 방지하기 위해 논스 값은 세션(Session) 마다 새로운 값을 갖도록 생성될 수 있다. 구체적으로, 악의의 침입자는 이전 세션에서 보조 인증 장치에 의해 생성된 메시지 인증 코드를 탈취한 뒤, 현재 세션에서 상기 탈취한 메시지 인증 코드를 컴퓨팅 장치(102)로 전송(즉, 리플레이 어택)할 수 있다. 이러한 리플레이 어택을 방지하기 위해 컴퓨팅 장치(102)는 매 세션 마다 새로운 논스 값을 생성하게 된다.

- [0052] 다음으로, 컴퓨팅 장치(102)는 논스 값을 무선 통신을 통해 인근의 보조 인증 장치(104)들로 브로드캐스팅 할 수 있다. 그러면, 컴퓨팅 장치(102)의 주변에 위치한 보조 인증 장치(104)들이 무선 통신을 통해 논스 값을 수신하게 된다. 여기서, 복수 개의 보조 인증 장치(104)들 중 적어도 일부는 근거리 무선 네트워크 환경 또는 컴퓨팅 장치(102)와의 거리 또는 장애물 유무 등에 따라 논스 값을 수신하지 못할 수도 있다.
- [0053] 다음으로, 논스 값을 수신한 보조 인증 장치(104)는 컴퓨팅 장치(102)와의 사이에서 약속된 키 값, 생성된 논스 값, 및 자신의 고유 아이디를 기 저장된 메시지 생성 알고리즘에 입력하여 메시지 인증 코드를 생성한다(S 209). 여기서, 하나의 세트로 마련되는 복수 개의 보조 인증 장치(104)는 각각 동일한 알고리즘 및 키 값을 구비할 수 있다. 또한, 컴퓨팅 장치(102)도 상기 알고리즘 및 키 값을 동일하게 구비할 수 있다. 여기서, 알고리즘은 키 값, 논스 값, 및 해당 보조 인증 장치의 고유 아이디를 입력받고, 이로부터 인증을 위한 메시지 인증 코드를 출력하는 알고리즘을 의미한다. 예를 들어, 상기 알고리즘은 보안 통신에서 일반적으로 사용되는 DES(Data Encryption Standard), AES(Advanced Encryption Standard) 등의 대칭키 암호화 알고리즘(Symmetric Key Cryptosystem)일 수 있다. 그러나 본 발명의 실시예들은 특정한 알고리즘에 한정되는 것은 아니며, 필요에 따라 다양한 메시지 생성 알고리즘이 제한 없이 사용될 수 있다.
- [0054] 일 실시예에서, 각 보조 인증 장치(104)는 수신한 논스 값의 앞 또는 뒤에 자신의 고유 아이디를 패딩(Padding)하고, 패딩된 문자열 및 키 값을 메시지 생성 알고리즘에 적용하여 메시지 인증 코드를 생성할 수 있다. 예를 들어, 보조 인증 장치의 고유 아이디를 ID, 논스 값을 R, 키 값을 K, 메시지 생성 알고리즘을 E로 지칭할 경우, 메시지 인증 코드는 다음과 같이 생성될 수 있다.
- [0055] 메시지 인증 코드 = $E_K(R||ID)$ 또는 $E_K(ID||R)$
- [0056] 상기 식에서 $R||ID$ 는 논스 값의 뒷 부분에 고유 아이디가 부가(패딩)되었음을 나타낸다.
- [0057] 다른 실시예에서, 각 보조 인증 장치(104)는 수신한 논스 값 및 키 값을 메시지 생성 알고리즘에 입력하고 이에 따른 출력값에 자신의 고유 아이디를 패딩하여 메시지 인증 코드를 생성할 수도 있다. 이를 수식으로 나타내면 다음과 같다.
- [0058] 메시지 인증 코드 = $E_K(R)||ID$ 또는 $ID||E_K(R)$
- [0059] 다음으로, 각 보조 인증 장치(104)는 생성된 메시지 인증 코드를 무선 통신을 통해 컴퓨팅 장치(102)로 전송한다(S 211).
- [0060] 다음으로, 컴퓨팅 장치(102)는 컴퓨팅 장치(102)에서 자체적으로 생성한 메시지 인증 코드(이하, 제1 메시지 인증 코드라 지칭)와 보조 인증 장치(104)들로부터 수신한 메시지 인증 코드(이하, 제2 메시지 인증 코드라 지칭)를 서로 비교하고, 일치하는 메시지 인증 코드의 개수가 기 설정된 개수 이상인지 여부를 확인한다(S 213). 본 발명의 실시예에서, 컴퓨팅 장치(102)는 한 세트의 보조 인증 장치(104)들과 동일한 메시지 생성 알고리즘, 키 값 및 각 보조 인증 장치(104)들의 고유 아이디를 저장한다. 이에 따라 컴퓨팅 장치(102)는 보조 인증 장치(104)들과 동일한 방식으로 메시지 인증 코드를 생성할 수 있다.
- [0061] 컴퓨팅 장치(102)는 자신이 생성한 제1 메시지 인증 코드와 보조 인증 장치(104)들로부터 수신한 제2 메시지 인증 코드를 비교하여, 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수가 기 설정된 개수 이상인지 여부를 확인할 수 있다. 컴퓨팅 장치(102)는 논스 값을 브로드캐스팅한 이후에 제1 메시지 인증 코드를 생성할 수도 있고, 보조 인증 장치(104)들로부터 메시지 인증 코드를 수신한 이후에 제1 메시지 인증 코드를 생성할 수도 있다. 그러나, 이에 한정되는 것은 아니며 제1 메시지 인증 코드는 새로운 논스 값을 생성한 이후 다양한 시점에 생성될 수 있다. 여기서, 제1 메시지 인증 코드 및 제2 메시지 인증 코드의 기재에서 "제1" 및 "제2"는 이들을 서로 구분하기 위한 것일뿐, 그 순서에 구애받는 것은 아니다.
- [0062] 컴퓨팅 장치(102) 및 보조 인증 장치(104)는 동일한 알고리즘, 키 값, 및 논스 값 등을 이용하여 메시지 인증 코드를 생성하므로, 정당한 보조 인증 장치(104)로부터 전송된 제2 메시지 인증 코드는 컴퓨팅 장치(102)에서 생성된 제1 메시지 인증 코드와 일치하게 된다. 따라서, 이 경우 컴퓨팅 장치(102)에서 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수는 제2 메시지 인증 코드를 전송한 보조 인증 장치(104)의 개수와 동일할 수 있다.
- [0063] 만약 단계 S 213의 확인 결과, 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수가 기 설정된 개수 이상인 경우, 컴퓨팅 장치(102)는 2차 인증이 성공한 것으로 판단하여 컴퓨팅 장치(102)의 잠금 상태를 해제

한다(S 215).

- [0064] 그러나 이와 달리 단계 S 213의 확인 결과, 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수가 기 설정된 개수 미만인 경우, 컴퓨팅 장치(102)는 2차 인증이 실패한 것으로 판단하여 컴퓨팅 장치(102)의 상태를 잠금 상태로 유지한다(S 217).
- [0065] 도 3은 예시적인 다른 실시예에 따른 컴퓨팅 장치의 인증 방법을 나타낸 흐름도이다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다. 또한 실시예에 따라 상기 방법에 도시되지 않은 하나 이상의 단계들이 상기 방법과 함께 수행될 수도 있다.
- [0066] 도 3을 참조하면, 컴퓨팅 장치(102)는 새로운 논스 값을 생성하고, 무선 통신을 통해 논스 값을 브로드캐스팅(Broadcastion) 한다(S 301). 컴퓨팅 장치(102)는 기 설정된 주기에 따라 논스 값을 브로드캐스팅 할 수 있다. 여기서, 논스 값은 주기마다 다른 값을 가질 수 있다.
- [0067] 다음으로, 논스 값을 수신한 보조 인증 장치(104)는 키 값, 논스 값, 및 자신의 고유 아이디를 기 저장된 알고리즘에 입력하여 메시지 인증 코드를 생성한다(S 303). 각 보조 인증 장치(104)는 생성한 메시지 인증 코드를 컴퓨팅 장치(102)로 전송하게 된다.
- [0068] 다음으로, 컴퓨팅 장치(102)는 제1 메시지 인증 코드와 일치하는 보조 인증 장치(104)들로부터 수신한 제2 메시지 인증 코드의 개수를 확인한다(S 305).
- [0069] 다음으로, 컴퓨팅 장치(102)는 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수에 따라 컴퓨팅 장치(102)의 인증 방식을 설정한다(S 307). 구체적으로, 컴퓨팅 장치(102)는 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수에 따라 컴퓨팅 장치(102)의 잠금 상태 해제를 위한 인증 절차의 개수 및 인증 수단 중 적어도 하나를 다르게 설정할 수 있다.
- [0070] 일 실시예에서, 컴퓨팅 장치(102)는 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수가 적을수록 컴퓨팅 장치(102)의 잠금 상태 해제를 위한 인증 절차의 개수가 많아지도록 설정할 수 있다. 예를 들어, 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수가 4개인 경우, 컴퓨팅 장치(102)는 1 단계 인증(즉, 인증 절차 개수 1개)(예를 들어, 무선 통신에 의한 인증)만으로 잠금 상태를 해제할 수 있도록 설정할 수 있다. 또한, 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수가 3개인 경우, 컴퓨팅 장치(102)는 2 단계 인증(즉, 인증 절차 개수 2개)(예를 들어, 사용자의 직접 입력에 의한 인증 + 무선 통신에 의한 인증)으로 잠금 상태를 해제할 수 있도록 설정할 수 있다. 다음으로, 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수가 2개인 경우, 컴퓨팅 장치(102)는 3 단계 인증(즉, 인증 절차 개수 3개)(예를 들어, 사용자의 직접 입력에 의한 인증 + 무선 통신에 의한 인증 + 지문 인증)으로 잠금 상태를 해제할 수 있도록 설정할 수 있다.
- [0071] 앞서 기술한 바와 같이, 사용자는 동일한 키를 가지는 복수 개의 보조 인증 장치(104)를 신체 또는 주변 사물에 구비하게 되는 바, 컴퓨팅 장치(102)는 주변에 보조 인증 장치(104)의 개수가 많을수록 보안 관점에서 더 안전한 환경으로 판단할 수 있다. 따라서, 전술한 바와 같이 본 발명의 일 실시예에서 컴퓨팅 장치(102)는 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수가 많을 경우 추가 인증 절차를 간소화하여 사용자의 편의성을 도모하고, 반대로 일치하는 제2 메시지 인증 코드의 개수가 적을 경우 부가적인 인증을 요구함으로써 보안성을 강화할 수 있다. 이와 같이 구성될 경우, 예를 들어 컴퓨팅 장치(102)와 함께 일부의 보조 인증 장치(104)가 악의적인 사용자에게 넘어간 경우에도 컴퓨팅 장치(102)의 잠금 상태가 악의적인 사용자에게 의해 해제되는 것을 효과적으로 차단할 수 있다.
- [0072] 다음으로, 컴퓨팅 장치(102)는 설정된 인증 방식에 따라 컴퓨팅 장치(102)의 잠금 해제를 위한 인증 절차를 수행한다(S 309).
- [0073] 한편, 컴퓨팅 장치(102)는 새로운 논스 값을 주기적으로 브로드캐스팅하고, 그때마다 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드의 개수를 확인하여, 컴퓨팅 장치(102)의 인증 방식을 재 설정 할 수 있다.

- [0074] 도 4는 예시적인 또 다른 실시예에 따른 컴퓨팅 장치의 인증 방법을 나타낸 흐름도이다. 도시된 흐름도에서는 상기 방법을 복수 개의 단계로 나누어 기재하였으나, 적어도 일부의 단계들은 순서를 바꾸어 수행되거나, 다른 단계와 결합되어 함께 수행되거나, 생략되거나, 세부 단계들로 나뉘어 수행되거나, 또는 도시되지 않은 하나 이상의 단계가 부가되어 수행될 수 있다. 또한 실시예에 따라 상기 방법에 도시되지 않은 하나 이상의 단계들이 상기 방법과 함께 수행될 수도 있다.
- [0075] 도 4를 참조하면, 컴퓨팅 장치(102)는 새로운 논스 값을 생성하고, 무선 통신을 통해 논스 값을 브로드캐스팅(Broadcastion) 한다(S 401). 컴퓨팅 장치(102)는 기 설정된 주기에 따라 논스 값을 브로드캐스팅 할 수 있다. 여기서, 논스 값은 주기마다 다른 값을 가질 수 있다.
- [0076] 다음으로, 논스 값을 수신한 보조 인증 장치(104)는 키 값, 논스 값, 및 자신의 고유 아이디를 기 저장된 알고리즘에 입력하여 메시지 인증 코드를 생성한다(S 403). 각 보조 인증 장치(104)는 생성한 메시지 인증 코드를 컴퓨팅 장치(102)로 전송하게 된다.
- [0077] 다음으로, 컴퓨팅 장치(102)는 제1 메시지 인증 코드와 일치하는 보조 인증 장치(104)들로부터 수신한 제2 메시지 인증 코드의 개수가 기 설정된 개수 이상인지 여부를 확인한다(S 405).
- [0078] 단계 S 405의 확인 결과, 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드가 기 설정된 개수 미만인 경우, 컴퓨팅 장치(102)는 기 설정된 시간 동안 대기한 후(S 407), 단계 S 401로 복귀한다.
- [0079] 단계 S 405의 확인 결과, 제1 메시지 인증 코드와 일치하는 제2 메시지 인증 코드가 기 설정된 개수 이상인 경우, 컴퓨팅 장치(102)는 컴퓨팅 장치(102)의 잠금 상태를 해제하기 위한 1차 인증이 된 것으로 판단한다(S 409). 컴퓨팅 장치(102)는 1차 인증이 된 상태를 기 설정된 시간 동안 유지할 수 있다. 여기서, 기 설정된 시간은 컴퓨팅 장치(102)의 배터리 잔여량 또는 컴퓨팅 장치(102)의 사용 시간 패턴 등에 따라 적절하게 설정될 수 있다.
- [0080] 다음으로, 컴퓨팅 장치(102)는 기 설정된 시간이 경과하는지 여부를 확인한다(S 411). 단계 S 411의 확인 결과, 기 설정된 시간이 경과하는 경우, 컴퓨팅 장치(102)는 단계 S 401로 복귀하여 새로운 논스 값을 브로드캐스팅 할 수 있다.
- [0081] 단계 S 411의 확인 결과, 기 설정된 시간이 경과하지 않은 경우, 컴퓨팅 장치(102)는 사용자 인터페이스를 통해 컴퓨팅 장치(102)의 잠금 상태 해제를 위한 값이 입력되는지 여부를 확인한다(S 413).
- [0082] 단계 S 413의 확인 결과, 사용자 인터페이스를 통해 컴퓨팅 장치(102)의 잠금 상태 해제를 위한 값이 입력되는 경우, 컴퓨팅 장치(102)는 2차 인증을 수행하여 컴퓨팅 장치(102)의 잠금 상태를 제어한다(S 415). 구체적으로, 사용자 인터페이스를 통해 입력된 값이 기 설정된 인증값과 일치하는 경우, 컴퓨팅 장치(102)는 2차 인증이 성공된 것으로 판단하여 컴퓨팅 장치(102)의 잠금 상태를 해제할 수 있다. 사용자 인터페이스를 통해 입력된 값이 기 설정된 인증값과 일치하지 않는 경우, 컴퓨팅 장치(102)는 2차 인증이 실패한 것으로 판단할 수 있다.
- [0083] 여기서는, 2차 인증 방식이 "사용자의 직접 입력에 의한 인증"인 것으로 설명하였으나, 이에 한정되는 것은 아니며 그 이외의 다른 인증(예를 들어, 지문 인증 또는 얼굴 영상 인증 등) 방식을 사용할 수도 있다. 또한, 2차 인증은 1 단계의 인증 절차로 이루어질 수 있으나, 그에 한정되는 것은 아니며 여러 단계(또는 여러 개)의 인증 절차로 이루어질 수도 있다.
- [0084] 한편, 무선 통신에 의한 1차 인증이 되지 않은 상태에서, 2차 인증이 시도되는 경우, 컴퓨팅 장치(102)는 2차 인증 시도를 차단할 수 있다. 예를 들어, 컴퓨팅 장치(102)는 1차 인증이 되지 않은 상태에서는 사용자 인터페이스를 통한 값을 입력하기 위한 화면을 제공하지 않을 수 있다. 또는, 컴퓨팅 장치(102)는 2차 인증에 따른 입력 값을 무시하고 아직 1차 인증이 완료되지 않았다는 메시지를 화면 또는 음성으로 출력할 수도 있다.
- [0085] 본 실시예에 따른 경우, 컴퓨팅 장치(102)에서 주기적으로 1차 인증을 수행함으로써 정당한 사용자일 경우 2차 인증만으로 용이하게 잠금 상태를 해제할 수 있다. 즉, 본 실시예에 따른 경우 주기적으로 무선 통신에 의한 인증이 이루어진 상태에서 사용자의 직접 입력에 의한 인증이 이루어지는 바, 사용자의 직접 입력에 의한 인증 후 무선 통신에 의한 인증을 위하여 추가적으로 소요되는 시간을 절감할 수 있게 되어 사용자 편의성을 증대시킬 수 있다.
- [0086] 도 5는 예시적인 실시예들에서 사용되기에 적합한 예시적인 컴퓨팅 장치를 포함하는 컴퓨팅 환경을 도시한다.

- [0087] 도 5에 도시된 예시적인 컴퓨팅 환경(500)은 컴퓨팅 장치(510)를 포함한다. 통상적으로, 각 구성은 상이한 기능 및 능력을 가질 수 있고, 이하에 기술되지 않았더라도 그 구성에 적합한 컴포넌트를 추가적으로 포함할 수 있다. 컴퓨팅 장치(510)는 가령 휴대폰, 스마트폰, 휴대용 미디어 플레이어, 휴대용 게임 장치, PDA(Personal Digital Assistant), 태블릿, 랩톱 컴퓨터, 웨어러블 기기, PC, 출입 관리 장치, 보안 장치, 서버 등과 같이 사용자와 연관된 컴퓨팅 장치(예를 들어, 컴퓨팅 장치(102))일 수 있다. 또한, 컴퓨팅 장치(510)는 사용자의 신체 또는 사물에 장착되는 컴퓨팅 장치(예를 들어, 보조 인증 장치(104))일 수 있다. 컴퓨팅 장치(510)가 사용자의 신체 또는 사물에 장착되는 컴퓨팅 장치인 경우, 일부 구성(예를 들어, 입출력 장치(570) 및 입출력 인터페이스(520) 등)이 생략될 수 있다.
- [0088] 컴퓨팅 장치(510)는 적어도 하나의 프로세서(512), 컴퓨터 판독 가능 저장 매체(514) 및 버스(560)를 포함한다. 프로세서(512)는 버스(560)와 연결되고, 버스(560)는 컴퓨터 판독 가능 저장 매체(514)를 포함하여 컴퓨팅 장치(510)의 다른 다양한 컴포넌트들을 프로세서(512)에 연결한다.
- [0089] 프로세서(512)는 컴퓨팅 장치(510)로 하여금 앞서 언급된 예시적인 실시예에 따라 동작하도록 할 수 있다. 예컨대, 프로세서(512)는 컴퓨터 판독 가능 저장 매체(514)에 저장된 컴퓨터 실행 가능 명령어를 실행할 수 있고, 컴퓨터 판독 가능 저장 매체(514)에 저장된 컴퓨터 실행 가능 명령어는 프로세서(512)에 의해 실행되는 경우 컴퓨팅 장치(510)로 하여금 소정의 예시적인 실시예에 따른 동작들을 수행하도록 구성될 수 있다.
- [0090] 컴퓨터 판독 가능 저장 매체(514)는 컴퓨터 실행 가능 명령어 내지 프로그램 코드(예컨대, 애플리케이션(530)에 포함되는 명령어), 프로그램 데이터(예컨대, 애플리케이션(530)에 의해 사용되는 데이터) 및/또는 다른 적합한 형태의 정보를 저장하도록 구성된다. 컴퓨터 판독 가능 저장 매체(514)에 저장된 애플리케이션(530)은 프로세서(512)에 의해 실행 가능한 명령어의 소정의 집합을 포함한다.
- [0091] 도 5에 도시된 메모리(516) 및 저장 장치(518)는 컴퓨터 판독 가능 저장 매체(514)의 예이다. 메모리(516)에는 프로세서(512)에 의해 실행될 수 있는 컴퓨터 실행 가능 명령어가 로딩될 수 있다. 또한, 메모리(516)에는 프로그램 데이터가 저장될 수 있다. 예컨대, 이러한 메모리(516)는 랜덤 액세스 메모리와 같은 휘발성 메모리, 비휘발성 메모리, 또는 이들의 적합한 조합일 수 있다. 다른 예로서, 저장 장치(518)는 정보의 저장을 위한 하나 이상의 착탈 가능하거나 착탈 불가능한 컴포넌트를 포함할 수 있다. 예컨대, 저장 장치(518)는 하드 디스크, 플래시 메모리, 자기 디스크, 광 디스크, 컴퓨팅 장치(510)에 의해 액세스되고 원하는 정보를 저장할 수 있는 다른 형태의 저장 매체, 또는 이들의 적합한 조합일 수 있다.
- [0092] 컴퓨팅 장치(510)는 또한 하나 이상의 입출력 장치(570)를 위한 인터페이스를 제공하는 하나 이상의 입출력 인터페이스(520)를 포함할 수 있다. 입출력 인터페이스(520)는 버스(560)에 연결된다. 입출력 장치(570)는 입출력 인터페이스(520)를 통해 컴퓨팅 장치(510)(의 다른 컴포넌트들)에 연결될 수 있다. 입출력 장치(570)는 포인팅 장치, 키보드, 터치 입력 장치, 음성 입력 장치, 센서 장치 및/또는 촬영 장치와 같은 입력 장치 및/또는 디스플레이 장치, 프린터, 스피커 및/또는 네트워크 카드와 같은 출력 장치를 포함할 수 있다.
- [0093] 한편, 소정의 실시예는 본 명세서에서 기술한 과정을 컴퓨터상에서 수행하기 위한 프로그램을 포함하는 컴퓨터 판독 가능 저장 매체를 포함할 수 있다. 이러한 컴퓨터 판독 가능 저장 매체는 프로그램 명령, 로컬 데이터 파일, 로컬 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 그 컴퓨터 판독 가능 저장 매체는 본 발명을 위하여 특별히 설계되고 구성된 것들일 수 있다. 컴퓨터 판독 가능 저장 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD와 같은 광 기록 매체, 플롭티컬 디스크와 같은 자기-광 매체, 및 롬, 램, 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함할 수 있다.
- [0094] 이상에서 본 발명의 대표적인 실시예들을 상세하게 설명하였으나, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자는 상술한 실시예에 대하여 본 발명의 범주에서 벗어나지 않는 한도 내에서 다양한 변형이 가능함을 이해할 것이다. 그러므로 본 발명의 권리범위는 설명된 실시예에 국한되어 정해져서는 안 되며, 후술하는 특허 청구범위뿐만 아니라 이 특허청구범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

[0095]

100 : 인증 시스템

102 : 컴퓨팅 장치

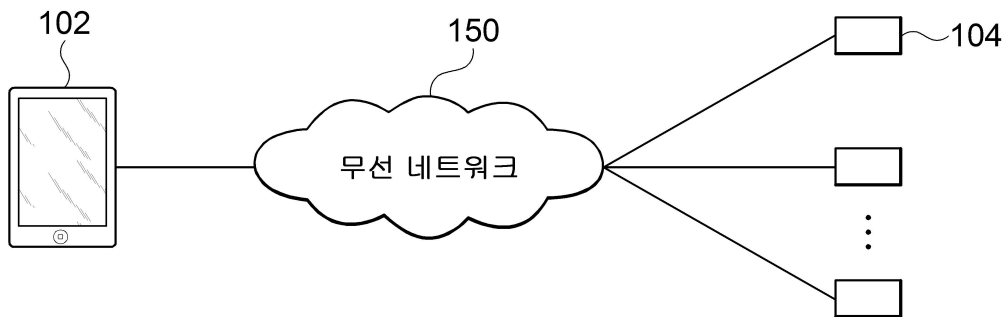
104 : 보조 인증 장치

150 : 무선 네트워크

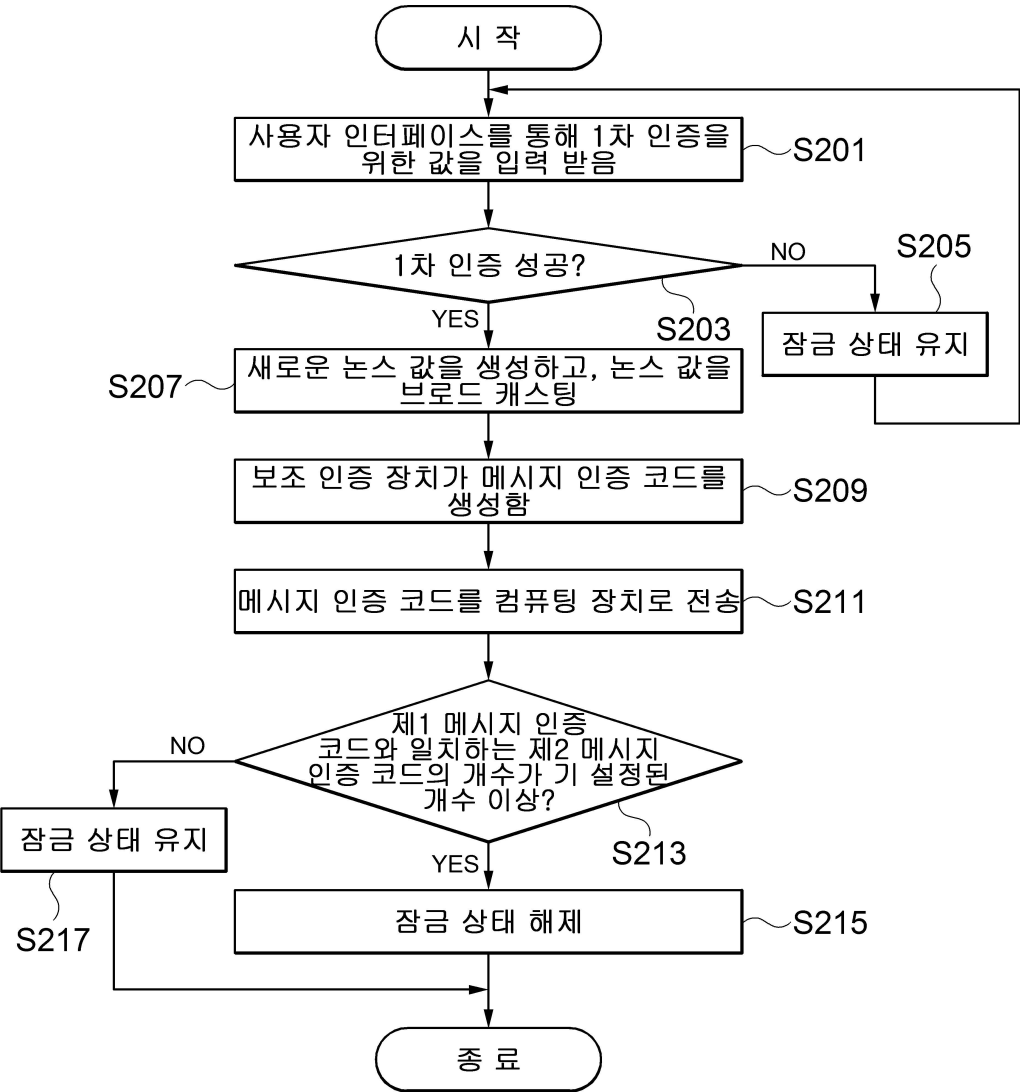
도면

도면1

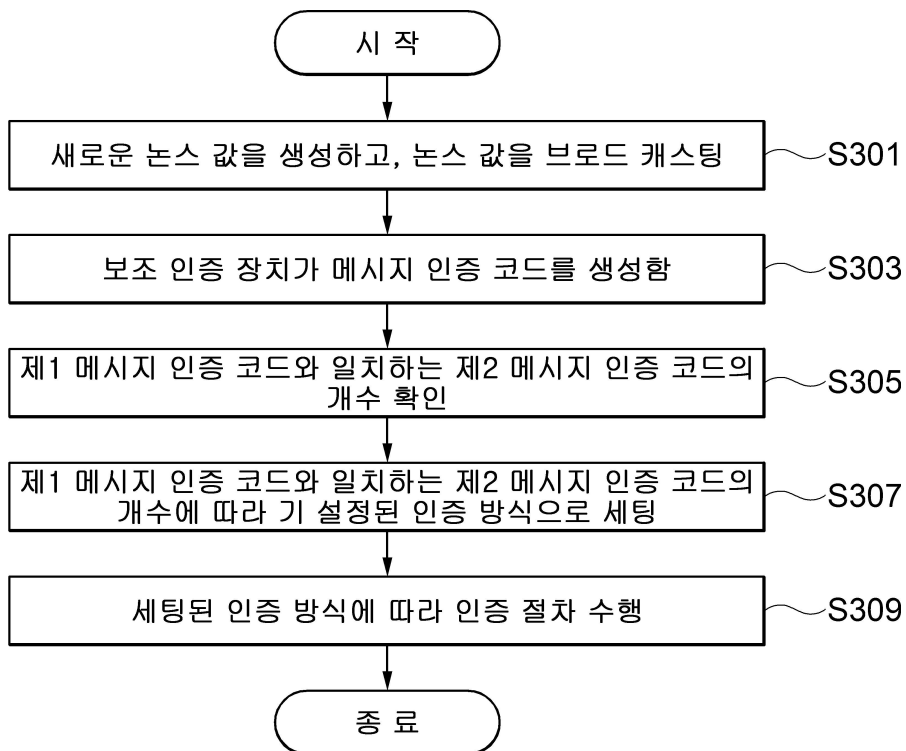
100



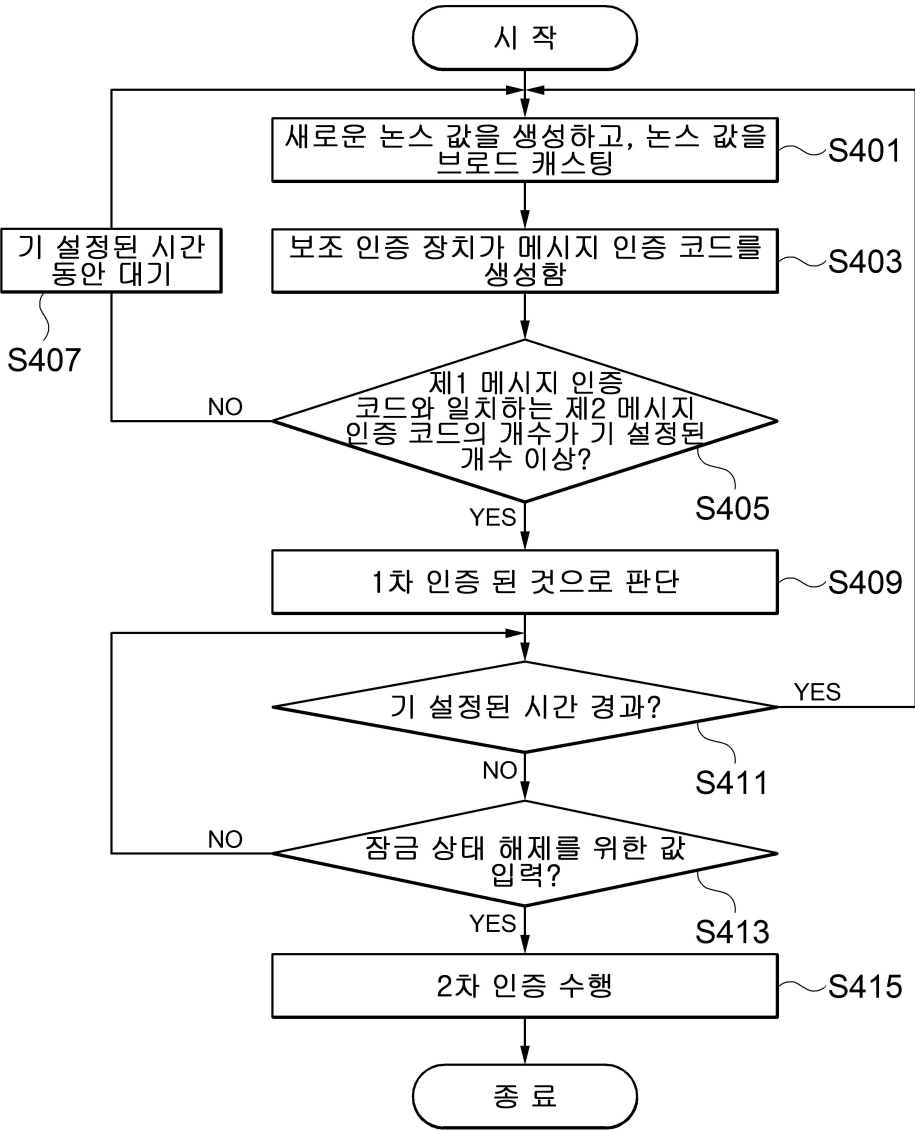
도면2



도면3



도면4



도면5

500

