프라이버시 보호를 위해 Perceptual Hash를 사용하는 블록체인 기반 블랙박스 영상 무결성 검증 시스템

조연서, 허가빈, 도인실*

이화여자대학교

dustjam0@ewhain.net, gjrkqls@ewhain.net, *isdoh1@ewha.ac.kr

Blockchain-based Dashcam Videos Integrity Verification System exploiting Perceptual Hash for Privacy Protection

Yeonseo Cho, Gabin Heo. Inshil Doh*

Ewha Womans University

요 약

차량용 블랙박스의 보편화로 블랙박스 영상이 교통법규 위반이나 범죄사건, 교통사고 등의 증거로 활용되는 경우가 늘고 있다. 그러나 블랙박스 영상은 무결성을 증명하기 어렵고 개인정보를 포함하기 때문에 영상과 메타 데이터의 공유가 어렵다는 문제가 있다. 이러한 문제를 해결하기 위해 본 연구에서는 Perceptual Hash를 사용하여 프라이버시를 보호하는 블록체인 기반 블랙박스 영상 무결성 검증 시스템을 제안한다.

Ⅰ. 서 론

시장 조사 기관 GIA에 따르면 2022년에 50억 달러로 추정되는 대시보드 카메라(블랙박스) 세계 시장은 2030년까지 126억 달러로 수정된 규모에 도달하여 2022년에서 2030년까지 CAGR 12.3%의 성장을 이룰 것으로 예측된다[1]. 이러한 시장의 증가에 따라 교통법규 위반 신고나 범죄사건, 교통사고, 보도 및 연구 자료의 영상 확보를 위해 블랙박스를 활용하고자 하는 수요도 늘고 있다. 하지만 개인이 소유하는 블랙박스 영상은 위조나 변조의 가능성으로부터 무결성을 검증하기 어렵다는 문제가 있다. 또한, 블랙박스 데이터는 이동 경로나 운전 습관과 같이 운전자의 개인정보뿐만 아니라 영상 속 보행자 등 타인의 개인정보를 포함하기 때문에 불특정 다수에게 노출되거나 재배포 되는 경우 프라이버시 침해의 우려가 있다. 이에 본 연구에서는 프라이버시 보호를 위해 Perceptual Hash를 사용하는 블록체인 기반 블랙박스 영상 무결성 검증 시스템을 제안하고자 한다.

Ⅱ. 관련 연구

1. 블록체인

블록체인은 블록 단위의 데이터를 시간순으로 연결해서 체인 형태로 저장하는 데이터베이스 유형이다. 각각의 블록은 이전 블록의 해시를 포함하고 네트워크의 모든 노드에 분산되어 공유되기 때문에 데이터의 위·변조가 불가능하여 투명성과 무결성이 보장된다.

이러한 특징을 이용해서 블랙박스의 메타 데이터를 LINK 블록체인에 저장하고 영상을 private 서버에 저장하는 연구[2]와 메타 데이터를 리프 노드로 하여 머클 트리 루트만을 퍼블릭 블록체인에 저장하는 연구[3]가 있지만, 거래 시스템이 명확하지 않고 원본 영상의 공유가 필요하여 프라이버시 침해 및 유출, 재배포와 같은 위험이 따른다는 문제가 있다.

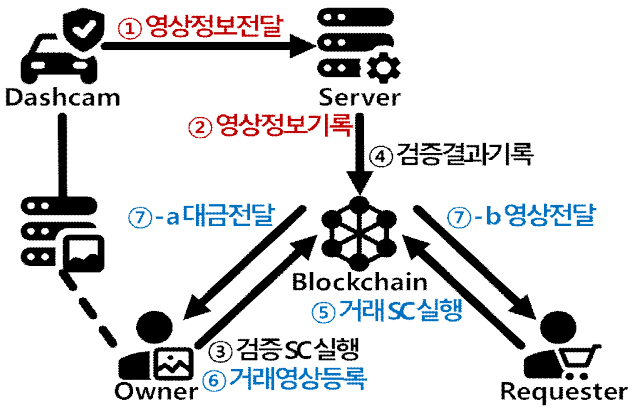
2. Perceptual Hash(PH)

Perceptual Hash는 이미지 해시로도 알려져 있으며 이미지나 오디오와 같은 멀티미디어 간의 유사성을 탐지하는 데 사용된다. 전통적인 암호화 해시와 달리 작은 변화가 큰 변화를 만드는 눈사태 효과를 따르지 않고 인지적으로 유사한 미디어는 유사한 해시를 가진다는 특징이 있다. 이러한 특징으로 이미지의 Perceptual Hash는 압축, 회전, 워터마크나 잡음 추가 같은 변형에 강하여 변조된 불법 복제물을 탐지하거나 이미지 인증, 이미지 검색 등 여러 분야에서 응용된다.

멀티미디어의 저작권 위반을 탐지하기 위해 블록체인과 Perceptual Hash를 사용하는 연구[4]에서는 영상의 Perceptual Hash를 생성하고 유사성을 계산하는 방법을 제시하지만, 원본 영상을 올려야 하고 블랙박스 영상과 같이 실시간 영상에는 적합하지 않은 문제가 있다.

Ⅲ. 블록체인 기반 블랙박스 영상 무결성 검증 시스템

본 연구에서는 프라이버시 보호를 위해 Perceptual Hash를 사용하는 블록체인 기반 블랙박스 영상 무결성 검증 시스템을 제안한다. 시스템에서 검증에 필요한 정보를 기록하는 서버는 지역 경찰서와 같이 신뢰할 수 있는 기관이다. 제안 시스템의 전반적인 프로세스는 다음과 같다.



[그림 1] 제안하는 시스템의 구조도

1. 블랙박스의 영상 정보 기록

(1) 블랙박스는 실시간으로 수집한 영상의 검증 정보(*VI*)와 Perceptual Hashs(*PHs*)를 서버에 전송한다.

여기서 *VI*와 *PHs*의 의미는 다음과 같다.

$$VI = H(Owner,\ Time,\ Location,\ Video)$$

*Owner*는 블랙박스 소유자의 주소, *Time*과 *Location*은 영상의 시간과 위치를 뜻한다. *Video*는 영상의 프레임으로 만든 머클 트리 루트다. 따라서, *H(Owner, Time, Location, Video)*는 영상의 소유자, 시간, 위치, 프레임의 정보를 더하고 암호화 해시 함수를 적용한 것이다.

*PHs*는 영상의 전체 프레임에서 이전 프레임과 해밍 거리가 충분히 멀 때마다 Perceptual Hash를 저장한 모음이다. 만약 영상의 모든 프레임이 거의 같은 Perceptual Hash를 가진다면 해당 영상의 *PHs*는 하나뿐이다.

(2) 서버는 전송받은 데이터를 주기적으로 블록체인에 기록한다.

이 단계에서 블랙박스 영상은 어떠한 방식으로도 외부에 저장되지 않는다. 서버에 기록되는 검증 정보 역시 암호화 해시 함수를 거쳐 개인정보를 포함하는 원래 데이터를 유추할 수 없다. 블랙박스는 영상 정보를 실시간으로 전송하여 소유자에 의해 위조 및 변조되기 어렵다.

2. 소유자의 검증 스마트 계약 실행

(1) 소유자는 검증 스마트 계약을 실행하고 검증을 원하는 영상 또는 이미지 파일과 *Time**, *Location**, *Video** 정보를 서버에 제출한다.

여기서 ***은 소유자가 제출한 정보임을 의미한다. *Video**은 영상의 머클 트리 루트이거나 머클 트리 루트를 계산할 수 있는 해시들의 모음을 의미한다.

(2) 서버는 스마트 계약을 실행한 소유자와 소유자가 제출한 정보가 올바른 검증 정보인지 확인하고 스마트 계약을 서버에 업데이트한다.

(3-a) 검증을 원하는 영상 프레임 또는 이미지의 해시가 *Video**에 포함된 경우, 무결성이 검증되므로 파일의 해시를 스마트 계약에 업데이트한다.

(3-b) 검증을 원하는 영상 프레임 또는 이미지의 해시가 *Video**에 포함되지 않는 경우, Perceptual Hash를 계산하여 확인된 검증 정보의 *PHs*와 유사도 비교 후 파일의 해시와 유사성을 스마트 계약에 업데이트한다.

이 단계에서 검증 스마트 계약을 실행한 소유자는 제출한 파일을 블록체인에 공개하지 않으면서 무결성 혹은 유사성을 검증할 수 있다. 스마트 계약에 업데이트된 검증 결과를 통해 시스템 내, 외부에서 검증된 파일을 증거로 제출하거나 해당 파일이 필요한 요청자에게 소유권을 증명할 수 있다.

3. 요청자의 거래 스마트 계약 실행

(1) 요청자는 영상의 소유자가 제공하는 영상의 일부 혹은 비식별화된 영상과 해당하는 검증의 결과를 통해 필요한 영상을 확인한다.

(2) 요청자는 필요한 영상을 전달받을 주소와 대금을 포함하여 거래 스마트 계약을 실행한다.

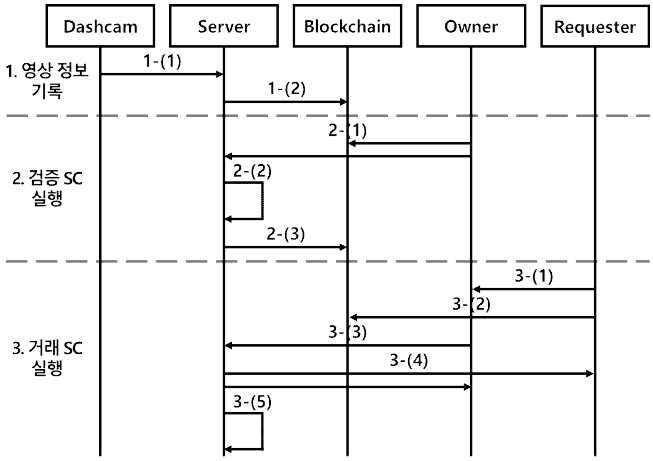
(3) 소유자는 요청자가 요청한 영상을 서버에 등록한다.

(4-a) 서버는 소유자가 등록한 영상의 무결성을 검증하고 전달받을 주소가 신뢰할 수 없는 경우, 요청자의 정보를 핑거프린트로 삽입하여 영상을 주소에 전달 및 대금을 소유자에게 전달한다.

(4-b) 서버는 전달받을 주소가 신뢰할 수 있는 경우, 소유자가 제출한 원본 영상을 주소에 전달 및 대금을 소유자에게 전달한다.

(5) 서버는 양측의 확인을 받거나 일정한 기간이 지나면 스마트 계약을 완료하고 원본 영상을 삭제한다.

이 단계에서 소유자는 요청자에게 대금을 받고 영상을 거래하되 요청자를 비롯하여 신뢰할 수 없는 주소가 영상을 전달받는 경우, 서버에서 삽입한 핑거프린트를 통해 영상의 재배포 시 유출자를 특정할 수 있다. 요청자는 서버로부터 유사성이 검증된 영상을 받아 요청한 거래의 목적에 맞게 법적 증거나 보도자료, 연구 자료 등으로 사용할 수 있다. 파일을 받는 주소가 공공기관을 비롯하여 신뢰할 수 있는 주소인 경우, 핑거프린트의 삽입 없이 무결성이 검증된 원본 영상을 전달할 수 있다.



[그림 2] 제안하는 시스템의 순서도

Ⅳ. 결론 및 향후 연구

본 연구에서는 프라이버시 보호를 위해 Perceptual Hash를 사용하는 블록체인 기반 블랙박스 영상 무결성 검증 시스템을 제안하였다. 소유자는 블랙박스 영상을 공개하지 않거나 영상의 일부, 혹은 프라이버시를 침해하지 않도록 가공된 영상으로도 무결성 및 유사성을 시스템에 의해 검증받을 수 있다. 요청자는 신뢰할 수 있는 서버에게 무결성 또는 유사성을 검증받은 개인 소유의 블랙박스 영상을 적법한 과정으로 획득하고 사용할 수 있다.

향후 연구에서는 제안하는 시스템의 성능을 분석하고 블랙박스 영상 외 카메라 장치의 영상을 지원하는 방안을 연구하고자 한다.

ACKNOWLEDGMENT

이 논문은 2023년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2023R1A2C1005712) (교신저자: 도인실)

참 고 문 헌

[1] Global Industry Analysts, Inc. (2023). Dashboard Camera.

[2] 안규황, 원태연, 박상민, 장경배, 서화정.(2019).LINK 블록체인을 적용한 차량용 블랙박스 시스템.한국정보통신학회논문지,23(8),1018-1023.

[3] Choi, J. H., & Jeong, I. R. (2023). Cost-Effectively Searchable Blackbox Data With Unlinkability Based on Public Blockchain. IEEE Access, vol. 11, pp. 100458-100464.

[4] Kumar, R., Tripathi, R., Marchang, N., Srivastava, G., Gadekallu, T. R., & Xiong, N. N. (2021). A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. Journal of Parallel and Distributed Computing, 152, 128-143.