Journal of The Korea Society of Computer and Information
Vol. 18, No. 6, June 2013
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2013.18.6.047

디지털 운행기록장치의 운행기록 데이터 디지털 인증 시스템

강 준 규*, 김 유 원*, 임 웅 택*, 전 문 석**

Digital Tachograph Vehicle Data Digital Authentication System

Joon-Gyu Kang*, Yoo-Won Kim*, Ung-Taeg Lim*, Moon-Seog Jun**

요 약

본 논문에서는 디지털 운행기록장치로부터 수집된 운행기록 데이터에 대한 효율적인 디지털 인증이 가능한 시스템을 제안하였다. 국내의 경우 수집된 운행기록 데이터가 위변조 되지 않은 신뢰성 있는 정보인지를 판단할 수 있는 방안이 마련되어 있지 않다. 제안하는 방법은 전자서명을 이용하여 전송된 운행기록 데이터가 위변조 되지 않았음을 증명할 수 있다. 디지털 인증을 위한 서명 값 생성은 운행기록 데이터의 해시 값을 구하여 전자서명 생성키로 생성한다. 그리고 데이터 위변조에 대한 확인은 전자서명 값으로부터 전자서명 검증키를 사용하여 해시 값을 구하여 보관된 해시 값과 일치 여부 확인을 통해 이루어진다. 제안하는 방법은 시스템 구현 및 실험을 통하여 운행기록 데이터에 대한 신뢰성을 보장함을 확인하였다.

▸ Keywords : 운행기록, 디지털 운행기록장치, 전자서명, 운행기록 분석시스템

Abstract

In this paper, we proposed an efficient digital authentication service system for the vehicle data collected from digital tachograph. In domestic, There is no method available to verify that information has not been forged and reliable information for collected vehicle data. The proposed method in this paper can prove transmitted vehicle data that have not been forged using the signature value. The signature value of digital authentication is produced with the digital signature generation key after obtaining the hash value of vehicle data. It is achieved through checking the stored hash value and the hash value match that is obtained with the digital signature verification key from the digital signature value. We confirmed the proposed system can

•제1저자 : 강준규 교신저자 : 김유원
•투고일 : 2013. 5. 5, 심사일 : 2013. 5. 20, 게재확정일 : 2013. 6. 3.
* 부천대학교 컴퓨터소프트웨어과(Dept. of Computer Software, Bucheon University)
** 숭실대학교 컴퓨터학과(Dept. of Computer Science, Soongsil University)

ensure reliability of vehicle data through the system implementation and experiment.

▸ Keywords : Vehicle Data, Digital Tachograph, Digital Signature, Digital Tachograph Analysis System

I. 서 론

디지털 운행기록장치의 운행기록 데이터 디지털 인증 시스템은 디지털 운행기록장치의 운행기록 데이터의 위변조 여부를 확인할 수 있도록 하는 시스템을 말한다. 디지털 운행기록장치의 운행기록 데이터를 이용하면 차량에 대한 운행정보 분석이 가능하여 안전 및 경제적 운전을 위한 각종 분석 자료 제공이 가능하고, 차량에서의 이벤트 발생과 같은 과학적인 사고분석이 필요할 경우에도 이 운행기록 데이터를 이용할 수 있다.

대부분의 경우 운행정보는 데이터 수집 위주로 되어 있어서 운행기록에 대한 데이터 분석은 가능하지만, 해당 데이터에 대한 위변조 여부를 판단할 수 있는 프로세스가 정의 되어 있지 않다. 따라서 수집 분석된 운행정보의 신뢰성 판단이 필요할 경우에 현재의 시스템 환경에서는 판단이 불가능하여 디지털 운행기록장치 제조사에 직접 분석을 의뢰하는 경우가 종종 발생하고 있다.

버스, 화물차와 같은 상용차의 경우 디지털 운행기록장치를 반드시 장착하도록 법령[1]으로 규제하고 있어서 운행기록 데이터 또한 지속적으로 증가하고 있으며, 운행정보 데이터의 위변조 여부를 판단해야 하는 사례가 빈번하게 발생하고 있어서, 이와 관련된 기술 및 적용 사례에 대해서 알아보고, 본 논문을 통하여 국내 실정에 적합한 시스템을 제안한다.

국내의 경우, 법령에 의하여 기 등록된 차량은 2012년 12월 31일까지, 일부 운수사업자의 경우 2013년 12월 31일까지, 신규 등록 차량의 경우는 2011년 1월 1일부터 운행기록장치를 장착하도록 의무화하고 있으며 운행기록장치 및 운행기록의 점검 등에서 운행기록의 조작 여부를 점검할 수 있도록 하고 있다[1,2]. 하지만, 조작 여부를 어떻게 점검할지에 대한 업무 절차나 시스템은 정의되어 있지 않다.

국내의 경우 전송된 운행기록 데이터가 위변조 되지 않았음을 증명할 수 있는 프로세스가 디지털 운행기록장치 및 관련 시스템 환경에 정의되어 있지 않기 때문에 디지털 운행기록장치로부터 수집된 운행기록 데이터에 대한 디지털 인증이 불가능한 상태로 개발되어 적용되고 있다. 따라서 운행기록 데이터 분석 시 데이터의 위변조 여부를 증명할 방안이 없다. 유럽처럼 RAW 데이터가 발생되는 디지털 운행기록장치에서의 디지털 인증기능 추가가 필요하지만 국내 디지털 기록장치 제조사의 경우는 설계 단계에서부터 적용하고 있지 않다.

현재는, 차량 운행정보 분석이 필요한 수사기관, 보험사 또는 기타 기관에서 직접 디지털 운행기록장치로부터 운행기록을 USB 또는 기타 인터페이스를 통하여 다운로드한 후 운행기록을 제조사가 제공하는 분석 소프트웨어를 이용하여 분석하거나 또는 차량으로부터 수거된 디지털 운행기록장치를 해당 제조사로 직접 보내서 운행기록 데이터의 분석을 의뢰하게 되는데, 이 경우 운행기록 데이터의 신뢰성을 검증할 수 있는 객관적인 프로세스가 없는 실정이다.

만일, 공인기관에서 운행기록과 함께 디지털 서명을 보관하여 제공하거나 또는 모든 차량의 운행기록을 한 곳에 수집하여 저장하게 되면, 상당한 크기의 스토리지가 필요하게 되므로 운행기록 데이터는 수집되는 기관별로 분산 저장 관리하고 운행기록 데이터에 대하여 해시코드(Hash Code)로 생성된 전자서명(Digital Signature)을 목록화한 테이블만 공인기관에서 저장 관리하면 이러한 문제를 해결 할 수 있다.

따라서 본 논문의 목적은 차량 운행정보에 대한 전자서명을 만들어 목록화 하고 검증할 수 있는 방안을 제시하고 이를 설계하여 시스템으로 구현, 실험 평가 하는 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구와 운행정보 관리에 대한 문제점을 알아보고, 3장에서는 본 논문에서 제안하는 운행기록 데이터 디지털 인증 시스템에 대해 기술한다. 4장에서는 실험을 통하여 제안 방법의 타당성을 검증하고 5장에서 결론을 맺는다.

II. 관련 연구 및 동향

1. 국내외 동향

디지털 운행기록장치에서의 운행기록 데이터에 대한 디지털 인증과 관련하여 유럽을 중심으로 연구 및 상용화가 진행

되었다[3,4]. 하지만 국내의 디지털 운행기록장치는 차량에서 발생하는 운행정보를 수집하는 용도 위주로 되어 있고 수집된 데이터에 대한 디지털 인증에 관한 방안은 마련되어 있지 않은 실정이다.

2. 운행기록장치

운행기록장치(Tachograph)는 차량의 안전운행 및 교통단속을 위하여 개발되어, 1960년~1970년에는 기계식 운행기록장치(Mechanical Tachograph)가 사용되었고, 그 이후에는 전자식 운행기록장치(Electronic Tachograph) 와 아날로그 운행기록장치(Analogue Tachograph)가 사용되었다. 그리고 2006년 이후부터는 디지털 운행기록장치(Digital Tachograph)로 계속 발전하였다[5,6,7].

디지털 운행기록장치는 그림 1 에서 보는바와 같이 CPU, 메모리, 여러 가지 IO 인터페이스, LCD 패널, 통신포트, GPS 및 G센서, 기타 센서 등 다양한 운행정보를 초 또는 1/100초 단위로 수집하여 내부 메모리에 저장하는 전자적인 장치이다.

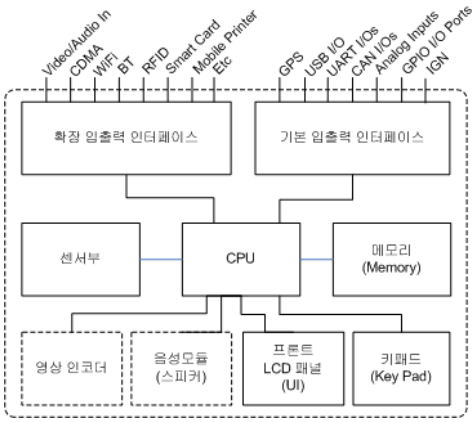

그림 1. 차량용 디지털 운행기록장치의 블록 구성도

Fig. 1. Architecture of Digital Tachograph

3. 운행기록 분석시스템 및 교통안전정보 포탈시스템

교통안전공단은 2011년 인터넷 포탈 형태의 교통안전정보 관리시스템[8]을 구축하여 다양한 관련 정보를 제공하고 있다. 또한 그림 2에서 보는바와 같이 운행기록분석시스템[9]을 구축하여 운수사업자가 보유한 차량으로부터 수집한 운행정보에 대한 다양한 분석 정보를 관리하고 운수사업자에게 제공하여 교통사고 예방과 과학적인 안전관리가 가능하도록 하였다.

사업용 차량을 보유한 운수사업자는 자체 관제 시스템의 일부로 운행기록 분석 시스템을 별도로 구성하여 자체 차량안전운전 및 관리용으로 사용하고 있다. 하지만, 대부분의 운수사업자는 자사 차량에 설치되는 디지털 운행기록장치 제조사가 제공하는 운행기록분석시스템을 사용하고 있다.

운행기록분석시스템은 운행기록을 USB와 같은 저장장치 또는 유무선 통신망을 이용하여 데이터를 수집하여 데이터베이스화하고 운행기록 조회, 종합 진단, 운행기록 분석, 운전패턴분석, 전자지도를 이용한 운행경로 확인 등 다양한 정보로 가공하여 운전 패턴 분석을 통한 사고감소, 운행기록 분석을 통한 차량 운영비용 절감, 운전자별 안전진단 등의 효과를 기대할 수 있다.

그림 2. eTAS 운행기록분석시스템[9]

Fig. 2. eTAS Digital Tachograph Analysis System[9]

4. 운행정보 수집 경로 및 보관

디지털 운행기록장치로부터 수집되는 차량운행정보는 정해진 수단 및 절차로 수집 보관된다. 그림 3에서 보는바와 같이 USB, WiFi, 모바일 네트워크와 같은 수단을 이용하여 운수사업자의 수집서버 또는 관제서버에 데이터를 수집하여 분석 활용하며, 이 데이터는 다시 정해진 포맷[1]에 맞추어 인터넷을 통해 교통안전공단의 eTAS라고 하는 운행기록분석시스템[9]으로 송신되어 공공목적으로 활용되는데, 이 정보는 운수사업자를 포함한 여러 수요처에서 웹으로 접속하여 다양한 폼으로 분석된 정보를 조회 및 활용할 수 있다.

운행정보는 디지털 운행기록장치, 운수사업자의 수집서버, 공공기관인 교통안전공단의 운행기록분석시스템 모두에 같은

정보가 보관되는 형태이다. 만일 어느 한 곳으로부터 운행정보를 받는다고 하면 그 정보가 다른 두 곳에 보관되어 있는 데이터와 동일한 것인지 판단하기가 어려운 경우가 발생한다.

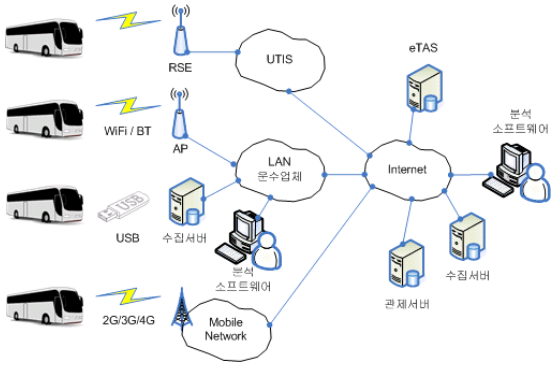

그림 3. 운행 정보 데이터 수집 보관 활용 절차
Fig. 3. Flow of Vehicle Data Collection and Management

5. 디지털 서명

디지털 서명은 지금까지 널리 일반화되어 종이 문서에 표기되던 수기 서명이나 인장의 효과를 전자적 매체 내에 저장 또는 전송되는 전자문서에 효과적으로 서명 효과를 부여하는 전자적 서명 방식을 말한다[10].

디지털 서명에서는 서명 주체자가 한 쌍의 디지털 서명키를 보유하게 된다. 하나는 전자 서명 시 사용하는 디지털 서명 생성키로 자신만이 비밀리에 보관해야 하는 개인키(Private Key)이고, 나머지 하나는 전자서명을 확인 할 때 사용하는 디지털 서명 검증키로서 검증을 원하는 사용자에게 공개할 수 있는 공개키(Public Key)이다[11,12].

디지털 운행기록장치의 운행기록 데이터 원본에 대한 훼손 또는 변경 사실이 없음을 증명하기 위한 디지털 인증 수단으로 디지털 서명 방식을 적용할 수 있다. 디지털 서명은 원본 데이터에 대해 해시함수를 통하여 해시 값을 구한 후에 이 값을 디지털 서명자만이 알고 있는 디지털 서명 생성키(Private Key)로 암호화하여 디지털 서명 값을 구하여 별도로 보관함으로서 이루어진다.

향후, 원본 데이터에 대한 훼손 또는 위변조 사실이 없음을 증명할 때는 증명할 원본 데이터에 대한 해시 값을 구하고, 이미 생성하여 보관 중인 디지털 서명 값을 디지털 서명 검증키(Public Key)로 복호화 하여 해시 값을 구한 후, 두 해시 값의 일치 여부를 비교함으로서 원본 데이터의 무결성을 검증하여 위변조 여부를 판단하게 된다.

III. 운행기록 데이터 디지털 인증 시스템

1. 시스템의 구조

본 논문에서 제안하는 디지털 운행기록 데이터에 대한 디지털 인증 시스템은 그림 4와 같이 운행 데이터 수집 블록인 DTG(Digital Tachograph)블록 및 전자서명 생성 블록과 전자서명 확인 블록으로 구성된다. 전자서명 생성 블록은 전자 서명을 하는 과정으로서 운수사업자가 보유한 차량에서 발생하는 운행기록 데이터로부터 해시 값을 구하여 해시 값에 전자 서명을 한 전자 서명 값을 보관하고 전자 서명 값과 전자서명 검증키를 공인기관에 전송하여 보관한다.

전자서명 확인 블록은 운행기록 데이터에 대한 무결성을 증명하는 과정으로서 운수사업자가 보유한 운행기록 데이터로부터 해시 값을 다시 계산하고, 교통안전공단과 같은 공인기관에서 보유하고 있는 전자서명 값으로부터 전자서명 검증키를 사용하여 해시 값을 복원하여 두 해시 값의 일치성 여부를 비교하여 운행기록 데이터의 무결성 여부를 판단하는 과정이다.

디지털 인증을 위해 운수사업자가 유지해야 할 운행기록 테이블 구조는 표 1과 같다. 필드 구성은 차량등록번호, 시동을 켠 시간인 IGN(Ignition) ON TIME, 시동을 끈 시간인 IGN OFF TIME, 전자서명 값, 전자서명 알고리즘으로 구

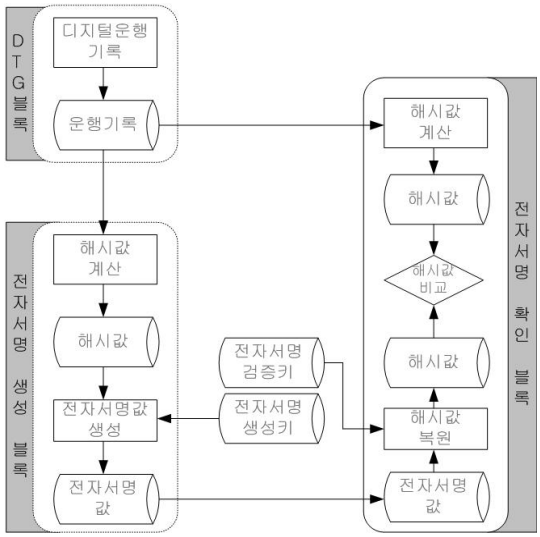

그림 4. 운행기록 데이터 디지털 인증 시스템의 구조
Fig. 4. System Architecture of Vehicle Data Digital Signature System

성된다. 공인기관에서 유지해야 할 디지털 인증 정보의 테이블 구조는 표 2와 같이 운수사업자의 테이블 구조에 전자서명 검증키가 추가된 구조이다.

표 1. 운수사업자 운행기록 테이블
Table 1. Table of Transport Operators's Vehicle Data

차량등록번호	IGN ON TIME	IGN OFF TIME	전자서명값	전자서명 알고리즘
12 byte	6 byte	6 byte	160 bit	6 byte
	YMDHMS	YMDHMS		SHA1(13)

표 2. 공인기관 운행기록 테이블
Table 2. Table of Certification Authority's Vehicle Data

차량등록번호	IGN ON TIME	IGN OFF TIME	전자 서명값	전자서명 알고리즘	전자 서명 검증키
12 byte	6 byte	6 byte	160 bit	6 byte	160 bit
	YMDHMS	YMDHMS		SHA1	

2. DTG 블록

DTG 블록에서는 차량에 부착된 디지털 운행기록장치에 의해 운행 기록 데이터 원본 D_i가 생성된다. 운행 기록 데이터 원본은 차량 운행 중 UTIS(Urban Traffic Information System), 모바일 네트워크를 이용하여 실시간으로 또는 운행을 마친 후 USB, WiFi, BT(Bluetooth)와 같은 다양한 인터페이스를 이용하여 배치(Batch) 작업으로 운수사업자에 의하여 최종적으로 수집되는 블록이다.

3. 전자서명 생성 블록

운수사업자에 의하여 수집된 차량의 운행기록 데이터 원본 D_i는 무결성 증명을 위해 아래와 같이 전자서명을 하여 서명값 DS_i을 첨부하여 안전한 곳에 저장 관리한다.

또한 그림 5에서 보는바와 같이 서명 값 DS_i는 전자서명 검증키 P_a와 함께 공인기관에 전송하여 차후에 있을 지도 모를 무결성에 대한 분쟁에 대비한다. 운수사업자는 공인기관으로 전자서명 값 DS_i를 전송할 때 전자서명 값을 식별할 수 있는 운행기록 데이터의 키 값에 해당하는 차량등록번호, IGN ON TIME, IGN OFF TIME도 함께 보내야 한다.

① 해시 값 생성: $h_i = h(D_i)$
② 서명 값 생성: $DS_i = E\{h_i\}S_a$
③ 운행기록 보관: $M_i = \{D_i , DS_i\}$
④ 공인기관으로 서명 값 전송: $R_i = \{DS_i, P_a\}$
D_i : 운행기록 데이터
S_a : 운수사업자의 전자서명 생성키
P_a : 운수사업자의 전자서명 검증키

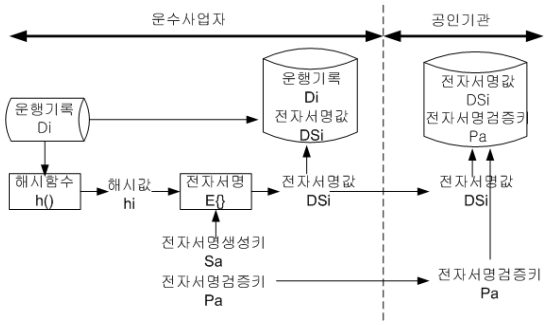

그림 5. 디지털 서명 생성 절차
Fig. 5. Flow of Digital Signature

4. 전자서명 확인 블록

운수사업자가 보관하고 있는 운행기록 데이터 원본에 대한 무결성 증명이 필요한 경우, 운수사업자와 공인기관이 각각 구한 해시 값을 비교함으로서 확인이 이루어진다.

그림 6에서 보는바와 같이 운수사업자는 해시 값 h_i를 보관중인 운행기록 데이터 원본 D_i를 해시함수로 계산하여 구하고, 공인기관에서는 보관중인 전자서명 값 DS_i를 전자서명 검증키 P_a로 복호화 하여 해시 값 h_i'를 구한다.

운행정보 데이터에 대한 위조여부 검증 또는 인증이 필요한 제 3의 기관 또는 사람은 만약 양쪽에서 구한 각각의 해시 값 h_i와 h_i'가 일치한다면 운행기록 데이터 원본에 대한 무결성이 증명되는 것으로 판단할 수 있다. 왜냐하면 공인기관에서 복원한 전자서명 값 h_i'는 운수사업자만이 보유한 전자서명 생성키로 만든 전자서명 값으로부터 구하였기 때문이다.

① 운수사업자가 해시 값 계산: $h_i = h(D_i)$
② 공인기관에서 해시 값 복원: $h_i' = D\{DS_i\}P_a$
③ 두 해시 값 비교: $\langle h_i == h_i' \rangle$?
D_i : 운수사업자가 보관중인 운행기록 데이터 원본
DS_i : 공인기관이 보관중인 전자서명 값

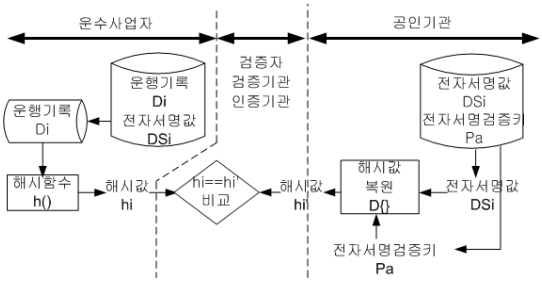

그림 6. 디지털 서명 복원 확인 절차
Fig. 6. Flow of Digital Signature Verification

V. 실험 결과

1. 실험 환경

검증을 위한 디지털 운행기록 정보는 그림 7에서와 같이 차량운행 시뮬레이터를 이용하여 차량 운행과 동일한 조건으로 동작시켜 케이블을 통해 디지털 운행기록장치로 수집 하였다.

수집된 운행정보는 디지털 운행기록장치로부터 USB 저장장치로 다운로드하여 PC에 설치된 분석 소프트웨어를 이용하여 데이터베이스화 한 후 실험을 진행하였다.

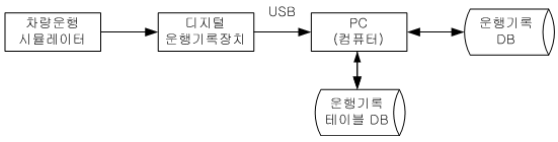

그림 7. 실험 환경 구성
Fig. 7. Environment of Experiment

그림 8에서 보는바와 같이 시뮬레이터와 디지털 운행기록장치를 전원, GND, CAN H/L, Speed, RPM, IGN, 기타 신호를 케이블로 연결 하여 운행정보를 수집할 수 있도록 하였다.

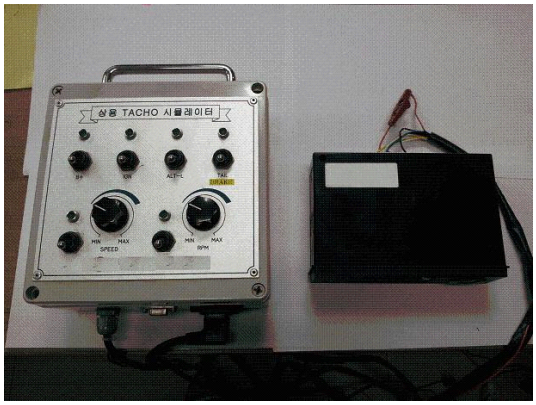

그림 8. 시뮬레이터와 DTG 연결도
Fig. 8. Connection Diagram of Simulator and DTG

2. 실험 및 검증

그림 7에서와 같이 차량운행 시뮬레이터에 연결된 디지털 운행기록장치를 이용하여 총 10개의 TRIP 정보를 생성한 후 RAW 데이터 형식의 운행정보를 국토교통부 교통안전공단에서 정의한 배열순서로 각각의 TRIP 데이터를 생성하고 실험에 이용하였다. 표 3은 각 TRIP 정보에 대한 운행기록 테이블 생성과 이에 대한 검증 결과를 나타낸다. 실험결과 각 TRIP 정보에 대한 운행기록 테이블 생성과 이에 대한 위변조 검증 결과 각각 성공한 것을 확인 할 수 있다.

표 3. 실험 결과
Table 3. Result of Experiment

TRIP 파일	Data Size (KByte)		운행 시간 (H:M:S)	운행기록 테이블 생성	위변조 검증 결과
	헤더	운행			
9999-130220-S001	79	287,640	01:10:30	OK	PASS
9999-130220-S002	79	233,444	00:57:13	OK	PASS
9999-130220-S003	79	377,740	01:32:35	OK	PASS
9999-130220-S004	79	294,508	01:12:11	OK	PASS
9999-130220-S005	79	353,804	01:26:43	OK	PASS
9999-130220-S006	79	172,924	00:42:23	OK	PASS
9999-130220-S007	79	396,780	01:37:15	OK	PASS
9999-130220-S008	79	578,884	02:21:53	OK	PASS
9999-130220-S009	79	104,720	00:25:40	OK	PASS
9999-130220-S010	79	400,452	01:38:09	OK	PASS

운행정보에 대한 위변조 여부 검증을 위한 실험은 그림 9에서 보여주는 바와 같이 검증이 필요한 운행정보 RAW 데이터 파일을 선택한 후 이미 생성된 해당 운행정보의 운행기록 테이블 정보를 이용하여 검증하는 실험을 진행 하였다. 검증이 필요한 운행정보 데이터를 전자서명을 이용한 검증결과 정상임을 표시하고 있다.

이 실험을 통하여 본 논문에서 제안하는 방법이 적용 가능함을 확인하였으며 현재 국내의 경우, 수집된 운행기록 데이터에 대한 위변조 여부를 확인하는 방법이나 시스템이 제시되어 있지 않아서 이에 대한 해결 방법 중 한 가지로서 의미를 가진다고 하겠다.

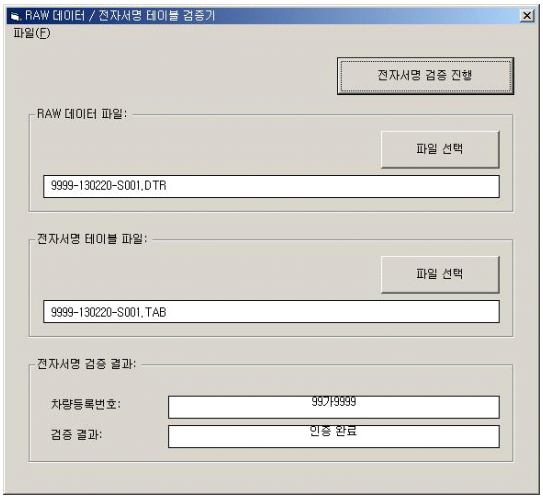

그림 9. RAW 데이터 파일 과 전자서명 목록 검증 UI
Fig. 9. Verification UI of RAW Data File and Digital Signature Table

Ⅵ. 결론

본 논문을 통하여 국내에서 적용이 가능한 디지털 운행기록장치로부터 수집된 운행정보 데이터에 대한 효율적인 인증 방안을 제안하고 프로세스를 설계하여 시스템을 구현하였다. 구현된 시스템은 운행기록 테이블 생성 소프트웨어와 검증이 필요한 운행정보 RAW 데이터의 위변조 여부를 검증하는 소프트웨어로 구성된다. 시스템을 평가하기 위하여 디지털 운행기록장치에서 운행기록 RAW 데이터를 수집하여 운행기록 테이블을 만들고 검증하는 실험을 하고 평가 하였다. 본 논문에서 제안하는 방법을 사용하면 운수사업자가 제공하는 디지털 운행기록장치의 운행기록 데이터에 대한 무결성을 확인 할 수 있으므로 제공되는 운행기록에 대한 신뢰성을 확보할 수 있을 것으로 기대한다. 향후 디지털 운행기록장치의 운행정보 원천 단계부터 데이터를 인증할 수 있는 연구가 추가로 필요할 것으로 판단된다.

참고문헌

〔1〕 Ministry of Land, Infrastructure and Transport Notice No. 2010-667, Sep. 2010.

〔2〕 Enforcement Decree of Traffic Safety Act 〔Enforcement Date 12. July, 2010〕

〔3〕 Thomas Wurtz, "Integrating the Digital Tachograph with Telematics for the new European Standard", Master of Science Thesis, Stockholm, Sweden, 2007.

〔4〕 Igor Furgel and Kerstin Lemke, "A Review of the Digital Tachograph System", Embedded Security in Cars, Springer-Verlag, p69-p94, 2006.

〔5〕 Vincent MAHIEU, "Next generation interconnected Tachograph: how to address privacy and data protection issues?", pp.2, JRC, ITS & Privacy workshop, June 2012

〔6〕 Monitoring of the Implementation of Digital Tachograph Online: http://www,eu-digitaltachograph.org

〔7〕 Confederation of Organizations in Road Transport Enforcement Online: http://www.corte.be/ Last accessed: 14. June 2007.

〔8〕 TMACS, Korea Transportation Safety Authority, http://tmacs.ts2020.kr

〔9〕 eTAS, Korea Transportation Safety Authority, http://etas.ts2020.kr

〔10〕 YJ Koo, "A Study on Electronic Notary based on Digital Signature", Master's Thesis of Sungkyunkwan University, 2005.

〔11〕 Armin Wasicek, "Embedded Security at a Glance: Security Concepts for Embedded Systems", Technical Report 182-1/2007/70, Vienna University of Technology, p47-p49, 2007.

〔12〕 ISO/IEC, ISO/IEC 9796-2 Information Technology - Security Techniques - Digital signature schemes giving message recovery, Second edition, Oct. 2002.

〔13〕 National Institute of Standards and Technology (NIST), FIPS Publication 180-3: Secure Hash Standard(SHS), Oct. 2008.

저 자 소 개

강 준 규

2000: 금오공과대학교 컴퓨터공학과 공학석사
2013: 숭실대학교 컴퓨터학과 박사수료
2007~현재: 부천대학교 컴퓨터소프트웨어과 조교수
관심분야: 지능형에이전트, 온라인게임, 정보보안, 텔레메틱스
E-mail : agent99@bc.ac.kr

김 유 원

1987: 경희대학교 기계공학과 학사
2003: 인하대학교 정보공학과 석사
2006: 인하대학교 컴퓨터정보공학과 박사수료
현재 : 부천대학교 컴퓨터소프트웨어과 겸임조교수
관심분야: 오토모티브 소프트웨어, 텔레메틱스, 인포테인먼트, 스마트카, ITS, 디지털방송, 컴퓨터비전
E-mail : ywkim@bc.ac.kr

임 웅 택

1992: 국방대학원 전자계산과 공학석사
2006: 숭실대학교 컴퓨터학과 공학박사
1997~현재: 부천대학교 컴퓨터소프트웨어과 정교수
관심분야 : 정보보안, 알고리즘
E-mail : utlim@bc.ac.kr

전 문 석

1986 : University of Maryland Computer Science 석사
1989: University of Maryland Computer Science 박사
1989~1991: New Mexico State University Physical Science Lab 책임연구원
1991~현재 : 숭실대학교 정교수
관심분야 : 인터넷 보안, 네트워크 보안, 인증 시스템, 정보보호
E-mail : mjun@ssu.ac.kr