JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 20, No. 2, pp. 405-411, Feb. 2019

# 자기검증이 가능한 가역정보 은닉 기반 자동차 블랙박스 영상의 무결성 보장기술

**강 상 욱**
상명대학교 컴퓨터과학과

# Self-Verifiable Video Integrity Technology for Car Dashboard Cameras using Reversible Data Hiding Method

**Sang-ug Kang**
Department of Computer Science, Sangmyung University, Seoul 123-456, Korea

**[요 약]**

차량용 블랙박스의 장착이 점차 보편화되고 의무화되고 있는 추세이다. 블랙박스 영상이 자동차 사고 등에 대한 정확한 증거자료로 사용되기 위해서는 적법절차에 의해 증거가 수집되었는지 여부가 중요하다. 이와 관련하여 블랙박스 소유자가 무제한적인 접근권한을 가지고 있는 블랙박스 영상에 대한 위변조 방지를 위한 동영상 무결성 확보 기술이 필수적이다. 본 논문에서는 H.264 동영상 코덱의 양자화 DCT 계수값인 QDC를 SHA-256 해쉬 함수의 입력값으로 하여 해쉬 이미지를 생성하였다. 또한 블랙박스 제작 시에 안전한 하드웨어적인 장소에 보관된 난수를 기반으로 생성한 키 값을 이용하여 HMAC을 생성하였고, 이를 무결성 확인 정보로 사용하였다. HMAC을 동영상 가역정보 은닉 알고리즘인 차이값 확장기법으로 동일 영상 내에 은닉하였다. 그 결과 정보은닉으로 인한 동영상의 왜곡은 약 0.01dB 수준으로 적으면서도 기존 연구와 달리 단일 파일 만으로 동영상 내용 확인과 무결성 확인이 동시에 가능한 기법을 제안하였다.

**[Abstract]**

The car dashboard camera is becoming increasingly common and mandatory. In order for dashboard camera videos to be used as accurate evidence for car accidents, it is important that the evidence is gathered by due process. In this regard, it is essential to secure video integrity to prevent forgery and falsification of video content, since black box owners have unlimited access rights. In this paper, a hash image is generated by using the quantization DCT coefficients of the H.264 video codec as the input value of the SHA-256 hash function. In addition, HMAC was generated using the key value generated based on the random number stored in the secure hardware place at the time of dashbard camera production and used as the integrity verification information. HMAC is concealed in the same video by the difference expansion technique. As a result, we proposed a technique that can view video contents and verify integrity with only a single file unlike the previous researches, while the distortion of video due to data hiding is as low as about 0.01dB.

**색인어 :** 자동차용 블랙박스, 가역 정보은닉, 실시간 무결성 자기검증, 영상 무결성 검증

**Key word :** Car Dashboadrd Camera, Reversible Data Hiding, Self verifiable Integrity, Video Integrity Verification

**http://dx.doi.org/10.9728/dcs.2019.20.2.405**



**Received** 07 January 2019; **Revised** 06 February 2019
**Accepted** 20 February 2019

***Corresponding Author; Sang-ug Kang**

**Tel:** +82-2-781-7588
**E-mail:** sukang@smu.ac.kr

## Ⅰ. 서 론

교통사고가 발생하는 경우에 사고 발생의 원인을 밝혀내고 책임 소재에 대한 판단을 용이하게 하며 사고 예방의 효과도 있는 등 다양한 이유로 택시 및 버스와 같은 대중교통 시설은 물론이고 개인 차량에도 교통사고 상황을 영상 및 음성으로 기록할 수 있는 차량용 영상기록 블랙박스 (VEDR: Video Event Data Recorder)의 장착이 증가하고 있다. 한 시장조사 전문기업의 설문조사 결과에 따르면 차량용 블랙박스의 필요성에 공감하는 비율이 2013년 84.2%, 2015년 91.5%, 2017년 93.2%로 지속적으로 증가하고 있다 [1]. 장착률 또한 2013년 38.2%, 2015년 61.6%, 2017년 79.3%로 조사되어 실제 차량에 설치하는 비율이 매우 빠른 속도로 증가하는 것으로 나타났다 [1]. 실제로 교통 사기단을 잡거나 블랙박스를 장착한 차량에 대한 보험할인을 받을 수 있는 등 실생활에서의 활용도가 크고, 향후에도 쓰임새가 증가할 것으로 보인다.

하지만 국내외 VEDR 기기에는 영상을 포함한 주행 기록에 대해 위조 및 변조를 방지하고 탐지하는 무결성 검증 및 부인방지 기능이 탑재되어 있지 않거나, 이에 대한 연구가 활발하지 않다. 영상을 포함한 주행속도, 녹화 시간, 녹화 위치 등의 주행기록은 사고조사 기관 및 법원에서 사고 원인 규명 및 사고 상황을 판단하는 데 참고 자료로 활용되고 있으나, VEDR 기기의 소유자가 완벽한 접근 권한을 가지고 있다는 특징 때문에 기록의 임의적인 파기나 조작이 용이하여 이에 대한 보안 조치가 필요하다. 따라서 차량용 블랙박스에서 체증된 기록을 완벽한 법적 증거로서 활용하기 위한 움직임이 활발해지고 있다. 미국에서는 California Assembly Bill 2133, Arkansas Senate Bill 51, Nevada Assembly Bill 315 등 여러 주에서 블랙박스와 관련한 사생활 보호 법률을 제정하여 블랙박스 정보를 법원이 명령할 때만 공개토록 하고 있다. 또한, 자동차용 블랙박스 장착 의무화를 포함하는 연방 자동차 안전 표준안인 49 CFR Part 571이 제정되었다 [2]. 유럽 연합에서는 2009년부터 EU 가입국내의 모든 차량에 대해서 블랙박스를 의무 장착하는 내용의 법안을 확정했고, 일본은 2008년부터 일부 차종에 따라 의무 장착을 시작해 택시, 버스, 트럭 등으로 확대하고 있다. 중국은 2008년에 모든 차량의 디지털 주행기록 장치 장착을 의무화 하기도 했다. 국내에서는 2010년 9월 9일 '디지털 운행기록장치'등 안전장치 비용의 정부지원을 골자로 한 교통안전법 개정안이 발의되었으며, 2011년 4월 국회를 통과하였다.

이러한 상황을 비추어 보면, 향후 블랙박스가 법원에서의 증거 능력을 지닌 제품으로 인정받기 위해서는 보안성 강화가 필요하여, 특히 영상기록의 무결성을 보장하기 위한 실용적인 기술 개발은 반드시 필요하다. 블랙박스라는 장치는 개인이 전적으로 소유하고 있고 데이터 생성과 저장이 동시에 이루어진다는 특성이 있으며, 이러한 특성을 반영하기 위해서는 실시간으로 무결성 및 기밀성 보장이 가능해야 한다. 김윤규 등은[3] 블랙박스에서 발생하는 압축된 영상 비트스트림을 일정한 크기로 나누고 이를 해쉬 함수의 입력으로 이용하여 해쉬 이미지를 출력하고 저장장치에 기록하였다. 만약 사고가 발생하면 증거로 사용될 비트스트림을 이용 하여 생성된 해쉬 이미지와 별도로 저장되어 있는 해쉬 이미지의 일치 여부를 판단하여 무결성을 검증한다. 이 방법은 해쉬 이미지가 별도로 저장되어 있어 무결성 검증 시 영상 비트스트림만 제출된다거나 영상 조작후에 다시 해쉬 이미지가 생성될 경우 무결성 검증 자체가 가능하지 않을 수 있다. 또한, 동영상 압축 프로세스의 양자화 테이블과 같은 헤더정보가 조금만 바뀌어도 영상의 무결성이 증명되지 못하여 영상의 내용과 상관없는 부분까지 무결성을 확보해야 하는 문제점이 있다.

T. Izu 등은[4] 영상의 크기가 커져도 인코딩 계산량을 증가시키지 않도록 영상 프레임 별로 해쉬 이미지를 생성하고 이를 다음 영상 프레임과 결합하여 다음 영상 프레임에 대한 해쉬 이미지를 생성하는 체인 방식의 무결성 검증 기법을 제안하였다. 이 방법 또한 무결성 정보가 별도로 존재하고 영상 내용과 관계없는 무결성 확보 문제가 있다.

이강 등은[5] 입력 영상을 일정한 크기의 블록 데이터로 잘라내어 각각의 블록 데이터를 해쉬 함수를 이용하여 전방 삭제, 후방 삭제, 중간 삭제 등 다양한 공격에도 영상의 무결성을 보장하기 위해 [4]에서 제안한 순환형 해쉬 체인 방식을 개선하였다. 또한 임의의 블록 데이터의 무결성을 검증할 때 발생하는 순차적 무결성 검증의 계산량을 감소시키는 방안을 제시하였다. 최진영 등은 [6] 블랙박스가 전원 탈거, 시동 꺼짐 등 사고 당시에 보이는 기능상의 불안전성을 예시로 보이면서 이에 대응하기 위해 필수적인 기능을 제안하였다. 특히, 불완전하게 영상 파일이 저장될 경우에도 그 시점까지의 무결성 검증이 가능하도록 하며, 전후방 데이터 삭제에도 앞뒤 프레임간의 해쉬 체인만을 사용하여 무결성 정보를 검출할 수 있는 방법을 제시하였다. 하지만 동작의 실시간성에 치중하면서 영상 정보와 해쉬 이미지의 결합성에 대해서는 다루지 않았다. [3]-[6]에서 제시된 방식은 모두 영상정보와 무결성 확인을 위한 정보가 별도의 파일로 존재한다. 또한 무결성 확인 정보를 안전하게 보관하는 방법이 언급되지 않거나, 언급되더라도 영상정보만을 증거로써 제출하는 경우에는 무결성 확인 기능이 무력화 될 수도 있다.

본 논문에서는 단일 영상 파일에 무결성 확인 정보를 가역정보 은닉 방식을 이용하여 삽입하여 무결성 확인 정보가 은닉된 상태로도 영상의 왜곡이 최소화된 상태로 영상을 확인 할 수 있고, 필요시 영상 정보에서 무결성 확인 정보를 추출하여 무결성을 검증하는 기법을 제안한다. 또한 영상 및 주행정보에 대해서 비밀키를 이용하여 무결성 검증용 해시값 (HMAC)을 생성하고 삽입하는 알고리즘을 구현하였다. 블랙박스는 임베디드 시스템의 일종으로 실시간 동작과 적은 컴퓨팅 리소스의 활용이 중요하기 때문에 많은 계산량이 요구되는 동영상 압축 및 복원 환경에서 최적화된 정보은닉 기법을 구현하였고, 제안된 기법을 이용한 시제품을 구현하였다.

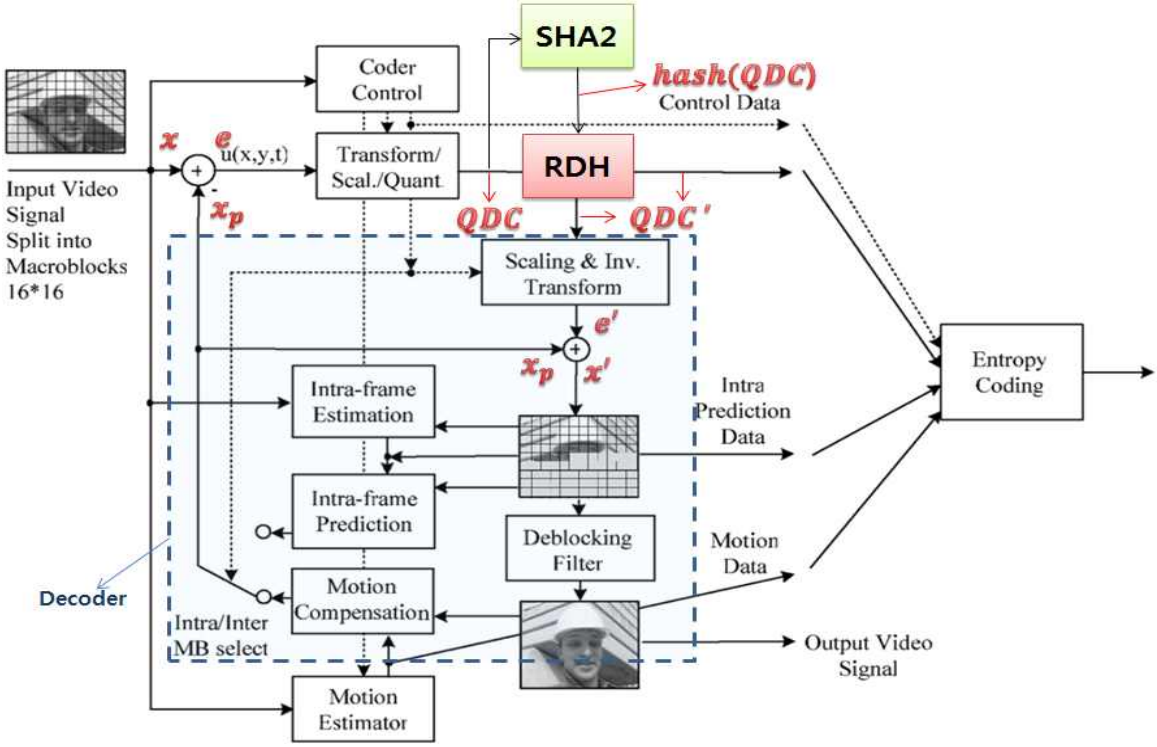



**그림 1.** H.264/AVC 코덱을 이용한 영상 무결성 검증 개념도
**Fig. 1.** The block diagram of video integrity verification based on H.264/AVC

## Ⅱ. 제안하는 영상 무결성 보장방법

가역 정보 은닉(Reversible Data Hiding, RDH) 방법은 멀티미디어 콘텐츠에 비밀 데이터를 삽입하여도 약간의 왜곡이 있는 상태로 콘텐츠를 즐길 수 있고, 비밀 데이터를 추출하고 나면 원래의 콘텐츠 값을 그대로 복원시킬 수 있는 기술이다. 그리고 H.264/AVC (Advanced Video Coding)은 동영상 압축 표준의 하나이며, 기존의 표준과 비교했을 때 절반 이하의 비트레이트(bitrate)에서 비슷하거나 더 좋은 화질을 얻을 수 있도록 개발되었다. 최근 H.265/HEVC (High Efficiency Video Coding)가 차세대 최종 표준안으로 승인되었으나 블랙박스 제품에서는 여전히 H.264/AVC가 많이 이용되고 있어 본 논문에서는 H.264에 기반한 동영상 무결성 검증 기술을 제안하고자 한다.

### 2-1 가역 정보 은닉 기술을 이용한 위변조 탐지 방법

#### 1) 전체 개념도

차량용 블랙박스 장치에 장착된 카메라를 통해 얻은 영상 정보는 표준 H.264/AVC 코덱에 의해서 압축되어 저장된다. 전체적인 영상 무결성 검증 개념도는 그림1에 나타내었다. 동영상 압축은 기본적으로 손실코딩이다. H.264의 동영상 압축 과정을 대략적으로 살펴보면 입력되는 동영상은 16×16크기의 매크로 블록으로 나뉘게 되고 각각의 매크로 블록은 공간 영역의 값을 주파수 영역으로 변환시켜주는 변환과정을 거치고 양자화 과정을 거쳐 중간 출력 값으로 양자화 계수를 생성한다. 이 양자화 계수는 복원할 경우 원래의 값으로 복원되지 않아 양자화 손실이 발생한다. 이후의 단계인 엔트로피 코딩 과정에서는 양자화 계수를 통계적인 기법을 이용하여 압축하기 때문에 손실이 발생하지 않는다. 따라서 양자화 계수를 입력으로 받는 해쉬 함수를 SHA-2를 이용하여 해쉬 이미지를 생성하고 이를 RDH 방식을 이용하여 다시 양자화 계수에 숨기는 방식으로 영상 자체에 무결성 정보를 혼재시켜 영상의 왜곡을 최소화하면서 무결성 검증도 할 수 있는 새로운 개념을 제안한다. 제안하는 방식은 압축과 동시에 무결성 확인 데이터가 생성되고, 헤더 정보의 변경과 무관하면서 영상 콘텐츠 자체의 무결성만 검증하는 방식이다. 그리고, SD카드에 최종적으로 저장되는 H.264 호환성이 보장되는 비트스트림 만으로 자체검증이 가능하다.

히스토그램 쉬프팅 (Histogram Shifting, HS) [7], 차이값 확장 기법 (Difference Expansion, DE) [8], 추정 에러값 확장 기법 (Prediction Expansion, PE) 등 다양한 RDH 방식이 존재하지만 양자화 계수 (Quantized DCT Coefficient, QDC)는 정보 은닉으로 인한 왜곡에 취약하다는 점과 실시간 계산이 필요하다는 점을 고려하여 QDC 값에 최적화된 DE 기법을 적용하는 것이 가장 적합하다. 특히, QDC의 변형으로 인한 현재 영상 프레임의 왜곡은 다음 영상 프레임에 그대로 전파될 수 있어 이를 고려한 최적화 알고리즘 설계가 필요하다. RDH 방식으로 해시 이미지

를 영상 내부에 삽입하므로, SD 카드에 저장하는 방식과 달리 직접 접근에 노출되지 않는 보안효과를 얻을 수 있고 영상 정보와 무결성 확인 정보의 정확한 동기화로 인해 전방, 후방, 중간 삭제 등의 다양한 공격에 대응할 수 있다. 그리고, 무결성 정보를 제출하지 않는 무력화 우려도 제거될 수 있다.

**2) 인코딩 알고리즘**

블랙박스의 카메라로부터 영상을 취득하여 압축과 동시에 무결성 검증을 위한 데이터를 생성 은닉하는 제안하는 상세한 알고리즘은 다음과 같다.

첫째, H.264 인코딩 과정에서 휘도 (Luminance) 성분의 I-frame을 대상으로 가역 정보 은닉 알고리즘을 적용한다. 이는 SHA-256으로 생성된 해쉬 이미지의 크기가 256비트에 불과하여 통상적으로 화질이 HD급인 영상 정보의 휘도 성분에만 은닉하기에 문제가 없으며 사람의 눈에 보다 민감한 색도 (Chrominace) 성분이 정보 은닉에 따른 왜곡이 생기지 않도록 한다. 또한 P-frame에 정보를 은닉하게 되면 같은 양의 은닉 정보에 대해 I-frame 보다 왜곡이 심해진다는 사실도 고려했다.

둘째, 원영상 $x$ 와 화면 내 예측영상 $x_p$의 차이영상 $e$ 값을 계산한다. $e$ 값을 입력으로 scaling, integer DCT, 양자화의 과정을 거쳐 QDC 값을 생성한다. 이 과정에서 rate distortion 최적화를 수행할 수 있는데 이 경우에는 최종 QDC 값을 이용한다.

셋째, 크기가 16x16인 매크로 블록 안에서 zigzag scanning 방식으로 QDC 값을 순차적으로 나열한다. 이런 방식으로 모든 매크로 블록의 QDC를 나열하고 모두 연결해서 하나의 스트림으로 완성시킨다. 이것을 SHA-256 해시 함수의 입력으로 사용하여 HMAC(The Keyed-Hash Message Authentication Code)를 구한다. 여기서, 키는 개인키를 그대로 해쉬 이미지의 앞뒤에 단순히 붙이는 방식이기 때문에 계산량이 적고 부인방지 용도로 사용 가능하다.

넷째, DE기법을 사용하여 하나의 매크로 블록에 1 비트를 숨긴다. zigzag scan 순서의 중간에 위치한 두 개의 양자화 계수 값 $p$, $q$을 이용하여 이들의 차이 값에 HMAC중 1 비트를 순차적으로 숨긴다. 여기서 원래의 QDC 값은 차이값과 숨긴 비트 값에 의존적으로 왜곡되어 QDC'로 수정된다. 처리 프로세스는 [8]에서 제시된 방법을 수정한 아래 수식을 이용한다.

original two QDC values in the middle : $p$, $q$

$$l = \left\lfloor \frac{p+q}{2} \right\rfloor, \; h = p - q$$

one bit hiding: $H = 2h + bit$ (difference expansion)

modified QDC' : $P$, $Q$

$$P = l + \left\lfloor \frac{H+1}{2} \right\rfloor, \; Q = l - \left\lfloor \frac{H}{2} \right\rfloor$$

$$\left(\text{since, } p = l + \left\lfloor \frac{h+1}{2} \right\rfloor, \; q = l - \left\lfloor \frac{h}{2} \right\rfloor \right)$$

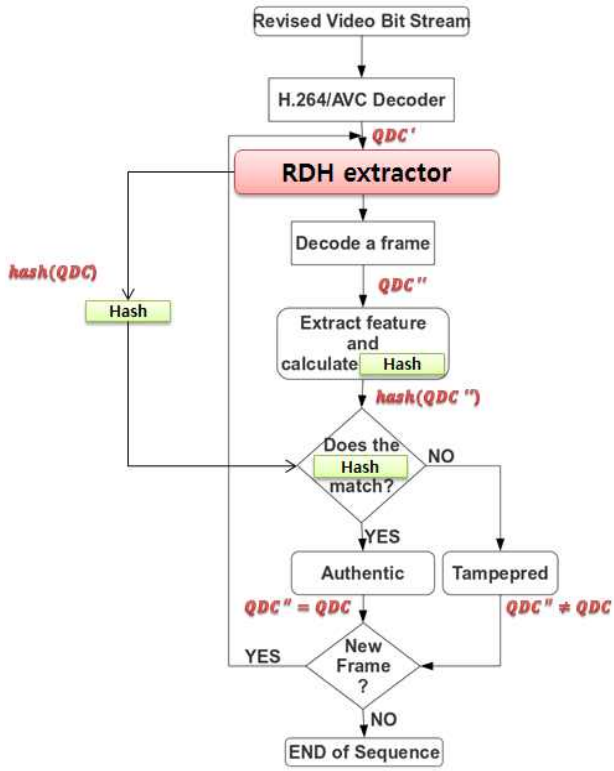



**그림 2.** 영상의 무결성 검증과정 흐름도
**Fig. 2.** The flowchart for video integrity verification

**3) 디코딩 및 검증 알고리즘**

블랙박스의 SD카드에 저장된 H.264 비트스트림은 있는 그대로 통상적인 H.264 player를 통해 영상을 확인할 수 있다. 하지만 무결성에 대한 검증이 필요한 경우 다음과 같은 알고리즘을 통해 무결성을 확인한다.

첫째, SD 카드에 저장된 H.264 비트스트림을 읽어 entropy decoding을 수행하여 수정된 양자화 계수값인 QDC'를 얻는다. 이때 H.264 디코더는 비트스트림의 헤더정보를 읽어 영상 복호화에 필요한 모든 정보를 취득한 상태이며, 본 실험을 위해 추가된 무결성 검증 옵션이 헤더정보에 포함되어 있어야 한다.

둘째, 매크로 블록 단위로 얻은 QDC' 값을 나열하고, zigzag scan 순서의 중간 위치에 있는 두 개의 QDC' 값인 $P$, $Q$를 얻는다. 그림 2의 “RDH extractor", 즉 가역 정보 추출기에 구현되어 있는 아래의 수식을 통해 삽입되어 있던 HMAC값을 순차적으로 추출해 냄과 동시에 원래 QDC 값이라 추정되는 QDC" 값 $p'$, $q'$를 계산한다. 모든 매크로 블록에 대해 이러한 과정을 되풀이 하여 최종적인 HMAC과 QDC"를 구한다.

셋째, zigzag scanning 방식으로 QDC" 스트림을 만들어서 hash(QDC")을 구한 후에 추출한 HMAC에서 구한 hash(QDC)과 일치하는 지 여부를 비교하여 일치하면 무결성이 보장되었다고 판단한다. 또한 동시에 추출된 key를 이용하여 영상의 소스를 검증하여 부인방지에 사용한다.

modified two QDC' values in the middle : $P$, $Q$

$$h = \left\lfloor \frac{H}{2} \right\rfloor, \; H = P - Q, \; l = \left\lfloor \frac{P+Q}{2} \right\rfloor$$

one bit extraction: $bit = H - 2h$

recovered QDC" : $p'$, $q'$

$$p' = l + \left\lfloor \frac{h+1}{2} \right\rfloor, \; q' = l - \left\lfloor \frac{h}{2} \right\rfloor$$

### 2-2 무결성 검증용 비밀키 관리

본 논문의 내용은 실제로 하드웨어적인 블랙박스 장치로 구현하였다. 따라서 비밀키 관리를 하드웨어적인 접근제어를 적용하여 이용자 및 일반인과 접근을 근본적으로 막았다. 블랙박스 내부에서 리눅스 임베디드 운영체제를 일부 수정해서 설치하여 일반적으로 사용자가 접근하기 어려운 NAND flash memory의 비밀 저장소에 R1 이라는 난수를 저장해두고 응용프로그램 실행 코드의 임의의 장소에 R2 라는 난수를 저장하였다. 그리고 두 난수의 배타적 논리합 연산을 통해 실제 키 값 K(2bytes) = R1⊕R2를 생성한다. 이 키는 K||hash(QDC)||K 형식의 HMAC 값을 만들 때 사용된다. 키 값을 가지고 있는 사람만이 똑같은 HMAC을 생성할 수 있는데, NAND flash memory에 접근해서 R1을 얻었다 할지라도, 그것은 실제 키 값이 아닌 난수이며, R2를 알지 못하면 키 값을 얻을 수 없는 구조이다.

키 값에 대한 분배는 키의 유출이 우려되는 온라인을 통해서 이루어지는 것이 아니고, 제조시에 하드웨어적인 방법으로 저장되는 방식이다. 또한 블랙박스가 네트워크에 연결되어 있지 않아 네트워크 취약점을 이용한 해킹의 염려도 없으며, 공격자가 차량의 잠금장치 해제 또는 파손의 방법으로 블랙박스 기기를 가져가는 것이 유일한 키 유출의 가능성이 있으나 이러한 상황은 물리적 보안 영역에 속한다.

## Ⅲ. 실험 결과

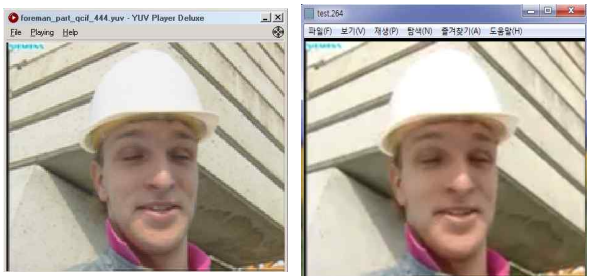
### 3-1 가역 정보 은닉 영상 생성 및 영상 변조

#### 1) 가역 정보 은닉 영상 생성

테스트 영상으로 176×144 크기의 QCIF (Quarter Common Intermediate Format) 해상도의 raw data를 가지는 foreman.yuv를 이용하였다. 그림 1에서 제시된 절차로 DH 기법을 이용하여 영상 무결성 확인 정보인 HMAC을 은닉한 결과는 표 1에 나타내었다. I-frame 5개에 대해 HMAC을 가역정보은닉 알고리즘으로 삽입하여 압축한 경우와 그렇지 않은 경우를 비교하였다. 그 결과 예상과 같이 압축 효율성이 다소 떨어지게 되어 비트수는 조금 늘어나고 영상의 품질은 다소 떨어진다. 이는 영상의 유사성과 비례하는 PSNR (Peak Signal-to-Noise Ratio) 값은 더 작아지고, 원본 영상과의 차이 값에 비례하는 MSE(Mean Squared Error) 값은 커지는 사실을 통해 알 수 있다.

**표 1.** foreman 테스트 영상에 대한 가역정보 은닉 결과
**Table 1.** The result of RDH for foreman test sequence

| | # of bits (bits) | PSNR (dB) | MSE |
|---|---|---|---|
| Original image | 76480 | 40.712 | 6.97950 |
| Stego image | 77200 | 40.703 | 7.00182 |



(a) (b)

**그림 3.** (a) 원본 영상 (b) 무결성 정보 은닉 영상
**Fig. 3.** (a) The original video (b) Integrity information hiddend video

위의 그림 3은 원본 영상과 무결성 정보 은닉 영상의 화질 차이를 비교한 예시인데, 육안 상으로는 그 차이가 미미하다는 것을 알 수 있다. 아래 표 2 및 그림 4는 실제 제작한 블랙박스 장치에서 실험한 결과를 보여준다. 테스트 영상과 마찬가지로 비트 수는 다소 늘어나지만 화질은 약간의 저하만 발생함을 볼 수 있다. 또한 그림 4에서는 카메라로 부터 HD급 화질의 입력 영상을 입력으로 해서 HMAC을 구하고 이를 화면의 왼쪽 윗부분에 나타내었다. 실제로는 비가시적으로 삽입되는데, 본 실험에서는 이해를 위해 해당 프레임 마다 가시적으로 보이게 구현하였다.

**표 2.** 실제 블랙박스 장치에서의 테스트 결과
**Table 2.** The result of RDH using real dashboard camera

| | # of bits (bits) | PSNR (dB) | MSE |
|---|---|---|---|
| Original image | 14,992,040 | 38.032 | 10.69774 |
| Stego image | 15,011,584 | 38.030 | 10.70393 |


**그림 4.** 블랙박스 장치 화면캡쳐
**Fig. 4.** The shot from the dashboard device

(a) original video (b) attacked video

**그림 5.** 영상 변조 예시 (신호등 변조)
**Fig. 5.** The example of video integrity attack (traffic light)

**2) 영상 변조**

영상변조 케이스 #1 : Adobe After Effect, SONY Vegas 등 다양한 동영상 편집 소프트웨어를 이용하여 압축된 비트스트림을 디코딩하여 raw data 상태의 영상에서 변조를 가할 수 있다.

변조 케이스 #2 : HEX 에디터 등을 이용하여 압축된 동영상 비트스트림 정보에 접근하여 변조를 가할 수 있다.

실제로 블랙박스 장치의 SD카드에 저장되는 파일은 음성과 영상 모두를 포함하고 있는 avi 형식의 컨테이너 파일인데, 영상의 각 프레임 헤더에는 ASCII 코드 “00dc (16진수)“라는 정보가 포함되어 있고 이를 통해 영상 정보를 찾아갈 수 있다. 본 실험에서는 H.264 압축코덱 전용칩인 TI 사의 DM385 DaVinci Digital Media Processor 를 사용하였다. 이 칩으로 인코딩이 될 때에는 30초에 한 번씩 나타나는 I-frame 헤더에서 27(16진수)이라는 고유의 정보가 생성되기 때문에 공격자가 이러한 정보를 인지한다면 악의적인 변조가 가능하다.

### 3-2 실시간 위변조 검증

본 논문에서 제안한 기술은 실시간으로 온라인 상에서 위변조 여부를 조회하는 방식에 적합하다. 블랙박스의 SD카드에 저장된 xxx.avi 파일만 검증 서버에 전송하면 서버에서 무결성을 판단하여 결과를 클라이언트 프로그램에 알려줄 수 있다. 이러한 기능을 구현하기 위해 개발한 동영상 위변조 검증 프로그램은 그림 6에 제시되어 있고 기능은 다음과 같다.

① HD 화질인 1280 x 740 까지 가능한 동영상 프레임 사이즈 입력부
② Raw data인 xxx.yuv 또는 압축 파일인 xxx.264 파일 열기
③ 무결성 정보 생성 및 RDH 기법으로 무결성 정보를 은닉하면서 H.264 부호화
④ 일반적 H.264 복호화 실행
⑤ 은닉된 해시값을 역 RDH기법으로 추출하면서 H.264 복호화 실행
⑥ 추출된 해시값과 원본 영상을 입력값으로 하여 새롭게 생성된 해시값 비교하여 무결성 검증. 이 기능은 온라인으로 수행하는 것이 바람직함
⑦ 동영상 재생기 관련 여러 기능들

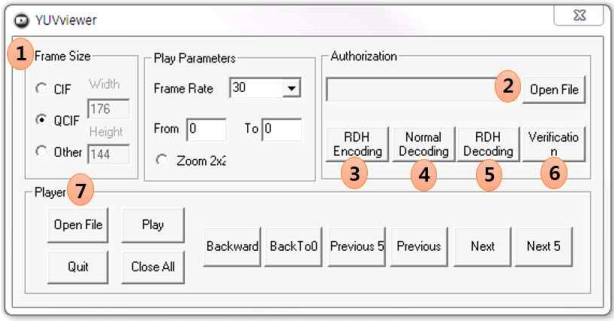



**그림 6.** 실시간 동영상 위변조 검증 클라이언트 프로그램
**Fig. 6.** The realtime video integrity verification client application

제작된 제품을 이용하여 1분 동안 실시간으로 영상을 기록하면서 처리 시간을 측정하였고 초당 30 프레임 (1초당 1개의 I frame) 이상의 영상을 처리할 수 있었다. 자세하게는 0.036초/1 frame, 0.107초/30 frame의 처리 속도를 보여 블랙박스의 여타 기능을 처리하면서도 제안한 알고리즘이 실시간으로 동작하는 것을 보여주었다.

## Ⅳ. 결론

차량용 블랙박스는 보안 및 안전성에 관해 지속적으로 법제화 및 의무화가 진행되고 있고, 무결성 문제를 해결해야 법적 증거 능력을 확보할 수 있다. 본 논문에서는 SHA-256 해쉬 함수를 이용한 하나의 프레임의 무결성 정보를 해당 프레임에 가역적으로 은닉하는 것이 큰 영상의 왜곡 없이 가능하다는 것을 보여주었다. 또한 별도의 무결성 확인을 위한 정보 없이 대부분의 블랙박스 압축 영상 포맷인 H.264기반의 avi 형태의 단일 파일만으로 영상의 내용확인과 무결성 증명이 실시간으로 이루어질 수 있어 보다 실질적인 기술을 제시하고 있다. 주행기록 정보도 영상정보와 함께 해쉬 함수의 입력으로 사용한다면 주행 정보에 대한 무결성도 동시에 확보할 수 있다. 또한 제안한 동영상 가역정보 은닉 기술을 H.264 코덱 칩에 적용시켜 무결성 검증하는 기술을 구현하여 임베디드 환경인 블랙박스 장치에 적용하였다. 본 연구에서 제안한 실제적인 블랙박스 동영상 무결성 확인 기술은 기존 블랙박스의 구조의 변화를 최소화하면서 구현 가능하다는 것이 큰 특징이다.

## 감사의 글

본 연구는 2017년도 상명대학교의 교내연구비 지원에 의하여 수행한 연구입니다.

## 참고문헌


[1] Embrain. Embrain trend monitor [internet]. Available: http://www.stat.co.kr/site/datanews/DTWork.asp?itemIDT=1002304&aID=20170310110319763&search_keyword=

[2] IRS Global, *The comprehensive analysis toward the business strategy and market forecast for 2014 car dashboard cameras*, 2013.

[3] Y. Kim, B. H. Kim, and D. H. Lee, “Real- time integrity for vehicle black box system,” *Korea Inst. Inf. Security & Cryptology*, vol. 19, no. 6, pp. 49-61, Dec. 2009.

[4] T. Izu, M.Takenaka, J. Yajima, T. Yoshioka, "Integrity Assurance for Real-time Video Recording," in *Proc. of the 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp.651-655, 2012.

[5] Yi Kang, Kyung-Mi Kim, Yong Jun Cho, "A Car Black Box Video Data Integrity Assurance Scheme Using Cyclic Data Block Chaining," *Journal of Korea Information Science*, vol.41 no.11, pp.982-991, 2014.

[6] Jin-young Choi, Nam Su Chang, "Integrity Verification in Vehicle Black Box Video Files with Hashing Method," *Journal of the KICS*, vol.42 no.1, pp.241-249. 2017.

[7] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, ”"Reversible data hiding,”" *IEEE Trans. on Circuits and Systems for Video Technoloy*, vol. 16, no. 3, pp.354-362, 2006.

[8] J. Tian, “Reversible data embedding using a difference expansion”, *IEEE Transaction on Circuits and Systems for Video Technology*, vol.13, no. 8, 2003.

[9] Hyunjung Kim, Sang-ug Kang, "Technology for ensuring the integrity of car dashboard video based on reversible watermarking technique using difference expansion," *in Proc. of IEEK summer seminar*, 1409-1411, 2014.



**강상욱**(Sang-ug Kang)

1996년 : University of Southern California (공학석사)
2011년 : 고려대학교 (공학박사-멀티미디어 보안)

1993년～1994년: 한국 IBM 주식회사
1996년～2002년: 삼성전자 중앙연구소
2002년～2012년: 한국정보화진흥원
2012년～현 재: 상명대학교 컴퓨터과학과 교수
※관심분야 : 인공지능, 디지털저작권, 멀티미디어 보안 등