

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)(11) 공개번호 10-2020-0046406
(43) 공개일자 2020년05월07일

(51) 국제특허분류(Int. Cl.)
G06F 21/64 (2013.01) B62D 41/00 (2006.01)
(52) CPC특허분류
G06F 21/64 (2013.01)
B62D 41/00 (2013.01)
(21) 출원번호 10-2018-0127525
(22) 출원일자 2018년10월24일
심사청구일자 2018년10월24일

(71) 출원인
동서대학교 산학협력단
부산광역시 사상구 주례로 47(주례동,
동서대학교)
(72) 발명자
김현호
부산광역시 부산진구 복지로21번길 39-1 대동레미
안 304호
김민규
부산광역시 사상구 가야대로318번길 69 영림4,
240호
(뒷면에 계속)
(74) 대리인
김석계

전체 청구항 수 : 총 3 항

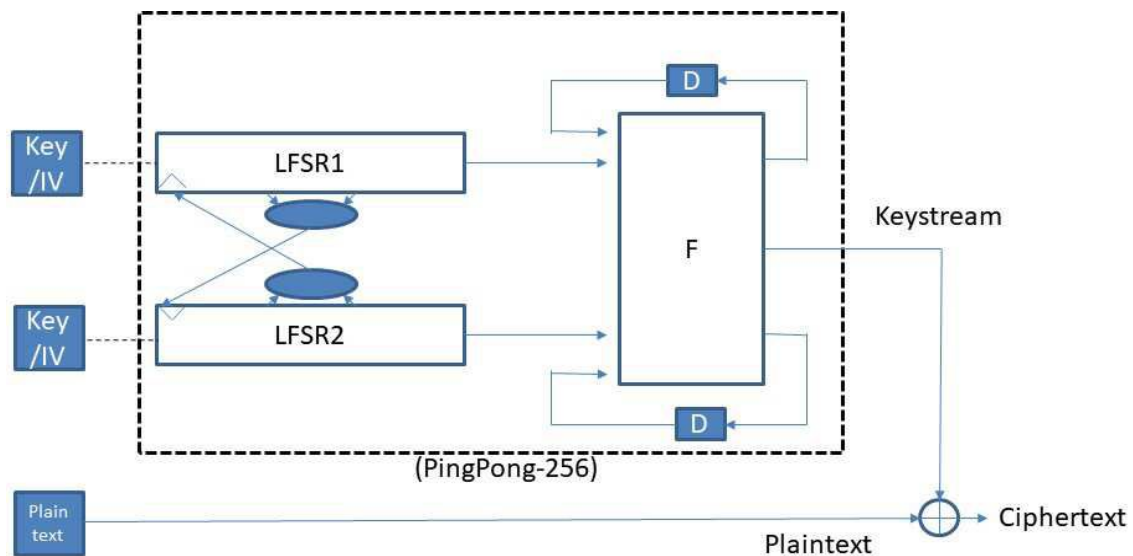
(54) 발명의 명칭 차량용 블랙박스 실시간 영상 위변조 방지방법

(57) 요약

본 발명은 키수열을 발생시키는 알고리즘을 적용함에 따라 얻는 출력 해시값(Hashed Value)을 통해, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하는 것으로,

본 발명 차량용 블랙박스 실시간 영상 위변조 방지방법은 키수열을 발생시키는 알고리즘을 적용함에 따라, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하되, 블랙박스에 저장된 최종적인 출력 해시값(Hashed Value)이 변경되는 것을 파악하여 변조사실을 검출하게 되는 현저한 효과가 있다.

대표도 - 도1



(72) 발명자

류수미

부산광역시 북구 만덕대로128번길 28, 501호

김기환

부산광역시 북구 화명대로 87 현대아파트 101동
1501호

강영진

부산광역시 사상구 가야대로318번길 84, 205호

이훈재

대구광역시 수성구 청호로85안길 11 선빌라 501호

이상곤

부산광역시 서구 대영로45번길 53 보현빌리지 803
호

이 발명을 지원한 국가연구개발사업

과제고유번호 2018-E-G023-010100

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 사회맞춤형 산학협력 선도대학(LINC+) 육성사업

연구과제명 사회맞춤형 산학협력 선도대학(LINC+) 육성사업(산학협력 고도화형)

기 여 율 1/3

주관기관 동서대학교 산학협력단

연구기간 2017.04.01 ~ 2022.02.28

이 발명을 지원한 국가연구개발사업

과제고유번호 1711073998

부처명 과학기술정보통신부

연구관리전문기관 정보통신기술진흥센터

연구사업명 정보보호핵심원천기술개발(R&D)(국가공공정보보호인프라강화)

연구과제명 기만공격에 의한 AI 역기능 방지 기술 개발

기 여 율 1/3

주관기관 동서대학교 산학협력단

연구기간 2018.04.01 ~ 2020.12.31

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1D1A1B01011908

부처명 교육부

연구관리전문기관 한국연구재단

연구사업명 이공분야기초연구사업(기본연구지원사업)

연구과제명 사물인터넷/무인비행기(IoT/Drone)에 적합한 초경량-고속 암호/인증 및 물리적 해킹 방어
기술 개발

기 여 율 1/3

주관기관 동서대학교 산학협력단

연구기간 2016.06.01 ~ 2023.05.31

명세서

청구범위

청구항 1

키수열을 발생시키는 알고리즘을 적용함에 따라 얻는 출력 해시값(Hashed Value)을 통해, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하는 것을 특징으로 하는 차량용 블랙박스 실시간 영상 위변조 방지방법

청구항 2

제 1항에 있어서, 상기 키수열을 발생시키는 알고리즘은 비밀키(Secret Key)와 초기벡터(iv, initialization vector)를 배타적 논리합(XOR, exclusive or)으로 연산하여 첫 번째 출력값을 발생시키고, 상기 첫 번째 출력값에 다수 개의 영상정보를 순서대로 배타적 논리합(XOR, exclusive or)으로 연산하여, 출력 해시값(Hashed Value)을 얻는 것을 특징으로 하는 차량용 블랙박스 실시간 영상 위변조 방지방법

청구항 3

제 2항에 있어서, 상기 블랙박스의 제어부는 출력 해시값(Hashed Value)이 변경된 것으로 판단되면, 블랙박스의 영상정보가 변조되는 것을 특징으로 하는 차량용 블랙박스 실시간 영상 위변조 방지방법

발명의 설명

기술 분야

[0001] 본 발명은 차량용 블랙박스 실시간 영상 위변조 방지방법에 관한 것으로, 보다 상세하게는 키수열을 발생시키는 알고리즘을 적용함에 따라, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하되, 블랙박스에 저장된 최종적인 출력 해시값(Hashed Value)이 변경되는 것을 파악하여 변조사실을 검출하게 되는 차량용 블랙박스 실시간 영상 위변조 방지방법에 관한 것이다.

배경 기술

[0003] 매년 점차 차량등록 대수가 늘어나는 동시에 차량들이 많이 증가하여, 이에 따른 교통사고 또한 계속해서 증가하고 있다. 이처럼 교통사고가 났을 때 문제를 해결하기 위해서는 증거와 증인이 있어야하지만, 대부분 상황에서 증인이 없고 증거로 해결을 봐야하는 경우가 많다.

[0004] 교통사고가 발생하는 경우 가해자와 피해자를 판단하여 상황에 맞게 처리해야하는데 현장에 목격자를 제외하고 유일한 증거가 될 수 있는 것이 현재는 차량용 블랙박스이며, 따라서 증거를 확보하기 위해 차량용 블랙박스 설치가 점점 의무화되고 있다.

[0005] 이로 인해 현재 대부분의 차량에는 차량용 블랙박스가 설치되어 있지만, 결국 블랙박스로 디지털증거물이기 때문에 회손, 변조하기 쉬우며, 결국 무결성이 입증되지 않으면 증거로 사용될 수 없는 것이다.

[0006] 그만큼 차량용 블랙박스는 자동차의 필수 설치대상이 되었지만, 블랙박스 또한 디지털 증거인만큼 증거 회손, 조작 등으로 인해 무결성을 입증해야한다. 즉, 입증되지 않은 무결성은 증거로 사용되기 어려우며, 원본데이터라는 것을 입증해야한다.

[0007] 종래기술로서 등록특허공보 등록번호 제10-1302562호의 블랙박스 데이터의 위변조 방지 장치 및 방법에는, 블랙박스에 의해 수집된 주행정보 데이터를 저장하는 주행정보 저장모듈; 기설정된 암호화 메커니즘으로 상기 주행정보 데이터를 암호화하여 위변조 판별 데이터를 생성하고, 상기 위변조 판별 데이터를 저장하는 위변조 방지모듈; 및 착탈식 매체로 구성되어, 저장된 상기 주행정보 데이터의 위조 또는 변조를 판별하기 위해 조립되어, 상기 암호화 메커니즘으로 상기 저장된 주행정보 데이터를 암호화하고, 이를 상기 위변조 판별 데이터와 비교하여 상기 주행정보 데이터의 위조 또는 변조 여부를 판단하는 위변조 판별모듈을 포함하는 블랙박스 데이터의 위변조 방지 장치이라고 기재되어 있다.

[0008] 다른 종래기술로서 등록특허공보 등록번호 제10-1008761호의 차량용 블랙박스의 위변조 방지 시스템에는, 렌즈를 통해서 입력된 광신호를 전기적신호로 변환하여 출력하는 촬상소자; 상기 촬상소자로부터 입력된 아날로그 영상신호를 소정 포맷을 갖는 디지털 영상신호로 변환하여 처리하는 영상신호 입력 처리부; 입력되는 차량정보를 인터페이스하는 차량정보 인터페이스부; 상기 차량정보 인터페이스부로부터 입력된 차량정보를 워터마크데이터로 변환하여 생성하고, 상기 변환 생성된 워터마크데이터를 상기 영상신호 입력 처리부로부터 입력된 위변조 방지처리대상인 영상데이터에 삽입하여 워터마크데이터가 삽입된 영상데이터를 생성하는 워터마킹 처리부; 상기 워터마킹 처리부에서의 워터마크데이터의 변환 생성, 워터마크데이터의 영상데이터에로의 삽입 및 워터마크데이터가 삽입된 영상데이터의 생성에 관한 실행을 제어하고 시스템 전체를 제어하는 MCU(Main Control Unit); 상기 MCU의 제어에 의해서, 상기 워터마킹 처리부에 의해서 생성된 워터마크데이터가 삽입된 영상데이터를 저장하고 있는 영상데이터 저장부; 상기 MCU의 제어에 의해서, 상기 차량정보 인터페이스부로부터 입력된 차량정보를 저장하고 있는 차량정보 저장부를 포함하는 차량용 블랙박스의 위변조 방지 시스템에 있어서, 영상데이터의 위변조를 방지하기 위한 위변조방지모드를 설정하는 위변조방지 설정부가 더 포함되어서 구성되고, 상기 MCU는 상기 위변조방지 설정부로부터 수신한 명령을 기초로 위변조방지실행제어신호를 상기 워터마킹 처리부로 출력하고, 상기 워터마킹 처리부는 MCU로부터 입력된 위변조방지실행제어신호에 의해서 상기 워터마크 데이터의 변환 생성, 워터마크데이터의 영상데이터에로의 삽입 및 워터마크데이터가 삽입된 영상데이터의 생성을 실행하는 것을 특징으로 하는 차량용 블랙박스의 위변조 방지 시스템이라고 기재되어 있다.

[0009] 그러나 상기와 같은 종래의 구성은 차량용 블랙박스가 영상정보를 변조되는 것을 방지만 할 뿐, 이미 변조된 영상정보가 있는지는 실시간으로 판단하지 못하여, 영상정보를 증거로 사용하기에 무결성을 증명하지 못하는 단점이 있었다.

발명의 내용

해결하려는 과제

[0011] 따라서 본 발명 차량용 블랙박스 실시간 영상 위변조 방지방법을 통하여, 키수열을 발생시키는 알고리즘을 적용함에 따라, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하되, 블랙박스에 저장된 최종적인 출력 해시값(Hashed Value)이 변경되는 것을 파악하여 변조사실을 검출하게 되는 차량용 블랙박스 실시간 영상 위변조 방지방법을 제공하고자 하는 것이다.

과제의 해결 수단

[0013] 본 발명은 키수열을 발생시키는 알고리즘을 적용함에 따라 얻는 출력 해시값(Hashed Value)을 통해, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하는 것을 특징으로 한다.

발명의 효과

[0015] 본 발명 차량용 블랙박스 실시간 영상 위변조 방지방법은 키수열을 발생시키는 알고리즘을 적용함에 따라, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하되, 블랙박스에 저장된 최종적인 출력 해시값(Hashed Value)이 변경되는 것을 파악하여 변조사실을 검출하게 되는 현저한 효과가 있다.

도면의 간단한 설명

[0017] 도 1은 본 발명 차량용 블랙박스 실시간 영상 위변조 방지방법의 알고리즘 원리 개념도

도 2, 3은 본 발명 차량용 블랙박스 실시간 영상 위변조 방지방법의 알고리즘 원리 순서도

발명을 실시하기 위한 구체적인 내용

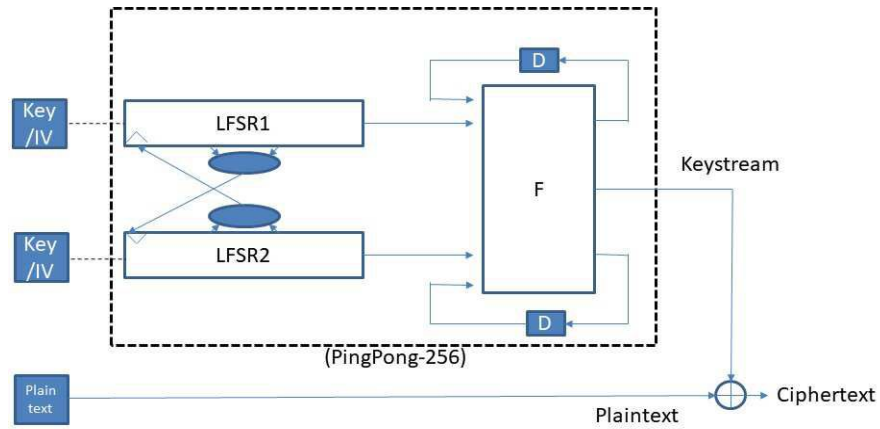
[0018] 본 발명은 키수열을 발생시키는 알고리즘을 적용함에 따라 얻는 출력 해시값(Hashed Value)을 통해, 차량용 블

랙박스의 영상정보에 대해 무결성을 입증하는 것을 특징으로 한다.

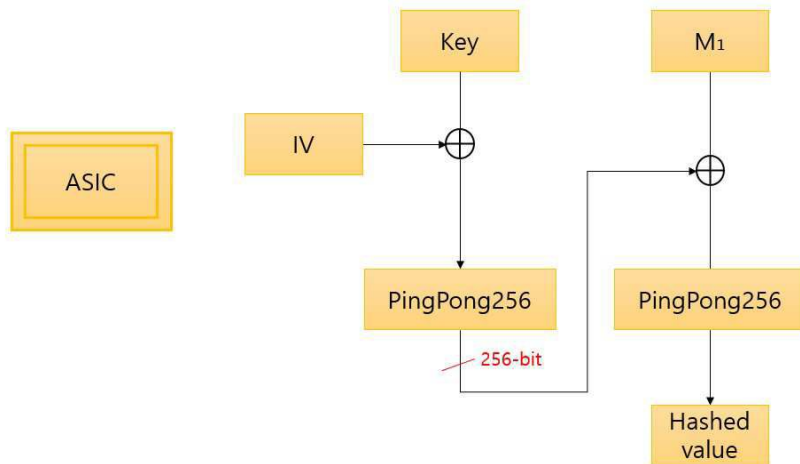
- [0019] 또한, 상기 키수열을 발생시키는 알고리즘은 비밀키(Secret Key)와 초기벡터(iv, initialization vector)를 배타적 논리합(XOR, exclusive or)으로 연산하여 첫 번째 출력값을 발생시키고, 상기 첫 번째 출력값에 다수 개의 영상정보를 순서대로 배타적 논리합(XOR, exclusive or)으로 연산하여, 출력 해시값(Hashed Value)을 얻는 것
- [0020] 또한, 상기 블랙박스의 제어부는 출력 해시값(Hashed Value)이 변경된 것으로 판단되면, 블랙박스의 영상정보가 변조되는 것을 검출하게 되는 것을 특징으로 한다.
- [0022] 본 발명을 첨부 도면에 의해 상세히 설명하면 다음과 같다.
- [0023] 도 1은 본 발명 차량용 블랙박스 실시간 영상 위변조 방지방법의 알고리즘 원리 개념도, 도 2, 3은 본 발명 차량용 블랙박스 실시간 영상 위변조 방지방법의 알고리즘 원리 순서도이다.
- [0024] 본 발명에 대해 구체적으로 기술하면, 본 발명은 키수열을 발생시키는 알고리즘을 적용함에 따라 얻는 출력 해시값(Hashed Value)을 통해, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하는 것이다.
- [0025] 상기 키수열을 발생시키는 알고리즘은 PingPong-256 알고리즘을 사용하는 것으로, 도 1에 도시된 바와 같이, 상기 PingPong-256 알고리즘은 LFSR1, LFSR2, 2-비트(bit) 메모리를 갖는 비선형 출력함수 F, 클럭조정 함수 등에 의하여 키수열(Keystream)을 발생하는 스트림암호 방식의 알고리즘인 것이다.
- [0026] 상기 키수열을 발생시키는 알고리즘으로 발생되는 해시 함수는, 생일 패러독스(Birthday Paradox)에 의하여 안전성 수준이 감소되는데, 결과적으로 안전성은 256-비트(bit)인 경우, $2^{256/2} = 2^{128}$ 이 된다.
- [0028] 상기 키수열을 발생시키는 알고리즘은 비밀키(Secret Key)와 초기벡터(iv, initialization vector)를 배타적 논리합(XOR, exclusive or)으로 연산하여 첫 번째 출력값을 발생시키고, 상기 첫 번째 출력값에 다수 개의 영상정보를 순서대로 배타적 논리합(XOR, exclusive or)으로 연산하여, 출력 해시값(Hashed Value)을 얻는 것이다.
- [0029] 더욱 자세하게는, 도 2 내지 3에 도시된 바와 같이, 상기 키수열을 발생시키는 알고리즘은 먼저 256-비트(bit)의 비밀키(Secret Key)와, 초기값 256-비트(bit)의 초기벡터(iv, initialization vector)를 배타적 논리합(XOR, exclusive or)으로 연산한 후에, 256-비트(bit)의 첫 번째 출력값(C1)을 발생시키고, 첫 번째 출력값과 256-비트(bit)의 첫 번째 영상정보(M1)를 배타적 논리합(XOR, exclusive or)으로 연산하여 256-비트(bit)의 두 번째 출력값을 발생시키고, 두 번째 출력값과 256-비트(bit)의 두 번째 영상정보(M2)를 배타적 논리합(XOR, exclusive or)으로 연산하여 256-비트(bit)의 세 번째 출력값을 발생시키는 것으로, 영상입력이 끝날 때까지 반복수행하되, 즉 N개의 영상정보가 있으면 첫 번째 영상정보(M1)부터 N번째의 영상정보(Mn)까지 배타적 논리합으로 연산하는 것을 순서대로 반복수행하여, 최종적으로 256-비트(bit)의 출력 해시값(Hashed Value)을 얻는 것이다.
- [0031] 상기 영상의 영상정보가 전체 또는 부분적으로 변조가 될 경우에는, 블랙박스에 저장된 최종적인 출력 해시값(Hashed Value)이 변경되므로 변조사실을 검출하게 되는 것이다.
- [0032] 즉, 상기 블랙박스의 제어부는 출력 해시값(Hashed Value)이 변경된 것으로 판단되면, 블랙박스의 영상정보가 변조되는 것을 검출하게 되는 것이다.
- [0033] 상기 블랙박스에는 다수 개의 영상정보(M1, M2, ..., Mn) 및 해시값(Hashed Value)이 저장되는 것이며, 영상정보는 실시간 차량용 블랙박스의 영상정보인 것이다.
- [0035] 따라서 본 발명 차량용 블랙박스 실시간 영상 위변조 방지방법은 키수열을 발생시키는 알고리즘을 적용함에 따라, 차량용 블랙박스의 영상정보에 대해 무결성을 입증하되, 블랙박스에 저장된 최종적인 출력 해시값(Hashed Value)이 변경되는 것을 파악하여 변조사실을 검출하게 되는 현저한 효과가 있다.

도면

도면1



도면2



도면3

