



# 블록체인 기반의 CCTV 영상 위·변조 검증 메커니즘

김진수\*, 조재영\*\*, 박남제\*\*\*

## Block Chain Based CCTV Image Forgery · Modulation Verification Mechanism

Jinsu Kim\*, Jaeyoung Cho\*\*, and Namje Park\*\*\*

### 요 약

영상감시 시스템에 의해 촬영되는 영상은 일반적으로 해당 시스템을 설치한 정당한 관리자에 의해 사용되며, 주로 해당 영역에 대한 불법적 침입을 확인하기 위한 하나의 수단으로서 사용된다. 특히, 범죄와 연결되는 경우에는 해당 영상을 법적 증거물로서 사용하기 위해 외부로 전달되어야 할 필요성이 있다. 제안된 논문에서는 영상의 위·변조에 의해 발생 가능한 문제를 해결하기 위해 영상과 사용자의 정보를 블록체인에 기록하여 기록의 무결성을 보장할 수 있도록 하였으며, 블록에 기록된 내용을 암호화하고, 암호화된 내용을 블록내에서 찾기 위해 공개키를 블록의 기타데이터에 기록함으로써 본인이 기록한 블록데이터를 찾을 수 있는 식별키를 사용하는 방식을 적용하였다. 본 논문에서는 CCTV(Closed Circuit Television) 영상의 메타데이터와 영상에 접근한 사용자를 블록체인 내의 블록으로서 저장하고, 공개키 기반 암호화방식을 통해 내용에 대한 보안성을 강화하는 메커니즘을 제안한다.

### Abstract

An image captured by a video surveillance system is generally used by a legitimate administrator who installed the system and is mainly used as a means for confirming illegal intrusion into the area. In particular, when linked to crime, there is a need to transmit the image to the outside in order to use it as legal evidence. In the proposed paper, to solve the problem that can be caused by image modulation, the image and user's information are recorded in the blockchain to guarantee the integrity of the recording. The contents recorded in the block are encrypted. In order to search for a favorite in a block, a public key is recorded in other data of the block so that an identification key is used to find the block data recorded by the user. In this paper, we propose a mechanism to store the metadata of closed circuit television (CCTV) images and users who access the images as blocks in the blockchain and to enhance the security of contents through public key based encryption.

### Keywords

closed circuit television, blockchain, video surveillance system, encryption, video metadata

\* 제주대학교 대학원 컴퓨터교육학과 박사과정  
- ORCID: <https://orcid.org/0000-0003-1009-3928>

\*\* Prairie View A&M University, College of Business, 교수  
- ORCID: <https://orcid.org/0000-0001-6810-4621>

\*\*\* 제주대학교 대학원 융합정보보안학과 교수  
- ORCID: <https://orcid.org/0000-0003-4434-8933>

· Received: Jun. 04, 2019, Revised: Aug. 07, 2019, Accepted: Aug. 10, 2019

· Corresponding Author: Namje Park

Dept. of Computer Education, Teachers College, Jeju National University,  
61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea  
Tel.: +82-64-754-4914, Email: [namjepark@jejunu.ac.kr](mailto:namjepark@jejunu.ac.kr)

## 1. 서 론

최근 범죄 예방을 위해 설치되고 있는 CCTV는 매년 증가하고 있으며, 국가지표체계에 공개된 내용에 따르면, 대한민국 공공기관의 CCTV 설치대수는 16년도부터 10만대 이상씩 설치되고 있음을 소개하고 있다[1]. 이처럼 증가하고 있는 CCTV에 비례하여 수집되고 있는 영상 또한 늘어나고 있으며, 영상을 관리하는 기관은 촬영된 영상에 대해 위·변조 사실을 파악하고, 영상의 신뢰성을 확보해야 할 필요성이 존재한다[2].

실례의 하나로 쇼단(Shodan)이나 인세캠(Insecam)에 의해 여러 국가의 CCTV에서 촬영된 영상이 유출되는 사건이 크게 화제가 되었다[3]. 화제가 된 두 사이트는 IoT 장치의 보안취약점 분석을 통한 보안성 강화를 목적으로 개설된 것으로, 보안취약점을 통해 영상장치에 접근하였다. 이는 해당 보안취약점을 이용하여 영상장치에 접근하고, 영상의 무결성을 훼손할 위험성이 존재함을 시사한다[4][5]. 그러므로 본 논문에서는 촬영된 영상의 메타데이터와 접근한 사용자의 기록을 블록체인에 기록함으로써 신뢰할 수 있는 기록을 생성하고, 이후 영상의 위·변조 사실을 확인해야 하는 경우, 기록된 내용과 대치함으로써 영상의 위·변조 사실과 시점을 확인할 수 있도록 하는 메커니즘을 제안하였다.

## II. 관련 연구

### 2.1 MPEG 계층 구조

MPEG은 영상이나 음성 신호 등을 압축하거나, 부호화, 전송, 표현 등의 제반 기술과 관련된 표준의 하나로써 많은 영상이 MPEG4 포맷을 활용하여 사용자에게 영상을 제공한다. MPEG은 화면비와 같은 속성을 가지는 Sequence Layer, 다수의 화면 데이터를 하나의 묶음으로 하는 GOP(Group of Pictures) Layer, 영상을 이루는 이미지 한 장에 대한 공통 속성을 가지는 Picture Layer, 매크로 블록을 여러개 합친 Slice Layer, 매크로블록 하나가 가지는 공통 속성을 가지는 Macro Block Layer, DCT (Discrete Cosine Transform) 처리 단위인 Block Layer의 6개 계층으로 구성된다[6].

### 2.2 블록체인의 이해

블록체인이란 관리하고자 하는 데이터를 블록단위로 소규모 데이터 단위로 구성하여 P2P(Peer-to-peer) 네트워크에 참여하는 모든 사용자가 블록데이터를 체인형태로 연결하여 블록데이터의 보안성을 강화하는 기술이다[7]. 블록체인에서 데이터는 P2P 네트워크에 참여하는 모든 사용자가 저장하며, 모든 블록데이터는 각각이 바로 이전의 블록에 대한 머클트리의 해시값 기록을 가지는 방식으로 연속해서 연결된다[8]. 블록데이터의 내용을 의도적으로 변경하기 위해서는 네트워크에 참여한 사용자의 반수 이상의 블록데이터를 변경하여야 하며, 블록데이터를 생성하고 계산된 머클해시값을 기반으로 해당 블록데이터 이후에 추가된 모든 블록데이터의 머클해시값을 다시 계산하여야만 한다. 블록체인에서는 이와 같은 방식을 통해 데이터의 위·변조를 방지한다[9].

### 2.3 관련 연구 동향

블록데이터의 위·변조가 어렵다는 면에서 블록체인은 큰 화제가 되었으며, 데이터의 위·변조가 발생할 수 있는 문제의 대처 방안으로서 떠올랐다. 그에 따라 다양한 분야에 접목하기 위한 연구가 진행되어 왔다. 본 항에서는 영상과 관련되어 진행되고 있는 선행 연구에 대한 동향을 소개하도록 한다[10]. Michael Kerr et al(2018)은 CCTV에 의해 촬영된 영상에 대해 블록체인 기술과 디지털 워터마킹 기술을 결합하여 분산 네트워크 환경에서 신뢰할 수 있는 증거를 보호하는 방법을 제안하였다[11]. Robert et al(2018)은 JPEG 이미지에 대해 블록체인을 적용하여 이미지의 변조를 찾는 기술을 제안하였다. 이 기술은 블록체인을 적용하여 탈중앙화를 통해 이미지에 대한 시그니처를 분산 저장함으로써 시그니처에 대한 변조 가능성을 줄였으며[12][13], Junichi Kishigami et al(2015)은 블록체인 기반의 디지털 콘텐츠 배포 시스템을 제안하였다. 제안된 시스템은 중앙집중형 시스템으로 창작물의 권한을 중앙에서 관리하였기에 블록체인을 통해 창작물의 권한 설정을 창작물의 권리가 관리할 수 있도록 하였다[14][15].

### III. 블록체인 기반 CCTV 영상 위·변조 감지 메커니즘

제안된 메커니즘은 기존의 영상감시 시스템에서 수집한 영상에 대해 추가적으로 발생한 시점과 이후 영상이 변경될 경우 해당 내용과 사용자를 블록에 기록함으로써 이후 위·변조가 발생할 경우, 발생한 시점과 사용자의 정보를 통해 영상의 무결성을 검증하는 것을 목적으로 한다[14][15]. 본 메커니즘은 카메라로부터 수집된 영상이 수집되는 서버에서 일정 시간 간격으로 촬영된 영상을 저장하고, 저장된 영상에 대한 사용자의 정보와 영상에 대한 정보를 블록데이터로 변환하여 블록체인네트워크에 전송함으로써 저장된 정보에 대한 위·변조 방지를 통해 신뢰할 수 있는 검증 데이터를 저장한다[17][18].

그림 1은 제안된 메커니즘의 개념도를 보이는 것으로 각 영상장치에 의해 촬영된 영상이 영상 서버로 전송되면, 해당 영상을 관리하는 관리자의 ID (Identity)와 영상이 수정되거나, 접근된 일자, 영상을 관리하는 장치의 IP(Internet Protocol) 주소, 영상의 저장된 이름과 영상의 용량, 영상의 해시값을 하나의 블록데이터로 생성하여 블록체인네트워크로 전송하는 과정을 보이는 것이다[19][20].

그림 2는 제안된 메커니즘의 진행 순서에 대해 순서도를 이용하여 보이는 것이다.

#### 3.1 용어

표 1은 제안된 메커니즘에서 블록데이터를 생성하는 과정에서 사용되는 용어를 보이는 것이다.

표 1. 용어 정리  
Table 1. Notation

| Content           | Abbreviation    |
|-------------------|-----------------|
| Video             | V <sub>D</sub>  |
| User ID           | U <sub>ID</sub> |
| Access date       | A <sub>D</sub>  |
| IP address        | A <sub>IP</sub> |
| Video name        | V <sub>N</sub>  |
| Video volume      | V <sub>V</sub>  |
| Video hash        | V <sub>H</sub>  |
| Block data        | B <sub>D</sub>  |
| Block hash        | B <sub>H</sub>  |
| String generation | Str             |

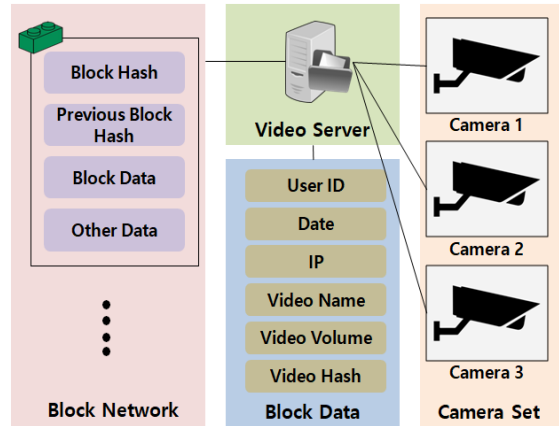
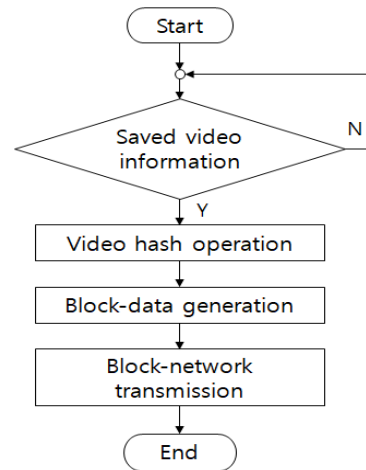
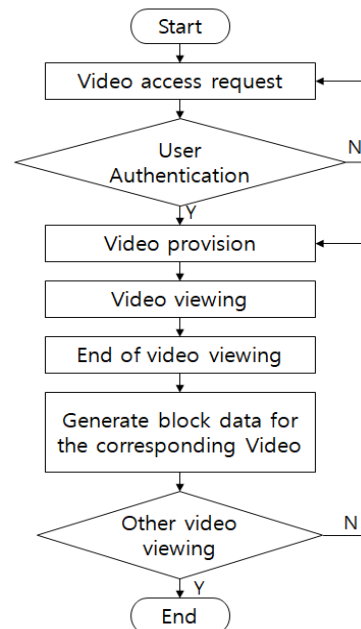


그림 1. 메커니즘 개념도  
Fig. 1. Concept of mechanism



(a) CCTV video acquisition phase



(b) Video access step

그림 2. 메커니즘 순서도  
Fig. 2. Flowchart of the mechanism

### 3.2 블록데이터 생성 단계

블록데이터 생성 단계는 선차적으로 영상이 수집되어 영상장치에 전송되었음을 가정하고 진행된다. 해당 단계에서는 수집된 영상의 해시를 검출하여 영상의 위·변조 검출을 위한 근거인 해시값을 연산하고, 해당 해시값을 포함하여 영상에 대한 블록데이터를 생성한다. 수집된 영상은 SHA(Secure Hash Algorithm) 연산을 통해 영상의 해시값을 구한다. 이때, 생성되는 해시값은 복원이 불가능하며, 이후 복원하여 확인하기 위한 데이터가 아닌 해당 영상의 검증이 요구될 경우, 같은 방식으로 연산하여 영상의 비교를 진행하기 위해 사용된다. 식 (1)은 영상의 해시값을 구하는 수식을 의미한다.

$$V_H = SHA256(V_D) \tag{1}$$

이후 구해진 영상의 해시는 블록데이터에 포함하며, 블록데이터는 ID, 관리자의 IP주소, 접근일자, 영상명, 영상의 용량, 영상의 해시값으로 구성되며, 해당 내용은 하나의 문자열로 저장되게 된다.

$$B_D = Str(V_{ID} + A_D + A_{IP} + V_N + V_V + V_H) \tag{2}$$

식 (2)는 블록데이터 생성과정을 보이는 수식을 의미한다. 블록데이터 BD는 VD, UID AD, AIP, VN, VV, VH를 문자열로서 저장함으로써 영상정보를 가진 하나의 문자열로서 변경되며, 해당 문자열은 이후, 영상의 검증 정보로서 사용된다.

### 3.3 블록데이터 해시 생성 단계

블록데이터 해시 생성 단계에서는 블록네트워크에 추가하기 위해 블록데이터의 해시값을 구하고, 공개키 기반의 암호화 방식을 통해 암호화된 블록데이터를 해시값을 이용하여 블록네트워크에 게시한다. 먼저 생성된 블록데이터는 RSA 공개키 암호화 방식에 기반하여 영상을 암호화하여 암호문과 두 쌍의 키를 생성한다. 생성된 공개키는 블록데이터에 추가함으로써 이후 정당한 관리자의 복원 요청이 발생할 경우, 관리자가 가진 공개키에 의해 복원될 수 있도록 한다. 식 (3)은 RSA 암호화에 의해 암호문과 키가 생성됨을 보이는 것이다.

$$RSA\ Encryption(B_D) = \begin{cases} Cryptogram \\ Private\ Key \\ Public\ Key \end{cases} \tag{3}$$

RSA 암호화에 의해 암호화된 블록데이터 BD는 다시 한 번 SHA 연산에 의해 해시값을 생성한다. 식 (4)는 SHA 연산을 수행하여 블록네트워크에 추가하기 위한 블록 해시를 연산하는 과정을 보이는 것이다.

$$B_H = SHA256(B_D) \tag{4}$$

식 (4)에 의해 연산된 블록 해시는 이후 블록네트워크의 변조를 어렵게 하기 위해 이후 생성되는 블록데이터에 대한 이전 주소의 역할로서 사용된다. 블록네트워크에 추가되는 두 번째 블록데이터부터는 이전에 연산된 블록 해시를 헤더에 추가한다.

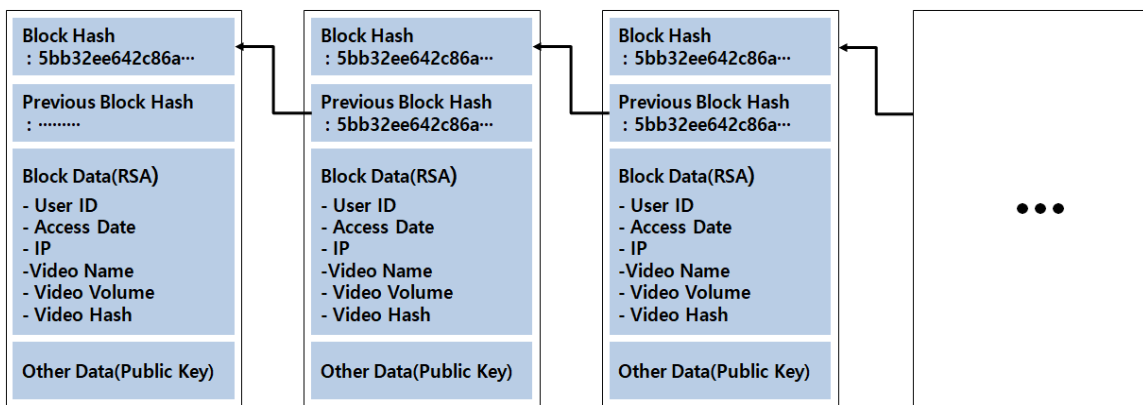


그림 3. 블록 구조  
Fig. 3. Block structure

생성된 블록네트워크는 내용의 변경을 위해서 이후 추가되는 모든 해시값을 재연산해야하기 때문에 해당 데이터에 대한 변조가 어려워지게 된다. 그림 3은 생성된 블록의 구조에 대한 예시를 보이는 것이다.

#### IV. 제안된 메커니즘 구현

제안된 메커니즘은 사용자의 ID, 영상 접근 일자, 영상의 이름, 영상의 용량, 영상의 해시값을 블록데이터로서 생성하였으며[21]-[24], 이와 같은 블록데이터를 생성하고, 블록데이터의 해시값을 기반으로 한 블록체인을 구현하였다. 그림 4는 구현 결과를 보이는 것이다.

구현된 메커니즘에서 영상정보는 1차적으로 블록데이터를 생성하는 과정에서 데이터 안에 포함되는 내용과 영상의 접근이 발생할 때 마다 블록이 발생하는 차수와 해당 블록데이터의 이전 해시값과 현재 해시값을 헤더에 기록하고[25]-[30], 최종적으로 해당 블록에 기록되어 있는 블록데이터를 확인하였다.

|  |
|--|
| 영상정보<br>사용자: ID1<br>접근일자: Wed May 22 20:22:36 2019<br>영상명: 3<br>용량: 7965987<br>해시: 681BF08E20741D9F6D62F779C51864A9545E221A<br>발생차수: 0<br>데이터<br>이전 해시: 0<br>현재 해시: 5bb51ff3759bd0057facc3f6c86e792752a97c3a1fdec6b71992a50ce9a4cf8b<br>데이터: ID1 Wed May 22 20:22:36 2019 3 7965987 681BF08E20741D9F6D62F779C51864A9545E221A   |
| 영상정보<br>사용자: ID3<br>접근일자: Wed May 22 20:22:50 2019<br>영상명: 4<br>용량: 8638723<br>해시: 68188D8E207415946D62F779C71864A9545E221A<br>발생차수: 1<br>데이터<br>이전 해시: 5bb51ff3759bd0057facc3f6c86e792752a97c3a1fdec6b71992a50ce9a4cf8b<br>현재 해시: 086fe972fffad69688f5da01b3c341aa25097144e88028a9b06c33437ff1a6f<br>데이터: ID3 Wed May 22 20:22:50 2019 4 8638723 68188D8E207415946D62F779C71864A9545E221A |
| 영상정보<br>사용자: ID1<br>접근일자: Wed May 22 20:25:00 2019<br>영상명: 8<br>용량: 663674<br>해시: 681BAD8620741D946D642F779C51864A1545021C<br>발생차수: 2<br>데이터<br>이전 해시: 086fe972fffad69688f5da01b3c341aa25097144e88028a9b06c33437ff1a6f<br>현재 해시: a05c735bc3f19ca430ef491ddf57140a01ea3b9aa0a2e06f9582e97b9fa04d41<br>데이터: ID1 Wed May 22 20:25:00 2019 8 663674 681BAD8620741D946D642F779C51864A1545021C   |

그림 4. 메커니즘 구현 결과  
 Fig. 4. Mechanism implementation result

#### V. 결론 및 향후 과제

영상감시 시스템에 의해 촬영된 영상은 이후 촬영된 장소에서 발생한 사건이나 사고 등에 대한 증거물로서 사용될 수 있으며, 이 경우 제출되는 영상은 위·변조가 없음이 증명되어야만 한다. 영상의 위·변조가 되었을 가능성이 있는 영상은 증거물로서 사용할 수 없으며, 영상의 위·변조를 방지하는 기술 적용을 통해 영상의 신뢰성을 확보할 수 있는 방안이 요구된다. 이에 대해 블록체인은 블록데이터 간의 연결이 바로 이전에 저장되어있는 블록데이터의 해시값을 헤더에 포함한다는 점을 이용한다. 모든 블록데이터는 바로 전 블록데이터의 해시값을 가지고 있으며, 어떤 블록데이터를 변경하기 위해서는 블록데이터를 변경하고 생성된 해시값을 이후에 생성된 블록데이터에 적용하여야하며, 이후에 생성된 모든 블록데이터는 새로운 해시값을 연산하여 적용하여야하기 때문에 블록데이터에 대한 위·변조가 어렵다는 장점을 가진다.

본 논문에서 제안한 블록체인 기반의 영상 위·변조 검증 메커니즘은 블록데이터에 영상의 정보를 저장함으로써 이후 영상의 제출이 요구될 경우, 해당 영상에 대해 신뢰성을 증명할 수 있는 비교검증 데이터를 생성하는 것을 목적으로 한다. 영상감시 시스템에 의해 촬영된 영상은 그 사용용도에 의해 위·변조에 민감하며, 영상의 위·변조를 증명하거나 혹은 위·변조 자체를 방지할 수 있는 메커니즘의 지속적인 연구가 필요하다.

#### References

- [1] Ministry of the Interior and Safety, CCTV installation and operation status of public institutions, [http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx\\_cd=2855](http://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=2855). [accessed: May. 17, 2019]
- [2] Jinsu Kim, Namje Park, Geonwoo Kim, and Seunghun Jin, "CCTV cctv video processing metadata security scheme using character order preserving-transformation in the emerging

- multimedia", *International Journal of Electronics*, Vol. 8, No. 4, pp. 412, Apr. 2019. doi:10.3390/electronics8040412.
- [3] Boannews, Korea IoT device vulnerability, exposure to Shodan, <https://www.boannews.com/media/view.asp?idx=73523>. [accessed: May. 17, 2019]
- [4] Donghyeok Lee, Namje Park, Geonwoo Kim, and Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", *International Journal of Peer-To-Peer Networking And Applications*, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.
- [5] Namje Park and Donghyeok Lee, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment", *International Journal of Personal and Ubiquitous Computing*, Vol. 22, Issue 1, pp. 3-10, Feb. 2018.
- [6] MPEG video data structure, MPEG digital video, [http://www.ktword.co.kr/word/abbr\\_view.php?m\\_tem p1=3143](http://www.ktword.co.kr/word/abbr_view.php?m_tem p1=3143). [accessed: May 20, 2019]
- [7] Donghyeok Lee and Namje Park, "Geocasting-based synchronization of almanac on the maritime cloud for distributed smart surveillance", *International Journal of Supercomputing*, Vol. 73, Issue 3, pp. 1103-1118, Mar. 2017.
- [8] Namje Park and Hyochan Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment", *International Journal of Security and Communication Networks*, Vol. 9, Issue 6, pp. 500-512, Apr. 2016.
- [9] JongKi Lee, "An exploratory case study of distributed ledger processing using ibm bluemix blockchain", *Journal of KCAR*, Vol. 15, No. 1, pp. 25-38, Jun. 2017.
- [10] Namje Park and Namhi Kang, "Mutual authentication scheme in secure internet of things technology for comfortable lifestyle", *International Journal of Sensors*, Vol. 16, No. 1, pp. 1-16, Dec. 2015.
- [11] M. Kerr, F. Han, and Ron G. van Schyndel, "A blockchain implementation for the cataloguing of cctv video evidence", *Conference of AVSS 2018*, Auckland, New Zealand, pp. 1-6, Nov. 2018.
- [12] R. A. Dobre, R. O. Preda, C. C. Oprea, and I.Pirnog, "Authentication of JPEG Images on the Blockchain", *Conference of ICCAIRO 2018*, Prague, Czech Republic, pp. 211-215, May 2018.
- [13] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, and A. Akutsu, "The blockchain-based digital content distribution system", *Conference of 2015 IEEE Fifth International Conference on Big Data and Cloud Computing*, Dalian, China, pp. 187-190, Aug. 2015.
- [14] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI mobile platform with secure service for mobile RFID network environment", *International Journal of Asia-Pacific Web Conference*, Harbin, China, pp. 741-748, Jan. 2006.
- [15] Namje Park, Hongxin Hu, and Qun Jin, "Security and privacy mechanisms for sensor middleware and application in internet of things (IoT)", *International Journal of Distributed Sensor Networks*, Vol. 2016, No. 1, pp. 1-3, Jan. 2016.
- [16] Seunglea Kim, "Smart Contract System by Blockchain of Real Estate Transaction", *Journal of Real estate law review*, Vol. 22, No. 3, pp. 93-124, Nov. 2018.
- [17] Daehee Lee, "Personal Data Issues in Applying Blockchain Technologies", *Journal of KIL*, Vol. 22, No. 3, pp. 244-272, Dec. 2018.
- [18] Namje Park, Byung-Gyu Kim, and Jinsu Kim, "A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission", *International Journal of Electronics*, Vol. 8, No. 7, pp. 735, Jul. 2019. doi:10.3390/electronics8070735.
- [19] Donghyeok Lee and Namje Park, "ROI-based efficient video data processing for large-scale



- cloud storage in intelligent CCTV environment", Journal of IJET, Vol. 7, No. 2.33, pp. 151-154, Mar. 2018.
- [20] Donghyeok Lee and Namje Park, "A Study on COP-Transformation Based Metadata Security Scheme for Privacy Protection in Intelligent Video Surveillance", Journal of KIISC, Vol. 28, No. 2, pp. 417-428, Apr. 2018.
- [21] Namje Park, Younghoon Sung, Youngsik Jeong, Soo-Bum Shin, and Chul Kim, "The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea", International Conference on Computer and Information Science, Springer, pp. 1-15, Jun. 2018.
- [22] Donghyeok Lee and Namje Park, "A Study on Metering Data De-identification Method for Smart Grid Privacy Protection", Journal of KIISC, Vol. 26, No. 6, pp. 1593-1603, Dec. 2016.
- [23] Donghyeok Lee and Namje Park, "Legislative Reform of Smart Grid Privacy Act", Journal of KIISC, Vol. 26, No. 2, pp. 415-423, Apr. 2016.
- [24] Donghyeok Lee and Namje Park, "Institutional Improvements for Security of IoT Devices", Journal of KIISC, Vol. 27, No. 3, pp. 607-615, Jun. 2017.
- [25] Donghyeok Lee and Namje Park, "Proposal of Technology and Policy Post-Security Management Framework for Secure IoT Environment", Journal of KIIT, Vol. 15, No. 4, pp. 127-138, Apr. 2017.
- [26] Jinsu Kim and Namje Park, "Inteligent Video Surveillance Incubating Security Mechanism in Open Cloud Environments", Journal of KIIT, Vol. 17, No. 5, pp. 105-116, May 2019.
- [27] Jinsu Kim, Sangchoon Kim, and Namje Park, "Face Information Conversion Mechanism to Prevent Privacy Infringement", Journal of KIIT, Vol. 17, No. 6, pp. 115-112, Jun. 2019.
- [28] Jae-Young Chang, Sung-Mun Hong, Damy Son, Hojin Yoo, and Hyoung-Woo Ahn, "Development of Real-time Video Surveillance System Using the Intelligent Behavior Recognition Technique", The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 19, No. 2, pp.161-168, Apr. 2018
- [29] Seung-Gag Lim, "A Performance Comparison of CCA and RMMA Algorithm for Blind Adaptive Equalization" The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 19, No. 1, pp. 51-56, Feb. 2019.
- [30] Young-Do Joo, "A Study on the Construction of Near-Real Time Drone Image Preprocessing System to use Drone Data in Disaster Monitoring", The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 18, No. 3, pp.143-149, Jun. 2019.

#### 저자소개

##### 김진수 (Jinsu Kim)



2017년 2월 ~ 2019년 8월:

강원대학교 정보통신공학전공  
학사, 석사

2019년 9월 ~ 현재 : 제주대학교  
대학원 컴퓨터교육학과 박사과정

2018년 9월 ~ 현재 : 제주대학교  
사이버보안인재교육원 연구원

관심분야 : 클라우드, 지능형 영상감시 시스템, IoT 등

##### 조재영 (Jaeyoung Cho)



2000년 : Korea Military Academy  
International Relations 학사

2013년 : Troy University 석사

2016년 : University of Houston  
Industrial Engineering 박사

2000년 ~ 2016년 : Korea Army  
Officer (UN본부 등)

2016년 ~ 2019년 : Lamar University Assistant Professor

2019년 8월 현재 : Prairie View A&M University,

Management & Marketing, Assistant Professor

관심분야 : Logistics / Supply Chain Management,

Safety and Security Management 등

박 남 제 (Namje Park)



2008년 2월 : 성균관대학교

컴퓨터공학과 박사

2003년 4월 ~ 2008년 12월 :

한국전자통신연구원

정보보호연구단 선임연구원

2009년 1월 ~ 2009년 12월 : 미국

UCLA대학교 공과대학 Post-Doc,

WINMEC 연구센터 Staff Researcher

2010년 1월 ~ 2010년 8월 : 미국 아리조나 주립대학교

컴퓨터공학과 연구원

2010년 9월 ~ 현재 : 제주대학교 교육대학

초등컴퓨터교육전공, 융합정보보안학과 교수

관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT,

해사클라우드 등