

<https://doi.org/10.7236/JIIBC.2021.21.3.15>

JIIBC 2021-3-3

# 블록체인 기반 설명 가능 CCTV 영상 무결성 지원 시스템

## Integrity Support System for Blockchain-based explainable CCTV Video

김태영\*, 홍준기\*\*, 강민구\*\*, 송성한\*\*, 이정훈\*\*, 김순태\*

Taeyoung Kim\*, Joongi Hong\*\*, Mingu Kang\*\*,  
Seounghan Song\*\*, Jeonghoon Lee\*\*, Suntae Kim\*

**요약** 사회의 변화에 따라 범죄들의 수법들도 다양해지며 그 수도 증가하고 있다. 그리고 이러한 현상은 사람의 밀집도가 높은 곳일수록 더 높은 추세를 보인다. 이에 따라 많은 기관에서는 CCTV를 설치함으로써 범죄를 줄이고 결정적 증거를 제공해준다. 그럼에도 불구하고 아직 CCTV를 대상으로 한 영상 조작과 같은 범죄들에 대해서는 그 대처가 미약하다. 이러한 영상의 조작을 방지하기 위해 블록체인 기반의 CCTV 영상 무결성 기법들을 적용하고 있음에도 불구하고, 이들은 전체 영상의 조작 무결성만을 보장할 뿐 영상의 특정 구간이 어떻게 조작되었는지 설명해 주지 못한다. 따라서 본 연구에서는 이러한 문제를 해결하기 위해 블록체인을 기반으로 한 설명 가능 CCTV 영상 무결성 지원 시스템을 제안한다.

**Abstract** The type of crimes is diverse and the number of crimes is increasing as society changes. This phenomenon is showing a higher trend in places with higher population density. Accordingly, many organizations install CCTV to reduce crime and provide key evidence of crime. Nevertheless, it is still weak to deal with crimes such as video manipulation targeting CCTV. Although blockchain-based CCTV image integrity techniques are applied to prevent manipulation, they only guarantee the manipulation integrity of the entire video and can't explain how certain sections of the video has been manipulated. Therefore, in this research, we propose a system for supporting explainable CCTV video integrity based on a block chain.

**Key Words** : Blockchain, Video manipulation, CCTV, Explainable CCTV Video integrity

### 1. 서론

사회의 빠른 발전과 성장에 따라 다양한 범죄들이 증가하고 그 수법이 다양해지고 있다. 특히, 사람의 밀집도

가 높은 곳일수록 이러한 범죄는 평균적으로 높은 추세를 보이고 있다<sup>[1]</sup>. 이에 따라 이러한 사회적 문제를 해결하기 위해 많은 지자체에서 CCTV(Closed Circuit Television)를 설치하고 있다<sup>[2]</sup>. CCTV는 범죄 현장을

\*준회원, 전북대학교 소프트웨어공학과

\*\*정회원, 전북대학교 소프트웨어공학과

접수일자 2021년 3월 23일, 수정완료 2021년 4월 23일

계재확정일자 2021년 6월 4일

Received: 23 March, 2021 / Revised: 23 April, 2021 /

Accepted: 4 June, 2021

\*Corresponding Author: stkim@jbnu.ac.kr

Department of Software Engineering, CAIIT, Jeonbuk National University, Korea

즉각적으로 기록하고 이를 보관함으로써 추후 범죄의 결정적 증거를 제시해 줄 수 있는 중요한 역할을 한다. 하지만 CCTV는 사회의 범죄에 대해 중요한 역할을 맡고 있음에도 불구하고 CCTV 자체에 대한 범죄(영상의 조작)에 대해서는 그 대응이 미약하다.

예를 들어 한국에서는 대표적으로 세월호 선내 CCTV 영상을 조작하여 범죄를 은폐하려고 하였으며 이러한 파 일은 모두 1만 8,353개에 달했다<sup>[3]</sup>. 그 외에도 다양한 곳에서도 영상을 조작하여 사건을 은폐하는 수법이 많아지고 있다<sup>[4, 5]</sup>. 이에 따라 CCTV 영상의 조작을 방지하고 이를 투명하게 관리하기 위한 영상의 무결성 방안이 필요하다.

CCTV 영상의 무결성을 보장하기 위해 많은 기존의 연구들이 블록체인을 기반으로 한 영상 무결성 기법들을 시도하고 있다<sup>[9-15]</sup>. 하지만 대부분의 연구는 저장된 전체 영상에 대한 조작의 무결성을 보장해 줄 뿐 영상의 특정 구간이 조작되었을 때 해당 구간이 어떻게 조작되었는지는 파악해줄 수 못하고 있으며 조작된 영상에 대한 원본 영상도 제공해주지 못하고 있다.

이에 따라 본 논문에서는 CCTV 영상의 무결성을 보장하여 영상의 상세 조작에 대한 검증을 지원해주는 블록체인 기반 설명 가능 CCTV 영상 무결성 시스템을 제안한다. 먼저 우리는 VMS(Video Management System)에 저장된 영상으로부터 I-Frame을 추출한다. 다음으로 추출된 I-Frame들은 해시화를 통해 전체 영상에 대한 MainHash를 만들어 준다. 추출된 I-Frame Set들은 IPFS로 저장되고 IPFS는 해시값을 반환해 준다. 마지막으로 IPFS 해시값과 영상의 MainHash값 그리고 영상의 시간 구간을 트랜잭션을 통해 블록체인에 저장한다.

영상 조작의 경우, 조작된 영상의 I-Frame을 추출 후 블록체인에 조회하고 없는 경우 영상 시간에 따라 트랜잭션을 조회하여 원본 영상을 가져오기 위해 IPFS에 해당 원본에 대한 IPFS 해시값을 조회한다. 그 후 블록체인에 조회된 트랜잭션의 MainHash를 조작된 영상과 비교하여 “추가”, “수정”, “삭제” 그리고 “정상” 등의 4가지 상태로 Label을 매겨 준다. 그리고 IPFS로부터 조회된 원본 영상은 검증된 I-Frame과 함께 제공되어 진다.

본 논문은 다음과 같은 순서로 구성되어 있다. 2절에서는 접근방안에 사용되는 주요 기술에 대한 배경지식을 다루고 있으며 3절에서는 Blockchain을 기반으로 영상의 무결성을 보장하는 연구들을 설명한다. 4절에서는 본 연구에서 제안하는 접근방안을 기술하며 5절에서는 본 연구에서 제안하는 시스템에 대한 안전성 평가와 6절에

서는 제안하는 시스템의 성능 평가를 다룬다. 마지막으로 7절에서는 본 연구의 결론을 다룬다.

## II. 배경지식

### 1. 블록체인

블록체인은 블록이라는 데이터 단위로 P2P 방식의 분산 네트워크에 체인 형태로 분산 저장하여 누구라도 임의로 수정할 수 없고 누구나 변경의 결과를 열어볼 수 있는 분산 컴퓨팅 기술 기반의 원장 관리 기술이다<sup>[6]</sup>. 이러한 블록체인은 근본적으로 분산 데이터 저장기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 데이터로써 분산 노드의 운영자에 의한 임의의 조작이 불가능하도록 설계되었다.

### 2. IPFS(InterPlanetary File System)

IPFS(InterPlanetary File System)는 P2P 네트워크 기반의 분산 파일 시스템으로써 데이터를 저장하고 공유하기 위한 프로토콜을 제공한다<sup>[7]</sup>. IPFS는 데이터 저장 시 데이터의 내용을 Key-Value pair 형태로 저장하며 이때 제공되는 Key 값은 데이터에 대한 해시값으로써 해당 데이터를 가져올 시 해당 해시값을 이용하여 여러 컴퓨터에 분산되어 저장된 데이터를 찾은 후 이를 잘게 나눠 빠른 속도로 가져와 하나로 합쳐 보여주는 방식을 사용한다.

## III. 관련연구

영상의 무결성을 보장하고 영상의 조작을 검증하기 위해 많은 기존 연구들이 블록체인 기술을 적용하였다. 그리고 이러한 블록체인 기반 연구는 크게 공용 블록체인과 사설 블록체인 방식으로 나누어질 수 있다. 공용 블록체인은 누구나 네트워크에 참여하여 블록체인에 데이터를 읽고 쓸 수 있는 특성으로 인해 데이터의 무결성을 위한 합의 과정이 복잡하다. 그에 비해 사설 블록체인은 허가된 참여자만이 블록체인에 데이터를 읽고 쓸 수 있다. 그래서 합의 과정이 다소 단순하며 처리속도가 빠르다 [8]. 우리는 이러한 블록체인의 유형에 따라 영상의 무결성을 보장하고 영상의 조작을 검증하는 연구들에 관해 소개한다.

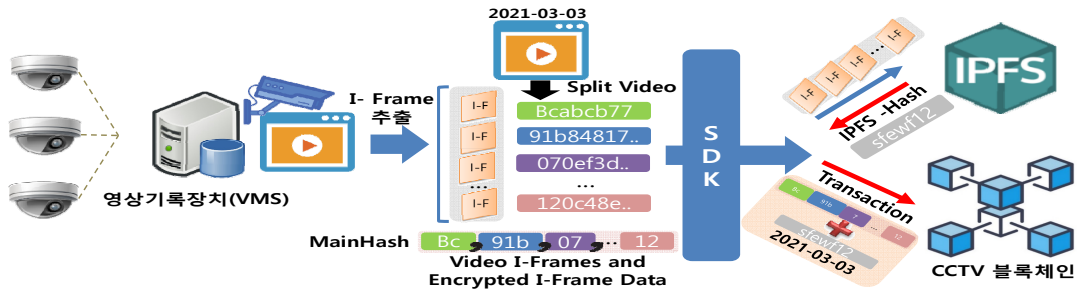


그림 1. CCTV 영상의 무결성 지원을 위한 저장 방안  
 Fig. 1. A storage method for supporting the integrity of CCTV video

## 1. 공용 블록체인 기반의 영상 무결성 지원 방안

공용 블록체인을 기반으로 영상의 무결성을 지원하기 위해 Gipp et al.<sup>[9]</sup>는 스마트 폰을 통해 10초 간격으로 영상을 기록한 후 해당 영상들을 해시화 하여 Bitcoin 블록체인 네트워크에 트랜잭션으로 전송함으로써 무결성을 보장해준다. Reilly et al.<sup>[10]</sup>은 스마트 시티 내의 CCTV 카메라와 같은 IoT기기의 무결성 보장을 지원하기 위해 Ethereum 블록체인에 780kb 크기의 data를 트랜잭션으로 저장하는 방식을 취하고 있다. Yatskiv et al.<sup>[11]</sup>은 Video Stream을 Frame 단위로 나누고 각 Frame을 해시화한 후 트랜잭션을 생성한다. 블록의 Hash는 각 Frame의 Hash를 합하여 생성한 것을 블록체인에 저장하는 방식을 사용한다.

이런 공용 블록체인을 기반으로 한 연구들은 누구나 네트워크에 참여하여 해당 데이터에 대한 열람이 가능하도록 허용해주기 때문에 CCTV와 같은 개인정보가 민감한 정보를 올리기에는 적절하지 못하며 공용 네트워크의 특성상 네트워크에 정보를 저장하기 위해서는 돈을 지불하고 트랜잭션을 전송해야 하므로 운영 측면에 대한 부담도 존재한다.

## 2. 사설 블록체인 기반의 영상 무결성 지원 방안

사설 블록체인을 통해 영상의 무결성을 지원하기 위해 Liu et al.<sup>[12]</sup>은 공공 기관에서의 영상의 데이터의 무결성을 보장하기 위해 10분 단위로 영상의 데이터를 가져와 이를 압축한 후 해시화 하여 블록체인에 저장하는 방식으로 기관마다 별도의 원본 영상에 대한 서버를 두게 하여 영상의 원본도 보관하게 하였다. Kerr et al.<sup>[13]</sup>은 개개의 CCTV에 블록체인의 노드로써 참여시키기 위한 IoT 기기를 설치 후 영상에 대해 워터마킹 및 해시화를 수행하여 사설 블록체인에 저장하는 방식을 사용한다.

Khan et al.<sup>[14]</sup>은 네트워크 내부의 정책에 따라 영상에서 I-Frame을 선별 후 해시화 하여 블록체인에 저장하여 영상의 무결성을 보장한다. 또한, Ghimire et al.<sup>[15]</sup>은 1분 단위로 영상을 가져와 SHA-256으로 해시화한 후 타원 곡선 암호화(elliptic curve cryptography)로 암호화를 하여 블록체인에 저장하여 영상의 무결성을 제공해준다.

이러한 연구들은 영상 자체에 대한 접근성과 무결성 측면의 보안성은 뛰어나지만, 영상의 특정 구간이 조작되었을 경우 해당 구간이 어떻게 조작되었는지는 파악을 못 해주고 있다. 또한, 대부분 접근방안이 원본 영상에 대한 별도의 저장소가 없어 조작된 영상에 대한 원본을 제공해주기 어려운 점이 있으며 원본에 대한 별도의 저장소를 가지고 있더라도 IPFS와 같은 분산된 네트워크가 아닌 노드마다 개인 서버를 구축해 원본 영상을 가지고 있으므로 해당 서버가 손상된다면 서버가 쥐고 있는 원본 영상이 모두 소실되게 된다.

본 논문에서는 이러한 문제점들을 해결하기 위해 무결성과 상세 검증을 가능하도록 지원해주는 방안에 대해 다음 장에서 기술한다.

## IV. 접근방안

우리는 블록체인을 기반으로 한 설명 가능 CCTV 영상 무결성 지원 시스템을 제안한다. 본 장에서는 CCTV 영상의 무결성 보장을 위한 저장 방안과 저장된 영상을 기반으로 영상의 상세 조작 검증 지원을 위한 방법에 관해 기술한다.

### 1. 영상의 무결성을 위한 CCTV 영상 저장

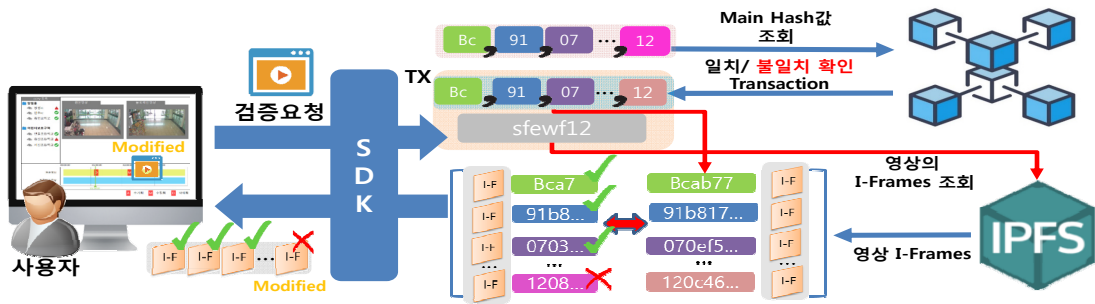


그림 2. 조작된 영상의 상세 설명을 위한 지원 방안  
Fig. 2. Method for supporting detailed explanation of manipulated video

다음의 그림 1은 CCTV 영상의 원본을 저장하고 무결성을 지원하는 방법에 관해 기술하고 있다. 먼저 영상의 무결성을 보장하기 위해서 CCTV 영상이 저장된 영상 기록 장치로부터 1분 단위로 영상을 가져온 후 그 안에서 I-Frame들을 추출한다. 추출된 각각의 I-Frame들은 해시화를 수행한다. 다음으로 각 I-Frame 해시값 사이에 구분자를 두고 이를 합하여 하나의 MainHash를 생성한다. 우리는 영상의 이미지에 대한 해시화를 위해 영상 해시화 알고리즘을 제공해주는 JImageHash를 사용한다<sup>[16]</sup>. 그 후 시스템의 SDK를 통해 먼저 IPFS에 영상의 I-Frame들을 저장한 뒤 IPFS로부터 반환된 해당 I-Frame들에 대한 해시값과 MainHash 그리고 영상에 대한 시간을 트랜잭션으로 구성하여 블록체인에 저장한다.

영상의 각 I-Frame들에 대한 원본 영상을 보존하기 위해, 우리는 블록체인에 IPFS를 같이 운용하여 사용한다. 비록 블록체인이 IPFS와 유사하게 분산 네트워크의 저장기술을 가지고 있음에도 영상의 원본을 저장하기 위해 블록체인을 사용하지 않는 이유는 블록체인에는 대용량의 데이터를 저장하는 것이 어렵기 때문이다. 예를 들어 초당 200MB의 영상 데이터를 블록체인에 계속 저장하게 되면 블록체인을 공유하는 모든 노드는 같은 용량의 데이터를 계속해서 가져야 한다. 이는 곧 시스템의 과부하를 초래하는 원인이 된다. 하지만 IPFS는 분산 네트워크를 기반으로 대용량의 내용을 저장하도록 지원한다. 따라서 우리는 영상의 I-Frame들을 IPFS에 저장한다.

## 2. 설명 가능한 영상의 상세 조작 검증

설명 가능한 영상의 상세 조작 검증은 다음의 그림 2와 같이 수행된다. 먼저 사용자가 특정 영상에 대해 시스템의 SDK로부터 검증 요청을 했을 때 저장방식과 유사하게 I-Frame을 추출 후 MainHash를 생성한다. 다음

으로 해당 MainHash값을 블록체인으로부터 조회하여 조작되었는지를 확인한다. 만약 특정 영상의 해시값이 블록체인에서 조회되지 않는다면 이는 조작이 되었다는 것이기 때문에 이때, 특정 영상의 시간 구간을 블록체인에서 조회된 트랜잭션 내의 MainHash와 IPFS 해시값을 통해 상세 검증을 수행한다. 상세 검증을 수행하기 위해, 우리는 먼저 MainHash를 생성할 때 넣은 구분자를 기반으로 MainHash를 나누어 MainHash로부터 각 I-Frame들에 대한 해시값을 추출한다. 그 후 추출된 I-Frame들의 해시값에 대해 비교를 수행함으로써 특정 영상에 대한 영상 조작의 3가지 상태(추가, 수정, 삭제)를 다음의 표 1과 같이 식별한다.

표 1. 3가지 영상 조작에 대한 식별 조건  
Table 1. The Identification Criteria for Three Image Manipulation

식별 상태	조건	Description
추가	비교 영상의 I-Frame 수 > 원본 영상의 I-Frame 수	원본과 같은 Frame을 제외한 추가 Frame이 있는 경우
수정	비교 영상의 I-Frame 수 = 원본 영상의 I-Frame 수	원본과 비교 영상의 Frame 수는 같지만, 그 안에 서로 다른 Frame이 존재하는 경우
삭제	비교 영상의 I-Frame 수 < 원본 영상의 I-Frame 수	원본 영상보다 프레임 수가 적으며 원본에 해당하는 프레임이 없는 경우

## V. 안정성 평가

본 논문에서 제안한 블록체인 기반 설명 가능한 CCTV 영상 무결성 지원 시스템에 대한 안전성 평가를 위해 이전 장의 표 1에서 설명한 영상 조작의 3가지 유

형에 따라 안전성 평가를 진행하였다.

### 1. 영상 추가 조작에 대한 안전성

“영상 추가”는 원본 영상의 I-Frame과 비교 영상의 I-Frame의 개수를 비교하여 비교 영상의 I-Frame의 수가 더 많은 경우의 영상 조작 유형으로써 악의적인 사용자는 VMS에 접근하여 원본 영상에 새로운 영상을 추가하여 영상을 조작할 수 있다. 이 같은 경우 영상의 검증을 하고자 하는 사용자는 영상 검증 시 해당 영상의 시간 구간에 따른 트랜잭션 값을 조회하여 트랜잭션 내의 원본 영상의 MainHash를 각각의 I-Frame들에 대한 해시값들로 나누어 검증하고자 하는 영상의 I-Frame과 비교한다. 만약 검증 영상의 I-Frame 수가 더 많은 경우 같은 I-Frame 해시값을 가지는 것들을 제외한 나머지 I-Frame에 대해서는 “추가”되었다고 지정하고 나머지는 “정상”으로 지정함으로써 악의적인 사용자의 영상 추가 조작을 식별할 수 있다.

### 2. 영상 수정 조작에 대한 안전성

“영상 수정”은 원본과 비교 영상의 I-Frame의 수가 같지만 그중 몇 개의 I-Frame들이 수정되거나 완전히 다른 영상 값들이 들어간 경우의 영상 조작 유형이다. 악의적인 사용자는 VMS에 접근하여 영상을 수정하여 조작할 수 있다. 이 같은 경우 영상 추가 식별과 동일한 과정을 거쳐 각 I-Frame들의 값들을 비교하여 같은 값들에 대해서는 “정상”이라 지정하고 다른 값들에 대해서는 “수정”이라 지정함으로써 악의적인 사용자의 영상 수정 조작을 식별할 수 있다.

### 3. 영상 삭제 조작에 대한 안전성

“영상 삭제”는 비교 영상의 I-Frame들의 수가 원본의 I-Frame들의 수보다 적은 경우의 영상 조작 유형이다. 악의적인 사용자는 VMS에 접근하여 원본 영상의 일부분을 지움으로써 영상을 조작할 수 있다. 이 같은 경우 사용자는 영상 추가, 수정과 동일한 과정을 거쳐 원본 영상과 검증 영상의 I-Frame들을 비교함으로써 동일한 각 I-Frame들에 대해서는 “정상”을 지정하고 원본 I-Frame에 존재하지 않는 부분에 대해서는 “삭제”로 지정함으로써 악의적인 사용자의 영상 삭제 조작을 식별할 수 있다.

## VI. 성능 평가

우리는 블록체인을 기반으로 한 설명 가능 CCTV 영상 무결성 지원 시스템의 성능을 평가하기 위해 다음의 그림 3과 같이 영상의 크기에 따른 트랜잭션 발행 속도 및 크기에 따른 데이터 처리량을 평가하였다. 제안한 시스템의 트랜잭션 처리 속도는 IPFS를 거쳐 블록체인까지 저장되는 시간을 나타낸다. 실험을 위해 우리는 다른 크기의 영상 4개를 사용하였으며 각 영상마다 100번의 트랜잭션을 발행하여 평균시간을 확인하였다. 결과적으로 트랜잭션 발행속도의 시간 평균은 영상의 크기에 따라 증가함을 볼 수 있다. 하지만, 시간(ms)당 영상의 byte 처리량을 봤을 때 영상의 크기가 증가함에 따라 시간(ms)당 처리하는 데이터량(byte)이 많아지므로 이는 영상의 크기가 커질수록 트랜잭션의 속도도 점점 빨라질 수 있다는 것을 또한 가리킨다.

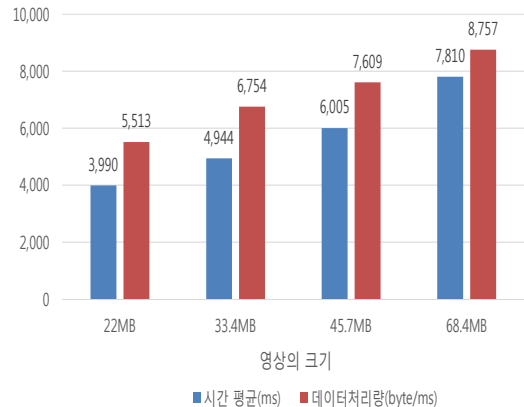


그림 3. 영상의 크기에 따른 트랜잭션 발행 속도 및 크기에 따른 데이터 처리량

Fig. 3. Average time to issue a transaction

## VII. 결 론

본 논문은 CCTV 영상의 무결성과 설명 가능한 영상의 상세 조작 검증을 지원하기 위한 블록체인 기반 설명 가능 CCTV 영상 무결성 지원 시스템을 소개하였다. 첫 번째로 VMS로부터 영상을 가져와 I-Frame들을 추출 후 이를 기반으로 해시화를 진행하여 MainHash를 생성하였고 해당 I-Frame들을 IPFS에 저장함으로써 원본 영상을 보존할 수 있게 하였다. 또한, IPFS로부터 반환된

해시값과 영상의 시간 그리고 MainHash를 기반으로 블록체인에 저장함으로써 영상정보의 무결성을 보장하였다. 마지막으로 설명 가능한 영상의 상세 조작 검증을 위해 트랜잭션에 저장된 MainHash를 구성된 I-Frame의 해시값들로 나누고 비교 영상과 비교하여 영상의 어느 I-Frame이 조작되었는지 판단하였으며 IPFS에 저장된 해당 원본 영상을 사용자에게 같이 제공함으로써 정확한 영상의 검증이 가능하도록 지원하였다.

## References

- [1] Jung Hoon Ki. (2015). A Study of Impact of Urban Population Characteristics on Violent Crimes. Journal of The Korean Regional Development Association, 27(1), 107-124.
- [2] Park, Tae-Sung. RTSP User Authentication Protocol for Blocking Malicious User in Network CCTV Environment. KAIS (2011): 239-242.
- [3] Seowall CCTV restoration video is traced to the operation... request for special investigation.. KBS NEWS. 2020.09.22.
- [4] Jinhyeon Park. "There is no reason to commit suicide, CCTV manipulation" VS "Even a homemade bomb... crime". KBS NEWS. 2019.10.15.
- [5] 권건보. "보육현장에 대한 전자적 감시의 법적 문제점." 세계헌법연구 17.3 (2011): 79-105.
- [6] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019. DOI: 10.2139/ssrn.3440802
- [7] IPFS White Paper - Juan Benet, "IPFS - Content Addressed, Versioned, P2P File System (DRAFT 3)"
- [8] Guegan, Dominique. "Public blockchain versus private blockchain." (2017).
- [9] Gipp, Bela, Jagrut Kostic, and Corinna Breiteringer. "Securing video integrity using decentralized trusted timestamping on the bitcoin blockchain." Mediterranean Conference on Information Systems (MCIS). Association For Information Systems, 2016.
- [10] Reilly, Elizabeth, et al. "A smart city iot integrity-first communication protocol via an ethereum blockchain light client." Proceedings of the International Workshop on Software Engineering Research and Practices for the Internet of Things (SERP4IoT 2019), Marrakech, Morocco. 2019.
- [11] Yatskiv, Vasyli, Nataliya Yatskiv, and Oleh Bandrivskiy. "Proof of Video Integrity Based on Blockchain." 2019 9th International Conference on Advanced Computer Information Technologies (ACIT). IEEE, 2019. DOI: 10.1109/acitt.2019.8780097
- [12] Liu, Mingda, et al. "VideoChain: trusted video surveillance based on blockchain for campus." International conference on cloud computing and security. Springer, Cham, 2018. DOI: 10.1007/978-3-030-00015-8\_5
- [13] Kerr, Michael, Fengling Han, and Ron van Schyndel. "A blockchain implementation for the cataloguing of cctv video evidence." 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). IEEE, 2018. DOI: 10.1109/avss.2018.8639440
- [14] Khan, Prince Waqas, Yung-Cheol Byun, and Namje Park. "A data verification system for CCTV surveillance cameras using blockchain technology in smart cities." Electronics 9.3 (2020): 484. DOI: 10.3390/electronics9030484
- [15] Ghimire, Sarala, Jae Young Choi, and Bumshik Lee. "Using blockchain for improved video integrity verification." IEEE Transactions on Multimedia 22.1 (2019): 108-121. DOI: 10.1109/tmm.2019.2925961
- [16] Zauner, Christoph. "Implementation and benchmarking of perceptual image hash functions." (2010).

## 저 자 소 개

### 김 태 영(준회원)



- 2018.2~: 전북대학교 박사 재학
- 2018: 전북대학교 공학석사
- 2016: 전북대학교 학사
- Email: r1axodud1200@jbnu.ac.kr

### 홍 준 기(준회원)



- 2019.9~: 전북대학교 석사 재학
- 2019: 전북대학교 학사
- Email: rlwns012@gmail.com

강 민 구(준회원)



- 2020.2~: 전북대학교 석사 재학
- 2020: 전북대학교 학사
- Email: 201314090@jbnu.ac.kr

송 성 한(준회원)



- 2019.9~: 전북대학교 석사 재학
- 2019: 전북대학교 학사
- Email: seounghansong@jbnu.ac.kr

이 정 훈(준회원)



- 2014.3~: 전북대학교 학사 재학
- Email: jhmake4419@jbnu.ac.kr

김 순 태(정회원)



- 2014~: 전북대학교 소프트웨어공학과 교수
- 2010: 서강대학교 공학박사
- 2007: 서강대학교 공학석사
- Email: stkim@jbnu.ac.kr

※ "본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음"  
(IITP-2021-2017-0-01628\*)