Journal of KIIT. Vol. 23, No. 6, pp. 131-141, Jun. 30, 2025. pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2025.23.6.131

블록체인 기반의 CCTV 영상 전주기 무결성 검증 시스템 설계

김 희 열*

Design of Blockchain-based CCTV Video Lifecycle Integrity Verification System

Heeyoul Kim*

이 논문은 2022학년도 경기대학교 연구년 수혜로 연구되었음

요 약

CCTV 영상이 법적 증거로 활용되기 위해서는 영상의 전주기에 대한 무결성이 보장되어야 하지만, 최근의 블록체인 기반 무결성 검증 기법들은 영상의 전주기에 대한 무결성의 실용적인 고려가 부족한 상황이다. 본 논문에서는 블록체인을 활용해 영상의 전주기 무결성을 검증하는 시스템 설계를 제안한다. 제안 시스템은 CCTV 기기에서 표준과 호환되는 무결성 데이터 생성 기술, 머클 트리를 이용한 효율적인 단일 영상 파일 무결성 검증 기술, 해시 체이닝을 이용한 연속된 영상 파일 시퀀스 무결성 검증 기술을 제공한다. 또한 퍼블릭·프라이빗 블록체인을 롤업으로 연계한 하이브리드 형태의 블록체인 연계 구축 방식을 제시한다. 제안 시스템은 기존 CCTV 인프라에 적용 가능하며, 중앙집중형 시스템의 문제를 해결하고 탈중앙화 기반의 고가용성을 제공하며, 영상의 전주기에 대한 무결성과 투명성, 고신뢰성을 충족하는 장점을 지닌다.

Abstract

For CCTV video as legal evidence, the integrity of the entire lifecycle of the video must be ensured. However, recent blockchain-based integrity verification methods often lack pragmatic consideration of this integrity. This paper proposes a system design that uses blockchain to verify the integrity throughout the entire lifecycle. The system provides techniques compatible with standard of CCTV equipment for generating integrity data, efficient single video file integrity verification using Merkle tree, and integrity verification of continuous video file sequences using hash chaining. Furthermore, we introduce a hybrid scheme that connects public and private blockchains through rollups. The design can be deployed on current CCTV infrastructure, eliminates the single point of failure of centralized solutions, and provides high availability via decentralization while ensuring integrity, transparency, and reliability.

Keywords

CCTV video, integrity verification, blockchain, Merkle tree, hash chaining

* 경기대학교 AI컴퓨터공학부 교수
- ORCID: https://orcid.org/0000-0001-6341-580X

· Received: Mar. 24, 2025, Revised: May 07, 2025, Accepted: May 10, 2025
· Corresponding Author: Heeyoul Kim
Dept. of AI Computer science, kyonggi University, 154-42, Gwanggyosan-ro, Korea
Tel.: +82-31-249-9607, Email: heeyoul.kim@kgu.ac.kr

Ⅰ. 서 론

CCTV 영상은 범죄 및 사고 분석을 위한 중요한 자료로 활용될 수 있으며, 국내에 1600만대의 CCTV가 운영 중인 것으로 추정된다. CCTV 영상의 변조를 방지하고 법적 증거로서의 가치를 지니기 위해서는 영상의 전주기 무결성이 보장되어야 하며, 이는 영상 데이터가 생성부터 저장, 전송 및 활용의 전주기 과정에서 변조되지 않고 원본 그대로의 상태를 유지하는 것을 의미한다.

CCTV 영상의 무결성 보장 및 검증을 위해 디지털 워터마크를 이용한 방식과[1] 전자서명을 이용한 방식[2], 암호화를 이용한 방식[3] 등이 연구되었다. 하지만, 이 방식들은 중앙집중화로 인한 단일실패지점 문제와 검증 시스템에 대한 신뢰성과 투명성 확보에 어려움을 겪고 있다.

이를 해소하기 위해 최근에는 블록체인을 이용한 무결성 검증 기법들이 제안되고 있다[4]-[8]. 하지만 기존 대부분의 연구가 저장된 단일 영상에 대한 무결성에만 집중되어 있고, 영상의 전주기에 대한 무결성 검증의 고려가 부족하다. 특히, 연속된 여러 영상파일들 전체에 대한 무결성을 보장하지 못하며, 일부 파일의 삭제 및 순서 조작 공격에 취약하다.

본 연구의 목적은 CCTV 영상의 생성-저장-전송-활용의 전 과정에 대한 전주기 무결성을 보장하는 검증 시스템의 설계를 제안함으로써, 기존 중앙집중형 검증 기법의 단일 실패 지점 문제와 신뢰성 문제를 해소하는 데 있다. 특히, 단일 영상파일 및 연속된 영상 시퀀스에 대한 무결성을 효율적이고 신뢰성 높게 증명하기 위한 블록체인 연계 방식을 모색한다.

본 논문에서는 다음과 같은 새로운 방법들을 제안하며, 이에 기반한 무결성 검증 시스템의 설계를 제시한다.

CCTV 기기에서 생성되는 영상에 대해 효율적으로 GOP 단위의 무결성 데이터를 생성하는 방법을 제공한다.

단일 영상 파일에 대해 머클 트리를 구성하고 머클 루트를 블록체인에 저장해 효과적으로 파일의 무결성을 검증하는 방법을 제공한다.

연속된 영상 시퀀스를 구조적으로 연결하는 해시 체이닝 방식을 제안해서 파일의 삭제 및 순서 변경 시도 공격을 방어한다.

민감한 데이터는 프라이빗 블록체인에 저장하고 롤업을 이용해 퍼블릭 블록체인에 앵커링해 투명성과 기밀성을 동시에 확보하는 하이브리드 블록체인 연계 방식을 제시한다.

본 논문의 구조는 다음과 같다. 2장에서는 블록체인과 이를 활용해 CCTV 영상의 무결성을 검증하기 위한 기존 연구들을 분석하며, 3장에서는 블록체인에 기반한 CCTV 영상의 무결성 검증 시스템 설계를 제공한다. 4장에서는 블록체인에 연계한 시스템 구축방식을 논의하고, 5장에서는 제안 시스템의 안전성을 분석한다. 마지막으로 6장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 블록체인 기술

블록체인은 분산 원장 기술(DLT, Distributed Ledger Technology)의 한 형태로, 거래 정보를 담은 블록을 해시값으로 서로 연결하여 체인 구조를 이루는 데이터 저장 방식이다. 각 블록에는 거래 내역, 생성 시각, 이전 블록 해시 등이 포함되며, 이들이 네트워크 참여 노드에 분산 저장·검증되기 때문에 단일 중앙 관리자가 부재한다[9]. 이러한 구조는 데이터 변경 시에 체인 전체의 해시 불일치가 즉시 드러난다는 변조 저항성, 모든 노드가 동일 원장을 공유함으로써 확보되는 투명성, 합의 알고리즘 기반의 탈중앙화 구조를 통한 고가용성을 동시에 보장한다.

또한, 블록체인은 스마트 컨트랙트를 통해 조건이 충족되면 자동으로 실행되는 코드를 온체인에 탑재할 수 있다. 스마트 컨트랙트는 사람이나 기관의 개입 없이도 거래·검증·정산 등을 자율적으로 수행하므로, 중개 비용과 처리 시간을 절감하고 사람에 의한 에러 가능성을 최소화한다. 이러한 특성 덕분에 금융, 부동산, 보험, 공급망 관리 등 다양한 산업 분야에서 업무 효율성 및 자동화를 극대화하는 핵심 인프라로 활용되고 있다.

본 논문의 전주기 무결성 검증 시스템은 위와 같은 블록체인의 투명성·불변성·자동화 이점을 CCTV 영상 보안에 접목한다. 구체적으로, 머클 루트·시퀀스 해시 등 무결성 증거를 블록체인에 기록하여 법적 분쟁 상황에서도 신뢰할 수 있는 증명력을 확보하고, 스마트 컨트랙트를 이용해 무결성 데이터의 저장·조회·접근 제어를 자동화함으로써 운영 비용과 관리 부하를 동시에 경감한다.

2.2 블록체인 기반 CCTV 영상 무결성 검증 기법

앞서 언급한 블록체인의 장점들을 이용해서 CCTV 영상의 무결성을 검증하는 기법들이 최근에 제시되고 있으며, 주요 연구 내용은 다음과 같다.

P. Khan et al.[4]은 전체 영상 중 일정 간격으로 추출한 일부 프레임들을 선택해 해시 및 전자서명한 뒤 블록체인에 기록하고, 관리 주체별 역할을 나누어 참가자들이 검증하는 시스템을 제안했다. 하지만, 이 시스템은 프레임 샘플링 방식이라서 영상의 시퀀스 단위에 대한 파일 삭제 및 순서 변조 공격을 탐지하지 못하며, 전주기 무결성에 대한 보장을 제공하지 못한다.

Z. Chen et al.[5]는 물류 모니터링 환경에서 영상은 IPFS에 저장하고 영상의 해시값을 블록체인에 기록하며, RBAC 기반의 접근제어를 수행하는 시스템을 제안했다. 하지만, 저 사양 CCTV에서의 효율적인 무결성 데이터 생성 방법이 제시되지 않아 현장 적용성이 제한적이며, 프라이빗 블록체인만 연계되어 투명성 및 신뢰성에 관한 부분이 미흡하다.

N. Alshuraify et al.[6]은 유전 파이프라인의 실시간 안전 감시에 초점을 두고 블록체인과 IPFS를 활용해 관제 시스템의 성능과 무결성을 향상하는 시스템을 제안했다. 하지만, 이 시스템은 이상 이벤트가 발생한 구간에 대해서만 해시값을 기록하는 방식이며 CCTV 영상 전체에 대한 무결성을 보장하지는 못하고 있다.

T. Kim et al.[7]은 블록체인을 기반으로 CCTV 영상의 특정 구간이 조작되었음을 검증할 수 있는 설명가능한 무결성 검증 체계를 설계했다. 하지만, 이 방식은 저장 효율성에 대한 한계가 존재하며, 성능 평가의 범위가 제한적이다. 또한, 조작의 탐지 범위가 I-Frame에 국한되어 있어 고수준의 무결성을 제공하기 어렵다.

V. Yatskiv et al.[8]은 각 프레임의 해시값이 블록에 저장되고 블록들이 연결되는 새로운 블록체인 구조를 제안했다. 하지만, 이 시스템은 무결성 데이터를 CCTV 기기에서 생성하지 않고 서버에서 처리하는 방식이며, 연속 시퀀스에 대한 고려가 없어 전주기 무결성을 제공하지 못한다.

III. 전주기 무결성 검증 시스템 설계

본 논문에서는 기존 연구들이 고려하지 못한 CCTV 영상의 생성부터 연속된 영상 시퀀스의 검증까지 전주기에 대한 무결성 검증 시스템의 설계를 제안한다. 표 1은 전주기의 단계별로 영상의 무결성과 신뢰성 확보를 위해 제시된 방법들의 요약을 보여주고 있다. 우선 CCTV 기기에서 영상에 대한 무결성 정보 생성 방법과 안전한 전송 방법을 제시하며, 이후 검증 서버에서 단일 파일에 대한 무결성 정보의 생성·기록·검증 방법을 제시한다. 그리고, 연속된 영상 파일들의 시퀀스에 대한 무결성 정보의 생성·기록·검증 방법을 제안한다.

제안 시스템은 그림 1과 같이 영상을 생성해 전송하는 CCTV 집합과 블록체인과 연계해 무결성을 검증하는 서버, 경찰이나 법원 등 영상을 활용하고 무결성 검증을 요청하는 외부 클라이언트로 구성된다. CCTV 기기는 프레임 단위의 무결성 데이터를 함께 생성해 제공하고, 검증 서버는 파일 단위의 무결성과 함께 연속된 영상 파일 시퀀스 전체에 대한 무결성 데이터를 관리한다. 이를 통해 영상의 생성 시점부터 파일 시퀀스 검증까지 전주기에 대한 무결성 검증을 제공한다.

3.1 CCTV 기기의 실시간 무결성 데이터 생성

CCTV 영상의 전주기 무결성을 보장하기 위해서는 영상을 생성하는 CCTV 기기에서 직접 실시간으로 무결성 검증 데이터를 생성해야 한다. 하지만, 기기의 낮은 성능과 기존 표준과의 호환성 문제로 어려움을 겪고 있다.

표 1. 전주기 단계별 무결성 보장을 위한 제안 방법
Table 1. Proposed methods for ensuring integrity at each stage of lifecycle

Lifecycle steps		Proposed methods
Integrity data on CCTV device	generation	• compute SHA-3 hash per each GOP • compatible with H.264/H.265
	secure transmit	• encrypted using AES algorithm • utilize secure keystore
Integrity data of a single video file	generation	• construct Merkle tree from GOP integrity data
	record	• store proof(Merkle root) on both blockchain and integrity server
	verification	• reconstruct Merkel tree • retrieve proof from blockchain • compare proof
Integrity data of video sequence	generation	• generate seq_proof by hash chaining
	record	• store seq_proof on both blockchain and integrity server
	verification	• reconstruct seq_proof from input sequence • retrieve seq_proof from blockchain • compare seq_proof

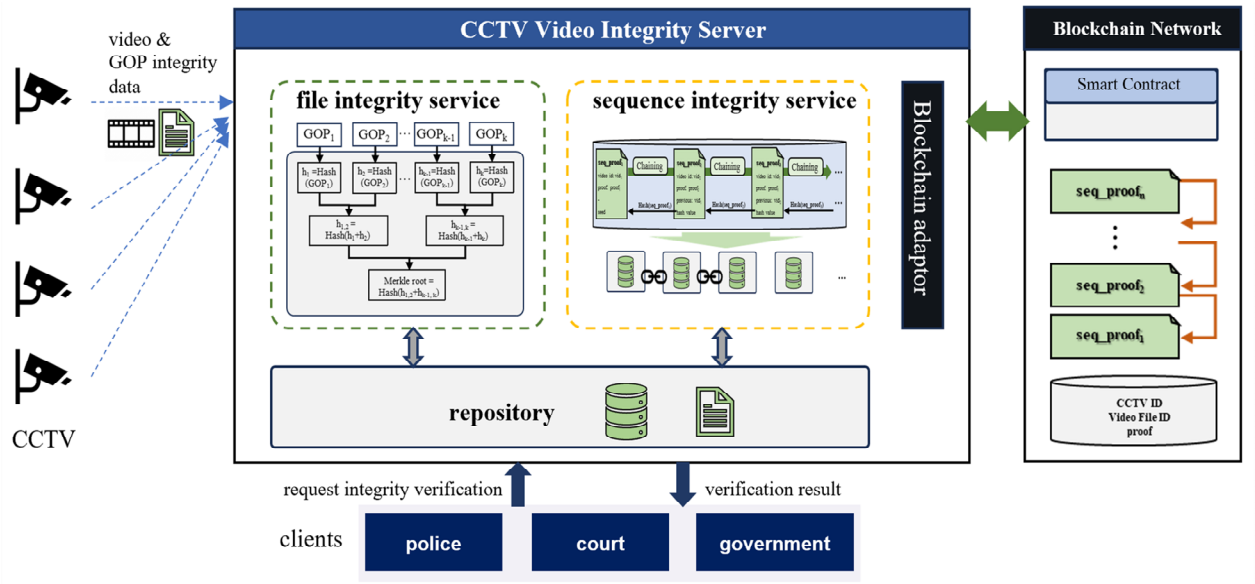


그림 1. 블록체인 기반 CCTV 영상 무결성 검증 시스템 구조
Fig. 1. System architecture of blockchain-based CCTV video integrity verification

제안 시스템은 그림 2와 같이 효과적이고 안전한 검증 데이터 생성 방식을 제공한다. 현재 CCTV 기기에서 가장 많이 사용되는 H.264/H.265[10] 동영상 압축 표준은 I-Frame, P-Frame, B-Frame들을 묶어서 하나의 GOP(Group Of Pictures)를 구성한다. 제안 방식은 CCTV 기기에서의 실시간 검증 데이터 생성을 위해 개별 프레임이 아닌 개별 GOP마다 SHA-3 해시함수로 해시값을 계산해 GOP 무결성 검증 데이터를 생성한다. 그리고 이 데이터는 안전한 전송을 위해 AES 알고리즘으로 암호화되며, 암호화 키는 사전에 CCTV의 등록 및 초기화 시점에 기기별로 설정되어 서버와 공유되고 기기 내의 TPM(Trusted Platform Module)에 기반한 키 저장소를 활용해 안전하게 관리된다.

제안 방식은 H.264/H.265 표준 포맷과의 호환을 위해 GOP 무결성 데이터를 SEI(Supplemental Enhancement Information) 헤더에 삽입하는 인코딩 방식을 적용하며, 기존 표준 코덱의 수정 없이 재사용이 가능하다는 장점이 있다. 생성된 영상과 검증 데이터는 NAL(Network Abstraction Layer)를 통해 검

증 서버로 전송되며, 서버는 CCTV와 공유된 암호화 키를 이용해 복호화 후 검증 데이터에 기반해 GOP의 무결성을 검증한다.

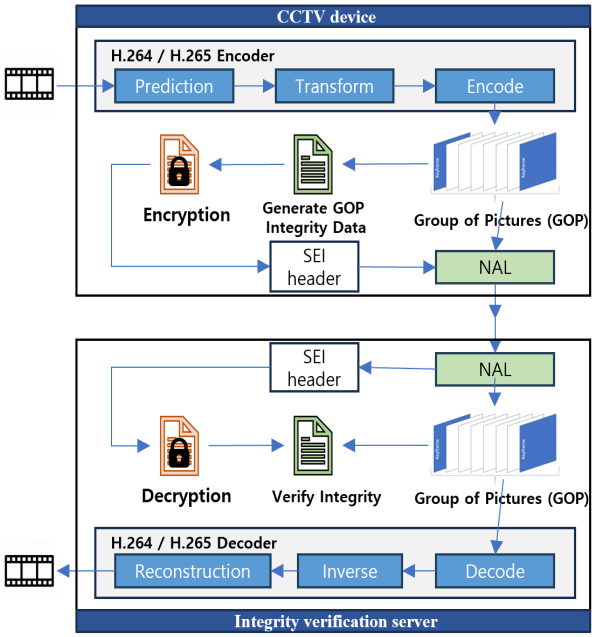


그림 2. CCTV의 무결성 데이터 생성 및 검증 프로세스
Fig. 2. Process of GOP integrity data generation & verification in CCTV

3.2 단일 영상 파일의 블록체인 기반 무결성 검증

CCTV를 통해 스트리밍되는 영상은 정책에 따라 k개의 GOP를 묶어 하나의 파일로 관리된다. 제안 시스템은 블록체인과 연계해 단일 파일의 무결성 데이터 생성을 위해 그림 3(a)와 같은 프로세스를 수행한다. 검증 서버는 단일 파일의 효율적인 무결성 검증 데이터 생성을 위해 머클 트리를 사용한다. 각 GOP의 무결성 데이터를 기반으로 머클 트리를 구성하고, 최상단의 머클 루트가 무결성 데이터인 $proof_i$가 되어 영상 파일 v_i와 함께 서버에 저장된다.

무결성 데이터의 저장과 검증을 검증 서버에만 의존하면 서버 내부의 조작이나 해킹으로 인한 변조의 위험성이 높으며, 분쟁 시 법적 증거로서의 신뢰성이 낮은 문제점이 있다. 제안 시스템은 블록체인과 연계해 이 문제점을 해결한다. 파일의 무결성 데이터는 블록체인에 기록되어 변조가 불가능해지며 높은 신뢰성을 보장한다. 또한, 블록체인의 타임스탬프 확인을 통해 영상 파일의 생성 시점에 대한 검증이 가능하며, 중앙집중식 시스템의 단일실패지점(Single point of failure) 문제로 인한 무결성 데이터의 손상을 방지하고 가용성을 높인다. 그리고 블록체인의 스마트 컨트랙트를 활용해 무결성 데이터 관리를 자동화하며, 블록체인 월렛 기반의 사용자 인증과 스마트 컨트랙트의 접근제어 기능을 이용해 보안성을 강화한다.

단일 파일의 무결성 검증 과정은 그림 3(b)와 같다. 클라이언트가 영상 파일 v_i에 대한 무결성 검증을 요청하면, 검증 서버는 v_i에 대한 머클 트리를 재구성해 머클 루트를 계산한다. 이후 블록체인 네트워크에 조회해서 무결성 데이터인 $proof_i$를 획득하고 두 값을 비교 검증한다. 또한, 서버 내의 로컬 저장소에 저장된 $proof_i$와 일치하는지 검사하고, 모두 일치하면 무결성이 검증되었음을 알린다. 블록체인에 저장된 $proof_i$는 변조가 불가능하므로, 만약 변조된 영상 파일 v_i'의 검증 요청이 오면 서버는 v_i'의 머클 루트와 $proof_i$가 불일치함을 항상 확인할 수 있다.

3.3 연속된 영상 파일 시퀀스의 블록체인 기반 무결성 검증

긴 시간 동안 스트리밍되는 CCTV 영상은 일반적으로 분 단위 혹은 시간 단위로 나뉘어 별도의 영상 파일이 연속적으로 생성된다. 즉, 단일 CCTV의 영상은 연속된 영상 파일의 시퀀스인 $(v_1, v_2, \ldots, v_n)$으로 표현할 수 있다. 하지만, 기존 연구들은 단일 영상 파일의 무결성 검증에만 집중되어 있으며, 여러 영상 파일들의 시퀀스에 대한 무결성을 고려하지 못하고 있다. 공격자는 특정 영상 파일을 변조하지 않고도 시퀀스에 대한 조작을 통해 다음의 두 가지 공격을 시도할 수 있다. 첫째, 공격자는 시퀀스 내의 특정 영상 파일을 삭제해 중요한 활동 정보가 담긴 부분을 제외할 수 있다. 둘째, 공격자는 시퀀스 내의 영상 파일들의 순서를 변경해서 범죄 행위를 은폐하거나 혼선을 주는 시도할 할 수 있다. 이 공격들은 개별 파일의 무결성은 훼손하지 않는 형태의 공격이기 때문에, 기존 기법들은 효과적으로 공격을 방어하지 못하고 있다.

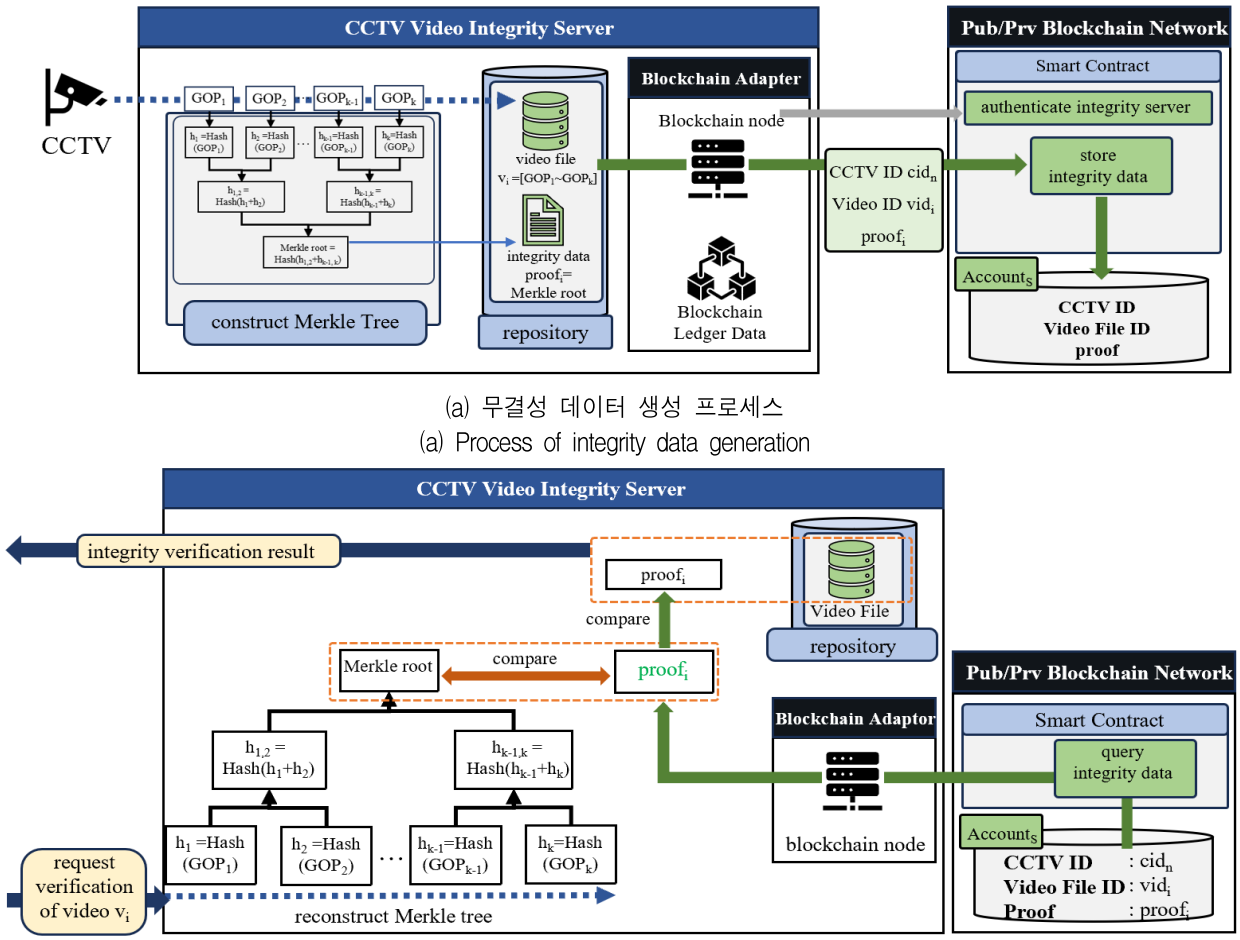
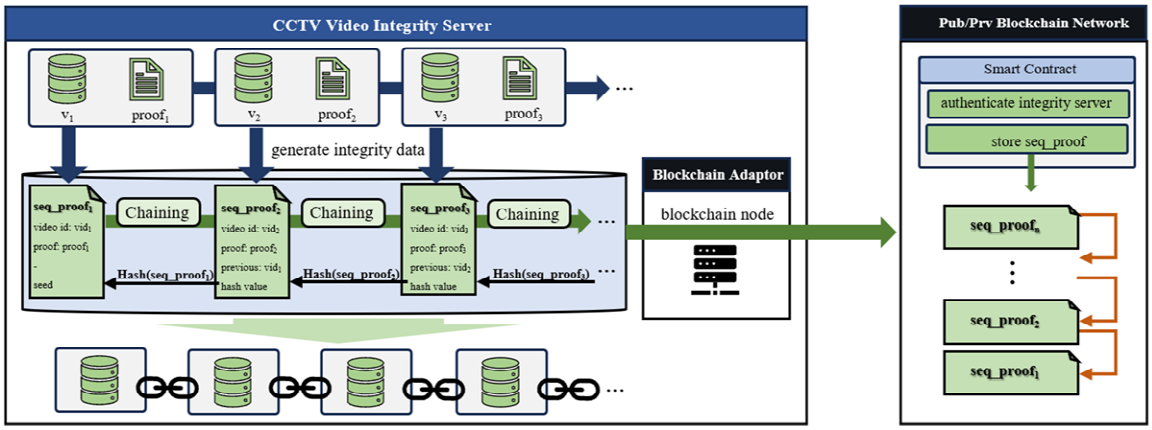


그림 3. 단일 영상파일의 무결성 데이터 생성과 검증 프로세스

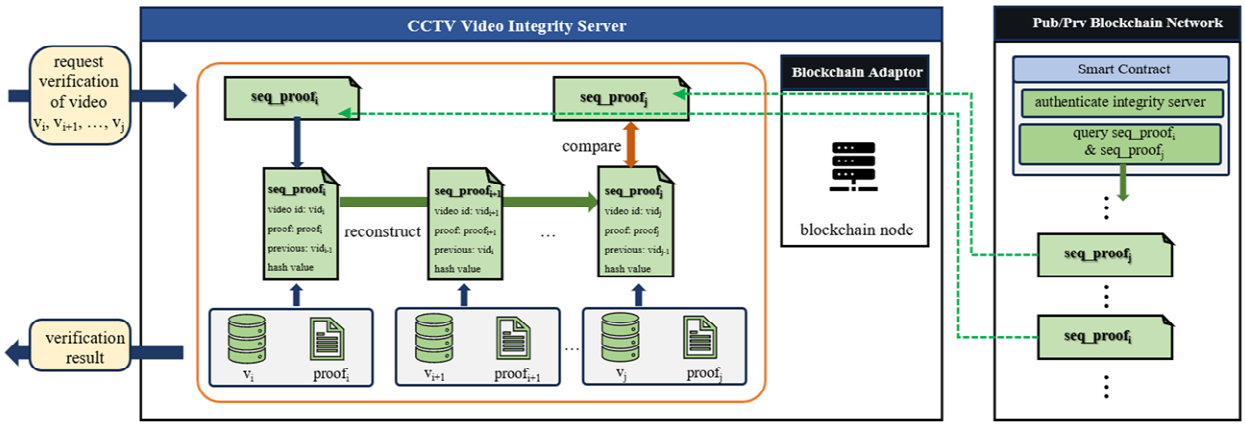
Fig. 3. Process of integrity data generation and verification of one video file

제안 시스템은 연속된 영상 파일 시퀀스 전체에 대한 무결성을 검증하고 위 공격을 효과적으로 방어하는 새로운 기법을 제공한다. 입력된 CCTV 영상에 대해 시퀀스 무결성 검증 데이터를 생성하는 과정은 그림 4(a)와 같다. 영상 파일 시퀀스 $(v_1, v_2, ..., v_n)$의 각 파일 v_i에 대해 시퀀스 검증 데이터인 seq_proof_i가 생성되며, 블록체인의 블록들이 체이닝되는 구조와 유사하게 각 seq_proof들도 체이닝된다. seq_proof_i는 해당 영상의 id인 vid_i, v_i의 무결성 데이터인 $proof_i$, 이전 영상의 vid_{i-1}을 포함하며, seq_proof_{i-1}의 해시값을 포함해서 이전 seq_proof에 연결되는 효과를 얻는다. 그리고 생성된 seq_proof_i는 스마트 컨트랙트를 활용해 블록체인에 저장되어 연속성에 대한 무결성 검증의 신뢰성을 확보한다.

연속된 영상 파일 시퀀스의 무결성 검증 과정은 그림 4(b)와 같다. 클라이언트가 특정한 영상 파일 구간 $(v_i, v_{i+1}, ..., v_j)$의 무결성 검증을 요청한다고 하자. 검증 서버는 블록체인에 조회해서 구간의 시작과 끝에 해당하는 seq_proof_i와 seq_proof_j를 획득한다. 이후에 서버는 seq_proof_i를 기반으로 다음 무결성 데이터인 seq_proof_{i+1}을 재생성하며, 마찬가지 방식으로 순차적으로 seq_proof_{i+2}, ..., seq_proof_j까지 재생성한다. 마지막 생성값과 앞서 블록체인에서 획득한 seq_proof_j가 일치하는지 검사해서 무결성 검증 결과를 결정해 반환한다. 검증 과정에서 생성되는 seq_proof들은 해시함수를 이용해 체이닝되기 때문에, 앞서의 파일 삭제 및 순서 변경 공격이 위의 검증 과정을 통과하지 못한다.



(a) 무결성 데이터 생성 프로세스
(a) Process of integrity data generation



(b) 무결성 검증 프로세스
(b) Process of integrity verification

그림 4. 연속된 영상파일 시퀀스의 무결성 데이터 생성과 검증 프로세스
Fig. 4. Process of integrity data generation and verification of continuous video file sequence

Ⅳ. 블록체인 연계 구축방식 토론

제안 시스템은 블록체인과 연계해 CCTV 영상의 무결성을 강화하고 투명성 및 가용성을 향상해 고신뢰성을 보장하도록 하고 있다. 본 장에서는 블록체인을 연계해 구축하는 방식의 고려사항들을 논의한다.

제안 시스템은 다양한 블록체인 네트워크와 검증 서버 사이의 인터페이스 역할을 하는 블록체인 어댑터를 포함한다. 블록체인 네트워크는 개방성 여부에 따라 퍼블릭 블록체인과 프라이빗 블록체인으로 나뉜다. Ethereum과 같은 퍼블릭 블록체인은 누구나 참여할 수 있는 개방형 네트워크이며, 모든 참여자가 블록체인에 기록된 데이터를 보고 검증할 수 있어 투명성이 높지만 데이터 처리 속도가 느리고 트랜잭션 수수료가 필요하다는 단점이 있다. Hyperledger Fabric과 같은 프라이빗 블록체인은 특정 조직의 구성원만 참여가 가능한 폐쇄형 네트워크이며, 사용자 인증과 접근제어를 통해 보안성을 강화하고 데이터 처리 속도가 빠른 장점이 있지만 투명성과 네트워크 전체에 대한 신뢰성을 확보하는 데 어려움이 있다.

CCTV 영상의 무결성 검증 시스템은 목적과 환경, 활용 분야에 맞춰 적합한 블록체인 네트워크를 선택하고 어댑터를 개발해 연계할 수 있다. 즉, 민감한 기업 비밀정보가 노출될 수 있는 환경에서는 기업 내에 프라이빗 블록체인을 구축하고 검증 시스템과 연계해서 기밀성을 높이고 정보의 유출을

차단하는 접근 방식이 적합하다. 그리고 범죄예방을 위한 공공장소 모니터링 등의 경우, 퍼블릭 블록체인과 연계해 공공성과 투명성을 높이고 누구나 검증 가능하도록 해서 신뢰성을 강화하는 방식이 적합하다.

그리고, 본 논문에서는 그림 5와 같이 퍼블릭 블록체인과 프라이빗 블록체인을 함께 활용하는 하이브리드 형태의 블록체인 연계 방식을 제시한다. 민감하고 유출 위험이 있는 영상 무결성 검증 데이터는 프라이빗 블록체인에 저장해 기밀성을 높인다. 그리고, ZK-Rollups[11]와 같은 롤업 방식을 이용해서 주기적으로 검증 데이터 집합에 대한 대푯값인 롤업 데이터를 생성해 퍼블릭 블록체인에 기록한다. 이 방식을 통해 무결성 검증 시스템의 기밀성과 투명성을 함께 강화할 수 있다.

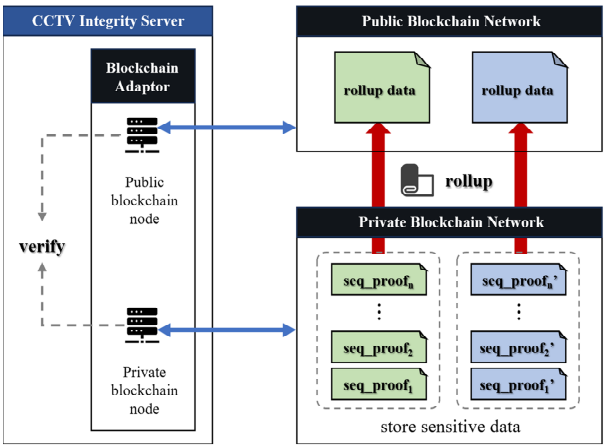


그림 5. 롤업을 이용한 하이브리드 블록체인 연계 방식
Fig. 5. Hybrid blockchain interconnection using rollups

제시된 하이브리드 블록체인 연계 방식을 기존의 프라이빗 블록체인 및 퍼블릭 블록체인 연계 방식과 비교 분석한 결과는 표 2와 같다. 하이브리드 방식은 롤업 데이터의 검증을 통해 퍼블릭 블록체인과 동등한 수준의 투명성과 고신뢰성을 확보한다. 그리고, 모든 데이터가 아닌 롤업 데이터만 퍼블릭 블록체인에 기록하기 때문에 낮은 트랜잭션 수수료만 요구된다. 또한, 주기적인 롤업 데이터 처리가 병행해서 수행되므로 기존 프라이빗 블록체인과 비슷한 수준의 처리 속도를 제공하는 장점도 가진다.

V. 안전성 분석

본 장에서는 제안 시스템의 핵심 기법인 연속된 영상 파일 시퀀스의 무결성 검증 방식에 대한 안전성을 분석한다. 단일 영상 파일의 무결성 검증 방식은 해시 함수의 충돌 저항성과 머클 트리 구조에 기반해 입증 가능하며, 시퀀스의 무결성 검증이 단일 파일의 무결성 검증을 기반으로 진행된다. 즉, 시퀀스의 무결성 검증에 대한 안전성 분석만으로도 시스템 전반의 무결성 보장을 논증할 수 있다.

5.1 영상 파일 시퀀스 무결성 검증 절차

시퀀스 무결성 검증의 목적은 연속된 CCTV 영상파일 시퀀스 $V=(v_1, v_2, ..., v_n)$의 순서와 위변조 여부를 판별하는 것이다. 여기서 v_i는 개별 영상 파일이며, 각 파일의 무결성 데이터 $proof_i$를 가진다. 시퀀스 무결성 데이터 seq_proof는 다음과 같은 해시 체이닝 방식으로 계산된다:

$$seq\_proof_i = H(vid_i \,||\, proof_i \,||\, vid_{i-1} \,||\, H(seq\_proof_{i-1}))$$

여기서, 해시함수 $H(\cdot)$는 충돌 저항성(collision resistance) 및 역상 저항성(preimage resistance)을 만족한다고 가정한다.

클라이언트가 CCTV 영상 시퀀스의 특정 구간 $V_{i:j}=(v_i, v_{i+1}, ..., v_j)$에 대한 무결성을 검증을 요청하면 $Verify(V_{i:j})$는 다음과 같은 절차를 따른다.

표 2. 블록체인 연계 구축방식의 비교분석
Table 2. Comparative analysis of blockchain interconnection approaches

Type	Transparency	Trustworthiness	Transaction fee	Speed
Private blockchain	low	low	none	fast
Public blockchain	high	high	high	slow
Hybrid blockchain	high	high	low	fast

입력

- $V_{i:j} = (v_i, v_{i+1}, ..., v_j)$: 검증 대상 시퀀스
- $P_{i:j} = \{proof_i, ..., proof_j\}$: 파일의 무결성 데이터
- $S_{i:j} = \{seq\_proof_i, seq\_proof_j\}$: 구간 시작과 끝의 시퀀스 무결성 데이터

검증 절차

1. 초기 설정 : $t = seq\_proof_i$
2. seq_proof 재생성

   for $k = i+1$ to j do

   $$t = H(vid_k \parallel proof_k \parallel vid_{k-1} \parallel H(t))$$
3. 최종 t와 seq_proof_j 값 비교

출력

- $$Verify(V_{i:j}) = \begin{cases} True, \text{ if } t = seq-proof_j \\ False, otherwise \end{cases}$$

5.2 공격 모델 정의

영상 파일 시퀀스의 무결성을 위협할 수 있는 공격자 A의 3가지 공격 모델을 다음과 같이 정의한다. 공격자는 표 3과 같이 각 영상 파일의 무결성 데이터에 대한 읽기와 재배치 권한은 있으나 변경의 권한은 없으며, 이는 연계된 블록체인을 통해 제한된다.

표 3. 영상 파일 시퀀스에 대한 공격자 행위 권한 여부
Table 3. Adversary capabilities for video file sequence manipulation

Adversary activity		Capability
video file sequence	read	O
	write & delete	O
	reordering	O
integrity data	read	O
	write & delete	X
	reordering	X

A. 파일 삭제 공격

공격자 A는 시퀀스 V에서 임의의 영상 파일 v_k를 제거하여 조작된 시퀀스 V'을 생성한다:

$$V'=(v_i, ..., v_{k-1}, v_{k+1}, ..., v_j)$$

그리고 $Verify(V')=True$가 되는 것을 목표로 한다.

B. 순서 변경 공격

공격자 A는 시퀀스 V 내 두 영상 파일인 v_p와 v_q ($p < q$)의 위치를 교환해 새로운 시퀀스 V'을 생성한다:

$$V'=(v_i, ..., v_q, ..., v_p, ..., v_j)$$

그리고 $Verify(V')=True$가 되는 것을 목표로 한다.

C. 파일 대체 공격

공격자 A는 특정 위치 k의 영상 파일 v_k를 다른 파일 v_k'로 대체해 새로운 시퀀스 V'을 생성한다:

$$V'=(v_i, ..., v_{k-1}, v_k', v_{k+1}, ..., v_j) \text{ where } v_k' \neq v_k$$

그리고 $Verify(V')=True$가 되는 것을 목표로 한다.

5.3 공격에 대한 안전성 정리

앞서 5.1절에서 서술된 제안 시스템의 무결성 검증 절차가 5.2절에서 정의된 3가지 공격 모델들에 대해서 안전함을 보이기 위해, 본 논문에서는 무시 가능한 함수(negligible function) $\varepsilon(\cdot)$에 기반한 정형 보안 증명을 제공한다. 여기서, 보안 매개변수 λ에 대해 $\varepsilon(\lambda)$는 사실상 0에 수렴하며, 현실적으로 앞서 정의된 공격 모델들의 성공 확률이 매우 작아서 무시할 수 있는 수준임을 보여주게 된다.

Theorem 1. 시퀀스 무결성 보장

해시 함수 $H:\{0,1\}^* \rightarrow \{0,1\}^\lambda$가 충돌 저항성 및 역상 저항성을 만족한다고 가정할 때, 제안된 시퀀스 무결성 검증 기법은 모든 조작 시퀀스 $V' \neq V$에 대해 다음을 만족한다:

$$\Pr[Verify(V')=True] \leq \varepsilon(\lambda)$$

여기서 $\varepsilon(\lambda)$는 보안 매개변수 λ에 대해 무시가능한 함수이다.

증명

다음은 3가지 공격 방식들에 대한 보조정리이다.

보조정리 1. 파일 삭제 공격 저항성

공격자가 임의의 영상 파일 v_k를 삭제해 조작된 시퀀스 V'를 이용해 검증을 요청하는 경우, 다음이 성립한다:

$$\Pr[Verify(V')=True] \leq \varepsilon_{col}(\lambda)$$

증명.

공격자가 검증을 통과하기 위해서는 $seq_proof_{k+1}'=seq_proof_{k+1}$가 되어야 한다. 하지만,

$seq\_proof_{k+1}'=H(vid_{k+1}||proof_{k+1}||vid_{k-1}||H(seq\_proof_{k-1}))$ 이며, 이 값이 seq_proof_{k+1}과 같아지게 하려면 H에 대한 충돌 저항성을 깨야 한다. 따라서, 공격자가 공격에 성공할 확률은 다음과 같다.

$\Pr[Verify(V')=True] \leq \Pr[\text{충돌저항성 공격}] = \varepsilon_{col}(\lambda)$

보조정리 2. 순서 변경 공격 저항성

공격자가 두 개의 영상 파일 v_p, v_q ($p < q$) 의 순서를 바꾼 시퀀스 V'를 이용해 검증을 요청하는 경우, 다음이 성립한다:

$$\Pr[Verify(V')=True] \leq \varepsilon_{col}(\lambda)$$

증명.

순서가 바뀐 경우, 적어도 seq_proof_p'는 원래의 seq_proof_p와 다르게 계산된다.

$seq\_proof_p=H(vid_p||proof_p||vid_{p-1}||H(seq\_proof_{p-1}))$

$seq\_proof_p'=H(vid_q||proof_q||vid_{p-1}||H(seq\_proof_{p-1}))$

이때, 서로 다른 입력값이 사용되므로 두 결괏값이 같아지게 하려면 H에 대한 충돌 저항성을 깨야 한다. 따라서, 공격자가 성공할 확률은 다음과 같다.

$\Pr[Verify(V')=True] \leq \Pr[\text{충돌저항성 공격}] = \varepsilon_{col}(\lambda)$

보조정리 3. 파일 대체 공격 저항성

공격자가 임의의 영상 파일 v_k를 다른 파일 $v_k' \neq v_k$로 대체하고 검증을 요청하는 경우, 다음이 성립한다:

$$\Pr[Verify(V')=True] \leq \varepsilon_{col}(\lambda)$$

증명.

검증을 통과하기 위해서는 $seq_proof_k'=seq_proof_k$를 만족해야 한다. 이를 위해서는 $proof_k'=proof_k$ 이어야 하며, 이 값들은 머클 루트이기 때문에 서로 다른 영상의 머클 루트를 동일하게 만들려면 H에 대한 충돌 저항성을 깨야 한다. 따라서, 공격자가 성공할 확률은 다음과 같다.

$\Pr[Verify(V')=True] \leq \Pr[\text{충돌저항성 공격}] = \varepsilon_{col}(\lambda)$

위의 3가지 보조정리를 통해 각각의 공격은 해시 함수의 충돌 저항성에 의해 무시가능한 성공 확률을 가짐을 보였다. 이를 토대로 하면, 모든 조작 시퀀스 $V' \neq V$에 대해 검증에 통과할 확률은 다음과 같다:

$$\Pr[Verify(V')=True] \leq 3\varepsilon_{col}(\lambda) = \varepsilon(\lambda)$$

따라서 제안된 시퀀스 무결성 검증 기법은 정의된 공격 모델 하에서 안전하다.

위의 3가지 보조정리를 통해 각각의 공격은 해시 함수의 충돌 저항성에 의해 무시가능한 성공 확률을 가짐을 보였다. 이를 토대로 하면, 모든 조작 시퀀스 $V' \neq V$에 대해 검증에 통과할 확률은 다음과 같다:

$$\Pr[Verify(V')=True] \leq 3\varepsilon_{col}(\lambda) = \varepsilon(\lambda)$$

따라서 제안된 시퀀스 무결성 검증 기법은 정의된 공격 모델 하에서 안전하다.

Ⅵ. 결 론

본 논문에서는 CCTV 영상의 전주기에 대한 무결성을 검증하는 블록체인 기반 시스템 설계를 제안하였다. CCTV 기기에서 영상 생성 시점에 H.264/H.265 표준과 호환되는 무결성 데이터 생성 및 전송 기술과 함께 머클 트리를 활용한 단일 영상 파일의 효율적인 무결성 검증 기술, 연속된 영상 파일 시퀀스에 대해 해시 체이닝을 이용한 새로운 무결성 검증 기술을 제공하였다. 또한, 시스템의 투명성과 보안성을 함께 강화할 수 있는 하이브리드 형태의 블록체인 연계 방식을 제시하였다.

제안 시스템을 통해 영상의 생성부터 저장, 관리, 검증의 전 단계에 대한 고신뢰성을 제공해서 영상이 법적 증거자료로 활용되는 근거를 마련하였다. 이 시스템은 기존 시스템에 비해 효율적이고 신뢰성 높은 서비스를 제공해 특히 공공안전, 금융기관 등 다양한 분야에서 유용하게 활용될 것으로 기대된다. 앞으로는 제안 시스템을 구현하고 실험을 통해 성능을 측정해 비교분석하고 실효성을 확인할 계획이다.

References

[1] P. Aberna and L. Agilandeeswari, "Digital image and video watermarking: methodologies, attacks, applications, and future directions", Multimedia Tools and Applications, Vol. 83, pp. 5531-5591, Jan. 2024.

https://doi.org/10.1007/s11042-023-15806-y.

[2] L. Linju and R. Shreelekshmi, "VECDSigL: Video integrity verification using elliptic curve digital signature links", Software Impacts, Vol. 15, Mar. 2023. https://doi.org/10.1016/j.simpa.2023.100474.

[3] S. Ghimire and B. Lee, "A data integrity verification method for surveillance video system", Multimedia Tools and Applications, Vol. 79, pp. 30163-30185, Nov. 2020. https://doi.org/10.1007/s11042-020-09482-5.

[4] P. Khan, Y. Byun, and N. Park, "A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities", Electronics, Vol. 9, No. 3, Mar. 2020. https://doi.org/10.3390/electronics9030484.

[5] Z. Chen, et al., "Video security in logistics monitoring systems: a blockchain based secure storage and access control scheme", Cluster Computing, Vol. 27, pp. 10245-10264, Nov. 2024. https://doi.org/10.1007/s10586-024-04667-1.

[6] N. Alshuraify, A. Yassin, and Z. Abduljabbar, "Hyperledger Fabric Blockchain Using CCTV Surveillance Cameras for Pipelines of Oil and Gas Fields", Proc. 11th WINCOM, Leeds, United Kingdom, pp. 1-8, Jul. 2024. https://doi.org/10.1109/WINCOM62286.2024.10656253.

[7] T. Kim, J. Hong, M. Kang, S. Song, J. Lee, and S. Kim, "Integrity Support System for Blockchain-based explainable CCTV Video", The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 21, pp. 15-21, Mar. 2021. http://doi.org/10.7236/JIIBC.2021.21.3.15.

[8] V. Yatskiv, N. Yatskiv, and O. Bandrivskyi, "Proof of Video Integrity Based on Blockchain", Proc. 9th International Conference on Advanced Computer Information Technologies, Ceske Budejovice, Czech Republic, pp. 431-434, Jun. 2019. https://doi.org/10.1109/ACITT.2019.8780097.

[9] M. Tabatabaei, R. Vitenberg, and N. Veeraragavan, "Understanding blockchain: Definitions, architecture, design, and system comparison", Computer Science Review, Vol. 50, Nov. 2023. https://doi.org/10.1016/j.cosrev.2023.100575.

[10] ITU-T, Recommendation ITU-T H.265, High efficiency video coding, 2013.

[11] T. Lavaur, J. Detchart, J. Lacan, and C. Chanel, "Modular zk-rollup on-demand", Journal of Network and Computer Applications, Vol. 217, Aug. 2023. https://doi.org/10.1016/j.jnca.2023.103678.

저자소개

김 희 열(Heeyoul Kim)

2000년 2월 : 한국과학기술원 전산학과(공학사)
2002년 2월 : 한국과학기술원 전산학과(공학석사)
2007년 2월 : 한국과학기술원 전산학과(공학박사)
2009년 3월 ~ 현재 : 경기대학교 컴퓨터공학부 교수
관심분야 : 정보보호, 블록체인