PingPong-256MAC을 이용한 차량용 블랙박스 실시간 영상 위변조 방지 기술

김현호[1] · 김민규[1] · 이훈재[2*]

[1]동서대학교 유비쿼터스IT학과 · [2]동서대학교 컴퓨터공학부

An Image forgery protection for real-time vehicle black box using PingPong-256MAC

HyunHo Kim[1] · Min-Kyu Kim[1] · HoonJae Lee[2*]

[1]Dongseo University UbiquitousIT · [2]Dongseo University Division of Computer Engineering

E-mail : feei_@naver.com / alsrb1030@naver.com / hjlee.dongseo.ac.kr

요 약

매년 국내 자동차 등록은 계속 증가하고 있으며, 차량이 많아짐에 따라 교통사고 또한 많아지는 중이다. 교통사고가 발생하는 경우 가해자와 피해자를 판단하여 상황에 맞게 처리해야한다. 이러한 상황을 판단할 때, 현장에 있었던 목격자를 제외하고 증거가 될 수 있는 것이 차량용 블랙박스이다. 차량용 블랙박스는 교통사고에 대비해 자동차에 필수 불가결한 장치가 되어가는 중이다. 그러나 블랙박스는 디지털 증거인만큼 증거 훼손, 조작 등으로 인해 무결성을 입증할 방법이 없다. 이에 따라 본 논문에서는 무결성 입증을 위해 PingPong-256 암호알고리즘을 이용하여 생성된 Hash값을 통해 영상의 무결성을 보장하는 방법을 제안한다.

ABSTRACT

Domestic vehicle registration is continuously increasing every year, traffic accidents are also increasing by an increase in the number of vehicles. In the event of a traffic accident, the perpetrator and the victim should be judged and handled appropriately. When judging the accident situation, the black box is what evidence can be except for witness who is at the accident scene. The black box becomes an essential role in order to prevent traffic accidents. However, there is no way to prove integrity by evidence corruption, fabrication and etc.

For this reason, we propose a method to guarantee the integrity of image through hash value generated by using PingPong 256 encryption algorithm for integrity verification in this paper.

키워드

PingPong256, Blackbox, Real-time image forgery prevention, Image information

Ⅰ. 서 론

매년 국내 자동차 등록은 계속해서 증가하고 있으며, 요즘은 1 가구당 자동차 대수도 평균 2대 이상 가지고 있는 가구도 늘어나고 있다. 이처럼 자동차 대수가 늘어남에 따라 차량소유자는 블랙박스 설치도 필수로 하고 있으며, 이는 블랙박스의 중요함을 알 수 있는 이유이다.

* Corresponding author

실제 차량용 블랙박스는 사고 규명에 결정적인 역할을 많이 하고 있으며, 이를 통해 과실 비중을 판단하는데도 중요한 증거로 활용되어지고 있다.

이렇게 블랙박스를 설치하고 사용하는 사람들이 늘어남에 따라 블랙박스 시장에도 많은 발전과 기술적 변화가 오고 있다. 초창기의 블랙박스는 자동차 전면에 사용했던 1 채널 블랙박스로 시작해서 기능은 단순히 영상만 녹화하면 되는 장치로 많이 사용되었지만, 지금은 앞뒤로 설치하는 2 채널이 평준화 되고 있으며, 4 채널 블랙박스도 상품화 되고 있다. 또한 카메라의 화질도 HD, FHD와 같이 점점 더 고화질로 녹화를 할 수 있는 기술도 적용되어 지고 있으며, 녹화한 날짜, 시간, GPS, 충격센서 등이 탑재되어 영상 정보 외 부가적인 정보로 인해 신뢰도가 상승하기도 한다. 하지만 일반적으로 영상을 확인할 때는 기본 영상 플레이어로 영상 재생 시 단순한 영상 정보(날짜, 시간)와 영상을 확인할 수 있는 경우가 보통이며, 제조사에서 제공하는 전용 프로그램을 이용해야 더 상세한 정보를 확인 할 수 있는 경우가 대부분이다[1]. 그리고 이러한 영상정보는 디지털정보이기 때문에 회손, 변조하기 쉬우며, 결국 무결성을 입증하기 위한 무언가가 필요하다. 이에 따라 논문에서는 이러한 영상정보의 무결성을 입증하기 위해 PingPong-256 알고리즘을 적용하여 영상의 무결성을 입증하는 방법을 제안하고자 한다.

II. 블랙박스 활용 및 동향

대부분의 사람들은 블랙박스는 차량에서 많이 사용되어지고 있는 장치로 많이들 알고 있다. 하지만 최근에는 비용 및 공간활용을 위해 방범용 및 상시녹화 장치로도 많이 활용되고 있다.

그림 1. 방범용 블랙박스 활용

그림 1은 일반적인 차량용 블랙박스이며, 무게가 가볍고 크기가 작아서 어디에나 쉽게 부착할 수 있다. 차량용 블랙박스의 경우 대부분 12V의 전압으로 동작한다. 따라서 차량을 제외한 다른 곳에서 전기콘센트를 이용하여 상시녹화를 할 경우 220V 콘센트에서 12V로 변환해주는 어댑터 하나면 전원 문제는 해결된다. 이를 이용해 상시로 녹화 할 수 있는 CCTV를 만들 수 있다.

예를 들어 방범용으로 많이 사용되어지고 있는 CCTV같은 경우 CCTV 1대 설치하는 예산이 만만치 않으므로 훨씬 저렴한 블랙박스를 인근에 여러대 설치하여 운영하는 경우[2], 가게에 설치하는 CCTV 또한 비용과 공간이 협소하여 설치하기 까다로운 경우도 작고 간편한 블랙박스를 대체해 CCTV로 활용하는 경우[3]처럼 영상녹화가 필요한 곳에 블랙박스를 설치하여 사용하는 경우도 늘어나고 있다. 이처럼 블랙박스는 고성능, 고화질, 저전력으로 장치가 발전함에 따라 활용도도 점점 넓어질 것이다.

III. 블랙박스 저장방식

블랙박스 시스템은 대부분 리눅스 방식의 OS시스템을 많이 사용한다. 이에 따라 리눅스 방식의 대표적인 파일시스템인 Ext2, Ext3, Ext4 방식을 사용하는 것이 좋다. 하지만 대부분의 사용자 컴퓨터에는 Windows OS가 설치되어 사용되어지는 경우가 대부분이며, 영상 확인을 위해서는 Windows에서 호환되는 파일시스템을 사용해야 영상을 볼 수 있는 문제가 있다[4]. 이와 관련해서 차량용 블랙박스 저장방식에 대한 최적화 연구가 계속 되고 있으며, 현재는 FAT32 파일시스템 방식이 많이 도입되고 있고, 영상은 AVI, MP4방식으로 저장되어지고 저장영상길이는 블랙박스 설정 모드(상시녹화, 이벤트녹화, 주차모드등)에 따라 1분~10분미만 단위로 녹화되어지고 있다.

IV. PingPong-256MAC

PingPong-256은 아래 그림 2과 같이 LFSR1 및 LFSR2 그리고 2비트 메모리를 갖는 비선형 출력함수 F, 클럭 조절 함수 등에 의하여 키수열(Keystream)을 발생하는 스트림암호 방식이다[5].

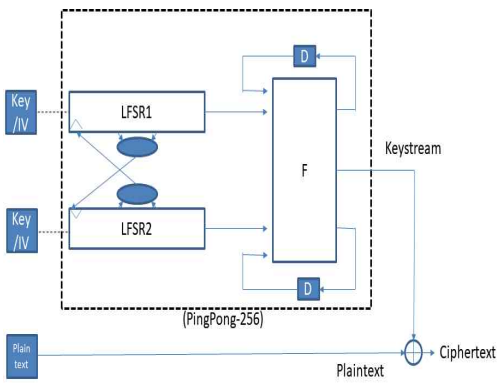

그림 2. PingPong-256 스트림 암호 원리

PingPong-256MAC은 아래 그림 3와 그림 4과 같이 설계할 수 있다.

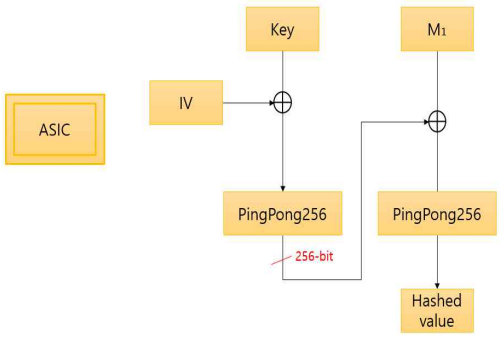

그림 3. 암호 모듈 및 암호과정 구상도

제안하는 암호 모듈 및 암호과정 구상도는 위의 그림 3와 같으며, IV(초기값 256비트)와 Key(비밀키 256비트)를 XOR시킨 후 나온 출력값을 영상정보만큼(M1… Mn)에 XOR시키고 끝으로 출력되어지는 결과가 Hashed value가 된다.

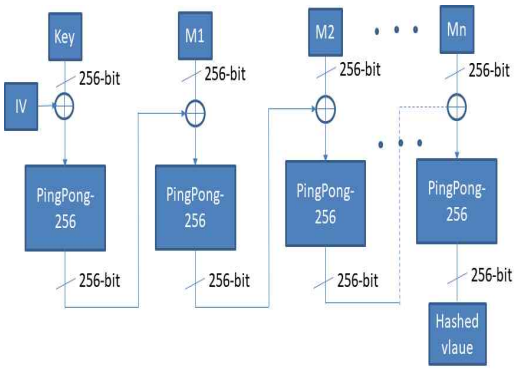

그림 4. PingPong-256MAC 암호과정 상세도

그림 3에서 설명한 배경을 바탕으로 최종적으로 암호과정이 상세하게 이루어지는 그림은 위의 그림 4과 같으며 그림 4에서와 같이 Key(비밀키 256-비트)와 IV(초기값 256-비트)을 XOR 시킨 후에 PingPong-256MAC을 사용하여 256비트 출력값(C1)을 발생시킨다. 그리고 첫 번째 출력값(C1)과 M1 영상정보(256-비트)를 XOR 연산하여 PingPong-256MAC을 사용하여 두 번째 출력값(C2)을 발생시킨다. 계속해서 두 번째 출력값(C2)과 M2 영상정보(256-비트)를 XOR 연산하여 PingPong-256MAC을 사용하여 세 번째 출력값(C3)를 발생시킨다. 이런 방법으로 영상입력이 끝날 때까지 반복수행하고, 최종적으로 256비트 출력 해시값(Hashed Value)를 얻는다.

M1, M2, ...Mn은 실시간 차량용 블랙박스 영상정보가 된다. 블랙박스에 저장되는 정보는 M1, M2, ...Mn 및 해시값(Hashed Value 256비트)가 저장되어야 한다.

만일 공격자에 의하여 Mi 영상 정보 또는 부분 영상정보가 변조 또는 위조가 될 경우에는 블랙박스에 저장된 최종 해시값이 변경되므로 쉽게 변조 사실을 검출할 수 있게 된다.

이때 PingPong-256MAC으로 발생되는 해시함수는 생일 패러독스(Birthday Paradox)에 의하여 안전성 수준이 감소되는데, 결과적으로 안전성은 지수승인 256/2배 즉, $2^{256/2} = 2^{128}$이 된다.

V. 결 론

현재 1 가구당 자동차 소유가 평균 2대 이상인 가구가 계속해서 증가하고 있다. 이처럼 자동차 대수가 늘어남에 따라 차량소유자는 블랙박스 설치도 필수로 하고 있으며, 이는 블랙박스의 중요함을 알 수 있는 이유이며, 이에 따라 블랙박스 제조사들도 더 안전하고 신뢰되는 영상을 저장하기 위해 많은 노력과 발전을 하고 있다. 대표적으로 주간 및 야간 영상녹화 화질 및 화소증가로 인한 판독 및 시안성 증가, 상시녹화 및 이벤트녹화를 저전력 및 GPS위치 기록, 충격감지센서 도입 등 좀 더 섬세하고 자세한 내용을 담기 위해 노력하고 있다.

하지만 블랙박스의 영상은 결국 디지털적인 증거이므로 회손 및 변조 되기 쉬우며 이에 따라 녹화된 영상의 무결성을 입증하지 않으면 증거로써의 효력이 떨어지는건 사실이다. 이러한 문제점을 해결하기 위해 본 논문에서는 영상정보의 무결성을 입증하기 위해 PingPong-256MAC 알고리즘을 적용하여 Hashed value를 생성함으로써 영상의 원본을 입증하고 이를 통해 무결성을 입증하는 방법을 제안하였다.

Acknowledgement

이 논문은 2018년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원(No.2018-0-00285,무인이동체를 위한 HD급 영상 데이터 및 제어 신호 암복호 처리용 고신뢰 듀얼코어 SoC 및 운용시스템 개발)과 2016년도 정부정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임(과제번호: NRF-2016R1D1A1B01011908).

References

[1] Hwihang An, Sangjin Lee, “The analysis of data structure to digital forensic of dashboard camera”, Journal of The Korea Institute of Information Security and Cryptology, Vol. 25, No. 6, pp. 1495-1502, Dec. 2015.

[2] Internet News[Internet]. Available : https://news.joins.com/article/11873710
[3] Internet Blog[Internet]. Available : https://m.blog.naver.com/PostView.nhn?blogId=ineriner&logNo=220353496990&proxyReferer=https%3A%2F%2Fwww.google.com%2F
[4] Hwan-Shin Yu, Eui-Bung Jeoung, "The Optimized File System Designed for Vehicle Black Box System", Journal of Korean Institute of Information Technology, Vol. 14, No. 2, pp.1-6, Feb. 2016
[5] KiHwan Kim, TaeYong Kim, SangGon Lee, WonTae Jang, HoonJae Lee, "Proposal of Parallelization Structure for PingPong256", Journal of Engineering and Applied Sciences, Vol. 13, No.5, pp. 1124-1129, 2018.