(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0054148
(43) 공개일자 2022년05월02일

(51) 국제특허분류(Int. Cl.)
G06F 8/65 (2018.01) *G06F 21/57* (2013.01)
G06F 21/60 (2013.01) *G06F 8/61* (2018.01)
(52) CPC특허분류
G06F 8/65 (2013.01)
G06F 21/57 (2013.01)
(21) 출원번호 10-2020-0186925
(22) 출원일자 2020년12월30일
심사청구일자 2020년12월30일
(30) 우선권주장
1020200138502 2020년10월23일 대한민국(KR)

(71) 출원인
고려대학교 산학협력단
서울특별시 성북구 안암로 145, 고려대학교 (안암동5가)
(72) 발명자
이동훈
서울특별시 종로구 사직로8길 34, 경희궁의아침 3단지 1404호
박승범
서울특별시 성북구 오패산로 90, 121동 1104호(하월곡동, 래미안월곡아파트)
(뒷면에 계속)
(74) 대리인
이대호, 박건홍

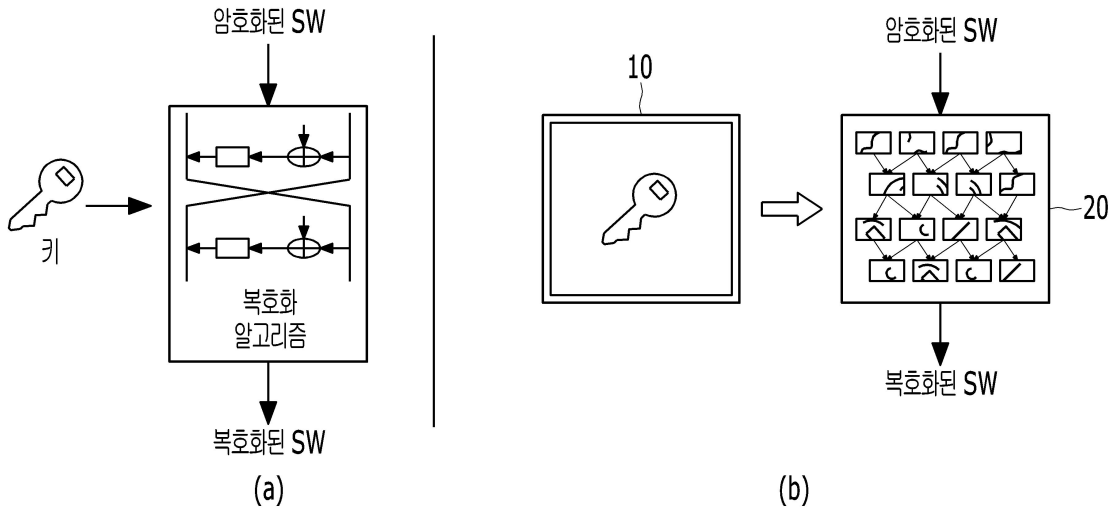
전체 청구항 수 : 총 8 항

(54) 발명의 명칭 **화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법**

(57) 요 약

본 개시의 몇몇 실시예에 따라, 차량과 관련된 컴퓨팅 장치의 프로세서에 의해 수행되는 차량 소프트웨어 업데이트 방법이 개시된다. 상기 방법은: 서버로부터 암호화된 소프트웨어를 수신하는 단계; 메모리에 저장된 화이트박스 복호화 알고리즘에 차량 고유 정보 및 상기 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득하는 단계; 및 상기 복호화된 소프트웨어를 이용하여 상기 차량 소프트웨어를 업데이트하는 단계;를 포함하고, 상기 화이트박스 복호화 알고리즘은, 상기 차량 고유 정보를 기초로 락킹된 화이트박스 테이블을 포함하고, 상기 화이트박스 테이블은, 상기 암호화된 소프트웨어의 암호화 키가 분산되어 저장된 테이블일 수 있다.

대 표 도 - 도3



(52) CPC특허분류
G06F 21/602 (2013.01)
G06F 8/61 (2013.01)

(72) 발명자
문혜란
경기도 성남시 분당구 정자일로 80, 408동(정자동, 상록마을보성아파트)

이선우
서울특별시 서초구 남부순환로309길 38, 5동 522호(방배동, 서초중앙하이츠빌라)

이 발명을 지원한 국가연구개발사업

과제고유번호	1615011292
과제번호	20TLRP-B152761-02
부처명	국토교통부
과제관리(전문)기관명	국토교통과학기술진흥원
연구사업명	교통물류연구(일반) 사업
연구과제명	자율협력주행 환경 도로교통체계 보안관제시스템 기술개발 및 테스트베드 구축
기 여 율	1/1
과제수행기관명	한국도로공사
연구기간	2019.04.30 ~ 2022.12.31

명 세 서

청구범위

청구항 1

차량과 관련된 컴퓨팅 장치의 프로세서에 의해 수행되는 차량 소프트웨어 업데이트 방법에 있어서,

서버로부터 암호화된 소프트웨어를 수신하는 단계;

메모리에 저장된 화이트박스 복호화 알고리즘에 차량 고유 정보 및 상기 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득하는 단계; 및

상기 복호화된 소프트웨어를 이용하여 상기 차량 소프트웨어를 업데이트하는 단계;

를 포함하고,

상기 화이트박스 복호화 알고리즘은,

상기 차량 고유 정보를 기초로 락킹된 화이트박스 테이블을 포함하고,

상기 화이트박스 테이블은,

상기 암호화된 소프트웨어의 암호화 키가 분산되어 저장된 테이블인,

차량 소프트웨어 업데이트 방법.

청구항 2

제 1 항에 있어서,

상기 암호화된 소프트웨어는,

상기 차량 소프트웨어의 업데이트에 이용되는 업데이트용 소프트웨어가 화이트박스 암호화 알고리즘에 입력됨에 따라 암호화되고,

상기 화이트박스 암호화 알고리즘은,

상기 화이트박스 테이블을 포함하는,

차량 소프트웨어 업데이트 방법.

청구항 3

제 1 항에 있어서,

상기 차량 고유 정보는,

상기 차량을 식별할 수 있는 차대번호에 대한 정보, 차량번호에 대한 정보, 차량 고유의 비밀번호에 대한 정보 및 차량모델에 대한 정보 중 적어도 하나를 포함하는,

차량 소프트웨어 업데이트 방법.

청구항 4

제 1 항에 있어서,

상기 서버로부터 암호화된 소프트웨어를 수신하는 단계는,

상기 서버로부터 암호화된 소프트웨어를 수신하기 전에 상기 서버로부터 소프트웨어 업데이트 알림 신호를 수신하는 단계;

상기 소프트웨어 업데이트 알림 신호에 대응하여, 소프트웨어 업데이트 요청 신호를 상기 서버로 전송하는 단계; 및

상기 서버로 상기 소프트웨어 업데이트 요청 신호를 전송한 후, 상기 서버로부터 상기 암호화된 소프트웨어를 수신하는 단계;

를 포함하는,

차량 소프트웨어 업데이트 방법.

청구항 5

제 1 항에 있어서,

상기 차량 소프트웨어의 업데이트가 완료된 경우, 상기 차량 소프트웨어의 업데이트 결과에 대한 업데이트 결과 정보를 상기 서버로 전송하는 단계;

를 더 포함하는,

차량 소프트웨어 업데이트 방법.

청구항 6

제 5 항에 있어서,

상기 서버로 상기 차량 소프트웨어의 업데이트 실패에 대한 상기 업데이트 결과 정보를 전송한 경우, 상기 서버로부터 상기 화이트박스 테이블을 업데이트 하기 위한 업데이트 정보를 수신하는 단계; 및

상기 업데이트 정보에 기초하여, 상기 화이트박스 테이블을 업데이트하는 단계;

를 더 포함하는,

차량 소프트웨어 업데이트 방법.

청구항 7

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램으로서,

상기 컴퓨터 프로그램은 차량과 관련된 컴퓨팅 장치의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은:

서버로부터 암호화된 소프트웨어를 수신하는 단계;

메모리에 저장된 화이트박스 복호화 알고리즘에 차량 고유 정보 및 상기 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득하는 단계; 및

상기 복호화된 소프트웨어를 이용하여 차량 소프트웨어를 업데이트하는 단계;

를 포함하고,

상기 화이트박스 복호화 알고리즘은,

상기 차량 고유 정보를 기초로 락킹된 화이트박스 테이블을 포함하고,

상기 화이트박스 테이블은,

상기 암호화된 소프트웨어의 암호화 키가 분산되어 저장된 테이블인,

컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램.

청구항 8

차량과 관련된 컴퓨팅 장치로서,

서버로부터 암호화된 소프트웨어를 수신하는 통신부;

화이트박스 복호화 알고리즘을 저장하고 있는 메모리; 및

상기 화이트박스 복호화 알고리즘에 차량 고유 정보 및 상기 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득하는 프로세서;

를 포함하고,

상기 프로세서는,

상기 복호화된 소프트웨어를 이용하여 차량 소프트웨어를 업데이트하고,

상기 화이트박스 복호화 알고리즘은,

상기 차량 고유 정보를 기초로 락킹된 화이트박스 테이블을 포함하고,

상기 화이트박스 테이블은,

상기 암호화된 소프트웨어의 암호화 키가 분산되어 저장된 테이블인,

차량과 관련된 컴퓨팅 장치.

발명의 설명

기 술 분 야

[0001] 본 개시는 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법에 관한 것으로, 보다 구체적으로 화이트박스 암호를 이용하여 차량에서의 안전한 Over-the-air(OTA) 소프트웨어 업데이트를 제공하는 기법에 관한 것이다.

배 경 기 술

[0002] 도 1을 참조하면, 최근의 스마트 차량들은 차량 내 소프트웨어의 OTA 서비스를 제공하고 있다. 기존에 물리적 연결을 통해 소프트웨어를 업데이트 하는 방법에 비해, OTA를 통해 보다 쉽게 차량 내 소프트웨어 업데이트가 가능하다. 이에 따라, OTA에 대한 요구가 점차 증가하고 있는 추세이다. 하지만, OTA를 통해 차량의 소프트웨어 업데이트를 진행하는 경우, 업데이트 된 소프트웨어에 악성 코드가 삽입되거나, 또는 허가되지 않은 차량에 올바르지 않은 소프트웨어가 업데이트 될 경우, 차량의 사고로 이어져 인명피해로 이어 질 수 있다는 우려가 존재한다.

[0003] 최근에는 안전한 소프트웨어 업데이트를 지원하기 위해 대칭키(Symmetric key), 해쉬체인(Hash Chain) 등과 같은 암호 기술을 적용하거나 안전한 하드웨어 모듈(HSM: Hardware Security Module)를 사용하는 방법들이 제안되고 있다.

[0004] 하지만, 소프트웨어 업데이트에 대칭키 및 해쉬체인과 같은 암호 기술을 적용할 경우, 소프트웨어의 기밀성 제공을 위해 미리 공유한 대칭키 관리 및 저장의 문제의 단점이 존재할 수 있다. 한편, 소프트웨어 업데이트에 HSM을 사용하는 경우, 추가적인 암호기술 적용보다 좀 더 안전할 수 있지만, 추가적인 하드웨어 사용으로 인한 추가 비용이 발생될 수 있다.

[0005] 따라서, 적절한 비용으로 소프트웨어의 기밀성을 유지하면서, 소프트웨어 업데이트가 안전하게 진행될 수 있는 기법에 대한 수요가 당업계에 존재할 수 있다.

선행기술문헌

비특허문헌

[0006] (비특허문헌 0001) Kim, Geunhyoung, and Im Y. Jung. "Integrity Assurance of OTA Software Update in Smart Vehicles." International Journal on Smart Sensing & Intelligent Systems 12.1(2019)

발명의 내용

해결하려는 과제

[0007] 본 개시는 전술한 배경기술에 대응하여 안출된 것으로, 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법을 제공하고자 한다.

[0008] 본 개시의 기술적 과제들은 이상에서 언급한 기술적 과제로 제한되지 않으며, 언급되지 않은 또 다른 기술적 과제들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0009] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 실시예에 따라, 차량과 관련된 컴퓨팅 장치의 프로세서에 의해 수행되는 차량 소프트웨어 업데이트 방법이 개시된다. 상기 방법은: 서버로부터 암호화된 소프트웨어를 수신하는 단계; 메모리에 저장된 화이트박스 복호화 알고리즘에 차량 고유 정보 및 상기 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득하는 단계; 및 상기 복호화된 소프트웨어를 이용하여 상기 차량 소프트웨어를 업데이트하는 단계;를 포함하고, 상기 화이트박스 복호화 알고리즘은, 상기 차량 고유 정보를 기초로 락킹된 화이트박스 테이블을 포함하고, 상기 화이트박스 테이블은, 상기 암호화된 소프트웨어의 암호화 키가 분산되어 저장된 테이블일 수 있다.

[0010] 또한, 상기 암호화된 소프트웨어는, 상기 차량 소프트웨어의 업데이트에 이용되는 업데이트용 소프트웨어가 화이트박스 암호화 알고리즘에 입력됨에 따라 암호화되고, 상기 화이트박스 암호화 알고리즘은, 상기 화이트박스 테이블을 포함할 수 있다.

[0011] 또한, 상기 차량 고유 정보는, 상기 차량을 식별할 수 있는 차대번호에 대한 정보, 차량번호에 대한 정보, 차량 고유의 비밀번호에 대한 정보 및 차량모델에 대한 정보 중 적어도 하나를 포함할 수 있다.

[0012] 또한, 상기 서버로부터 암호화된 소프트웨어를 수신하는 단계는, 상기 서버로부터 암호화된 소프트웨어를 수신하기 전에 상기 서버로부터 소프트웨어 업데이트 알림 신호를 수신하는 단계; 상기 소프트웨어 업데이트 알림 신호에 대응하여, 소프트웨어 업데이트 요청 신호를 상기 서버로 전송하는 단계; 및 상기 서버로 상기 소프트웨어 업데이트 요청 신호를 전송한 후, 상기 서버로부터 상기 암호화된 소프트웨어를 수신하는 단계;를 포함할 수 있다.

[0013] 또한, 상기 방법은, 상기 차량 소프트웨어의 업데이트가 완료된 경우, 상기 차량 소프트웨어의 업데이트 결과에 대한 업데이트 결과 정보를 상기 서버로 전송하는 단계;를 더 포함할 수 있다.

[0014] 또한, 상기 방법은, 상기 서버로 상기 차량 소프트웨어의 업데이트 실패에 대한 상기 업데이트 결과 정보를 전송한 경우, 상기 서버로부터 상기 화이트박스 테이블을 업데이트 하기 위한 업데이트 정보를 수신하는 단계; 및 상기 업데이트 정보에 기초하여, 상기 화이트박스 테이블을 업데이트하는 단계;를 더 포함할 수 있다.

[0015] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 실시예에 따라, 컴퓨터 판독가능 저장 매체에 저장된 컴퓨터 프로그램이 개시된다. 상기 컴퓨터 프로그램은 차량과 관련된 컴퓨팅 장치의 프로세서로 하여금 이하의 단계들을 수행하기 위한 명령들을 포함하며, 상기 단계들은: 서버로부터 암호화된 소프트웨어를 수신하는 단계; 메모리에 저장된 화이트박스 복호화 알고리즘에 차량 고유 정보 및 상기 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득하는 단계; 및 상기 복호화된 소프트웨어를 이용하여 차량 소프트웨어를 업데이트하는 단계;를 포함하고, 상기 화이트박스 복호화 알고리즘은, 상기 차량 고유 정보를 기초로 락킹된 화이트박스 테이블을 포함하고, 상기 화이트박스 테이블은, 상기 암호화된 소프트웨어의 암호화 키가 분산되어 저장된 테이블일 수 있다.

[0016] 전술한 바와 같은 과제를 해결하기 위한 본 개시의 몇몇 실시예에 따라, 차량과 관련된 컴퓨팅 장치가 개시된다. 상기 장치는: 서버로부터 암호화된 소프트웨어를 수신하는 통신부; 화이트박스 복호화 알고리즘을 저

장하고 있는 메모리; 및 상기 화이트박스 복호화 알고리즘에 차량 고유 정보 및 상기 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득하는 프로세서;를 포함하고, 상기 프로세서는, 상기 복호화된 소프트웨어를 이용하여 차량 소프트웨어를 업데이트하고, 상기 화이트박스 복호화 알고리즘은, 상기 차량 고유 정보를 기초로 락킹된 화이트박스 테이블을 포함하고, 상기 화이트박스 테이블은, 상기 암호화된 소프트웨어의 암호화 키가 분산되어 저장된 테이블일 수 있다.

[0017] 본 개시에서 얻을 수 있는 기술적 해결 수단은 이상에서 언급한 해결 수단들로 제한되지 않으며, 언급하지 않은 또 다른 해결 수단들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

발명의 효과

[0018] 본 개시는 업데이트되는 소프트웨어에 대한 기밀성뿐만 아니라 차량에 올바른 소프트웨어가 설치되도록 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기술을 제공할 수 있다.

[0019] 본 개시에서 얻을 수 있는 효과는 이상에서 언급한 효과로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

도면의 간단한 설명

[0020] 다양한 양상들이 이제 도면들을 참조로 기재되며, 여기서 유사한 참조 번호들은 총괄적으로 유사한 구성요소들을 지칭하는데 이용된다. 이하의 실시예에서, 설명 목적을 위해, 다수의 특정 세부사항들이 하나 이상의 양상들의 총체적 이해를 제공하기 위해 제시된다. 그러나, 그러한 양상(들)이 이러한 특정 세부사항들 없이 실시될 수 있음은 명백할 것이다. 다른 예시들에서, 공지의 구조들 및 장치들이 하나 이상의 양상들의 기재를 용이하게 하기 위해 블록도 형태로 도시된다.

도 1은 종래의 차량 내 소프트웨어의 OTA 서비스의 개요를 도시한 도면이다.

도 2는 본 개시의 몇몇 실시예에 따른 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 방법을 수행하기 위한 차량과 관련된 컴퓨팅 장치의 블록 구성도이다.

도 3은 종래의 소프트웨어 암호화 방식과 본 개시의 소프트웨어 암호화 방식의 개요를 도시한 도면이다.

도 4 및 도 5는 본 개시의 몇몇 실시예에 따른 소프트웨어의 암호화 및 복호화 방식의 일례를 설명하기 위한 도면이다.

도 6은 본 개시의 몇몇 실시예에 따른 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 방법의 일례를 설명하기 위한 흐름도이다.

도 7은 본 개시내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도를 도시한다.

발명을 실시하기 위한 구체적인 내용

[0021] 다양한 실시예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 감지될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다. 구체적으로, 본 명세서에서 사용되는 "실시예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하다거나, 이점이 있는 것으로 해석되지 않을 수도 있다.

[0022] 이하, 도면 부호에 관계없이 동일하거나 유사한 구성 요소는 동일한 참조 번호를 부여하고 이에 대한 중복되는 설명은 생략한다. 또한, 본 명세서에 개시된 실시예를 설명함에 있어서 관련된 공지 기술에 대한 구체적인 설명이 본 명세서에 개시된 실시예의 요지를 흐릴 수 있다고 판단되는 경우 그 상세한 설명을 생략한다. 또한, 첨부된 도면은 본 명세서에 개시된 실시예를 쉽게 이해할 수 있도록 하기 위한 것일 뿐, 첨부된 도면에 의해 본 명세서에 개시된 기술적 사상이 제한되지 않는다.

[0023] 비록 제 1, 제 2 등이 다양한 소자나 구성요소들을 서술하기 위해서 사용되나, 이들 소자나 구성요소들은 이들 용어에 의해 제한되지 않음은 물론이다. 이들 용어들은 단지 하나의 소자나 구성요소를 다른 소자나 구성요소와 구별하기 위하여 사용하는 것이다. 따라서, 이하에서 언급되는 제 1 소자나 구성요소는 본 발명의 기술적 사상 내에서 제 2 소자나 구성요소 일 수도 있음은 물론이다.

[0024] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0025] 더불어, 용어 "또는"은 배타적 "또는"이 아니라 내포적 "또는"을 의미하는 것으로 의도된다. 즉, 달리 특정되지 않거나 문맥상 명확하지 않은 경우에, "X는 A 또는 B를 이용한다"는 자연적인 내포적 치환 중 하나를 의미하는 것으로 의도된다. 즉, X가 A를 이용하거나; X가 B를 이용하거나; 또는 X가 A 및 B 모두를 이용하는 경우, "X는 A 또는 B를 이용한다"가 이들 경우들 어느 것으로도 적용될 수 있다. 또한, 본 명세서에 사용된 "및/또는"이라는 용어는 열거된 관련 아이템들 중 하나 이상의 아이템의 가능한 모든 조합을 지칭하고 포함하는 것으로 이해되어야 한다.

[0026] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다. 또한, 달리 특정되지 않거나 단수 형태를 지시하는 것으로 문맥상 명확하지 않은 경우에, 본 명세서와 청구범위에서 단수는 일반적으로 "하나 또는 그 이상"을 의미하는 것으로 해석되어야 한다.

[0027] 더불어, 본 명세서에서 사용되는 용어 "정보" 및 "데이터"는 종종 서로 상호교환 가능하도록 사용될 수 있다.

[0028] 어떤 구성 요소가 다른 구성 요소에 “연결되어” 있다거나 “접속되어” 있다고 언급된 때에는, 그 다른 구성 요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성 요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성 요소가 다른 구성 요소에 “직접 연결되어” 있다거나 “직접 접속되어”있다고 언급된 때에는, 중간에 다른 구성 요소가 존재하지 않는 것으로 이해되어야 할 것이다.

[0029] 이하의 설명에서 사용되는 구성 요소에 대한 접미사 “모듈” 및 “부”는 명세서 작성의 용이함만이 고려되어 부여되거나 혼용되는 것으로서 그 자체로 서로 구별되는 의미 또는 역할을 갖는 것은 아니다.

[0030] 본 개시의 목적 및 효과, 그리고 그것들을 달성하기 위한 기술적 구성들은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 본 개시를 설명하는데 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 개시의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 개시에서의 기능을 고려하여 정의된 용어들로써 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다.

[0031] 그러나 본 개시는 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있다. 단지 본 실시예들은 본 개시가 완전하도록 하고, 본 개시가 속하는 기술분야에서 통상의 지식을 가진 자에게 개시의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 개시는 청구항의 범주에 의해 정의될 뿐이다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0033] 도 2는 본 개시의 몇몇 실시예에 따른 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 방법을 수행하기 위한 차량과 관련된 컴퓨팅 장치의 블록 구성도이다.

[0034] 도 2를 참조하면, 컴퓨팅 장치(100)는 프로세서(110), 통신부(120) 및 메모리(130)를 포함할 수 있다. 다만, 상술한 구성 요소들은 컴퓨팅 장치(100)를 구현하는데 있어서 필수적인 것은 아니어서, 컴퓨팅 장치(100)는 위에서 열거된 구성요소들 보다 많거나, 또는 적은 구성요소들을 가질 수 있다.

[0035] 본 개시의 몇몇 실시예에 따른 컴퓨팅 장치(100)는 차량과 관련될 수 있다. 구체적으로, 컴퓨팅 장치(100)는 차량에 구비되어, 차량의 다양한 기능을 제어할 수 있다.

[0036] 컴퓨팅 장치(100)는 예를 들어, 마이크로프로세서, 메인프레임 컴퓨터, 디지털 프로세서, 휴대용 디바이스 및 디바이스 제어기 등과 같은 임의의 타입의 컴퓨터 시스템 또는 컴퓨터 디바이스를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0037] 컴퓨팅 장치(100)의 프로세서(110)는 통상적으로 컴퓨팅 장치(100)의 전반적인 동작을 제어한다. 프로세서(110)는 컴퓨팅 장치(100)에 포함된 구성요소들을 통해 입력 또는 출력되는 신호, 데이터, 정보 등을 처리하거나 메모리(130)에 저장된 응용 프로그램을 구동함으로써, 사용자에게 적절한 정보 또는 기능을 제공 또는 처리할 수 있다.

[0038] 또한, 프로세서(110)는 메모리(130)에 저장된 응용 프로그램을 구동하기 위하여, 컴퓨팅 장치(100)의 구성요소들 중 적어도 일부를 제어할 수 있다. 나아가, 프로세서(110)는 상기 응용 프로그램의 구동을 위하여, 컴퓨팅 장치(100)에 포함된 구성요소들 중 적어도 둘 이상을 서로 조합하여 동작시킬 수 있다.

[0039] 본 개시의 몇몇 실시예에 따르면, 컴퓨팅 장치(100)의 프로세서(110)는 서버로부터 차량을 업데이트하기 위한 업데이트용 소프트웨어를 수신하도록 통신부(120)를 제어할 수 있다.

[0040] 구체적으로, 프로세서(110)는 서버로부터 차량을 업데이트하기 위한 암호화된 소프트웨어를 수신하도록 통신부(120)를 제어할 수 있다. 이 경우, 프로세서(110)는 화이트박스 복호화 알고리즘에 차량 고유 정보 및 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득할 수 있다. 그리고, 프로세서(110)는 복호화된 소프트웨어를 이용하여 차량 소프트웨어를 업데이트할 수 있다.

[0041] 본 개시의 서버는 차량 제조사 또는, 차량 소프트웨어 관리 업체와 관련될 수 있다. 구체적으로, 서버는 차량에 구비된 컴퓨팅 장치(100)의 소프트웨어를 주기적으로 업데이트하기 위한 업데이트용 소프트웨어를 차량으로 전송하여, 차량을 관리할 수 있다.

[0042] 이하, 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 방법에 대한 설명은 도 3 내지 도 6을 참조하여 후술한다.

[0043] 컴퓨팅 장치(100)의 통신부(120)는, 컴퓨팅 장치(100)와 차량 사이 또는 컴퓨팅 장치(100)와 사용자 단말 사이의 통신을 가능하게 하는 하나 이상의 모듈을 포함할 수 있다. 또한, 상기 통신부(120)는, 컴퓨팅 장치(100)를 하나 이상의 네트워크에 연결하는 하나 이상의 모듈을 포함할 수 있다.

[0044] 컴퓨팅 장치(100)와 차량 사이의 통신을 연결하는 네트워크는 임의의 형태의 데이터 및 신호 등을 송수신할 수 있는 임의의 유무선 통신 네트워크일 수 있다.

[0045] 본 개시의 실시예들에 따른 네트워크는 유선 및 무선 등과 같은 그 통신 양태를 가리지 않고 구성될 수 있으며, 단거리 통신망(LAN: Local Area Network), 원거리 통신망(WAN: Wide Area Network) 등 다양한 통신망으로 구성될 수 있다. 또한, 상기 네트워크는 공지의 월드와이드웹(WWW:World Wide Web)일 수 있으며, 적외선(IrDA:Infrared Data Association) 또는 블루투스(Bluetooth)와 같이 단거리 통신에 이용되는 무선 전송 기술을 이용할 수도 있다.

[0046] 본 명세서에서 설명된 기술들은 위에서 언급된 네트워크들뿐만 아니라, 다른 네트워크들에서도 사용될 수 있다.

[0047] 컴퓨팅 장치(100)의 메모리(130)는 프로세서(110)의 동작을 위한 프로그램을 저장할 수 있고, 입/출력되는 데이터들을 임시 또는 영구 저장할 수도 있다. 메모리(130)는 플래시 메모리 타입(flash memory type), 하드디스크 타입(hard disk type), 멀티미디어 카드 마이크로 타입(multimedia card micro type), 카드 타입의 메모리(예를 들어 SD 또는 XD 메모리 등), 램(Random Access Memory, RAM), SRAM(Static Random Access Memory), 롬(Read-Only Memory, ROM), EEPROM(Electrically Erasable Programmable Read-Only Memory), PROM(Programmable Read-Only Memory), 자기 메모리, 자기 디스크, 광디스크 중 적 어도 하나의 타입의 저장매체를 포함할 수 있다. 이러한 메모리(130)는 프로세서(110)에 제어에 의하여 동작 될 수 있다.

[0048] 소프트웨어적인 구현에 의하면, 본 명세서에서 설명되는 절차 및 기능과 같은 실시예들은 별도의 소프트웨어 모듈들로 구현될 수 있다. 상기 소프트웨어 모듈들 각각은 본 명세서에서 설명되는 하나 이상의 기능 및 작동을 수행할 수 있다. 적절한 프로그램 언어로 쓰여진 소프트웨어 어플리케이션으로 소프트웨어 코드가 구현될 수 있다. 상기 소프트웨어 코드는 컴퓨팅 장치(100)의 메모리(130)에 저장되고, 컴퓨팅 장치(100)의 프로세서(110)에 의해 실행될 수 있다.

[0050] 도 3은 종래의 소프트웨어 암호화 방식과 본 개시의 소프트웨어 암호화 방식의 개요를 도시한 도면이다.

[0051] 먼저, 도 3의 (a)를 참조하면, 종래의 대칭키 암호화 방식의 개요이다. 도시된 바와 같이, 종래의 대칭키 암호화 방식은 암호화 및 복호화에 암호화 키가 사용될 수 있다. 이 경우, 암호화 키를 저장하거나, 전송할 때 높은

수준의 보안이 요구될 수 있다.

[0052] 한편, 도 3의 (b)를 참조하면, 본 개시의 암호화 방식은 암호화 키를 이용해 소프트웨어에 대한 암호화를 수행할 수 있다.

[0053] 구체적으로, 본 개시의 암호화 키는 화이트박스 암호화 방식이 이용될 수 있다.

[0054] 좀더 구체적으로, 화이트박스 암호화 방식에서 암호화 키(10)는 복잡한 암호 알고리즘을 통해 소프트웨어에 뒤섞여 삽입되어 분산된 형태로 변경될 수 있다. 즉, 화이트박스 암호화 방식은 화이트박스 테이블(20)을 암호화 키처럼 사용될 수 있다.

[0055] 따라서, 본 개시의 차량 소프트웨어 업데이트 방법은 암호화 키가 분산되는 화이트박스 암호화 방식을 통해 암호화 키 추출이 불가능하도록 하여 기존의 대칭키 암호화 방식보다 차량 소프트웨어에 대한 기밀성을 높일 수 있다.

[0056] 또한, 본 개시의 차량 소프트웨어 업데이트 방법은 악의적인 사용자에 의해 소프트웨어에 악성코드가 삽입되는 것을 막을 수 있다. 즉, 본 개시의 차량 소프트웨어 업데이트 방법은 차량 소프트웨어에 대한 안전성을 보장할 수 있다.

[0057] 이하, 도 4 및 도 5를 참조하여 화이트박스 암호화 방식이 이용된 차량용 소프트웨어 업데이트 방법을 설명한다.

[0059] 도 4 및 도 5는 본 개시의 몇몇 실시예에 따른 소프트웨어의 암호화 및 복호화 방식을 설명하기 위한 도면이다.

[0060] 도 4을 참조하면, 컴퓨팅 장치(100)의 프로세서(110)는 통신부(120)를 통해 서버로부터 암호화된 소프트웨어를 수신할 수 있다(S110).

[0061] 구체적으로, 컴퓨팅 장치(100)의 프로세서(110)는 서버로부터 암호화된 소프트웨어를 수신하기 전에 통신부(120)를 통해 상기 서버로부터 소프트웨어 업데이트 알림 신호를 수신할 수 있다. 이 경우, 프로세서(110)는 소프트웨어 업데이트 알림 신호에 대응하여, 소프트웨어 업데이트 요청 신호를 서버로 전송하도록 통신부(120)를 제어할 수 있다. 그리고, 프로세서(110)는 서버로 소프트웨어 업데이트 요청 신호를 전송한 후, 통신부(120)를 통해 상기 서버로부터 암호화된 소프트웨어를 수신할 수 있다.

[0062] 즉, 본 개시의 컴퓨팅 장치(100)는 차량과 관련될 수 있다. 구체적으로, 컴퓨팅 장치(100)는 차량에 구비되어, 차량의 다양한 기능을 제어할 수 있다. 한편, 본 개시의 서버는 차량 제조사 또는, 차량 소프트웨어 관리 업체와 관련될 수 있다. 구체적으로, 서버는 차량에 구비된 컴퓨팅 장치(100)의 소프트웨어를 주기적으로 업데이트하기 위한 업데이트용 소프트웨어를 차량으로 전송하여, 차량을 관리할 수 있다.

[0063] 한편, 본 개시의 암호화된 소프트웨어는 차량 소프트웨어의 업데이트에 이용되는 업데이트용 소프트웨어가 화이트박스 암호화 알고리즘에 입력됨에 따라 암호화된 것 일 수 있다. 또한, 화이트박스 암호화 알고리즘은 화이트박스 테이블을 포함할 수 있다.

[0064] 여기서, 화이트박스 테이블은 컴퓨팅 장치(100)가 서버로부터 암호화된 소프트웨어를 수신하기 전에, 상기 서버에서 상기 컴퓨팅 장치(100)로 전송될 수 있다. 구체적으로, 서버가 컴퓨팅 장치(100)와 관련된 차량 고유 정보를 이용해 화이트박스 테이블을 락킹(Locking)하고, 락킹된 화이트박스 테이블을 컴퓨팅 장치(100)로 전송할 수 있다. 예를 들어, 차량 고유 정보는 차량을 식별할 수 있는 차대번호에 대한 정보, 차량번호에 대한 정보, 차량 고유의 비밀번호에 대한 정보 및 차량모델에 대한 정보 중 적어도 하나를 포함할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0065] 즉, 소프트웨어의 암호화 또는 복호화에 이용되는 화이트박스 테이블은 차량 고유 정보로 락킹되어, 업데이트 대상이 되는 차량만 암호화된 소프트웨어를 획득할 수 있다.

[0066] 따라서, 본 개시의 차량 소프트웨어 업데이트 방법은 적합하지 않은 소프트웨어 업데이트를 사전에 방지하여, 차량의 안전 사양을 보장할 수 있다.

[0067] 한편, 컴퓨팅 장치(100)의 프로세서(110)는 서버로부터 암호화된 소프트웨어를 수신한 경우, 화이트박스 복호화 알고리즘에 차량 고유 정보 및 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득할 수 있다(S120). 여기서, 화이트박스 복호화 알고리즘은 컴퓨팅 장치(100)의 메모리(130)에 저장되어 있을 수 있다.

[0068] 한편, 본 개시의 화이트박스 복호화 알고리즘은 차량 고유 정보를 기초로 락킹된 화이트박스 테이블을 포함할 수 있다. 그리고, 화이트박스 테이블은 암호화된 소프트웨어의 암호화 키가 분산되어 저장된 테이블일 수 있다.

[0069] 도 5를 참조하면, 본 개시의 컴퓨팅 장치(100)는 서버로부터 미리 수신하여 메모리(130)에 사전 저장된 화이트박스 테이블(또는, 화이트박스 암호 테이블)에 암호화된 소프트웨어와 차량 고유 정보를 입력하여, 복호화된 소프트웨어를 획득할 수 있다.

[0070] 즉, 본 개시의 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 방법에 따르면, 차량의 고유 정보를 보유한 차량(즉, 컴퓨팅 장치)만이 암호화된 소프트웨어를 복호화 할 수 있다.

[0071] 따라서, 본 개시의 화이트박스 암호를 이용한 차량 소프웨어 업데이트 기법은 업데이트 대상이 되는 차량으로 기밀성이 보장된 소프트웨어를 안전하게 전송하여, 안전한 소프트웨어 업데이트를 제공할 수 있다.

[0072] 상술한 바와 같이, 본 개시의 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법은 안전한 차량 소프트웨어 업데이트를 제공하기 위한 방법을 사용자에게 제공할 수 있다.

[0073] 본 개시의 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법은 화이트박스 암호를 사용함에 따라, 소프트웨어의 기밀성을 보장하기 위해 사용되는 암호키가 화이트박스 테이블에 암호화 알고리즘과 뒤섞여 존재하기 때문에 공격자가 암호화 키를 추출하는 것을 막을 수 있다.

[0074] 따라서, 본 개시의 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법은 기존의 대칭키 또는, 해쉬 체인 등과 같은 암호기술 적용 시 발생하는 키 관리 및 저장 문제를 해결할 수 있다.

[0075] 추가적으로, 본 개시의 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법은 하드웨어 기반 HSM을 사용하는 기법과 비교 시 소프트웨어 사용(화이트박스 암호 테이블)만으로 암호 알고리즘의 중간 연산 값 및 암호화 키를 보호할 수 있다.

[0076] 또한, 본 개시의 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법은 각 차량의 고유정보로 화이트박스 테이블을 락킹 시킴으로써, 소프트웨어 업데이트에 해당되는 차량으로 기밀성이 보장된 소프트웨어를 제공할 수 있다.

[0077] 또한, 본 개시의 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법은 보안 문제 발생으로 인해 소프트웨어 암호화에 사용되는 키 업데이트가 필요할 시 쉽게 테이블만 업데이트 시킬 수 있기 때문에 안전성을 향상시킬 수 있다.

[0078] 다시 도 4를 참조하면, 컴퓨팅 장치(100)의 프로세서(110)는 복호화된 소프트웨어를 획득한 경우, 복호화된 소프트웨어를 이용하여 차량 소프트웨어를 업데이트할 수 있다(S130).

[0079] 그리고, 프로세서(110)는 차량 소프트웨어의 업데이트가 완료된 경우, 상기 차량 소프트웨어의 업데이트 결과에 대한 업데이트 결과 정보를 상기 서버로 전송할 수 있다.

[0080] 구체적으로, 프로세서(110)는 서버로 차량 소프트웨어의 업데이트 실패에 대한 업데이트 결과 정보를 전송한 경우, 통신부(120)를 통해 서버로부터 상기 화이트박스 테이블을 업데이트 하기 위한 업데이트 정보를 수신할 수 있다. 그리고, 프로세서(110)는 업데이트 정보에 기초하여, 화이트박스 테이블을 업데이트할 수 있다.

[0081] 따라서, 본 개시의 차량 소프트웨어 업데이트 방법은 추후 발생될 수 있는 업데이트 실패를 방지하여, 업데이트 안정성을 향상시킬 수 있다.

[0083] 도 6은 본 개시의 몇몇 실시예에 따른 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법의 일례를 설명하기 위한 흐름도이다.

[0084] 먼저, 본 개시의 화이트박스 암호를 이용한 차량 소프트웨어 업데이트 기법에 따르면, 차량과 관련된 컴퓨팅 장치(100)는 도 5와 같이 각 차량의 차량 고유 정보로 락킹 된 소프트웨어 암호화 키가 숨겨져 있는 화이트박스 테이블이 저장하고 있을 수 있다.

[0085] 차량의 소프트웨어 업데이트를 담당하는 원격 유지관리 서버(200)는 컴퓨팅 장치(100) 또는, 사용자(사용자 단말)에게 차량에 존재하는 소프트웨어의 업데이트가 있음을 알릴 수 있다. 예를 들어, 원격 유지관리 서버(200)는 컴퓨팅 장치(100) 또는, 사용자 단말로 소프트웨어 업데이트와 관련된 메시지를 전송할 수 있다. 다만, 이에

한정되는 것은 아니다.

[0086] 한편, 소프트웨어 업데이트에 대한 알림을 수신한 컴퓨팅 장치(100) 또는, 사용자는 원격 유지관리 서버로 소프트웨어 업데이트를 요청할 수 있다. 예를 들어, 사용자는 컴퓨팅 장치(100) 또는, 사용자 단말을 이용하여, 소프트웨어 업데이트 요청과 관련된 메시지를 원격 유지관리 서버로 전송할 수 있다. 다만, 이에 한정되는 것은 아니다.

[0087] 소프트웨어 업데이트에 대한 요청을 수신한 원격 유지관리 서버(200)는 화이트박스 암호화 알고리즘을 통해 암호화된 소프트웨어를 컴퓨팅 장치(100) 또는, 사용자 단말로 전송할 수 있다. 여기서, 원격 유지관리 서버(200)는 소프트웨어를 암호화하여 전송함으로써, 업데이트된 소프트웨어에 대한 기밀성을 제공할 수 있다.

[0088] 한편, 암호화된 소프트웨어를 수신(또는, 다운로드)한 컴퓨팅 장치(100) 또는, 사용자 단말은 암호화된 소프트웨어를 복호화 하기 위해 도 5와 같이 차량의 고유 정보와 암호화된 소프트웨어를 인풋으로 넣어 복호화 과정을 수행할 수 있다. 여기서, 복호화된 소프트웨어를 얻기 위해 차량의 고유 정보가 인풋으로 들어가기 때문에, 업데이트에 해당되는 차량만이 복호화된 소프트웨어를 획득할 수 있다.

[0089] 컴퓨팅 장치(100) 또는, 사용자 단말은 암호화된 소프트웨어에 대한 복호화를 완료한 경우, 복호화된 소프트웨어를 컴퓨팅 장치(100)에 설치할 수 있다. 그리고, 컴퓨팅 장치(100) 또는, 사용자 단말은 업데이트 결과를 원격 유지관리 서버(200)로 전송할 수 있다. 추가적으로, 원격 유지관리 서버(200)는 컴퓨팅 장치(100) 또는, 사용자 단말에서의 업데이트 실패 시 차량이 저장되어 있는 화이트박스 테이블을 업데이트하여, 추후의 소프트웨어 업데이트의 안전성을 향상시킬 수 있다.

[0091] 도 7은 본 개시내용의 실시예들이 구현될 수 있는 예시적인 컴퓨팅 환경에 대한 일반적인 개략도를 도시한다.

[0092] 본 개시내용이 일반적으로 하나 이상의 컴퓨터 상에서 실행될 수 있는 컴퓨터 실행가능 명령어와 관련하여 전술되었지만, 당업자라면 본 개시내용 기타 프로그램 모듈들과 결합되어 및/또는 하드웨어와 소프트웨어의 조합으로서 구현될 수 있다는 것을 잘 알 것이다.

[0093] 일반적으로, 본 명세서에서의 모듈은 특정의 태스크를 수행하거나 특정의 추상 데이터 유형을 구현하는 루틴, 프로시져, 프로그램, 컴포넌트, 데이터 구조, 기타 등등을 포함한다. 또한, 당업자라면 본 개시의 방법이 단일-프로세서 또는 멀티프로세서 컴퓨터 시스템, 미니컴퓨터, 메인프레임 컴퓨터는 물론 퍼스널 컴퓨터, 핸드헬드 컴퓨팅 장치, 마이크로프로세서-기반 또는 프로그램가능 가전 제품, 기타 등등(이들 각각은 하나 이상의 연관된 장치와 연결되어 동작할 수 있음)을 비롯한 다른 컴퓨터 시스템 구성으로 실시될 수 있다는 것을 잘 알 것이다.

[0094] 본 개시의 설명된 실시예들은 또한 어떤 태스크들이 통신 네트워크를 통해 연결되어 있는 원격 처리 장치들에 의해 수행되는 분산 컴퓨팅 환경에서 실시될 수 있다. 분산 컴퓨팅 환경에서, 프로그램 모듈은 로컬 및 원격 메모리 저장 장치 둘다에 위치할 수 있다.

[0095] 컴퓨터는 통상적으로 다양한컴퓨터 판독가능 매체를 포함한다. 컴퓨터에 의해 액세스 가능한 매체 로서, 휘발성 및 비휘발성 매체, 일시적(transitory) 및 비일시적(non-transitory) 매체, 이동식 및 비-이동식 매체를 포함한다. 제한이 아닌 예로서, 컴퓨터 판독가능 매체는 컴퓨터 판독가능 저장 매체 및 컴퓨터 판독가능 전송 매체를 포함할 수 있다.

[0096] 컴퓨터 판독가능 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보를 저장하는 임의의 방법 또는 기술로 구현되는 휘발성 및 비휘발성 매체, 일시적 및 비-일시적 매체, 이동식 및 비이동식 매체를 포함한다. 컴퓨터 판독가능 저장 매체는 RAM, ROM, EEPROM, 플래시 메모리 또는 기타 메모리 기술, CD-ROM, DVD(digital video disk) 또는 기타 광 디스크 저장 장치, 자기 카세트, 자기 테이프, 자기 디스크 저장 장치 또는 기타 자기 저장 장치, 또는 컴퓨터에 의해 액세스될 수 있고 원하는 정보를 저장하는데 사용될 수 있는 임의의 기타 매체를 포함하지만, 이에 한정되지 않는다.

[0097] 컴퓨터 판독가능 전송 매체는 통상적으로 반송파(carrier wave) 또는 기타 전송 메커니즘(transport mechanism)과 같은 피변조 데이터 신호(modulated data signal)에 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터등을 구현하고 모든 정보 전달 매체를 포함한다. 피변조 데이터 신호라는 용어는 신호 내에 정보를 인코딩하도록 그 신호의 특성들 중 하나 이상을 설정 또는 변경시킨 신호를 의미한다. 제한이 아닌 예로서, 컴퓨터 판독가능 전송 매체는 유선 네트워크 또는 직접 배선 접속(direct-wired connection)과 같은 유선 매체, 그리고 음향, RF, 적외선, 기타 무선 매체와 같은 무선 매체를 포함한다. 상술된 매체들 중 임의의 것

의 조합도 역시 컴퓨터 판독가능 전송 매체의 범위 안에 포함되는 것으로 한다.

[0098] 컴퓨터(1102)를 포함하는 본 개시의 여러가지 측면들을 구현하는 예시적인 환경(1100)이 나타내어져 있으며, 컴퓨터(1102)는 처리 장치(1104), 시스템 메모리(1106) 및 시스템 버스(1108)를 포함한다. 시스템 버스(1108)는 시스템 메모리(1106)(이에 한정되지 않음)를 비롯한 시스템 컴포넌트들을 처리 장치(1104)에 연결시킨다. 처리 장치(1104)는 다양한 상용 프로세서들 중 임의의 프로세서일 수 있다. 듀얼 프로세서 및 기타 멀티프로세서 아키텍처도 역시 처리 장치(1104)로서 이용될 수 있다.

[0099] 시스템 버스(1108)는 메모리 버스, 주변장치 버스, 및 다양한 상용 버스 아키텍처 중 임의의 것을 사용하는 로컬 버스에 추가적으로 상호 연결될 수 있는 몇 가지 유형의 버스 구조 중 임의의 것일 수 있다. 시스템 메모리(1106)는 판독 전용 메모리(ROM)(1110) 및 랜덤 액세스 메모리(RAM)(1112)를 포함한다. 기본 입/출력 시스템(BIOS)은 ROM, EPROM, EEPROM 등의 비휘발성 메모리(1110)에 저장되며, 이 BIOS는 시동 중과 같은 때에 컴퓨터(1102) 내의 구성요소들 간에 정보를 전송하는 일을 돕는 기본적인 루틴을 포함한다. RAM(1112)은 또한 데이터를 캐싱하기 위한 정적 RAM 등의 고속 RAM을 포함할 수 있다.

[0100] 컴퓨터(1102)는 또한 내장형 하드 디스크 드라이브(HDD)(1114)(예를 들어, EIDE, SATA)-이 내장형 하드 디스크 드라이브(1114)는 또한 적당한 섀시(도시 생략) 내에서 외장형 용도로 구성될 수 있음-, 자기 플로피 디스크 드라이브(FDD)(1116)(예를 들어, 이동식 디스켓(1118)으로부터 판독을 하거나 그에 기록을 하기 위한 것임), 및 광 디스크 드라이브(1120)(예를 들어, CD-ROM 디스크(1122)를 판독하거나 DVD 등의 기타 고용량 광 매체로부터 판독을 하거나 그에 기록을 하기 위한 것임)를 포함한다. 하드 디스크 드라이브(1114), 자기 디스크 드라이브(1116) 및 광 디스크 드라이브(1120)는 각각 하드 디스크 드라이브 인터페이스(1124), 자기 디스크 드라이브 인터페이스(1126) 및 광 드라이브 인터페이스(1128)에 의해 시스템 버스(1108)에 연결될 수 있다. 외장형 드라이브 구현을 위한 인터페이스(1124)는 예를 들어, USB(Universal Serial Bus) 및 IEEE 1394 인터페이스 기술 중 적어도 하나 또는 그 둘 다를 포함한다.

[0101] 이들 드라이브 및 그와 연관된 컴퓨터 판독가능 매체는 데이터, 데이터 구조, 컴퓨터 실행가능 명령어, 기타 등등의 비휘발성 저장을 제공한다. 컴퓨터(1102)의 경우, 드라이브 및 매체는 임의의 데이터를 적당한 디지털 형식으로 저장하는 것에 대응한다. 상기에서의 컴퓨터 판독가능 저장 매체에 대한 설명이 HDD, 이동식 자기 디스크, 및 CD 또는 DVD 등의 이동식 광 매체를 언급하고 있지만, 당업자라면 집 드라이브(zip drive), 자기 카세트, 플래쉬 메모리 카드, 카트리지, 기타 등등의 컴퓨터에 의해 판독가능한 다른 유형의 저장 매체도 역시 예시적인 운영 환경에서 사용될 수 있으며 또 임의의 이러한 매체가 본 개시의 방법들을 수행하기 위한 컴퓨터 실행가능 명령어를 포함할 수 있다는 것을 잘 알 것이다.

[0102] 운영 체제(1130), 하나 이상의 애플리케이션 프로그램(1132), 기타 프로그램 모듈(1134) 및 프로그램 데이터(1136)를 비롯한 다수의 프로그램 모듈이 드라이브 및 RAM(1112)에 저장될 수 있다. 운영 체제, 애플리케이션, 모듈 및/또는 데이터의 전부 또는 그 일부분이 또한 RAM(1112)에 캐싱될 수 있다. 본 개시가 여러가지 상업적으로 이용가능한 운영 체제 또는 운영 체제들의 조합에서 구현될 수 있다는 것을 잘 알 것이다.

[0103] 사용자는 하나 이상의 유선/무선 입력 장치, 예를 들어, 키보드(1138) 및 마우스(1140) 등의 포인팅 장치를 통해 컴퓨터(1102)에 명령 및 정보를 입력할 수 있다. 기타 입력 장치(도시 생략)로는 마이크, IR 리모콘, 조이스틱, 게임 패드, 스타일러스 펜, 터치 스크린, 기타 등등이 있을 수 있다. 이들 및 기타 입력 장치가 종종 시스템 버스(1108)에 연결되어 있는 입력 장치 인터페이스(1142)를 통해 처리 장치(1104)에 연결되지만, 병렬 포트, IEEE 1394 직렬 포트, 게임 포트, USB 포트, IR 인터페이스, 기타 등등의 기타 인터페이스에 의해 연결될 수 있다.

[0104] 모니터(1144) 또는 다른 유형의 디스플레이 장치도 역시 비디오 어댑터(1146) 등의 인터페이스를 통해 시스템 버스(1108)에 연결된다. 모니터(1144)에 부가하여, 컴퓨터는 일반적으로 스피커, 프린터, 기타 등등의 기타 주변 출력 장치(도시 생략)를 포함한다.

[0105] 컴퓨터(1102)는 유선 및/또는 무선 통신을 통한 원격 컴퓨터(들)(1148) 등의 하나 이상의 원격 컴퓨터로의 논리적 연결을 사용하여 네트워크화된 환경에서 동작할 수 있다. 원격 컴퓨터(들)(1148)는 워크스테이션, 서버 컴퓨터, 라우터, 퍼스널 컴퓨터, 휴대용 컴퓨터, 마이크로프로세서-기반 오락 기기, 피어 장치 또는 기타 통상의 네트워크 노드일 수 있으며, 일반적으로 컴퓨터(1102)에 대해 기술된 구성요소들 중 다수 또는 그 전부를 포함하지만, 간략함을 위해, 메모리 저장 장치(1150)만이 도시되어 있다. 도시되어 있는 논리적 연결은 근거리 통신망(LAN)(1152) 및/또는 더 큰 네트워크, 예를 들어, 원거리 통신망(WAN)(1154)에의 유선/무선 연결을 포함한다.

이러한 LAN 및 WAN 네트워킹 환경은 사무실 및 회사에서 일반적인 것이며, 인트라넷 등의 전사적 컴퓨터 네트워크(enterprise-wide computer network)를 용이하게 해주며, 이들 모두는 전세계 컴퓨터 네트워크, 예를 들어, 인터넷에 연결될 수 있다.

[0106] LAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 유선 및/또는 무선 통신 네트워크 인터페이스 또는 어댑터(1156)를 통해 로컬 네트워크(1152)에 연결된다. 어댑터(1156)는 LAN(1152)에의 유선 또는 무선 통신을 용이하게 해줄 수 있으며, 이 LAN(1152)은 또한 무선 어댑터(1156)와 통신하기 위해 그에 설치되어 있는 무선 액세스 포인트를 포함하고 있다. WAN 네트워킹 환경에서 사용될 때, 컴퓨터(1102)는 모뎀(1158)을 포함할 수 있거나, WAN(1154) 상의 통신 서버에 연결되거나, 또는 인터넷을 통하는 등, WAN(1154)을 통해 통신을 설정하는 기타 수단을 갖는다. 내장형 또는 외장형 및 유선 또는 무선 장치일 수 있는 모뎀(1158)은 직렬 포트 인터페이스(1142)를 통해 시스템 버스(1108)에 연결된다. 네트워크화된 환경에서, 컴퓨터(1102)에 대해 설명된 프로그램 모듈들 또는 그의 일부분이 원격 메모리/저장 장치(1150)에 저장될 수 있다. 도시된 네트워크 연결이 예시적인 것이며 컴퓨터들 사이에 통신 링크를 설정하는 기타 수단이 사용될 수 있다는 것을 잘 알 것이다.

[0107] 컴퓨터(1102)는 무선 통신으로 배치되어 동작하는 임의의 무선 장치 또는 개체, 예를 들어, 프린터, 스캐너, 데스크톱 및/또는 휴대용 컴퓨터, PDA(portable data assistant), 통신 위성, 무선 검출가능 태그와 연관된 임의의 장비 또는 장소, 및 전화와 통신을 하는 동작을 한다. 이것은 적어도 Wi-Fi 및 블루투스 무선 기술을 포함한다. 따라서, 통신은 종래의 네트워크에서와 같이 미리 정의된 구조이거나 단순하게 적어도 2개의 장치 사이의 애드혹 통신(ad hoc communication)일 수 있다.

[0108] Wi-Fi(Wireless Fidelity)는 유선 없이도 인터넷 등으로의 연결을 가능하게 해준다. Wi-Fi는 이러한 장치, 예를 들어, 컴퓨터가 실내에서 및 실외에서, 즉 기지국의 통화권 내의 아무 곳에서나 데이터를 전송 및 수신할 수 있게 해주는 셀 전화와 같은 무선 기술이다. Wi-Fi 네트워크는 안전하고 신뢰성 있으며 고속인 무선 연결을 제공하기 위해 IEEE 802.11(a,b,g, 기타)이라고 하는 무선 기술을 사용한다. 컴퓨터를 서로에, 인터넷에 및 유선 네트워크(IEEE 802.3 또는 이더넷을 사용함)에 연결시키기 위해 Wi-Fi가 사용될 수 있다. Wi-Fi 네트워크는 비인가 2.4 및 5 GHz 무선 대역에서, 예를 들어, 11Mbps(802.11a) 또는 54 Mbps(802.11b) 데이터 레이트로 동작하거나, 양 대역(듀얼 대역)을 포함하는 제품에서 동작할 수 있다.

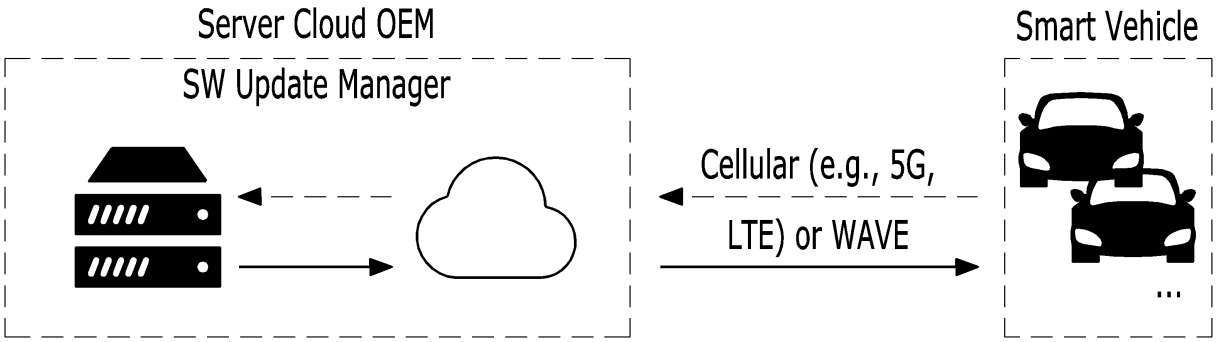
[0109] 본 개시의 기술 분야에서 통상의 지식을 가진 자는 여기에 개시된 실시예들과 관련하여 설명된 다양한 예시적인 논리 블록들, 모듈들, 프로세서들, 수단들, 회로들 및 알고리즘 단계들이 전자 하드웨어, (편의를 위해, 여기에서 "소프트웨어"로 지칭되는) 다양한 형태들의 프로그램 또는 설계 코드 또는 이들 모두의 결합에 의해 구현될 수 있다는 것을 이해할 것이다. 하드웨어 및 소프트웨어의 이러한 상호 호환성을 명확하게 설명하기 위해, 다양한 예시적인 컴포넌트들, 블록들, 모듈들, 회로들 및 단계들이 이들의 기능과 관련하여 위에서 일반적으로 설명되었다. 이러한 기능이 하드웨어 또는 소프트웨어로서 구현되는지 여부는 특정한 애플리케이션 및 전체 시스템에 대하여 부과되는 설계 제약들에 따라 좌우된다. 본 개시의 기술 분야에서 통상의 지식을 가진 자는 각각의 특정한 애플리케이션에 대하여 다양한 방식들로 설명된 기능을 구현할 수 있으나, 이러한 구현 결정들은 본 개시의 범위를 벗어나는 것으로 해석되어서는 안 될 것이다.

[0110] 여기서 제시된 다양한 실시예들은 방법, 장치, 또는 표준 프로그래밍 및/또는 엔지니어링 기술을 사용한 제조 물품(article)으로 구현될 수 있다. 용어 "제조 물품"은 임의의 컴퓨터-판독가능 장치로부터 액세스 가능한 컴퓨터 프로그램 또는 매체(media)를 포함한다. 예를 들어, 컴퓨터-판독가능 저장 매체는 자기 저장 장치(예를 들면, 하드 디스크, 플로피 디스크, 자기 스트립, 등), 광학 디스크(예를 들면, CD, DVD, 등), 스마트 카드, 및 플래쉬 메모리 장치(예를 들면, EEPROM, 카드, 스틱, 키 드라이브, 등)를 포함하지만, 이들로 제한되는 것은 아니다. 용어 "기계-판독가능 매체"는 명령(들) 및/또는 데이터를 저장, 보유, 및/또는 전달할 수 있는 무선 채널 및 다양한 다른 매체를 포함하지만, 이들로 제한되는 것은 아니다.

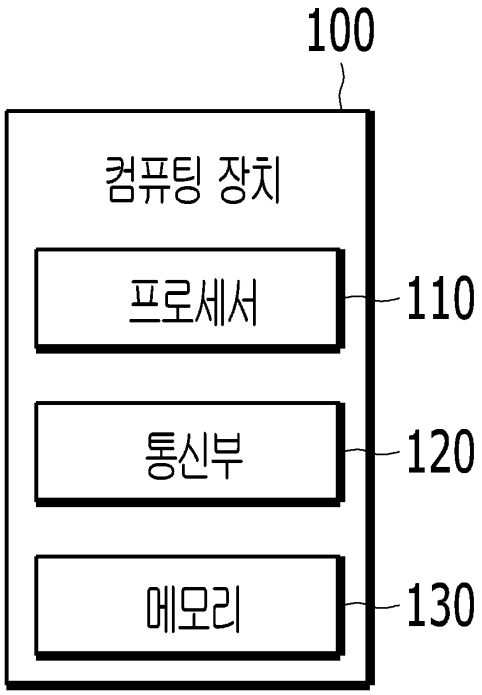
[0112] 제시된 실시예들에 대한 설명은 임의의 본 개시의 기술 분야에서 통상의 지식을 가진 자가 본 개시를 이용하거나 또는 실시할 수 있도록 제공된다. 이러한 실시예들에 대한 다양한 변형들은 본 개시의 기술 분야에서 통상의 지식을 가진 자에게 명백할 것이며, 여기에 정의된 일반적인 원리들은 본 개시의 범위를 벗어남이 없이 다른 실시예들에 적용될 수 있다. 그리하여, 본 개시는 여기에 제시된 실시예들로 한정되는 것이 아니라, 여기에 제시된 원리들 및 신규한 특징들과 일관되는 최광의의 범위에서 해석되어야 할 것이다.

도면

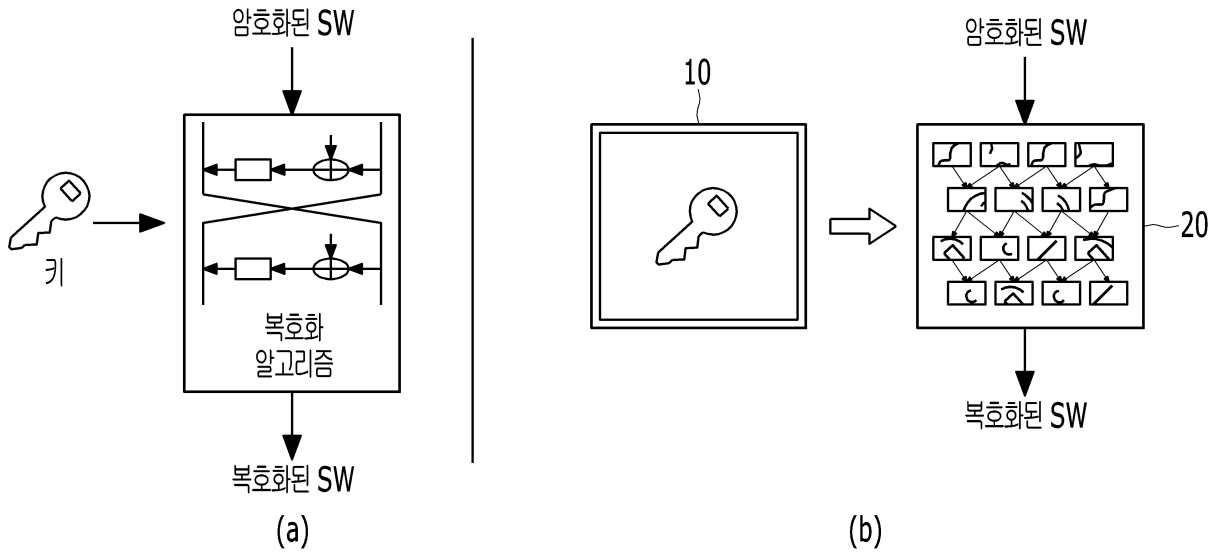
도면1


Server Cloud OEM
SW Update Manager
Cellular (e.g., 5G,
LTE) or WAVE
Smart Vehicle
...

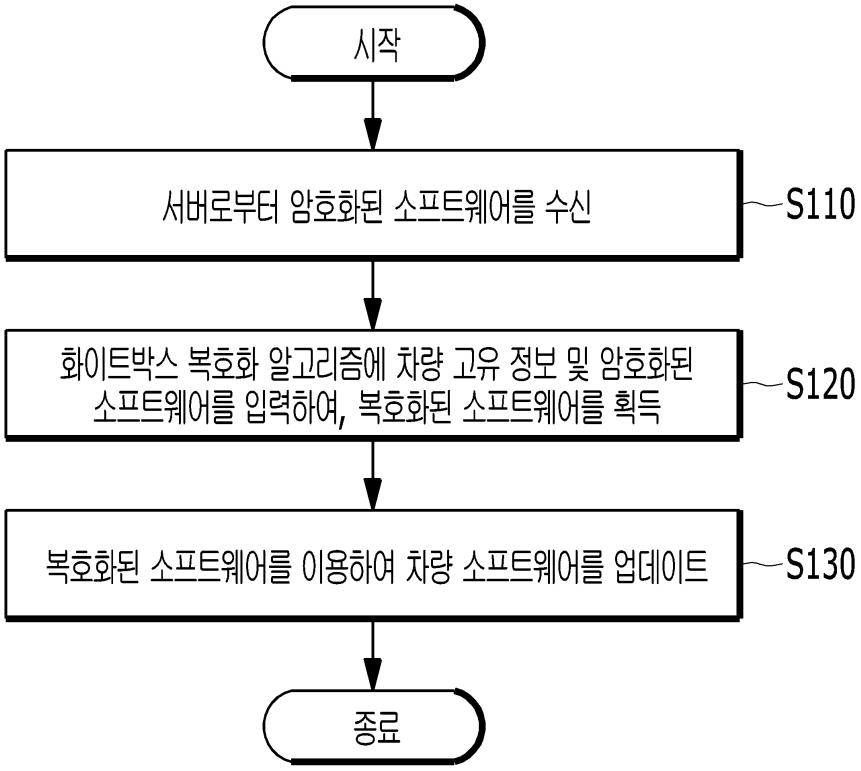
도면2


100
컴퓨팅 장치
프로세서
110
통신부
120
메모리
130

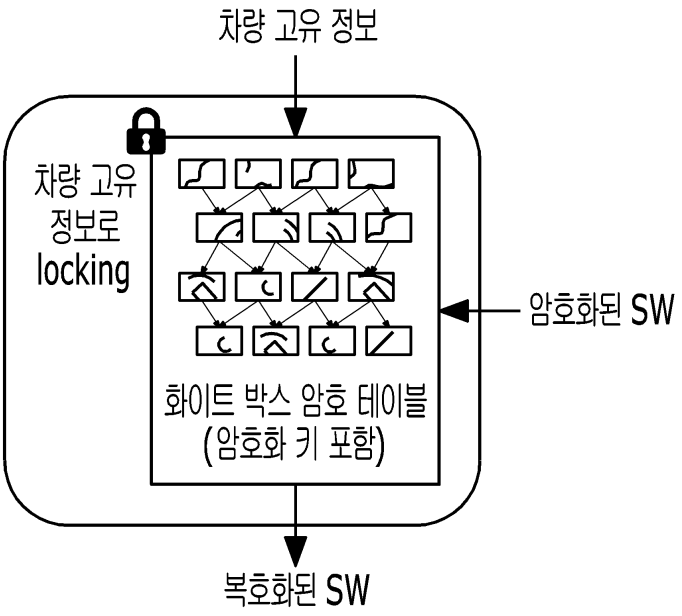
도면3


암호화된 SW
키
복호화
알고리즘
복호화된 SW
(a)
10
암호화된 SW
20
복호화된 SW
(b)

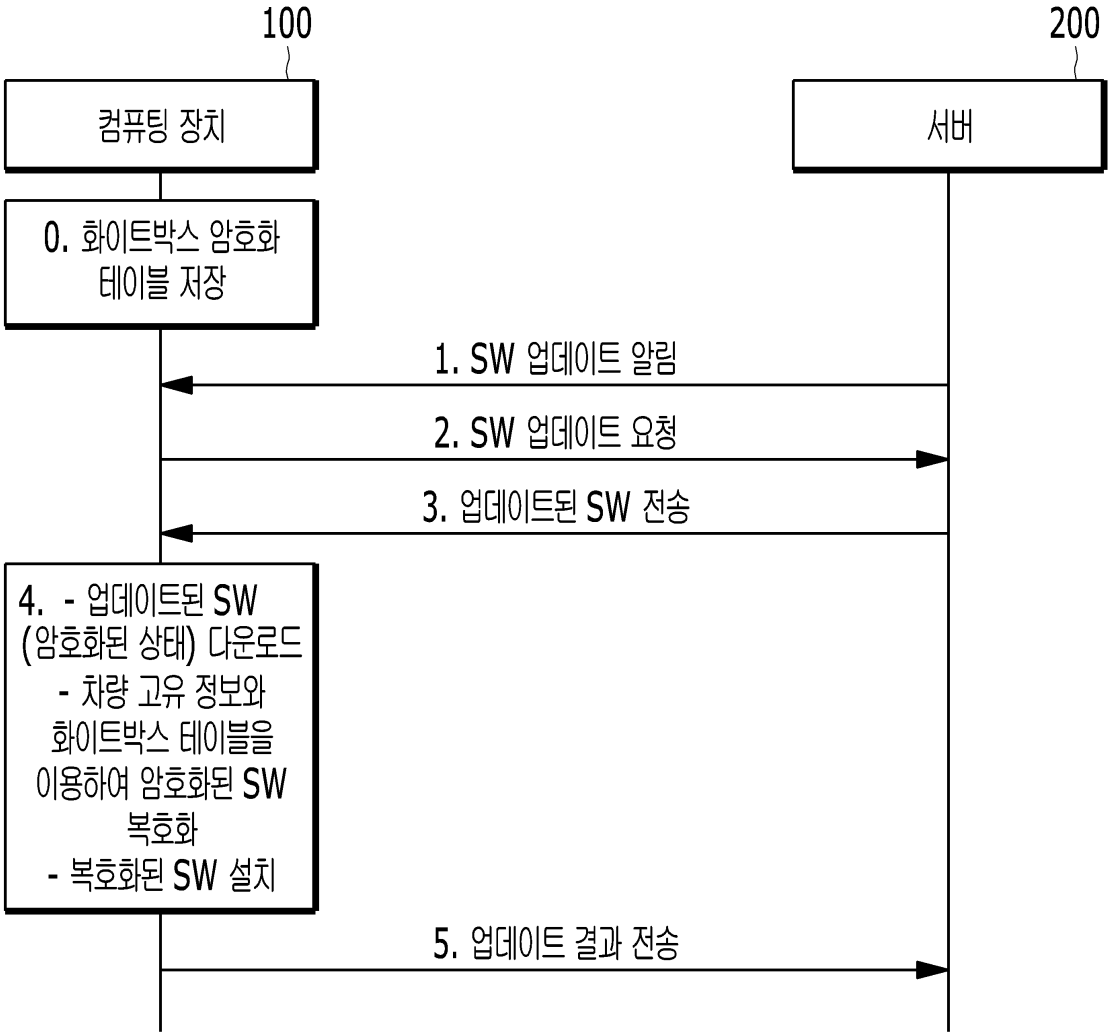
도면4


시작
서버로부터 암호화된 소프트웨어를 수신
S110
화이트박스 복호화 알고리즘에 차량 고유 정보 및 암호화된 소프트웨어를 입력하여, 복호화된 소프트웨어를 획득
S120
복호화된 소프트웨어를 이용하여 차량 소프트웨어를 업데이트
S130
종료

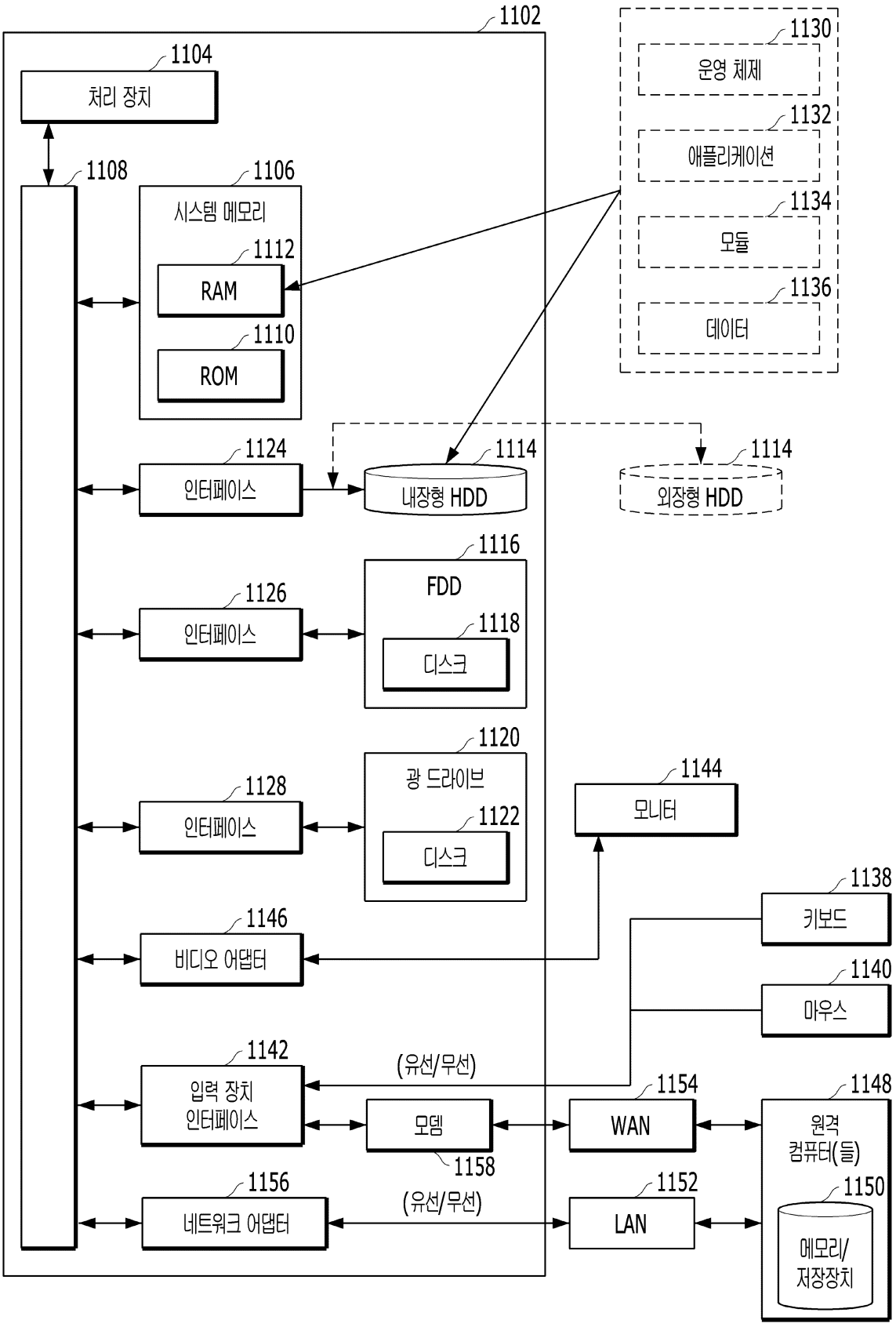
도면5


차량 고유 정보
차량 고유 정보로 locking
암호화된 SW
화이트 박스 암호 테이블 (암호화 키 포함)
복호화된 SW

도면6


100
200
컴퓨팅 장치
서버
0. 화이트박스 암호화 테이블 저장
1. SW 업데이트 알림
2. SW 업데이트 요청
3. 업데이트된 SW 전송
4. - 업데이트된 SW (암호화된 상태) 다운로드
- 차량 고유 정보와 화이트박스 테이블을 이용하여 암호화된 SW 복호화
- 복호화된 SW 설치
5. 업데이트 결과 전송

도면7


1102
1104
처리 장치
1108
1106
시스템 메모리
1112
RAM
1110
ROM
1130
운영 체제
1132
애플리케이션
1134
모듈
1136
데이터
1124
인터페이스
1114
내장형 HDD
1114
외장형 HDD
1116
FDD
1126
인터페이스
1118
디스크
1120
광 드라이브
1128
인터페이스
1122
디스크
1144
모니터
1138
키보드
1146
비디오 어댑터
1140
마우스
1142
입력 장치
인터페이스
(유선/무선)
1154
WAN
1148
원격
컴퓨터(들)
모뎀
1158
1156
네트워크 어댑터
(유선/무선)
1152
LAN
1150
메모리/
저장장치