JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 22, No. 10, pp. 1707-1713, Oct. 2021

Check for updates

영상감시장치 위변조 방지를 위한 검증 모듈의 암호화 키 생성 및 펌웨어 구현에 관한 연구

양 재 수[1*]
[1]*단국대학교 전자전기공학부 교수

A Study on Firmware Implementation and Encryption Key Generation of Verification Module to prevent Forgery and Falsification of Video Surveillance Device

Jae Soo Yang[1*]
[1]*Department of Electronic and Electrical Engineering, Dankook University, Gyeonggi-do 16890, Korea

[요 약]

CCTV 영상감시 시스템은 국가중요시설의 외곽방호와 공공방범을 목적으로 폭넓게 운용되는 시스템이다. 그러나, 이렇게 중요한 영상감시 시스템은 위.변조 가능성이 제기되고 있고, 각종 감시 설비의 대부분 영상감시 시스템은 해킹 등 보안에 취약하다. 무분별한 AS 및 불법 카메라 교체작업을 통한 DDoS 공격과 같은 과부하 공격으로 관제실내 중요장비를 무력화 가능성에 노출되어 있다. 따라서, 본 연구에서는, CCTV 펌웨어 변형을 사전에 감지하여, 거짓영상 송출을 차단하여 안정성과 신뢰성 있는 영상 운영을 보장할 수 있도록 디바이스 모듈의 펌웨어 검증코드를 구현 할수 있는 SW 적용 기술을 제시하고자 한다. 연결된 CCTV의 펌웨어 내용을 실시간 검사하여 비인가 CCTV 또는 이기종 시스템의 연결을 자동 차단하는 기능을 구현하고자 한다. 영상감시장치의 펌웨어에 대한 변조 파생 공격으로부터 방어할 수 있는 보안 강화형 영상감시장치의 펌웨어 검증 모듈의 암호화 키 생성 및 구현에 방안을 제시하고자 한다.

[Abstract]

The CCTV video surveillance system is widely operated for the purpose of protecting the perimeter of important national facilities and preventing public crime. However, the possibility of forgery and falsification of such an important video surveillance system is raised, and most of the video surveillance systems of various surveillance facilities are vulnerable to security such as hacking. It is exposed to the possibility of incapacitating important equipment in the control room due to overload attacks such as DDoS attacks through reckless AS and illegal camera replacement. Therefore, in this study, we intend to present a SW application technology that can implement the firmware verification code of the device module to detect CCTV firmware modification in advance and block false image transmission to ensure stability and reliable image operation. It is intended to implement a function that automatically blocks the connection of unauthorized CCTVs or heterogeneous systems by inspecting the firmware contents of the connected CCTV in real time. An attempt is made to propose a method for generating and implementing an encryption key of a firmware verification module of a security-enhanced video surveillance device that can protect against tamper-derived attacks on the firmware of the video surveillance device.

색인어 : CCTV 영상감시 시스템, 위.변조 , CCTV 펌웨어, 검증 코드, 암호화 키
Keyword : CCTV video surveillance system, Counterfeit/falsification, CCTV firmware, Verification code, Encryption key

http://dx.doi.org/10.9728/dcs.2021.22.10.1707

Received 16 August 2021; **Revised** 07 September 2021
Accepted 29 September 2021

***Corresponding Author; Jae Soo Yang**
Tel:
E-mail: jsyang@dankook.ac.kr

Ⅰ. 서 론

PS 영상감시장치 CCTV는 일상 생활 환경에서나 산업현장에서 물리적 보안, 소방재난 안전관리, 각종 감시장치 등 지능화 되어 가고 있고, 활용성이 갈수록 높아지고 있다. 이렇게 중요한 CCTV는 위,변조 가능성이 제기되고 있고, 이에 따라 실시간 모니터링 기능이 중요해져 가고 있다[1]-[4].

무분별한 AS 및 불법 카메라 교체작업을 통한 DDoS 공격과 같은 과부하 공격으로 관제실내 중요장비를 무력화 가능성에 노출되어 있다. 연결된 장치의 실시간 모니터링을 통해 비인가 장치 연결 시 물리적 네트워크 차단으로 공격을 방어할 수 있어야 한다[4]-[6].

IP 모듈 펌웨어의 내용을 변형하여 실시간 영상이 아닌 거짓영상(과거 영상) 송출과 무인화로 운용되는 지능형 영상감시의 감지기만 행위 등으로 실제와는 다른 상황을 만들어 침입 및 테러를 가능하게 하고 있다. 따라서, 펌웨어 변형을 사전 감지하여 거짓영상 송출을 차단하여 신뢰성 있는 영상운영을 보장할 수 있어야 한다. 영상감시장치는 국가중요시설의 외곽방호와 공공방범을 목적으로 폭넓게 운용되는 시스템으로써 CCTV를 포함한 현장제어나 관제가 효과적으로 이루어져야 한다[7]-[9].

이에, CCTV 펌웨어 안전 검증이 필요하다. 실시간으로 연결된 CCTV 펌웨어 내용을 검증하는 기술이 필요하며, 검증결과에 따라 네트워크 연결 및 차단 기능을 수행하여 설치 된 CCTV를 불법적인 교체 및 펌웨어 위변조를 방지할 수 있어야 한다. 이러한 목적에서 본 논문에서는 CCTV 펌웨어의 데이터 암호화 생성 기술과 소프트웨어 기반의 펌웨어 검증 모듈 구현에 대한 방안을 제시하고자 한다. 이를 위해, 1회성 검증코드 생성 기능, 데이터 암호화 키 생성, 그리고, 기존 제품 대비 호환성 및 보안성능 강화에 대한 암호화 알고리즘 등 관련 검토와 CCTV 펌웨어 검증 구현에 대한 핵심 기술이 필요하다.

Ⅱ. CCTV 영상감시장치 현황과 운영실태 분석

2-1 CCTV 영상감시 장치 운영 실태

CCTV 영상감시장치는 촬상부, 전송부, 감시부, 제어부로 구성되는데,'촬상부'란 카메라와 다양한 기능을 구현하기 위한 액세서리(렌즈, 하우징, 회전대 등)를 모두 포함하며, '전송부'는 유.무선을 망라한 다양한 통신수단을 의미하고, '감시부'는 DVR/ NVR/ VMS 등의 감시모니터로 구성된다[1-3].

최근의 4세대 CCTV는 아래와 같은 특징을 갖는다.

기존의 아날로그 카메라와 비디오서버의 CCTV 시스템은 별도로 비디오서버를 구매해야 하는 불편함과 비용부담이 있었다. 이에 카메라 자체에 네트워킹을 지원하는 기술개발이 진행되어 구성이 간단해 지고 비용이나 고장에 대한 부담도 줄어들게 한 IP 카메라가 탄생되었다[1], [3], [7].

IP 카메라 중에서도 팬틸트와 카메라 일체형 Speed Dome 카메라를 사용하면 이 구성은 더욱 간단해지며, 실제로 촬상부 측에는 카메라 하나만 설치하면 될 정도로 간단히 구성할 수 있게 되었다[10], [11].

CCTV 영상감시 장치는 국가 중요 핵심시설의 방범용 보안설비 등 생활방범 용도로 많이 구축되지만 주차관제나 교통법규 위반차량 단속 및 교통 통제수단 등으로 오래전부터 사용하고 있으며, 국가 및 공공기관, 민수산업시설 등 다양한 분야에서 활용하고 있는 설비로 개발되어 사용되고 있다.

CCTV 영상감시 장치의 주요 기술로는, 동작 감지와 추적기술, 지능형 영상 추적 및 분석기술, 광학문자인식 기술(OCR, Optical Character Recognition) 등이 있다. OCR은 차량번호판 인식시스템(LPRS)과 영상인식 주차관제시스템 및 주차유도시스템 등에 널리 사용되고 있다[10]-[13].

2-2 영상감시 장치의 문제점 분석과 개선해야 할 점

현재는 CCTV로부터 수집된 영상 정보는 위변조의 가능성이 충분히 내재되어 있으므로 현장에서 취득한 영상의 신뢰성 확보 기능이 요구된다. 무분별한 AS 및 불법 카메라 교체작업을 통한 보안 위협(Fake Video, DDoS 공격 등)으로 IP 모듈 펌웨어의 내용을 변형되어 실시간 영상이 아닌 거짓영상(과거 영상) 송출과 무인화로 운용되는 지능형영상감시의 감지기만 행위 등으로 실제와는 다른 상황을 만들어 침입 및 테러를 가능하게 함으로서 펌웨어 변형을 사전 감지하여 거짓영상 송출을 차단하여 신뢰성 있는 영상운영을 보장하여야 한다.

기존 CCTV 영상감시 장치는 현장 제어부에서 획득된 영상을 센터에 전송하여 DVR(Digital Video Recorder), 또는 NVR(Network Video Recorder)등에 저장하도록 하는 구조로 구성된다. 이와 같은 구조로 설치된 CCTV는 고의적인 의도로 다른 CCTV로 쉽게 교체되고 이로 인하여 관리자의 제어권이 상실됨에 따라 CCTV에서 실시간 촬영되는 영상이 해킹, 영상의 위변조, 불법적인 공격행위 등을 방지할 수 없다[13]-[15].

현장 제어부에서 실시간 촬영되는 영상을 보호하기 위한 보안 대책이 현실적으로 필요한 실정이며, CCTV의 펌웨어 갱신은 설치된 다수의 CCTV 각각에 대하여 일일이 펌웨어를 갱신해야 함에 따라 시간, 인력 소요를 비롯하여 경제적으로 많은 경비가 소요되는 등 문제점이 있어 대응기술을 필요하다.

또한, CCTV 펌웨어 제어 기술에 대해 설계와 구현에 대한 방안 제시가 필요하다. CCTV는 카메라 렌즈와 촬영에 해당하는 메카 펌웨어와 압축과 전송 및 원격제어 기능이 있는 IP 모듈 펌웨어로 구성되어 있다. IP 모듈 펌웨어의 위변조 공격으로 거짓영상 송출/CCTV 모니터링 정지공격/DDoS 공격에 노출 가능하며. IP 모듈 펌웨어의 실시간 검증이 필요하다. 이에 IP 모듈 펌웨어를 검증하는 실시간 펌웨어 검증기술과 CCTV장치 내 설치되어 데이터보호를 위한 암호화키 생성과 1회성 검증코드를 생성하는 Securiy Library Module 제공되어 적용되어야 한다.

데이터 암호화 키 생성기술은 크게, 검증코드 생성 데이터를 암호화키로 암호화하는 기술과 하드 코딩 사용 방지를 위한 난수 테이블과 암호화 데이터를 사용하는 방법이 있다.

기존 Hash값에 CCTV고유정보, 검증키, ARIA128암호화를 사용하여 생성된 1회성 검증코드로 실시간으로 펌웨어를 검증하는 기술이 필요하다. 기존 기술의 동일한 Hash 값을 사용하는 경우 유출의 문제가 있고, 외부 개입에 의해 불법펌웨어가 보내는 Hash 값을 정상 Hash값으로 인식하여 펌웨어 검증 기술을 회피하는 개선된 기술이 필요하다[12]-[16].

Ⅲ. CCTV 펌웨어 적용 암호화 생성기술과 검증 모듈 구현

3-1 데이터 암호화와 키 생성 기술 방안

기존 기술에 데이터를 암호화하기 위한 키 생성과정은 있으나 단순 데이터로 키 노출이 발생하여 데이터가 유출되는 문제가 있으며, 키를 내부의 정형화 된 곳에서 나오는 데이터를 활용하여 기기마다 동일한 테이블에서 키를 순차적으로 획득하여 사용함에 따라 키 노출이 쉬웠다.

또한, 아이디로 장치마다 키를 생성함에 따라 아이디 유출 시 설치된 키가 유출될 수 있어서 모든 장치에 축적된 데이터가 안전하게 보호되기 어려운 문제점이 있어 데이터 암호화 키 생성기술이 필요하다[2], [3], [16-18].

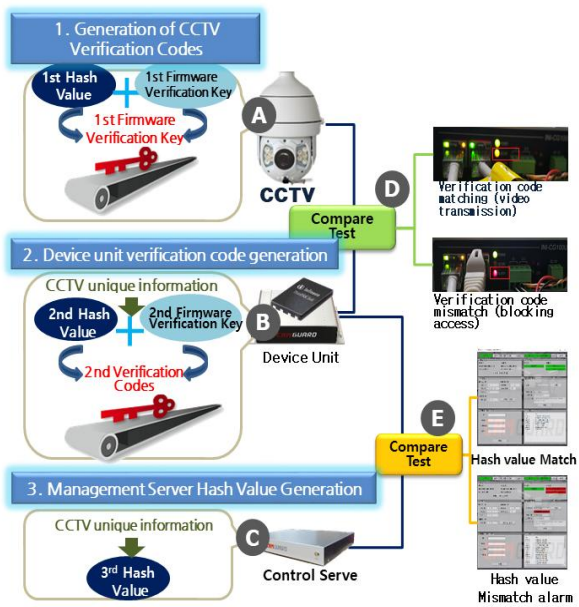

그림 1. CCTV 및 디바이스 유닛과 관제서버간 펌웨어 검증코드 생성과 상관도

Fig. 1. Firmware verification code generation and Correlation among CCTV, Device unit and Control serve

표 1. CCTV 및 디바이스와 관제서버간 검증코드 단계

Table 1. Verification Code Step among CCTV, Device and Control server

A	First verification code generation step for firmware installed in CCTV
B	Second verification code generation step in the device unit
C	The third hash value generation step in the control server
D	Comparing whether the first verification code and the second verification code are the same in the security chip unit
E	Equality comparison step between the third hash value of the control server and the second hash value of the device unit

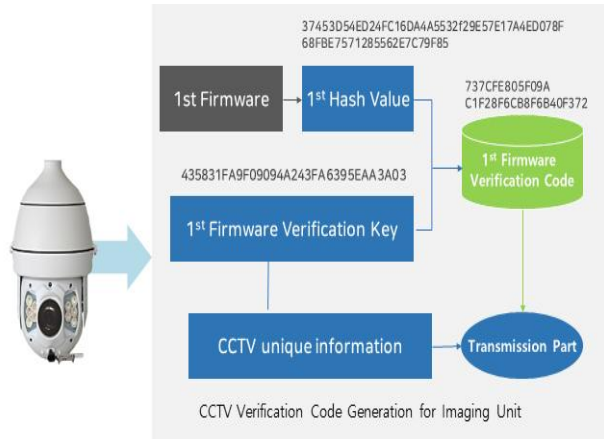

그림 2. CCTV 촬상부 펌웨어 검증 코드 생성

Fig. 2. CCTV Firmware Verification Code Generation of Imaging Unit

따라서, 검증기능 수행 시 실시간 1회성 검증코드를 생성하고, 장치 간 검증에 사용되는 모든 데이터는 암호화하여 전달되도록 했다. 다시 말해, 디바이스 모듈에 대한 기만행위(검증코드 유출 및 재사용)를 원천 차단하기 위해, 검증기능 수행 시 실시간 1회성 검증코드를 생성하고, 장치 간 검증에 사용되는 모든 데이터는 암호화하여 전달해야 한다[18], [19]. 표 1은 그림 1에서 제시한 CCTV 및 디바이스와 관제서버간 검증코드 단계를 설명해 준다.

그림 1의 A에 해당하는 CCTV 제1검증코드 생성 알고리즘 원리는 그림 2와 같다[19], [20].

① CCTV에 설치된 제1 펌웨어에 대한 제1해시값을 추출

② CCTV 고유정보를 이용한 제1펌웨어 검증키를 생성

③ 해시값과 펌웨어검증키로 제1검증코드 생성 후 CCTV 고유정보와 함께 송신

다음, “디바이스 유닛”부의 검증코드 생성 알고리즘과 “관제서버”부의 제3해시값 생성 알고리즘 및 검증코드와 해시값 비교 알고리즘 원리는 지면상 생략하고자 한다.

3-2 데이터 암호화 키 생성 기술과 절차

본 CCTV 펌웨어 검증코드를 생성할 때 데이터 암호화 키 방식을 적용하여 데이터 보호수준을 향상시키고 유출 시 복호화를 방지할 수 있어야 한다. 그림 3은 데이터 암호화 키 생성기술과 과정의 구성도를 나타낸다[14], [18-20].

데이터 암호화 키는 난수테이블 생성부, 테이블 추출부, 키 설정부와 암호화와 서명으로 이루어진 저장부로 구성되어지며, CCTV 검증코드 생성을 위한 데이터를 안전하게 보호하는 암호화 키를 생성한다.

Ⓐ 테이블생성부에서 '생성된 테이블'들이 갖는 각 데이터의 총합을'생성된 테이블'개수(m)로 나눈 나머지 값에 해당하는 순번의 테이블을 선택하여 추출한다.

Ⓑ 키 설정부는 '추출된 테이블'이 갖는 데이터 값의 총합을 테이블 데이터 개수(n)로 나눈 나머지 값은 키의 위치 값이 된다. 키의 위치 값에서 키의 값을 찾고, 키의 값은 다음 키의 위치 값이 된다. 키 길이만큼 반복해서 키의 위치 값에서 키의 값을 찾는다.

Ⓒ 암호화키는 데이터를 암호화 알고리즘(ARIA128)을 통해 암호화/서명 한 후 저장한다. CCTV와 디바이스 유닛에서 사용되는 암호화 알고리즘은 ARIA128-CBC(Cipher Block Chaining) Mode를 사용하였다.

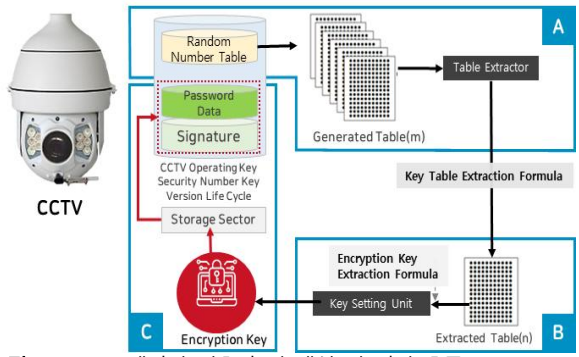

그림 3. CCTV 데이터 암호화 키 생성 및 상관 흐름도
Fig. 3. CCTV Data Encryption Key Generation and Correlation Flowchart

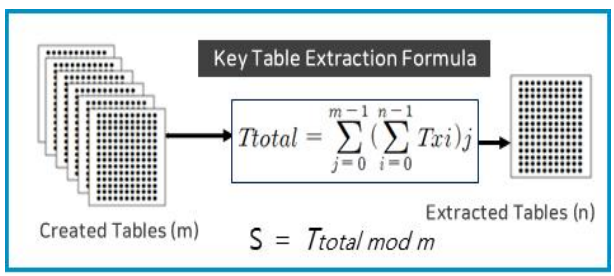

그림 4. 암호화 키 테이블 추출식
Fig. 4. Encryption Key Table Extraction Formula

그림 4와 5는 각각 암호화 키 테이블 추출식과 난수 암호화 키 생성 추출식을 도식화하여 보여준다.

연구기술을 통하여, 개선된 기술은 기존 제품 대비 호환성 및 보안성능이 강화되었다. 이에 대한 동작원리와 특징은 다음과 같다[19], [20].

- CCTV장치 내 동작 기술은 Security Library Module로 적용 동작하여 자사의 CCTV장치뿐만 아니라 타사의 CCTV에도 적용가능하게 개발되었으며, Security Library Module을 적용이 되면 신청 제품의 디바이스 유닛과 호환하여 동작한다.
- 본 연구기술개발은 다양한 제품군에서 활용이 가능하여 CCTV뿐만 아니라 IoT Device 장치에도 손쉽게 탑재가 가능하고 저용량(약 5Kbytes 미만)으로 동작하도록 설계 되었다.
- 디바이스 유닛은 보안성을 보다 강화하기 위해 H/W 보안칩을 적용하여 보안칩 내부에서 연산 및 저장을 하여 외부 공격으로부터 안전하도록 구성하였다.
- 두 단계의 인증이 정상적으로 이루어져 검증이 완료가 되면 디바이스 유닛에 의해 차단된 네트워크를 해제 하여 CCTV에서 관제부로 영상이 전달되도록 설계하여 구현하였다[19].

CCTV와 디바이스 유닛의 키 인증에는 Operating Key 생성, Session Key 생성, 서명 생성 알고리즘이 필요하다. 서명 생성에 있어서는, 디바이스 유닛과 CCTV 사이에 통신하는 데이터는 외부 공격에 의해 위변조 되지 않는 무결성을 확인하기 위해 서명(Sign)을 만들어 확인을 하게 된다.

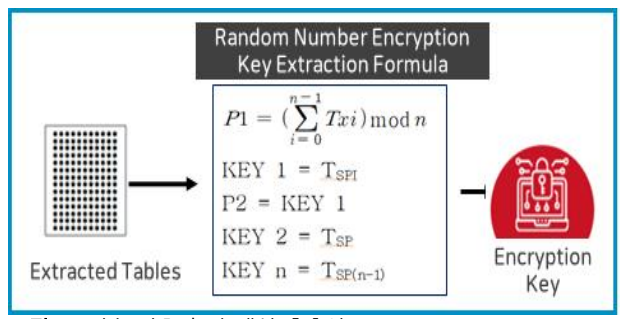

그림 5. 난수 암호화 키 생성 추출식
Fig. 5. Extraction Formula for generating a Random Number Encryption Key

3-3 CCTV와 디바이스 유닛의 키 인증과 펌웨어 검증

CCTV와 디바이스 유닛의 펌웨어 검증에 있어서는, Security Library Module로 관리되는 키로 1차 키 인증이 완료가 되고, 디바이스 유닛은 CCTV의 펌웨어 인증을 한다. 2차 펌웨어 검증이 완료되면 모든 인증 과정이 완료된다. 그림 6은 CCTV와 키 인증 프로토콜간 검증 핸드 세이킹을 보여준다.

- 펌웨어 검증은 키 인증에서 만들어진 세션키를 모두 사용하며, 검증코드 생성, 데이터 암호화 알고리즘이 추가로 있다.

검증코드는 키 인증에서 생성되는 펌웨어 검증키로 만들고, 펌웨어 검증키는 Session 마다 다른 값을 가지고 있으므로 1회성 검증 코드를 가질 수 있다.

검증 코드는 1회성으로 생성되고 사용되더라도 보안성 강화를 위해 CCTV에서 디바이스 유닛으로 전달되는 과정에는 데이터 암호화 되어 전달된다.

그림 7에서 보여주는 바와 같이 관제서버에서 디바이스 유닛의 Hash 값 확인에 있어서, 관제서버는 디바이스 유닛에서 사용되는 Hash 값이 맞는지 확인하고, 검증을 한다. Hash 값이 맞지 않다면 관제서버는 알람을 발생하게 된다[19], [20].

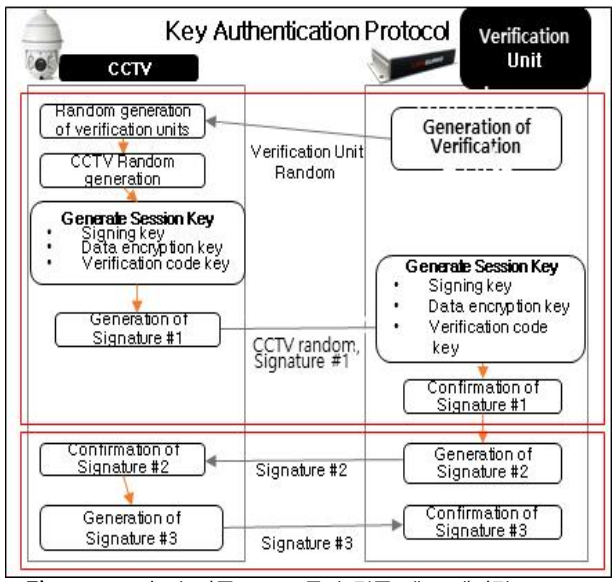

그림 6. CCTV와 키 인증 프로토콜간 검증 핸드 세이킹
Fig. 6. Verification Handshaking between CCTV and Key Authentication Protocol

Ⅳ. 실험 결과 및 고찰

본 연구 논문에서 영상감시 시스템인 CCTV의 펌웨어 위.변조 방지 영상감시 시스템 구현에 관한 성능을 보장하는 기술 개발에 대해 실험 결과를 고찰하였다.

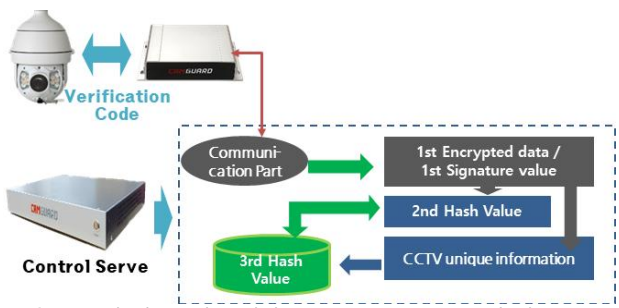

그림 7. 관제 서버에서 디바이스 모듈의 Hash 값 확인 과정
Fig. 7. The Process of checking the Hash Value of the Device Module in the Control Server

이는 CCTV의 펌웨어 위.변조 공격을 사전 감지하여, 자동 차단하는 보안 강화형 영상감시 시스템으로서 일반적인 영상감시 시스템의 운용환경에 적용이 가능한 방안을 검토하고 관련 펌웨어 암호화 기능을 구현하였다.

현재까지의 기술개발 제품 수준을 비교해 보면, 본 논문에서 제시한 연구기술개발은 아래와 같은 측면에서 매우 우수함을 확인하였다. '실시간 CCTV 펌웨어 검증 시기에 있어서, 기존 제품의 기술은 '펌웨어 검증확인 test 전'에는 이상유무 검증이 가능했으나, 본 연구논문에서 제시한 연구기술은 펌웨어 업데이트 전은 물론 업데이트 후나 운용 중에도 실시간으로 모니터링이 가능하다. 또 CCTV 교체 후 영상전송에 있어서는, 기존 기술은 ' 조건 전송'이었으나, 본 연구에서는 'CCTV의 IP, ID/PWD 정보를 알고 있는 동일한 환경에서만 검증이 완료되어야만 영상이 전송'되도록 설계되었다. '암호화 키 위치'면에 있어서는, 기존 기술은, '고정 위치 저장' 이었으나 본 연구에서는 '난수 테이블내에 임의의 위치에 저장(암호화키는 키추출식으로 추출하여 사용)'하는 방식으로 우수하다. '암호키 교체'면에 있어서도, 기존기술 대비 본 연구개발에서는 '난수테이블 재생성으로 키 값의 변경'이 가능하여 보안성이 높다.

특히 본 연구기술개발을 통하여, 확인한 4가지 관점에서의 성능과 동작 여부를 요약하면 아래와 같다.

- CCTV 펌웨어 검증
  · CCTV의 일회성 검증코드를 검증하여 펌웨어 일치 여부를 확인
- 외부함체 열림 감지
  · 외부함체 열림을 감지하고, 열림 감지 시 알람 발생, 영상 화면에 함체 열림을 표시
- 이기종 IP Device 연결 감지
  ·펌웨어 검증이 되지 않는 장치의 연결을 확인
- 네트워크 차단
  · 펌웨어 검증실패 시 네트워크 차단을 통하여 외부 공격으로부터 방어

그림 8은 펌웨어 위.변조 공격에 따른 거짓영상 전송 실험 영상을 보여준다. 그림에서 보는 바와 같이 펌웨어 위.변조된 영상에서는 침입자가 보이지 않고 있지만 정상적인 펌웨어에서는 침입자가 보이고 있다[19].

이에 적용된 핵심기술로서, Securiy Library Module에는 "CCTV 펌웨어 검증"과 "데이터 암호화 키 생성"의 핵심기술이 적용되어 있으며, 디바이스 모듈은 "CCTV 펌웨어 검증"의 핵심기술이 적용되어 이상 없이 동작함을 확인하였다.

디바이스 모듈에서"CCTV 펌웨어 검증"을 진행하는 과정은 1차 키 인증과 2차 펌웨어 검증 두 단계로 구성이 되어 있다. 두 단계의 인증은 CCTV에서는 Security Library Module에서 인증 절차가 진행되고, 디바이스 모듈에서는 보안 칩 내부에서 인증 절차가 진행되는데, 이러한 프로세스가 정상적으로 기능을 발휘 함을 확인하였다.

그림 8. 펌웨어 위.변조 공격에 따른 거짓영상 전송 실험
Fig. 8. False Image Transmission Experiment according to Firmware Forgery Attack

두 단계의 인증이 정상적으로 이루어져 검증이 완료가 되면 디바이스 모듈에 의해 차단된 네트워크를 해제하여 CCTV에서 관제부로 영상이 전달되고, 관제부에서 CCTV를 컨트롤 할 수 있게 되었고, 인증이 실패 한다면 디바이스 모듈은 CCTV와 관제부의 네트워크를 차단하여 CCTV의 영상 전달을 막고, 관제부에서 CCTV를 컨트롤 할 수 없도록 하였다.

다음, DDoS 공격에 따른 악성코드를 이용한 NVR 정지공격에 대해서도 이상 유무를 확인하여, 알람으로 경고가 울림을 인지 할 수 있었다.

실시간 CCTV 펌웨어 검증 결과에 있어서도 아래와 같은 실험 결과를 얻을 수 있었다. 기존 기술은 CCTV 펌웨어의 검증 절차 부재로 인해, 펌웨어가 위.변조된 CCTV 혹은 이기종의 IP Device가 연결되면 판단 및 검증이 불가하여 영상의 보안 위협에 쉽게 노출될 수 있다. 반면 본 연구개발 기술을 통하여 실시간으로 CCTV 펌웨어의 검증코드를 생성하고 비교·판단을 통해 영상의 위변조를 사전에 차단하는 기능을 수행함을 확인하였다.

Ⅴ. 결 론

본 논문의 연구를 통하여 구현한 CCTV 펌웨어 위.변조 방지 영상감시 시스템은 국가중요시설의 외곽방호와 공공방범을 목적으로 폭넓게 운용되는 시스템으로써, 해킹 등 보안에 취약한 시스템을 보강하여 안전한 영상감시 활동이 가능하게 되어졌음을 확인할 수 있었다.

CCTV 영상감시 시스템 운용 중에 무분별한 AS(After Service) 및 불법 카메라 교체 작업을 통한 DDoS 공격 등과 같은 과부하 공격으로 관제실의 통합관제 중요 장비를 무력화 할 수 있는 가능성에 노출되어 있는 것을, 연결된 장치의 실시간 모니터링을 통해 비인가 장치 연결 시 물리적 네트워크 차단으로 공격을 방어할 수 있는 기술의 개발과 이의 성능이 원활하게 동작함을 실험을 통하여 구현하였다.

CCTV 펌웨어 검증에 있어서는, 실시간으로 연결된 CCTV 펌웨어내용을 검증하는 기술로 검증결과에 따라 네트워크 연결/차단 기능을 수행하여 설치 된 CCTV를 불법적인 교체 및 펌웨어 위.변조를 방지할 수 있었다.

데이터 암호화 키 생성에 있어서는, 보안이 취약한 CCTV 장치 내 중요 데이터 보호를 위한 데이터 암호화키 생성기술로 Securiy Library Module로 개발되어 하드웨어 구조 변경이 어려운 CCTV장치에 적용 가능하여 CCTV 장치의 보안성을 강화하였다.

본 연구를 통하여, 관련 산업에도 파급 효과가 지대할 것으로 예측된다. 국내.외 최초의 CCTV 펌웨어 위.변조를 실시간으로 검증·차단하는 영상감시 시스템으로서 영상감시 운용의 안전성 확보와 네트워크를 이용한 해킹 우려를 감소시킬 수 있다. 또한, 추가 시스템의 구성없이 기존 시스템 운용이 가능하다. 독립 운영(CCTV, 디바이스 모듈)이 가능한 기술로 기존 영상감시 시스템과 호환이 가능하다. 카메라 내 검증 기능을 ANSI-C 코드로 제작된 Security Library 모듈화로 기존 카메라와 검증모듈 간 기능 연계가 가능하게 되었다.

비용절감 측면에서도, 펌웨어 검증 기능을 구현하기 위해서는 여러 대의 서버를 이용해야 구축이 가능하지만, 신청기술은 서버 급 장비를 구축하지 않고도 검증모듈을 적용하여 자체적인 CCTV 펌웨어 검증이 가능하여 서버 구입비용, 유지보수 비용, 전력사용 비용 등을 절감할 수 있다. 앞으로 많은 국내 보안시장 뿐만 아니라 해외 수출 증대에도 기여할 것으로 기대된다.

감사의 글

본 연구는 2021학년도 단국대학교 대학연구비 지원으로 연구되었습니다.

참고문헌

[1] Gunwoo Kim, Hyunsoo Cho, “Intelligent CCTV Technology Status and Application Cases”, *Korea Regional Information Development Institute*, 2017.

[2] Advanced Encryption Standard (AES), FIPS PUB 197 (http://csrc.nist.gov/publications/fips/fips197/fips- 197.pdf)

[3] Data Encryption Standard (DES), FIPS PUB 46-3 (http://csrc.nist.gov/publications/fips/fips46-3/fips46- 3.pdf)

[4] FIPS PUB 180-2 Federal Information Processing Standards Publication 180-2, 2002: *Specifications for the Secure Hash Standard: U.S. Department Of Commerce, Technology*

Administration, National Institute Of Standards And Technology, 2002.

[5] FIPS PUB 197 Federal Information Processing Standards Publication 197, 2001: Specification for the Advanced Encryption Standard (AES): *U.S. Department Of Commerce, Technology Administration, National Institute Of Standards And Technology,* 2001.

[6] FIPS PUB 198 Federal Information Processing Standards Publication 198, 2002: Standard for the Keyed-Hash Message Authentication Code (HMAC): *U.S. Department Of Commerce, Technology Administration, National Institute Of Standards And Technology.*

[7] Security Requirements for Cryptographic Modules, FIPS PUB 140-2, and Annex A to D, May, 2001 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf).

[8] DRAFT Security Requirements for Cryptographic Modules (Revised Draft), FIPS-140-3, Dec., 2009 (http://csrc.nist.gov/ publications/ drafts/fips140-3/ revised-draft-fips140-3_PDF-zip_document- annexA-to-annexG.zip).

[9] NIST, http://csrc.nist.gov/publications/drafts/fips140-3 /revised-draft-fips 140-3_PDF-zip _document-annexA-to-annexG.zip) SP 800-90 A, Rev 1, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), May, 2011, (http://csrc.nist.gov/ publications/drafts/800-90/Draft_SP800-90A-Rev1_ May-2011.pdf).

[10] Issue Quest Editorial Department, "Intelligent Video Surveillance System (CCTV) and Convergence Security, Safety Related Technology, Market Status and Prospect," *Issue Quest,* 2016.

[11] NIST SP 800-22 Rev 1a, Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010, (http://csrc.nist.gov/publications /nistpubs/800-22-rev1a/SP800- 22rev1a.pdf).

[12] BSI AIS20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 18. Sept. 2011, (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Zertifierung/Interpretation/AIS31_Functionality_classes_for_random_number_generators.pdf)

[13] Common Criteria Certification The Federal Office for Information Security / Bundesamt für Sicherheit in der Informationstechnik (BSI) publicly provides the certification report and security target for a certified product. These documents can be downloaded at https://www.bsi.bund.de.

[14] ISO/IEC 3309 Information Technology – Telecommunications and information exchange between systems – High-level data link control (HDLC) procedures – Frame structure – Fifth Edition 1993-12-15.

[15] ICAO Technical Report - RF Protocol and Application Test Standard for E-Passport - Part2 - Tests for Air Interface, Initialization, Anticollision and Transport Protocol; Version: 1.02, Feb. 20, 2007

[16] PKCS#1 (RFC 2437) - PKCS #1 v2.0: RSA Cryptography Standard, RSA Laboratories, October 1998 (RFC 2437).

[17] ISO 8731-1:1987 [IS8731-1] Banking - Approved algorithms for message authentication – Part 1: DEA.

[18] ISO/IEC 8825-1:2002 | ITU-T Recommendation X.690 (2002) Information technology – *ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

[19] Sang Woo Lee, "A Study on the Implementation of Video Surveillance System to Prevent Forgery and Modification of CCTV Firmware, Department of Information and Communication", *Master's thesis, Graduate School of Information Convergence Technology and Entrepreneurship,* Dankook University, Feb., 2021.

[20] Sang Woo Lee , Jin Gi Park , Jae Soo Yang,, A Study on Data Encryption Key Generation to Prevent Forgery and Alteration of CCTV Video Surveillance Devices, A*dvanced Engineering and ICT-Convergence Proceedings (AEICP),* Vol.4, No.1, Jan., 7, 2021.

양재수(Jae Soo Yang)

1993년 : 미 NJIT 전기 및 컴퓨터공학과 공학박사(공학박사)
1991년 : 서울대학교 MBA 수료
2006년 ~ 2011년 : 광운대 교수
2011년 ~ 현 재 : 단국대 교수
1981년 MIC 통신사무관
2007년 ~ 2011년 : 경기도 정보화특보
1982년~2006년: KT 인터넷사업국장, 상품개발팀장, 월드컵 통신팀장, 수도권강북본부 고객지원센터장/사업총괄담당상무

※ 관심분야 : IT융합기술, 보안융합, RFID/IP-USN, 정보통신 산업정책, 그린 에너지, u-City 등